On inter-organizational trust engineering in networked collaborations : modeling and management of rational trust

Msanjila, S.S.

Publication date
2009

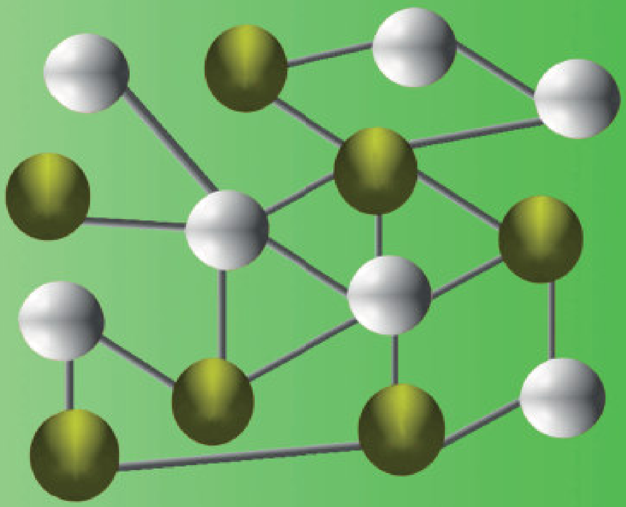
Document Version
Final published version

Link to publication

Citation for published version (APA):
Msanjila, S. S. (2009). *On inter-organizational trust engineering in networked collaborations : modeling and management of rational trust*. [Thesis, fully internal, Universiteit van Amsterdam].

On Inter-Organizational Trust Engineering in Networked Collaborations

Modeling and management of rational trust



Simon Samwel Msanjila

On Inter-Organizational Trust Engineering in Networked Collaborations

Modeling and management of rational trust

Simon Samwel Msanjila

The cover was designed by the author.

ISBN: 10: 9057761963
ISBN: 13: 9789057761966

On inter-organizational trust engineering in networked collaborations

Modeling and management of rational trust

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. D.C. van den Boom
ten overstaan van een door het college voor promoties
ingestelde commissie,
in het openbaar te verdedigen in de Agnietenkapel
op dinsdag 29 September 2009, te 12:00 uur

door

Simon Samwel Msanjila

geboren te Ihumwa, Dodoma, Tanzania

Promotiecommissie

Promotor:	Prof. dr. P. M. A Sloot
Co-promotor:	Dr. H. Afsarmanesh
Overige Leden:	Prof. dr. B. J. Wielinga
	Prof. L. M. Camarinha-Matos
	Prof. dr.-ing. Bernhard R. Katzy
	Prof. dr. M.T. Bubak
	Prof. drs. M. Boasson

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

This work was supported in part by the ECOLEAD (European Collaborative networked Organizations LEADership initiative) project, funded by the European Commission, under FP6 IP 506958 contract.

UNIVERSITEIT VAN AMSTERDAM

Contents

List of Abbriviations

CBT	Calculus Based Trust
CN	Collaborative Networks
CNO	Collaborative Networked Organizations
COC-Plan	Collaborative Opportunity Characterization and rough Planning
CO-Finder	Collaborative Opportunity Finder
DSS	Decision Support System
ECOLEAD	European Collaborative networked Organizations LEADership initiatives
FiXs	Federation for identity and cress-credentialing system
HICI	Hierarchical, Impact and Causal Influence
IBT	Identification Based Trust
ICT	Information and communication technology
MGP	Managerial Perspective
MRQ	Main Research Question
MSMS	Membership Structure Management System
ODMS	Ontology Discovery Management system
OOM	Object-Oriented Modeling
PCMS	Profile and Competency Management System
PVC	Professional Virtual Community
PSS	Partner Selection and Suggestion system
SME	Small and Medium Enterprise
SOP	Social Perspective
SRQ	Sub-Research Question
STP	Structural Perspective

TL	Trust Level
TEP	Technological Perspective
TRE	Trustee organization
TRO	Trustor organization
TrustMan	Trust Management
TTT	Tendency To Trust
VBE	Virtual organizations Breeding Environments
VCS	VO Creation Services
VIMS	VO Information Management System
VO	Virtual Organizations
UML	Unified Modeling Language
WizAN	Negotiation Wizard

Chapter 1

Introduction and research problem analysis

This chapter introduces the problem area addressed in the thesis and presents the domain in which the subsequent research results are applied. It presents the research challenges at high-level and briefly introduces the proposed solution for each challenge. It then addresses the discipline of collaborative networks, which constitutes the domain in which our research results are applied. The chapter further analyzes various background definitions and base concepts of trust and discusses three application example cases which are applied to describe the research motivation as well as problem area addressed in this thesis. Therefore, the chapter presents the problem description, research objectives, the motivating research questions, the scope and the applied methodology to this research. Finally, the chapter introduces the project ECOLEAD in which this research was conducted.

1.1 Introduction

Change has been a keyword in recent decades. Organizations increasingly find themselves in new, more challenging and dynamic environments. In relation to business areas, technology and its practical application change quite frequently. Technological developments and breakthroughs have given rise to varying productivity rates, customer demands, market conditions, standards of living, and so forth.

Faced with (1) ever-fluctuating internal and external demands, (2) continuous changes in operating environments, and (3) changes in facilitating technologies, current organizations and in particular *Small and Medium Enterprises* (SMEs) are forced more than ever to reconsider the way in which they structure, coordinate and handle their businesses and all related processes [Vreed, 1995]. Even the survival of SMEs in the current turbulent market is continuously at risk and has become uncertain. Furthermore, increasing market competitions, current governments' tendencies towards trade liberalization and globalization, scarce resources and changes in customers' demands, volatile business opportunities are among the key factors catalyzing this uncertainty, especially for SMEs [Jones, et al., 2000]. Therefore, organizations and SMEs in particular, are increasingly less able to acquire and respond to business opportunities individually and the traditional point-to-point connections between organizations are being rapidly replaced by participation in cooperation networks.

Among the aborning cooperation networks, one type that is gaining momentum at a fast rate both in business and in research is the so-called *collaborative networked organization* (CNOs). A CNO, as further described in Section 1.2, may include partners (individuals or organizations) that are geographically separated and potentially unknown to each other in advance. One form of CNO is the short-term goal-oriented networks (e.g. virtual organizations

– VOs). A challenge for short-term goal-oriented CNOs is that they must be established dynamically and fluently so as to address a targeted goal, such as to compete in acquisition of and response to volatile business opportunities. Furthermore, in order to efficiently collaborate in such networks, participating organizations need to share a common infrastructure, to effectively exchange information and to share their resources and capabilities in order to, for instance, co-design and co-develop towards the aim of the collaboration. These requirements justify the need for the pre-existence of long-term CNOs, as these provide the necessary base conditions for the dynamic creation of VOs, e.g. the pre-existence of strategic alliances called Virtual organizations Breeding Environments - VBEs.

One key challenge related to both the establishment and operation of CNOs, and in particular to short-term goal-oriented CNOs, is the identification and selection of trustworthy partners for the purpose of collaboration and with the aim of fulfilling business opportunities. As further discussed in Sections 1.2.4 and 1.4, this thesis proposes several innovative solutions to the research challenges that relate to the identification of trustworthy organizations for collaboration, and thus also addresses the challenges that relate to the realization of inter-organizational trust. The main challenges that have been addressed are grouped into the following four categories:

- Characterization of trust and trust relationships in Chapter 2.
- Analysis of concepts and aspects of inter-organizational trust, as addressed in Chapters 3 and 4.
- Rational assessment of organizations' level of trust, as addressed in Chapter 5.
- Development of a VBE trust management (TrustMan) system, as addressed in Chapter 6.

The approaches, mechanisms and services proposed in this thesis address these challenges and are needed to support the realization of trust in organizational collaborations. Systematic steps for establishing trust relationships among organizations are proposed (in Chapter 2). A multi-criteria approach for analyzing inter-organizational trust is proposed, and then used to identify and analyze the trust elements and their inter-relations (in Chapter 3) and to model those elements (in Chapter 4). Using the identified, analyzed and modeled trust elements, a conceptual modeling approach is proposed (in Chapter 5). This approach is based on the mathematical equations developed for formulating mechanisms that support the rational assessment of organizations' level of trust. Based on the above contributions, a model for developing services supporting processes related to the management of inter-organizational trust is proposed (in Chapter 6).

The remainder of this chapter focuses mainly on the presentation and characterization of the research problems. In order to enhance the analysis and presentation of these challenges, we present the domain in which our research results are applied in Section 1.2. In Section 1.3 we present the background to the definition of trust and its base concepts, and in Section 1.4 we present the research motivation of the thesis, further addressing the above key challenges and introducing several examples cases to which this applies. In Section 1.5 we present the main questions addressed by the thesis and the research objectives, namely the contributions achieved. In Section 1.6, we present the research methodology and in Section 1.7 we briefly introduce the ECOLEAD research and development project, within which this research was performed, and its specific areas of focus. In Section 1.8 we present the structure of the thesis and finally, in Section 1.9 we present the conclusion of this chapter.

1.2 Collaborative networked organizations and breeding environments

During the last decade, digital technology has changed the world in profound and exciting ways. Today, organizations communicate and interact instantly with each other, and securely exchange sensitive information - such as those needed for businesses collaborations - without the traditional limitations of time and location. Collaborative networks, such as global supply chains, have enabled industries to manufacture and deliver products to markets with incredible speed and efficiency. Advances in technology, specifically those related to ICT (*Information and Communication Technologies*), have enhanced the mobility and flexibility of organizations by, for example, facilitating collaboration irrespective of geographic and physical location.

As an increasing amount of information, communication, and commerce are now in digital form and are facilitated through continuously advancing ICT, doors are being opened to a new world of connected experiences that link organizations' interests and market operations into a seamless whole that extends across local, regional, national, international, and global markets. An emerging effective approach for organizations to co-work in such evolving and expanding markets, while taking advantage of the advanced ICTs, is through the configuration of CNOs. The following definition of a CNO is adopted in this thesis.

> *A CNO is an alliance constituting a variety of entities (e.g. organizations and people) that are largely autonomous, geographically distributed, and heterogeneous in terms of their operating environment, culture, social capital, and goals, and that cooperate/collaborate to better achieve common or compatible goals, and whose interactions are supported by the computer network [Camarinha-Matos & Afsarmanesh, 2006].*

In observation of the trends over the last decades and in order to enhance their survivability in the market, organizations in general and SMEs in particular are increasingly interested in attracting others for the purpose of cooperation and/or collaboration. Today, more organizations are ready to share the resources, knowledge, and skills they have, which are scarce in the market, as well as their gained profits, in order to be involved in more business opportunities and to be able to share their risks and potential losses. They now realize that acting together can enhance their competitive power and thus improve their chances of acquiring more and better business opportunities. Therefore, organizations no longer consider forcing others out of the market to be an effective sustainable working approach [Afsarmanesh, et al., 2007].

This thesis addresses two specific forms of CNOs in detail, namely one short-term type (i.e. VOs) and one long-term type (i.e. VBEs). VOs represent short-term goal-oriented collaborations between partners, while VBEs represent long-term cooperation. The definitions of a VO and a VBE adopted in this thesis are as follows.

> *A VO is an association of (legally) independent organizations (VO partners) that come together and share resources and skills to achieve a common goal, such as acquiring and executing a market/society opportunity [Camarinha-Matos & Afsarmanesh, 2006].*

> *A VBE is defined as a "strategic" alliance of organizations (VBE members) and related supporting institutions (e.g. firms providing accounting, training, etc.), adhering to a base long-term cooperation agreement and adopting common operating principles and*

> *infrastructures, with the main goal of increasing both their chances and preparedness of collaboration in potential VOs [Afsarmanesh & Camarinha-Matos, 2005].*

As mentioned earlier, VOs are configured within the VBE environments and, therefore, the potential VO partners are selected among the VBE member organizations. As stated earlier, one important aspect during the configuration of a VO is the identification of trustworthy partners that may be invited to join the collaboration. This thesis mainly addresses the analysis of inter-organizational trust in VBEs and in particular with respect to facilitating the formation of VOs.

Organizations interoperate and collaborate within VO and VBE networks while being facilitated by computer networks, in order to achieve certain common or compatible goals, such as the acquisition of and response to larger, better, and more business opportunities. As stated earlier, different kinds of co-working are applied in short-term and long-term CNOs and in order to further describe and distinguish between the cooperation and collaboration concepts related to CNOs, the following definitions are applied in this thesis [Camarinha-Matos & Afsarmanesh, 2008]:

> *Cooperation, practiced in long-term CNOs, involves not only the exchange of information and alignment of activities, but also the sharing of resources for achieving compatible goals. Cooperation is achieved by the division of some minor labor (not extensive) between participants. However, a common plan exists that in most cases is not defined jointly, but is designed by a single entity (perhaps by the coordinator/administrator of the cooperation alliance), and which requires some low-level of cooperation.*
>
> *Collaboration that is practiced in short-term CNOs on the other hand is a process in which entities share information, resources and responsibilities in order to jointly plan, implement, and evaluate a series of activities that will help them achieve the common collaboration goal. It implies a group of entities that work intensively together and enhance each other's capabilities. It also implies sharing risks and rewards that, if desired by the group, can also provide outside observers with the impression of a joint identity. Collaboration involves the mutual engagement of participants to solve a problem together, which requires strong trust relationships and thus takes time, effort, and dedication.*

Among other challenges, one basic perceived obstacle to cooperation and collaboration within VOs and VBEs respectively is the creation of trust between the parties involved, which constitutes the main subject of this thesis. Unlike other networks, collaboration in VOs is an intentional property that derives from the shared belief that together the VO partners can achieve goals that otherwise cannot be achieved, or that would otherwise involve much higher costs if attempted individually.

The challenge is to enable the organizations involved to trust each other and to take advantage of the technologies that have been provided to facilitate their cooperation. The effectiveness of collaboration between organizations that are configured to respond to business opportunities has been shown to depend on their ability to quickly create trust in and between each other, which in turn facilitates their sharing of information, resources, costs, and so on. [Msanjila & Afsarmanesh, 2007a]. This thesis mainly addresses the analysis of inter-organizational trust within VBEs and in particular with the aim of facilitating the formation of VOs in VBEs. To enhance the presentation of the thesis, therefore, we first address the concept of a VBE in Section 1.2.1.

1.2.1 Virtual organizations Breeding Environment - VBE

The market and society continuously evolve to cope with the complexity of today's connected digital world. Therefore, the preparedness of an organization that is required to facilitate collaborative initiatives must match the evolution of market. It is more difficult to individually achieve the required preparedness for this matching. Other principal aspects of preparedness and configuration of long-term CNOs - such as VBEs - include establishing common operating principles, acquiring an interoperable infrastructure, and creating trust between organizations. When achieved, these aspects of an organization's preparedness enhance the chance of being able to configure more successful VOs quickly and efficiently.

Certain previous studies have assumed that the most suitable partners for establishing a new VO may easily be identified and selected from the open universe of available organizations, for example through the Internet, and merged into the required VO. However, this assumption overlooks a large number of obstacles in this process, among which the following can be mentioned [Afsarmanesh & Camarinha-Matos, 2005].

- How to learn of the mere existence of potential partners in the open universe and deal with incompatible sources of information.
- How to acquire basic profile information about organizations, when no common template or standard format exists.
- How to quickly establish an inter-operable collaboration infrastructure, given the heterogeneity of organizations at multi-levels, and the diversity of their systems.
- How to build trust between organizations, which is the base for any collaboration.
- How to develop and agree on the common principles of sharing and working together.
- How to quickly define the agreements on the roles and responsibilities of each partner in order to reflect the sharing of tasks, the rights on the produced results, and so on.

As a basic rule, supporting the dynamic/fluent formation of collaborative networks, such as in a VO consortium, requires its potential partners to be *ready and prepared to participate* in such a collaboration environment, as addressed in Figure 1.1. The foundation of this readiness should include reaching commonality agreements on aspects such as the interoperable infrastructure, operating rules, and cooperation. Any collaboration also requires that all involved organizations meet the required level of competency and performance to be considered trustworthy by other partners. Therefore, the concept of a VBE has emerged as the necessary context for the effective creation of dynamic virtual organizations.

A main aim of the VBE is focused on the transition from point-to-point connections between organizations to a network structure in order to increase the chances of its member organizations' involvement in opportunities for collaboration, and to reduce the costs and time needed to configure opportunity-oriented VOs (Figure 1.1). To conclude, the transition from point-to-point connection to networked structure enhances organizations' preparedness in the following aspects [Afsarmanesh & Camarinha-Matos, 2007].

- Maintaining common sharing and operating principles.
- Acquiring an interoperable infrastructure.
- Achieving the same level of understanding through common ontology.
- Defining common value systems and performance metrics.
- Creating trust between organizations.
- Acquiring systems for assisting the management of cooperation and collaboration.

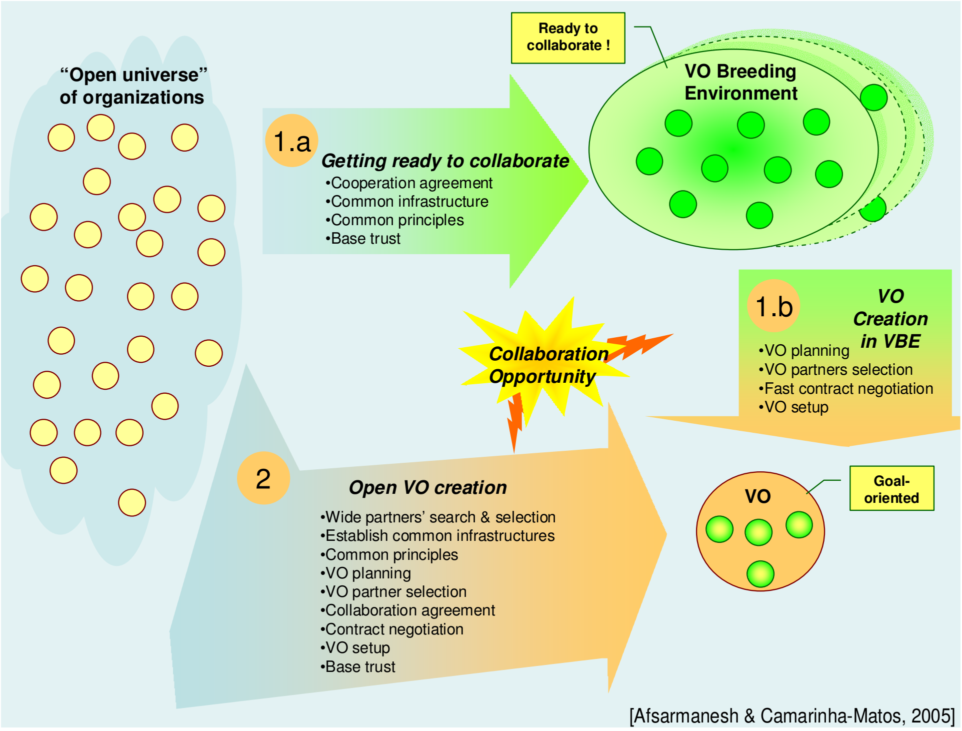


Figure 1.1: The visualization of a VBE concept

This figure shows two possibilities for creating a VO, namely, through the VBE and directly from the open universe. It also shows the role of the VBE in providing chances for organizations to address some preparatory aspects a-priori to the configuration of the VO. In this figure: (1.a) exemplifies the preparedness aspects that are addressed within the VBE a-priori to acquiring an opportunity; (1.b) shows the preparedness aspects that shall be addressed to configure a VO within a VBE after acquiring the opportunity; and (2) exemplifies some aspects that need to be addressed when configuring a VO involving partners from the open universe.

1.2.2 Addressed challenges and gained advantages for organizations joining VBEs

A large number of factors both force and motivate organizations to operate in a very dynamic manner [Geerlings, et al., 2001], what is supported through the VBEs. Influential factors here include continuous advances in ICT infrastructure, dynamic changes in markets and customer demands, increased services quality requested by customers, new political factors such as market globalization and liberalization, and turbulent economic situations. Business-based and politically-based decisions now have to be taken much faster (i.e. needing quick response) in order to seize opportunities that are themselves scarce and volatile, and that require the application of advanced technologies for the support of decisions [Msanjila, et al., 2005]. In addition to the required fast response to emerging opportunities, the volatility of the production markets, such as the *perishable product* market that have been used as examples to define some of the approaches presented in the thesis, has been increasing. In particular, Chapter 5 characterizes the following emerging business requirements and challenges that motivate organizations to join VBEs.

- ***Required competencies***: Production and manufacturing industries must acquire and maintain sufficient, varied, and strong competencies to be able to cope with the current demands that need to be met for each business opportunity. It is becoming ever-more difficult and rare for a single industry to equip itself with the increasing number of competencies that are required for the entire life cycle of production.
- ***Required resources:*** Various - and sometimes an immense amount of - resources are needed to produce each kind of product, and in some cases dedicated to a single business opportunity. These resources are not always reusable for other business opportunities, since different customers' requirements change continuously and become more one of a kind. Therefore, acquiring and keeping all required resources has proven expensive and difficult for individual industries.
- ***Required investment:*** Business opportunities demand a large start-up investment a priori to their execution. In some cases, the costs incurred during the pre-investment stage may not even be repaid during the execution of the business opportunity, and thus become a part of the fixed costs. In principle, fixed costs do take more time to be repaid; however, since customer requirements are continuously changing there is no guarantee that such investments will be re-used to meet other customers' needs. Cooperation and/or collaboration with other organizations can help to prevent the incurrence of certain unnecessary fixed costs by re-using some of the investments made previously by other organizations.
- ***Short delivery time:*** Customers now demand shorter delivery times. They need their products and services to reach the market before their competitors' products do in order to generate more profit, which an enterprise alone can hardly afford.
- ***Change in requirements:*** The current market environments are very volatile. Consequently, business requirements change continuously. This further raises the pressure on industries to advance capabilities and to equip themselves with much-needed resources, competencies, and so on.

Once an organization joins the VBE there are a large number of potential benefits that can be gained. These include the following [Afsarmanesh & Camarinha-Matos, 2005]:

i) *Agility in opportunity-based VO creation*: supporting a reduction in the needed efforts and complexity, flexibility for VO re-configurability, and cost effectiveness.

ii) *Provision of base effective ICT infrastructures for members*: the common grounds for interoperability, inheritability and collaboration.

iii) *The VBE bag of assets*: providing properties of interest for its members and general sharable information or knowledge (e.g. standardized product definitions and processes), software tools, lessons learned.

iv) *Provision of mechanisms, guidelines, and assisting services*: for both motivating and facilitating the configuration and establishment of VOs, and for creating a system of incentives, mechanisms to create positive reputation, and services for partner searches, contract negotiation, etc.

v) *Proactive management of competencies in VBE:* assuring coverage of the needed competency/resources within the VBE.

vi) *Assuring continuity support through support institutions*: Supporting insurance, branding, training, etc.

vii) *Supporting creation of trust among VBE members:* by recording the performance history, and definition of criteria for organizations' trustworthiness.

viii) *Provision of general guidelines for collaboration*: constituting rules of conducts, working and sharing principles, value systems, collaboration ethics and culture, IPR protection, etc.

ix) *Enhancing the chance for VO involvement:* through the provision of members' profiles in the VBE catalog, including their competencies, resources, products, services, and so on, and helping member organizations to acquire opportunities.

x) *Improving the potential / capacity of risks taken by the VO initiators*: due to a reduction in the VO setup efforts/time, and the availability of both a wide variety of competencies (resources) and indicators of the level of trust and past performances of VBE members.

1.2.3 Readiness for joining VBEs

To reduce the severity of the challenges mentioned in Section 1.2.2, most organizations and particularly SMEs in production and service industries increasingly link with other organizations and join in different forms of CNOs. For example, in the perishable products market, as exemplified in Chapter 5 for the analysis of organizations' trust level this trend is observed.

It is clear that every organization needs to go through the preparation/readiness stage in order to join a CNO. However, the preparation stage is much easier for an organization if it joins a long-term *cooperation alliance* in advance (e.g. to become a VBE member), as opposed to if it joins an opportunity-based *collaboration network*, (e.g. to become a VO partner), which involves a more extensive preparation stage that starts from scratch. Facilitating the preparedness of organizations for their participation in VOs is in fact one of the main reasons for establishing a VBE.

In order for an organization to effectively participate in a VBE, at the base of its preparation stage are the adoption of the VBE's common ICT infrastructure and the interoperability approach, which together constitute the minimum base for any cooperation/collaboration network. Furthermore, the main requirements for preparation and adjustment of organizations for the purpose of joining a VBE are reviewed specifically in terms of the following aspects [Msanjila & Afsarmanesh, 2007a]:

- ***Sharing processes:*** organizations must be capable of participating in required (business) processes and be prepared to join and inter-link their efforts with each other, while different organizations may exercise different sets of processes, standards and practices, and a different level of autonomy. Depending on the level of cooperation required within a VBE, this requirement can prove to be very challenging and complex.
- ***Sharing resources:*** organizations must possess resources that are valuable to a VBE and be willing to share them with others. They must also be capable and willing to use other partners' resources. In addition to willingness, in order for an organization to share, this requirement implies compliance with the common VBE sharing policies, and the need for experience, skill, knowledge, and so on to prepare the sharable objects, and to support this sharing activity. For example, in order to prepare to share a technology-related resource (such as computation facilities), the organization must make sure that the resources comply with some standards in a VBE, such as those relating to communication and interoperability.
- ***Sharing competencies:*** it is difficult for an organization to acquire all the competencies that are necessary to assure its existence in business and thus get competitive opportunities. In collaborative networks, there is a chance to share competencies of other organizations and the proper management of these available and emerging competencies

in VBEs is the necessary base element to support this requirement. Organizations must be prepared to offer some of their own competencies for this purpose, as well as benefit from the pool of available competencies in the VBEs. For example, in order to share programming-related competencies, such as re-using each others sharable codes, a certain level of programming knowledge and competencies are required of the employees in an organization (e.g. the availability of scientific programmers, computer science graduates, etc.) and must be demonstrated.

- ***Coping with contradicting interests, goals, and culture:*** each member organization in a VBE has its own internal interests, goals, and culture. Beyond the common interests and goals that have been planned to be achieved together, each organization may wish to achieve some of its own internal interests and goals, which might sometimes contradict those of the other organizations. Organizations must be prepared and expect to collaborate towards the common VBE goals, and to tolerate or adjust to differences that fall beyond it.
- ***Sharing governance rules and value system:*** organizations must comply with the common rules of operation and behavior in a VBE. These rules aim at ensuring that every organization joining the VBE or maintaining its membership in the VBE possesses at least the basic qualifications (such as possessing the required set of competencies, having at least the allowed minimum level of trust, etc.) and also commit itself to a number of aspects related to the operation of the VBE (such as agreeing to the operating and sharing principles, agreeing to the VBE administration principles, rewarding and sanctions policies, etc.). To evaluate whether organizations meet such set of VBE rules, organizations will be required to provide their related information. For example, they must contribute to the information needed for the assessment of their trust level that constitutes a base for their readiness to cooperate/collaborate in a VBE, as well as meet/preserve the base level of trust that is required by the VBE in which they are involved.

1.2.4 VBE management and the need for trust

This section mainly addresses the management of VBEs and its need for inter-organizational trust as the means to facilitate the performance of VBE management-related activities. It first presents the general aspects of traditional organization management in order to distinguish and compare the focus of activities will be performed in the VBE with those of traditional organizations. Furthermore, it presents the general necessary VBE management activities relating to each stage of the VBE life cycle. Finally, it addresses and justifies the fundamental need for establishing inter-organizational trust in VBEs.

In principle, management comprises directing and controlling a group of people or entities (e.g. departments, or organizations) for the purpose of coordinating and harmonizing that group towards accomplishing a common goal (Howe, 2004). In traditional practices, management often encompasses the deployment and manipulation of human resources, financial resources, technological resources, and natural resources in a company. However, it can also refer to the individual or a group of people who perform the act(s) of management. The generic categories of management include (Center, 2008).

- o *Organizing:* making optimum use of the existing resources to enable the successful implementation of plans.
- o *Controlling/monitoring:* checking progress against plans, which may need plan modification according to feedbacks.

- *Planning:* deciding what needs to be performed in future, e.g. immediately or in weeks, months, years, etc.), and generating plans of action to reach the objectives.
- *Leading/Motivating:* applying mechanisms and strategies to get others into playing an effective part in achieving plans.

The above definitions have been applied successfully to the management of traditional organizations with static structures, such as traditional business companies. These organizations typically practice repetitive and fixed business processes. The following fundamental aspects indicate the static nature of traditional organizational structures:

- ***Fixed or known resources***: products or services that a traditional organization can offer to its customers are usually well defined and standardized. These products or services can only be customized to meet specific customer requirements, but usually they do not require re-development. Thus, the resources that are needed for manufacturing products or providing services are usually known before a specific opportunity is acquired. These resources can be obtained and kept in an organization a priori to the search for and the acquisition of business opportunities. The management of resources mostly focuses on either ensuring their availability within an organization or on time acquisition whenever is needed.
- ***Fixed or known competencies***: as stated above, products or services that a traditional organization can offer are usually known and standardized. Thus, the competencies that are required to support the manufacture of products or the provision of services are also known and standardized. The management of such competencies is mainly focused on either enhancing the existing ones (e.g. through specialized training of employee) or acquiring new or qualified employees.
- ***Static and specific business strategies***: products or services that can be offered by traditional organizations are usually standardized. Therefore, these organizations maintain static or long-term business strategies. These strategies focus on, for example, keeping past customers for as long as possible, or acquiring as many new customers as possible. The management of these processes follows well-defined organizational business strategies.
- ***Static sharing and operating principles***: most traditional organizations have a culture of sharing achievements (e.g. percentage of yearly profit) with their employees, which may be offered as a motivation benefit (e.g. end of year bonus). The principles used to distribute such benefits are usually known and standard within an organization and depend on aspects such as salary levels, employee positions and employee performances. The management of these activities therefore, follows defined principles within the organization.

On the other hand, unlike the traditional organizational structures, VBEs have dynamic structures and the required business processes are unique. For example, the VO creation within a VBE is unique to each configured VO since it responds to a specific opportunity. Among others, the following fundamental aspects indicate the dynamic nature and characteristics of the VBE structures.

- ***Dynamic resources***: VBEs can offer their products or services to their customers only through the configuration of VOs. The resources that are required to manufacture products or provide services belong to VBE's member organizations. Therefore, VOs are uniquely configured constituting "best-fit" organizations that are capable of sharing or exchanging their resources in order to respond to opportunities. The partners may change for every VO that is configured, even if the same product or service has to be provided to a customer. Therefore, the availability of the resources cannot be known or guaranteed a priori to configuring the VO. The management of such resources in VBEs mostly focuses on ensuring that the resources needed in the current market can be provided by its VBE members.

- ***Changing competencies***: VBE competencies constitute a set of the aggregated competencies of its member organizations. Thus, VBEs do not have competencies of their own beyond those of their members. The management of competencies focuses on ensuring that all of the related competencies that are needed in the market exist within the VBE. One fundamental approach to fill competency gaps is through inviting external organizations to become VBE members and thus provide missing competencies.
- ***Dynamic business strategy***: VBE business strategies need to change depending on the market changes, i.e. with a consideration for the following areas of focus: the acquisition of potential member organizations, support for opportunity brokerage, the facilitation of VO configuration, the provision of information to actors in a VBE for the purpose of making informed decisions, and so forth. In other words, the VBE administration primarily focuses on facilitating the success of some of these processes and subsequently carries out dynamic changes to the VBE's strategy as perceived necessary.
- ***Opportunity-based sharing and operating principles***: the fundamental benefits of operating in a VBE are gained through participation in VOs. Potential VO partners negotiate on how benefits will be shared while operating in the VO and the VBE administration advices/supports such negotiation by providing these with necessary information and negotiating templates.

Considering the differences between the management aspects in traditional organizations and in those of VBEs, as addressed above, it is clear that a VBE administration cannot directly apply the traditional management approaches in handling its activities. In addition to the above differences, the VBE management activities and the focus on every activity may change according to the specific stage of the VBE life cycle. Therefore, a priori to addressing the general VBE management activities, where we demonstrate the need for establishing inter-organizational trust, we first present below the background VBE management activities typically performed in practice by the VBE administrations, during different VBE life cycle stage.

VBE life cycle stages and their related management activities

The management of a VBE may need to perform different activities at different phases of the respective VBE's life cycle. Thus, to enhance the presentation of the basic VBE management processes we first briefly address the VBE's life cycle, which comprises three high level distinct phases as follows.

Each VBE first undergoes the *creation phase,* during which a number of elements are characterized and initiated. This occurs during its two sub-phases, namely the *initiation & recruiting* and the *foundation* (see Figure 1.2). During the initiation & recruiting sub-phase, the VBE administration performs (or supports the performance of) the following main activities: setting up & running the VBE management system and ICT- tools, loading existing ontology & thesaurus, setting up domain parameters & nodes, and so on. During the foundation sub-phase, the VBE administration performs (or supports performing) the following main activities: adapting the VBE ontology, adapting database schema and creating repositories & interfaces for database access, entering administrative data, and registering founding members.

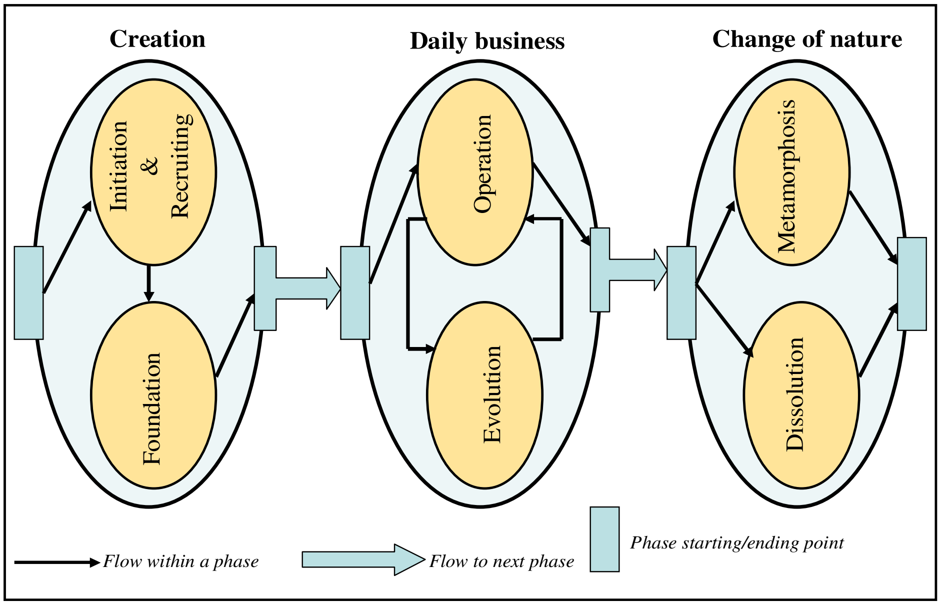


Figure 1.2: Phases of the VBE life cycle

As shown in this figure and explained in this section, the sub-phases occur in certain orders as follows: (i) in the creation stage, sub-phases occur in sequential order, (ii) in the daily business stage, sub-phases occur in concurrent order and (iii) in the change of nature stage only one of the two sub-phases can occur at a time.

Following the *creation phase*, the VBE undergoes the *daily business phase*. This phase has two parallel sub-phases, namely the "*operation*" and the "*evolution*". This phase constitutes the bulk of the VBE's life-time and thus it is a relatively much longer than the other two phases. During this phase many collaborative activities, such as repetitive acquisitions of and responses to business opportunities, are performed in the framework of achieving the VBE objectives. During this phase therefore, the main management activities of the VBE administration are aimed at supporting acquisition and supporting such responses to business opportunities. An example of this may include activities related to ensuring that competencies required in the market actually exist within the VBE. Furthermore, during the *operation* sub-phase minor changes become sporadically required, e.g. inviting new member organizations to fill the gaps in competencies discovered in the VBE. In response to such minor changes the VBE undergoes the *evolution* sub-phase. In this phase, the VBE administration performs (or supports performing) the activities that are required to facilitate evolution of the VBE.

The last high-level phase is called the *change of nature*. This phase has two independent, disjoint and parallel sub-phases, namely the *metamorphosis* and the *dissolution*. However, since a VBE is a long-term alliance and considering the valuable bag of assets (including sharable knowledge, resources, etc.) that are gradually collected within the VBE, its *dissolution phase* – the closure of the VBE – is a very unusual situation. Instead, it is much more probable that the VBE goes through the other sub-phase - the *metamorphosis phase* - where it can undergo a major evolution that changes its form and purpose. During the *change of nature* period, the VBE administration is responsible for ensuring that all the assets are either inherited or transferred to another VBE when metamorphosis occurs or to another specific organization(s) when dissolution occurs. The following section zooms in within the VBE's daily business phase, and addresses four specific VBE management activities that require establishment of inter-organizational trust in the VBEs.

The need for inter-organizational trust in VBEs

As stated earlier, the analysis of inter-organizational trust in VBEs, and in particular for the formulation of VOs within VBE environments, is fundamental for effectiveness of VBEs. Four key processes for the VBE administration that require rationally managed inter-organizational trust in VBEs are discussed below. These include: *VO configuration, new membership evaluation & registration, opportunity brokerage,* and *decision-making for managing daily activities*.

a) Process 1: VO configuration

Upon the brokerage of an opportunity, the VO planner - which is the organization appointed to configure the VO - selects potential partners among the VBE member organizations to configure the VO. One challenging issue related to the selection of such partners is the analysis of their level of trust, in order to select the "best fitting" set of partners for that specific VO. As observed in practice, VO partners only collaborate effectively when they are assured about the trustworthiness of others. Consequently, the organizations' level of trust must be thoroughly analyzed so as to support the performance of this VBE management process. The main focus of this thesis is establishing an approach that rationally analyzes inter-organizational trust and supports for reasoning on such subsequent results of its analysis.

b) Process 2: new membership evaluation and registration

VBEs are not closed border environments, rather controlled border environments. This implies that any organization wanting to join a VBE may apply for VBE membership. An organization may become a member of a VBE in one of the following two ways:

- The first case is when an organization realizes that operation within a VBE is more beneficial than operating individually, and thus decides to join. In this case, membership process is initiated by the organization itself and by sending an application to the VBE.
- The second case is when a VBE administration identifies some gaps, such as in competencies, which need to be filled in order to enhance a VBE's competitiveness in the market and within society, and thus decides to invite external organizations into the VBE. In order to fill such gaps, a VBE may in this case actively search in the market for the most suitable organizations to invite. The process for becoming a member is thus initiated by the VBE by means of an invitation to these organizations.

Irrespective of which approach initiated the membership processes, a VBE administration must preserve a certain level of trust throughout its organizations, which is usually the level at which they are considered to be potential VO partners. Therefore, all membership applicants must meet this level of trust in order to be registered and to remain in the VBE. Organizations invariably possess different characteristics, such as their business focuses, capabilities and past performance records. A rational analysis of trust should capture all such heterogeneous aspects in order to support an examination of the trust level on the one hand and on the other hand to make it possible to reason on the results. This thesis addresses these specific aspects of inter-organizational trust.

c) Process 3: opportunity brokerage

Each VBE operates in a normal market/society that contains competitors, including other VBEs and large strong companies. Customers that either provide the opportunities or identify which providers should acquire those opportunities must trust the respective VBE. Therefore, VBEs should demonstrate their trustworthiness for the purpose of acquiring the opportunities for which they bid. Aspects that customers might prefer to analyze in order to decide on a VBE's trustworthiness may include the "trust level" of the VBE's organizations. This thesis addresses these aspects of inter-organizational trust.

d) Process 4: decision-making for managing daily activities

A number of administrative decisions are made daily in a VBE for the purpose of its effectiveness and smoothing its continuity. Some crucial decisions include, for example, accepting new membership applicants, rewarding or sanctioning member organizations, appointing an organization to take an administrative role (e.g. VO planner) and defining new VBE policies or principles. These decisions are typically made by the VBE administration. Nevertheless, such decisions indirectly affect all VBE's members. Therefore, the organizations making such decisions must be itself be trusted by all participating VBE members. These aspects of inter-organizational trust are addressed further in Section 3.3 of this thesis.

1.3 Background on definition of trust and its emerging base concepts

In this section we define the base concepts related to the rational establishment of trust between organizations. We also present a survey of a number of existing trust definitions in order to provide a comparison with the definition of trust as applied in this thesis.

1.3.1 Diversities among definitions of trust

Trust is a complex subject and is related to many aspects in multi-disciplinary areas. It is addressed, for example, in relation to the security, risks, privacy, belief, honesty, truthfulness, competency, reliability, past history, and so on of the trusted parties. Due to the variations in its interpretation and the variations in its perception by involved parties in both practice and research, the concept of trust is defined differently in various disciplines. There is still no consensus in the literature on what trust means and what constitutes the management of trust between different entities, such as individuals or organizations [Povey, 1999]. However, many researchers have recognized its importance for smoothening interactions and cooperation between both individuals and organizations [Camarinha-Matos & Afsarmanesh, 2006]. The significance of trust in today's collaboration is due to the fact that it is an important factor for enabling interactions and cooperation between both individuals and organizations [Blomqvist, 2005].

The lack of consensus on the definition of trust has led researchers to define trust differently for the purposes of providing a common understanding in their specific domain or application environment. For example, despite the need to standardize the definition of trust for online transactions, different researchers simply use and assume definitions of trust in relation to their specific topic, such as the authentication, security, reliability and availability of the supporting system, or even the ability of the customer to pay for a purchase online by using well known credit cards, etc. In each application area, however, certain researchers have tried to approach and analyze trust in a generic way.

With respect to online transaction technology, Kini and Choobineh [1998] have addressed the theoretical framework of online trust, examining it from the perspective of personality theorists, sociologists, economists, and psychologists. In their work they started by defining trust according to the Webster dictionary as: *an assumed reliance on a person or something. It is a confident dependence on the character, ability, strength, or truth of someone or something. It is a charge / duty imposed in faith / confidence or as a condition of a relationship. Thus it simply means to place confidence in an entity.*

Using this definition, they further highlighted the implication of trust in daily practices and combined this with the results from their analysis of the social psychological aspects of trust, in order to establish a definition of trust in online systems, which proceeded as follows: *"a belief that is influenced by the individual's opinion about certain critical system features"* [Kini & Choobineh 1998]. Although their analysis and conclusion addresses the general concept of trust in a system, it also focuses on individuals' trust and specifically in relation to those involved in e-commerce.

The European Commission Joint Research Center defined trust *as "the property of a business relationship such that reliance can be placed on the business partner and the business transactions developed with them"* [Jones, et al., 2000]. This view of trust is based on the area of business management and provides an interesting analysis of what must be done to enable and enhance trust between partners in business. In the analysis related to her work, Jones [Jones et al., 2000] stated that the following aspects of trust are fundamental for partners in business:

- The identification and reliability of business partners.
- The confidentiality of sensitive information.
- The integrity of valuable information.
- The prevention of unauthorized copying and use of information.
- The guaranteed quality of products and services.
- The availability of critical information.
- The management of risks relating to critical information.
- The dependability of computer services and systems (the availability, reliability, and integrity of infrastructure; the guaranteed level of services; and the management of risks relating to critical infrastructure).

The Oxford Dictionary defines trust as *the firm belief in the reliability, truth or strength of an entity*. In this definition, a trustworthy entity is basically highly reliable and so will not fail during the course of an interaction; will provide a service or perform an action within a reasonable period of time; will tell the truth and remain honest with respect to interactions; and will not disclose confidential information.

In view of these varied definitions, trust can be regarded as a composition of many different attributes: reliability, dependability, honesty, truthfulness, security, competency, past history of individuals, timelines, and so forth. Any of these may be considered, depending on the environment and application for which the trust is being specified.

In spite of the attempts to define trust in research and the difficulty to reach consensus among researchers, the word "trust" in relation to inter-personal trust in particular and as used daily by individuals refers to one person's opinion of another person.. Not only is an estimation of another's intention needed to establish inter-personal trust relationships, but also an estimation of others' potential competencies. Gambetta [Gambetta, 1988] provided a definition of individuals' trust and this definition is widely used: …*the subjective probability* *by which an individual "A" expects another individual "B" to perform a given action on which A's welfare depends*. Furthermore, the three following definitions dominate current research into the trust in different entities:

- *Trust is the willingness of a trustor to be vulnerable to the actions of another party based on the expectations that the trustee will perform a particular action important to the trustor irrespective of the ability to monitor or control the trustee [Mayer, et al., 1995].*
- *Trust is the belief in the competency of an entity to act dependably, securely and reliably within a specified context [Grandison & Sloman, 2000].*
- *Trust is a psychological condition comprising the trustor's intention to accept vulnerability based upon positive expectation of trustee's intentions and behavior [Rousseau, et al., 1998].*

The diversity between the existing definitions and the differences among their identified elements make it challenging for us to properly characterize trust as it needs to be addressed today. As we pointed out previously, there are many theories on trust, some of which diverge only in their identification of the grounds on which they are based [Settle, 1998]. Despite the difficulties in solidifying the definition of trust, the concept of trust is applied daily in practice as a base for cooperation and collaboration between both individuals and organizations. Past research on VBEs reports that the effectiveness of the establishment of trust and the effectiveness of VO creation depend on the balance of organizations' level of trust [Mezgar, 2006].

As addressed further in Chapters 2 and 3, trust relationships in VBE environments must be addressed from three specific points of view, namely those of *the VBE member organizations, the external stakeholder organizations,* and *the VBE administration organization*. Therefore, while this work can benefit from general past research on trust relationships between individuals, the results of such research cannot be directly applied. Trust between organizations in VBEs is a more complex subject, which must be addressed in relation to the interdisciplinary between the domains and the heterogeneities and contradictions between the interests and the goals of organizations involved [Msanjila & Afsarmanesh, 2007a]. In our research, the *identification and tuning of trust elements, modeling of trust and trust elements, assessment of trust level,* and the *establishment and promotion of trust relationship* constitute the main focus of the management of trust among organizations in VBEs [Msanjila & Afsarmanesh, 2007d]. The following definition of trust between two organizations is applied in this work:

> *Trust between two organizations, as it is applied in VBEs, is the objective-specific confidence of a trustor organization to a trustee organization based on the results of rational (fact-based) assessment of the trustee organization's level of trust [Msanjila & Afsarmanesh, 2007c].*

Therefore, a rational (fact-based) trust creation refers to the process of creating trust between organizations using the results of a rational (fact-based) assessment of their level of trust. Only measurable elements (numeric data) are used for such an assessment and the resulting trust levels can be supported with formal reasoning (i.e. mathematical equations) that is used during the rational assessment of level of trust, which in turn supports reasoning about results [Msanjila & Afsarmanesh, 2007a].

1.3.2 Base concepts of trust

As described in Section 1.3.1, the concepts of trust are interpreted and perceived differently. Consequently, these differences affect the understandability of the base concepts of inter-organizational trust in research and practice. In this thesis we use the following definitions of base concepts of trust parameters for organizations [Msanjila & Afsarmanesh, 2007a].

- ***Trust actors:*** refer to the two parties involved in a specific trust relationship. The first party is the organization that needs to assess the trustworthiness of another, and is referred to as the trustor. The second party is the organization that needs to be trusted and which will thus have its level of trust assessed; and it is referred to as the trustee.

- ***Trust level:*** refers to the level of intensity of trust for a trustee organization in a trust relationship, based on an assessment of the values for a set of necessary trust criteria. Clearly enough, the criteria for assessment of organizations' level of trust vary and have a wide spectrum, depending on the specific purpose (e.g. the requirements, the perspective, and the objective of the establishment of trust). When the level of trust is assessed for a specific purpose - such as inviting a member into a VO - and the assessment is based on specific trust criteria for that specific purpose, the evaluated trust level results are referred to as the *specific trustworthiness* of that organization.

- ***Trust level assessment:*** refers to the examination of the trustworthiness of an organization using certain defined indicators. Many approaches are used to assess different entities' level of trust. As addressed in Chapters 3 and 5, we propose a multi-criteria approach for analyzing the trust in organizations. Based on this approach, rational mechanisms have been developed to assess the level of trust in organizations.

- ***Trust relationship:*** a relationship is a state of connectedness between people or organizations, or a state involving mutual dealing between people or parties. Here, trust relationship refers to the state of connectedness between a trustor and a trustee whose intensity is characterized and based on the trust level.

- ***Time:*** a trust relationship (and its intensity) between the trustee and trustor is time-bound and may thus differ from day-to-day. In other words, an organization's level of trust is not static and may alter with time, depending on the number of changes to specific aspects used in the assessment. Therefore, the time at which the results will be applied needs to be considered when analyzing trust in VBEs.

1.4 Research motivation and problem area description

In Section 1.2.4 we addressed the need for the establishment and management of trust in VBEs. For example, one key need in relation to trust described in that section is the identification of potential trustworthy VO partners. In this section, we present the main research motivations for the thesis and describe a few exemplary representative problems related to analyzing inter-organizational trust. Three specific example cases are used for this purpose and the focus is on addressing the identification of potential VO partners. The aim of presenting these real examples is to clarify the challenges relating to this problem area and to illustrate the different level of complexities faced by trustors.

The three example scenario cases below address the selection of trustworthy organization(s) for invitation to participate in a VO, and focus on (1) *delivering expensive and delicate products to the market,* (2) *providing support services to street children,* and (3) *building a parliament house*. Different sets of requirements, criteria, and so on become of main concern/preference to the trustor, in the process of measuring the trustworthiness of trustee organizations, depending on the “objective” for the assessment/establishment of trust as further described below.

i) Case I: A VO to deliver expensive and delicate products (VO-EDP)

Imagine that a broker has acquired a business opportunity in a market which will address the delivery of expensive and delicate products (e.g. flat screen LCD TVs and laptops) to the market. The delivery needs to meet the large demand of the geographically distributed market - such as the European market or African market - and the organizations involved need to be capable of covering both pre-investment, such as transport means, and insurance during transportation.

With the help of the VBE administrator, the broker then appoints a VO planner. One important task for a VO planner is to select suitable VO partners among the VBE member organizations. A VO planner must select the most trustworthy organizations to be invited into the VO on the basis of the specific objective. Since the main requirement in the case of this VO is that the potential partners are capable of covering the costs of pre-investments and certain potential losses that may occur during the operation phase of the VO, such as some damage to the products, the VO planner may focus primarily on assessing the *economical trustworthiness* of the organizations. Consequently, *capital and financial stability* will be considered as the fundamental aspects (Section 3.3.1) that have to be met by the potential VO partners. The set of exemplary measurable parameters in this case, the values of which must be available from organizations at the VBE, might include *cash capital, physical capital, profits from past VOs* and *operational capital*.

ii) Case II: A VO to provide support for street children (VO-SSC)

In developing countries, the problems relating to street children (children who are homeless and thus live on streets without proper support of food, shelter, clothing, etc.) are serious and ever-more challenging. As an example, therefore, we consider an international organization that wants to configure a VO that will constitute the following two types of partners: (1) Organizations that are capable of providing funding to support the acquisition of resources necessary for the provision of services to street children in certain cities in a country, and (2) Representative organizations in the local cities those are able to deliver the necessary services to the designated children.

In such a network, namely an international organization that assumes the role of the VO planner, the social life of these children is of paramount importance. Therefore, the potential VO partners should also have the same perception and concern for the social values pertaining to this problem. The provision of social support to people should be of particular primary importance in the daily business of the respective organizations, and must be proven by some rational (fact-based) data. This means that *primarily,* the VO planner might assess the *social trustworthiness* of the potential VO partners. Exemplary factors such as community service provision, community standards commitment (e.g. child labor laws) and so on (Section 3.3.1) will be considered for the assessment of organizations’ level of trust in this case.

Furthermore, the VO planner prefers the local partners to be capable of using certain internal resources, such as employees, to deliver the required services. Therefore, the number of employees, personnel expertise, number of branches/offices, organizational competencies, and so forth of the local organizations might be the second most important aspect for the VO planner in his evaluation of trustworthiness. As a result of this, the *structural trustworthiness* of potential partners will be also assessed.

Lastly, each organization - and in particular local organizations - should be able to support themselves financially in any activities that are not directly related to the delivery of the service. For example, the costs of visits by employees to the centers where the children are hosted should be covered by the respective organizations. As a consequence, the economical stability of the potential local organizations needs to be taken into account. The VO planner may thus also prefer to assess the *economical trustworthiness* of the local partners.

iii) Case III: A VO to build a parliament house (VO-BPH)

A parliament is a legislature, especially in those countries that have a governmental system based on the Westminster system of government, which is modeled after that of the United Kingdom system. The construction of a parliament house needs to carefully address many aspects such as security, facilities and privacy. The configuration of a VO to build such a house is a challenging task and especially when it comes to the selection of potential trustworthy partners for invitation to join such a VO. The construction of such a VO is not only costly, but also touches the interests of the entire public in the country and demands modern and complex technologies for both ensuring security and providing high quality results.

To be selected to join a VO, the image that the potential partners (usually reputable organizations) portray to the entire public is fundamentally important. Traditionally, the image of an organization is represented by its managerial image, both internally and externally. Consequently, the issues related to the management of organizations, such as experience and stability, as well as past opportunistic behavior, corruption scandals, and so on shall be considered in the evaluation of the *managerial trustworthiness* of potential partners. However, since the privacy and security of the building must be ensured, the technology to be used must be both available and proven within the organizations. Therefore, although experience and the ownership of technology within an organization are not the only factors, they are certainly fundamental ones. In conclusion, the VO planner will *primarily* assess both the *managerial* and the *technological trustworthiness* of the potential partners.

Moreover, inviting an organization with a bad social image - such as that caused by failing to meet certain community standards - into the VO of this particular project may also have negative implications in relation to the future of the entire project. Therefore, organizations' social images are also a fundamental aspect that needs to be assessed when establishing the trustworthiness of the potential partners. Furthermore, the plan for the construction of such houses needs to remain confidential; despite signing the contract, the VO planner may need assurance that confidential material, such as the security mechanisms for the building, will not be disseminated outside VO partners. As a consequence, the availability of, for example personnel experts, competencies, and so on within the organization also becomes important. Hiring temporary employees from other organizations for the purpose of providing the skills needed in the project is quite discouraged. Therefore, the specific trustworthiness of potential organizations will also be assessed in relation to their internal structure. In this case, the VO planner will *secondarily* evaluate both *social* and *structural trustworthiness* of the potential partners. Lastly, the potential partners must be able to invest a priori in the project towards the first payment, which means that they also need to be financially strong and stable, especially in relation to operational capital. Ternary consideration for the VO planners may therefore include the *economical trustworthiness* of potential partners.

Analysis of the complex nature for inter-organizational trust

The trustors as described in the three example cases above (VO-EDP, VO-SSC, and VO-BPH) are concerned about different aspects relating to the evaluation of their potential partners' trustworthiness for the purpose of inviting them into the respective VOs. Even when the same aspects are considered, the order of importance and preferences usually vary (Table 1.1). This shows that different specific parameters need to be applied for assessing potential VO partners' level of trust, depending on the VO's objectives.

Table 1.1: Summary of trustor organizations' concerns and preferences for trust assessment

	VO-EDP	**VO-SSC**	**VO-BPH**
Economical trustworthiness	■	░	░
Social trustworthiness	□	■	▨
Technological trustworthiness	□	□	■
Managerial trustworthiness	□	□	■
Structural trustworthiness	□	▨	▨

■	▨	░	□
Primary	**Secondary**	**Ternary**	**No interest**

The three cases presented above reveal that there are a large number of open issues to be addressed in order to enhance the management of trust among organizations in VBEs. These issues include:

(a) Differences in concerns/preferences for the aspects that are considered by trustor organizations to assess trust level of trustee organizations.
(b) Variations of requirements and purposes for the assessment of trust level of organizations, which in turn influences the perceptions of trust of the trustor organizations.
(c) The identification of diverse trust elements to support any emerging concern/preference of trustor organizations.
(d) The identification and modeling of inter-relations among factors (trust elements) to support the analysis of inter-organizational trust and to provide reasoning about the results achieved.
(e) The management of fact-based data for parameters preferred by the trustor organizations and the collection (provision) of those data from organizations involved.
(f) Mechanisms to dynamically support the rational assessment of trust level of organizations, taking into account the changing parameters.
(g) The development of services supporting processes related to the management of trust between organizations, such as processes for assessing organizations' level of trust, mechanisms for establishing trust relationships between organizations, etc.
(h) The provision and presentation of the resulting levels of trust, which must be as understandable as possible to all of stakeholders in the environment, regardless of their expertise on trust and such aspects.

These open issues are among those addressed in this thesis as contributions towards providing the approaches, mechanisms and tools needed to support the management of inter-organizational trust in VBEs. In the following section we present more details regarding the research questions addressed by this thesis. Each of the above listed open issues is addressed by at least one of the open research questions indicated in Section 1.5.

1.5 Research questions, objectives, and scope of the thesis

A number of research questions must be properly addressed to support the realization of rational trust in VBEs. It is clear that trust relationships between organizations play a preconditional role in achieving smooth and successful cooperation in VBEs and collaborations in VOs. The following series of main research questions (MRQ) and their respective sub research questions (SRQ) are addressed in this thesis.

MRQ1: How the diversities in the purposes for which trust among organizations need to be established (from trustor to trustee) as well as trustor's concerns and preferences can be handled?

This first main research question - which covers open issues (a), (b), and (c) mentioned in Section 1.4 - is primarily related to the characterization of inter-organizational trust as applied in VBEs. It is addressed mainly in Chapters 3 and 5. These chapters address different possible perceptions about organizations' trust and their preferences on the set of related trust criteria to be used for assessing organizations level of trust. This main question has the following two sub-questions.

SRQ1.1: Which trust criteria and how many must be applied to measure an organization's level of trust in a VBE?

We present an approach for identifying trust elements in Chapter 3 and also an approach for customizing the mechanisms to assess organizations' level of trust in Chapter 5. These two chapters collectively address the following sub-question:

SRQ1.2: Which values of trust criteria shall be improved by a trustee organization in order to reach higher trustworthiness within a VBE?

In Section 2.4, we present aspects that can be considered while deciding about the required trust related data to support the establishment of trust between organizations. In Section 2.5, we propose systematic steps for establishing sustainable trust relationships among organizations in VBEs. These proposed steps are supported with defined approaches and/or functionalities (addressed in Chapters 3, 5, and 6) for creating trust among involved organizations.

MRQ2: How can the understanding of many elements and concepts related to rational trust within a VBE be supported for its stakeholders?

This second main question, which covers open issues (a), (b), (g) and (h), is primarily focused on modeling inter-organizational trust related elements. It is mainly addressed in Chapter 4 and it has one following sub-question:

SRQ2.1: What models can suitably represent the concepts related to both trust and trust relationships between organizations?

In Chapter 4 we discuss the modeling needs related to trust and we present three kinds of modeling approaches for trust and trust relationship between organizations. In this chapter, we thus address both the main question and its sub-question.

MRQ3: How can formal mechanisms be developed to rationally assess and formally reason about the level of trust in organizations?

The third main research question mainly addresses four open issues, namely as listed earlier in items: (c), (d), (e), (f) and (g) in Section 1.4. Primarily, this question is related to the development of mechanisms for measuring the level of trust in organizations within a VBE. It has the following four sub-questions:

SRQ3.1: Can the level of trust in an organization be rationally measured within a VBE?

SRQ3.2: What is the relation between every measured trust criterion and the level of trust in an organization?

SRQ3.3: How to analyze the inter-relations and influences among different trust criteria?
SRQ3.4: How to develop formal mechanisms for assessing trust level of organizations?

In Chapter 3 we present an approach for analyzing the inter-relations among rational trust elements as well as examining the influence of each factor to the trust level of an organization. To address the influence of a factor to the trust level of an organization, we present an impact analysis approach to analyze the impact of varied values of one factor on the trust level of an organization. Further, to address the inter-relations and influences among rational trust elements and in particular the measurable criteria, we present the causal analysis approach, applied for analyzing the causal influences among different trust factors. The results of causal analysis are then formulated into mathematical equations. Later on, in Chapter 5 we introduce formal mechanisms for assessing trust level of organizations, applying the mathematical equations derived from the analysis of causal influences among trust criteria. Therefore, in Chapters 3 and 5 we address this main question and its four sub-questions.

MRQ4: How can the establishment of inter-organizational trust relationships in VBEs be facilitated?

This fourth main research question covers open issues (a), (b), (d), (e), (f), (g), and (h) and is primarily related to the development of trust management support system. In Section 2.5 we present fundamental steps that can be followed to assure the establishment of sustainable trust relationships between organizations. In relation to those proposed steps, in Section 2.5 we thus address the following first two sub-questions.

SRQ4.1: How to convince involved organizations about trustworthiness of others?
SRQ4.2: How to sustain inter-organizational trust relationships in VBEs?

Furthermore, in Chapter 6 we present the Trust Management (TrustMan) system, which provides services that can be invoked with other remote systems and as well web-based functionalities that are accessed by human users through the web. The services are designed to support trustors to properly analyze trust of trustees in order to make informed decision while establishing trust relationships. In Chapter 6, we thus address this main question, as well as its sub-question that follow.

SRQ4.3: How can the trust management system facilitate establishment of trust relationships through both periodical and occasional measurements of organizations' rational trust level?

The main contributions this thesis makes are thus achieved by answering the above series of research questions. *The approach designed for identifying trust elements for organizations* (Chapter 3), *the developed mathematical (conceptual) models applied to formulate mechanisms for assessing level of trust* (Chapter 5), and *the designed/developed trust management system* (Chapter 6), however constitute the main contributions of this thesis. These contributions are further complemented by fundamental aspects of our research, namely comparisons with existing work and the characterization of aspects of inter-organizational trust (Chapter 2), and modeling identified trust elements (Chapter 4). Therefore, through the integration of these contributions we have achieved the following two main research objectives:

Achieved Research Objective 1 (RO1):
To properly support the management of trust aspects in VBE, providing generic and comprehensive "concepts, approaches, mechanisms and models" needed for supporting:

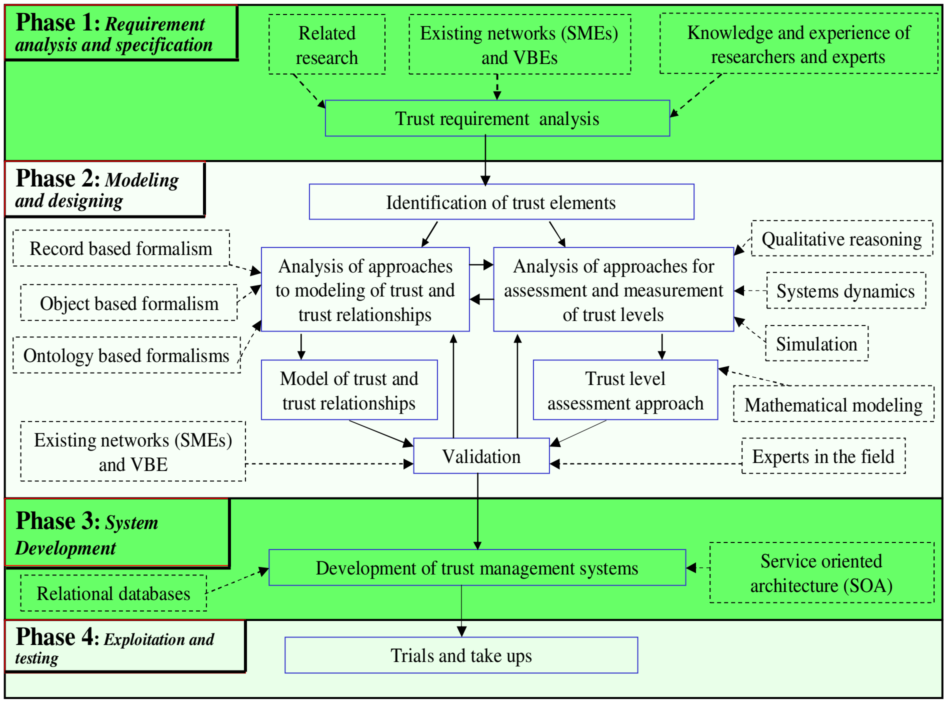
- *Common understanding of the aspects relating to rational trust,*
- *Assessment of organizations' level of trust,*
- *Creation of inter-organizational trust,*
- *Establishment of trust relationships between organizations".*

Achieved Research Objective 2 (RO2):
Providing a validated prototype implementation for a trust management system in VBEs in order to assist organizations in achieving various trust-related objectives.

In Chapter 7 we analyze how the research carried out in this thesis has achieved these two objectives. The scope of the research addressed in this thesis is at the level of organizations, and primarily applied to the VBE environment. Furthermore, rational trust among organizations is the focus of this thesis. However, when needed, also the subjective trust and inter-personal trust are briefly addressed, to enhance the presentation of the focused topics.

1.6 Research methodology

The methodology applied in our research is classified into four phases that are shown in Figure 1.3. Each phase produces results that are used as input concepts in the subsequent phases. Describing and defining these phases supports the understanding of their inter-relations.



Phase 1: Requirement analysis and specification
Related research
Existing networks (SMEs) and VBEs
Knowledge and experience of researchers and experts
Trust requirement analysis
Phase 2: Modeling and designing
Identification of trust elements
Record based formalism
Object based formalism
Ontology based formalisms
Analysis of approaches to modeling of trust and trust relationships
Analysis of approaches for assessment and measurement of trust levels
Qualitative reasoning
Systems dynamics
Simulation
Model of trust and trust relationships
Trust level assessment approach
Mathematical modeling
Existing networks (SMEs) and VBE
Validation
Experts in the field
Phase 3: System Development
Development of trust management systems
Relational databases
Service oriented architecture (SOA)
Phase 4: Exploitation and testing
Trials and take ups

Figure 1.3: The detailed methodology that was followed during our research period

The Solid-line boxes represent tasks that were performed in our research and whose output contributed to the results that are reported in this thesis. Dash-line boxes represent concepts, theories, knowledge of experts, or research results that were considered as potential input materials to our research.

Phase 1: included an analysis and specification of the requirements for the management of trust between organizations in a VBE.

Phase 2: focused on analyzing and defining approaches for modeling trust and trust relationships. It also focused on analyzing and defining approaches for assessing organizations' level of trust. These two analyses addressed requirements related to managing inter-organizational trust, as identified in phase 1.

Phase 3: addressed the development of a trust management system. The development of this system applied the requirements specified in phase 1 and the trust models and mechanisms for trust level assessment that were designed in phase 2.

Phase 4: addressed the testing phase of the developed approaches and the systems in the real environments, such as to support VBEs with managing trust between their member organizations. This phase also considered the potential future areas and domains for exploiting the results of this research.

1.7 The ECOLEAD project and related scientific publications

The work presented in this thesis was carried out partially within the ECOLEAD project. The research on inter-organizational trust was one of the many fundamental topics addressed by this project. In this section we provide a short overview of the research achievements related to the fundamental topics addressed in the project.

1.7.1 The ECOLEAD project

Reinforcing the effectiveness of collaborative networks and creating the necessary conditions for making them an endogenous reality in the worlds of business and industry - mostly based on SMEs - is a key factor for the globalization of an economy. Collaborative networks provide a basis for competitiveness, world-excellence, and agility in turbulent market conditions. They can support SMEs in the identification and exploitation of new business potential, boost innovation, and increase an SME's capabilities. The networking of SMEs with large-scale enterprises also contributes to the success of larger companies in the global market. This was the key motivation for the ECOLAED project.

ECOLEAD stands for European Collaborative networked Organizations LEADership initiative. This project aimed at creating the necessary strong foundations and mechanisms for establishing advanced collaborative and network-based industries. The fundamental assumption in the project was that a substantial impact in materializing networked collaborative business ecosystems requires a comprehensive holistic approach. Assuming that given the complexity of the area and multiple inter-dependencies among involved business entities, social actors, and technologic approaches, substantial breakthroughs cannot be achieved with incremental innovation from isolated areas. As such, ECOLEAD addressed three most fundamental and inter-related areas of focus – its vertical pillars - that are the basis for dynamic and sustainable networked organizations, including: (1) *Virtual Organization Breeding Environments, (2) Dynamic Virtual Organizations Management, and (3) Professional Virtual Communities.*

The work presented in this thesis was mostly achieved in ECOLEAD project, and specifically in relation to the *Virtual Organizations Breeding Environments*. The ECOLEAD project proposed a holistic approach, reinforced and sustained on two horizontal layers: *(1) Theoretical foundation for collaborative networks, and (2) Horizontal ICT infrastructure.*

These two layers are "horizontal" in the sense that they support and affect the three areas of focus as vertical pillars. The theoretical foundation provides the basis for technology-independent understanding of the area and its phenomena. Furthermore, the existence of an invisible, horizontal ICT infrastructure is a pre-condition for the establishment of truly dynamic collaborative networks. The conceptual, methodological and prototypical results of ECOLEAD significantly impact the industrial competitiveness and societal mechanisms by providing means to effectively exploit opportunities deriving from the deployment of VOs, and by designing and enabling new professional work paradigms capable of enacting knowledge-based societies. Figure 1.4 shows the logo of ECOLEAD indicating the inter-relations among its five areas of focus.

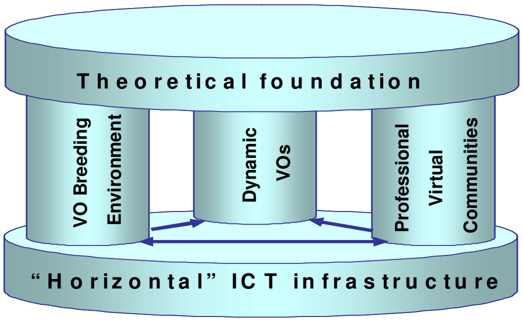

Theoretical foundation
VO Breeding Environment
Dynamic VOs
Professional Virtual Communities
"Horizontal" ICT infrastructure

Figure 1.4 : ECOLEAD logo showing main areas of focus

This figure shows the five main focus areas of the ECOLEAD project. This research falls within one of sub-areas, namely the VO breeding environment.

We briefly addressed the notion of the VBE (VO breeding environments) in Section 1.2. Below we briefly address these five main areas of focus of the ECOLEAD project.

a) Virtual organizations Breeding Environments and their management

This area of focus addresses support for establishment and management of VBEs, by performing comprehensive requirement analysis, and provision of methodologies, concepts, mechanisms and functionalities to support administration of VBEs. This is achieved through developing adequate VBE organization models, establishing operating principles, and providing ICT facilitating tools. Therefore, the area of focus mainly addresses the following three categories of challenges:

i) *The characterization and typology of VBE environments*: This topic addresses the characterization of a VBE's constituting elements, actors, and features; as well as defining a VBE's working and sharing principles. It also focuses on the definition and modeling of organizations' competencies, expertise, skills, and so on, and the development of methods to gather and organize such related information. Furthermore, this topic addresses the establishment of a common ontology in a VBE that supports the harmonization of a conceptual understanding between VBE actors. Finally, it addresses the identification of a common value system and the development of mechanisms to guide the creation of inter-organizational trust in a VBE.

ii)*The development of a VBE management system*: this topic addresses the specification, design and implementation of functionalities and services that are necessary to support the management of the VBEs. As further addressed in Chapter 6, a number of fundamental functionalities (subsystems) which constitute the VBE managements system were specified and developed. These functionalities mainly support the management of VBE structure and membership, organizations' competency aspects, inter-organizational trust, management of VBE's bag of assets, and decision support systems and so on.

iii) *Support for the creation of VOs within VBE environments*: this topic addresses how to find and characterize VO related opportunities in the market and society, and mechanisms for VO planning, intelligent matchmaking and launching. It also addresses the provision of a negotiation support framework that helps potential VO partners to smoothly reach consensus/agreement on discussions concerning the respective VO. Provision of services to support all steps and activities necessary to create and launch a VO are also further addressed in Chapter 6.

b) Dynamic VOs and their management

This area of focus addresses the methodologies, models, services and management tools that are needed to support the initiation, operation and dissolution of virtual organizations. A holistic approach to dynamic VO management is achieved in the ECOLEAD project and with the integration of concepts from other areas of focus.

The main challenges for VO managements are influenced by the following two aspects: the temporary nature of dynamic VOs and the distribution of processes in independent organizations that have to collaborate to achieve common goals, while their own interests are also being met. As illustrated in the ECOLEAD project, an effective VO that achieves its goals throughout its life cycle can seldom be configured without the need for a preparatory environment – a VBE. The most challenging aspects of managing dynamic VOs to be identified by ECOLEAD included:

i) The basis for VO management models, which was addressed through an investigation of the distributed business process modeling, decision-making methods, VO management support tools and VO categorization. The basic framework for dynamic VO management was achieved.

ii) A VO Performance Measurement system constituting a methodology supported by a software tool was achieved. This system takes into account multi-objective and VO-specific multi-perspective approaches. It also addresses the distributed business processes, pro-active management, analysis methods and decision support. The performance of organizations are measured during the operation phase of a VO and transferred to a VBE as inheritance during the VO dissolution phase.

iii) The governing principles of VO dissolution and inheritance management were also addressed to support the transition from operation phase to the dissolution phase. This also supports the transfer of inheritance from a VO to a VBE, which include dissolution management, joint knowledge management and the ownership, collection and management of outputs and results created by the VO concerned (IP ownership, liabilities and enforcement mechanisms).

c) Professional virtual communities

This area of focus addresses the methodologies, mechanisms, and approaches needed to jointly establish a robust framework for the deployment of Professional Virtual Communities (PVCs). It also addresses laying the foundation for new methodological and technological frontiers that provide collaborative approaches and knowledge sharing within the different scenarios of Virtual Communities.

In the ECOLEAD project, the PVC was defined as: *an association of individuals that are explicitly pursuing an economic objective identified by a specific knowledge scope,* with the aim of *generating value through members' interaction, sharing and collaboration,* which is *optimized by the synergic use of ICT mediation* [Crave, et al., 2006]. ECOLEAD dealt with the fundamental challenges in the establishment of PVCs by addressing the following aspects.

i) The identification and specification of the base requirements, and their related social or legal implications.

ii) The development of models that represent and support the understanding and deployment of the requirements for establishing and managing PVCs.

iii) The designing and implementation of ICT support facilities, and operating principles to help individuals join and remain part of PVC.

iv) The development of supporting tools required for proper functioning of communities and related supporting entities.

PVCs are analogous of VBEs, their main differences being their constituent members. While in VBEs the smallest entities considered to be member are the organizations, in PVCs individuals constitute the members. PVCs are communities in which virtual and remote coordination is the rule and geographical regrouping is practiced. Typically, such communities are established with certain business objectives in mind and for this reason PVCs are still believed to emerge in future business scenarios [Crave, et al., 2006]. However, various types of communities, such as practice communities and epistemic communities, demonstrate certain similar characteristics that may be considered in PVCs

PVCs are therefore long-term strategic alliances involving individual professionals who join their initiatives for the purpose of enhancing their preparedness for involvement in emerging and acquired business opportunities. Once a business opportunity is brokered, potential individuals are selected and invited to form a consortium. This form of short-term consortium involving individuals and configured for the purpose of addressing a specific business opportunity is called a *Virtual Team (VT).*

d) Horizontal ICT infrastructure

This area of focus addresses the establishment of a strong foundation for an ICT-independent infrastructure that supports the operation and interoperability of various tools and systems within the CNO environments. ICT infrastructure also provides functional, organizational and technical services that fundamentally impact each enterprise, global consistency, and interoperability. Owing to the heterogeneity of the Enterprise Applications and the dynamics of the business relations, the Enterprise Applications Integration in the form of the "federated model" has been the most suitable for traditional collaborations. However, CNOs need to study and incorporate more efficient approaches that address short time impacts and new technological standards. Furthermore, the following series of questions are usually raised when establishing a business model:

- Who is the provider of services?
- What are the technical and commercial requirements?

- What is the product?
- What are the benefits for respective stakeholders of this product? and;
- What is the market and what is the marketing plan?

Business models need to be addressed in order to identify the essential requirements for the approach - namely the essential modality of doing business and the essential cost/benefit plan - so that it may be accepted and that stakeholders are willing to pay for these services. The following aspects with respect to ICT-infrastructure were considered in order to address the technical and business model requirements:

i) The development of a reference architecture that covers different forms of collaboration (ad-hoc, mediated, pre-planned, etc.), the different stages of the collaboration life cycle (initiation, planning, operations, dissolution, etc.), and in order to be independent from the sector (industry, government, etc.), the application (supply chain, e-learning, etc.), the number of the organizations involved and the typology of the network (chain, ecosystem, etc.).In order to develop a comprehensive architecture in particular the following aspects were considered:

1. A framework for ICT technology-independent reference architecture for collaborative networks.
2. The foundation of interoperability principles derived from past R&D on VO.
3. Approaches for enterprise applications, integration and interoperability.
4. Semantic mediation over formats, protocols and models through multi-language differentiation mediation.
5. A base prototype infrastructure mapping the reference architecture to current / emerging technologies.

*ii)*The defining and devisal of business models for the developed ICT infrastructure. The deployment and maintenance of ICT infrastructures require different approaches than the traditional ones and must consider the emerging business characteristics and nature of CNOs. It addresses:

1. The elaboration of suitable business models and characterization of stakeholders in the “CNO infrastructure” business.
2. Cost-efficient deployment methods for business models.
3. Assessment models and methods for business achievements of the ICT infrastructure.

iii) A security framework based on an independent ICT infrastructure. Two aspects were addressed, which together contribute to the security framework:

1. Security by establishing trust between several partners that aim to collaborate in a certain business opportunity. What are the key criteria for assessing not only individual trust in a digital or virtual market, but also organizational trust? This aspect is addressed in this research as a technological aspect of trust.
2. Security by developing tools, technologies, digital signature, data encryption and private networks that can protect knowledge, intellectual property or the competitiveness of the VO, the PVC and each contributor.

e) Theoretical foundation for CNOs

This area of focus addresses the establishment of a sound theoretical foundation for collaborative networked organizations through the promotion and assessment of the adoption of formal and semi-formal modeling methods and tools, as a means to consolidate the fragmented existing and emerging knowledge in this area. The establishment of a theoretical foundation follows a similar approach to that of the *establishment of a new scientific discipline*. One of the first steps in this concept is to address the assessment and adoption of promising theories and formal modeling methods that have been developed in other disciplines. The following aspects were addressed to build a comprehensive theoretical foundation for CNOs:

i) The collection and assessment of contributions from other disciplines that can provide a starting basis for a rigorous theoretical foundation and formal modeling approaches for collaborative networks. The main modeling facets or purposes (e.g. structure, roles, behavior, processes) were identified and a set of modeling tools and base theories were proposed for each one.

ii) The elaboration and formulation of a reference model for collaborative networked organizations. The concept of "reference model" itself in relation to CNOs was well-established and the main business entities (breeding environment, virtual organization, and professional virtual community) were covered. This included:

1. The consolidation of CNO concepts and their abstraction in terms of a general reference model (semi-formal and easily understandable by humans)
2. The development of an engineering methodology for the purpose of applying the reference model

iii) The establishment of a reference framework for CNOs was another important task in this area of focus. A comprehensive reference framework is proposed that covers the concepts involved in all forms of CNOs [Camarinha-Matos & Afsarmanesh, 2006].

1.7.2 Scientific publications related to the dissertation

The bulk of the content of this thesis has already been published in different forms, including book chapters, journal articles, international conference papers (peer reviewed) and technical reports, e.g. ECOLEAD project deliverables. The table below is a summary of the author's publications, according to the different subjects addressed in the thesis. The numbers in the table above include both those papers that are published and those accepted for publications. A detailed description of author's publications is provided in Annex A.

Table 1.2: Summary of author's publications

Subject covered	**Journals**	**Book chapters**	**Confe-rences**	**Technical reports**	**Total**
Requirement analysis and specification on trust	1	1	2	2	**6**
Modeling and designing mechanisms and systems for trust level assessment	2	1	2	5	**10**
Developing and testing the trust management system	4	1	3	4	**12**
Total	**7**	**3**	**7**	**11**	**28**

Table 1.2, which will also be partially indicated later in every chapter, shows how aspects of this thesis (namely trust modeling, assessments, and management) have already appeared in a relatively large number of publications read by organizations that are involved in cooperation / collaboration.

1.8 Thesis structure

This thesis addresses the approaches, mechanisms and tools that are used to support the management of inter-organizational trust within VBEs. Its structure conforms to the inter-connections between the subsequent presented results. The results are inter-related in the sense that the concepts presented in each preceding chapter constitute a fundamental contribution to the understanding of successive chapters. The following structure has been adopted to facilitate the readability and understandability of the thesis.

- ***The results on requirement analysis and specification of trust are addressed in:***

Chapter 1: This chapter has introduced the problem area addressed in this thesis and has presented the domain in which the produced research results are applied. First, it has presented at high-level the research challenges addressed in the thesis and then briefly introduced the proposed solution for each challenge. Second, it has addressed the discipline of collaborative networks which is the domain in which our research results are applied. Third, the chapter has analyzed various background definitions of trust and presented the base concepts of trust. Fourth, it has presented three examples of cases of application in order to describe the research motivation and problem area addressed in this thesis. Fifth, it has presented the objectives, the motivating research questions, the scope and the applied methodology to this research. Finally, the chapter has introduced the project – ECOLEAD – in which this research was conducted.

Chapter 2: This chapter presents the general concept of trust and introduces the characterization of inter-organizational trustworthiness. Firstly, it surveys existing work on inter-personal trust and then compares this with inter-organizational trust. Secondly, it surveys related work on trust as addressed across different disciplines, such as sociology, psychology, computer science, and so forth. Finally, it introduces the characterization of inter-organizational trust in VBEs. This chapter presents also fundamental steps to guide the establishment of inter-organizational trust relationships in VBEs. The proposed steps consider the fundamental contributions of this thesis, namely the classification and characterization of trust elements as presented in Chapter 3, the assessment of organizations' level of trust, as presented in Chapter 5, and the services for supporting the management of inter-organizational trust, as presented in Chapter 6.

- ***The results on modeling and designing mechanisms and systems for the assessment of trust level are addressed in:***

Chapter 3: This chapter addresses the identification, analysis and characterization of trust elements for organizations. Firstly, it presents the proposed HICI approach and its three main concepts, which also constitute its three stages, namely hierarchical analysis (first stage), impact analysis (second stage), and causal influence analysis (third stage). Lastly, the chapter presents the trust elements that have been identified by applying the HICI approach and which empirically validated by industrial VBE networks.

Chapter 4: This chapter presents the conceptual modeling of trust elements for organizations. Firstly, it presents the related work on trust models that have been developed for different applications, for example e-commerce, inter-organizational network effectiveness, multi-agent systems, and so on. Secondly, it introduces trust parameters and trust elements that are used for modeling inter-organizational trust. Lastly, it addresses three conceptual modeling formalisms applied in this thesis, namely object-based, record-based and ontology-based formalisms.

Chapter 5: This chapter addresses the formulation of mechanisms for assessing organizations' level of trust. These mechanisms are formulated using mathematical equations that are derived from the results of an analysis of causal influences between different measurable trust parameters. The chapter presents a conceptual model that is used to formulate the formal mechanisms for assessing organizations' level of trust. Firstly, it surveys existing work on the assessments of actors' level of trust in specific environments, such as online communities, social networks, and so on. Secondly, it addresses the concepts relating to organizations' comparative levels of trust and in particular the presentation and interpretation of these levels of trust. Lastly - and with the aid of an example - the chapter presents the approach used to formulate mechanisms for assessing organizations' level of trust.

✦ ***The results on developing and testing systems are addressed in:***
Chapter 6: This chapter presents a Trust Management (TrustMan) system which has been designed and developed to provide services for the management of inter-organizational trust in VBEs. First, the chapter presents a VBE management system (VMS) and its related subsystems (the TrustMan system is one of the many subsystems of VMS); second the chapter addresses concepts applied to implement mechanisms for assessing organizations' level of trust; third, it presents specification of the TrustMan system; and fourthly, it addresses the architectural design of the TrustMan system. Lastly, the chapter presents the implementation of the TrustMan system and its adaptation by industrial VBEs networks.

✦ ***A summary of the results is addressed in:***
Chapter 7 This chapter summarizes the subsequent results of our research and in particular the innovative contributions. It discusses how the results have been accepted in both research and business communities and presents proposed future work in this area of research. Finally, it concludes the thesis.

1.9 Chapter discussion and conclusion

This chapter has introduced the research problems addressed in this thesis. In order to enhance the presentation of these research problems, the descriptions of the base trust concepts have been given. The concepts related to the application domain for this thesis – the VBE – are also addressed. Based on the research problems, a number of research questions are stated, which in turn guide the formulation of the research objectives. Lastly, the structure of this thesis is also presented in this chapter, which details the inter-relations and flow of concepts presented in this thesis.

The emergence of collaborative networks as a scientific discipline marks another step in scientific and engineering developments. This thesis addresses a fundamental topic in this discipline by introducing a new approach that can be used to analyze "inter-organizational trust". The research challenges introduced in this chapter are systematically addressed in this thesis (as described in Section 1.8) in order to give a clear presentation of the innovative contributions that support this research.

Therefore, this chapter has presented the base concepts of inter-organizational trust that are necessary for further understanding of the research results presented in the remaining parts of the thesis. It has also presented the main research challenges and research questions that one by one are addressed in the next chapters.

Chapter 2

Aspects and characterization of trust

Traditionally, the concept of trust has been addressed at the individuals' level. It is also mostly assumed to be a phenomenon that naturally emerges rather than being created. At individuals' level, most research and practice have considered trust as a subjective aspect. However, today the concept of trust has become an amenable factor for smoothening inter-organizational collaboration and thus has raised the need to address trust from a new angle. Traditional approaches and mechanisms for both assessing the level of trust in individuals and applying such results for creation of trust are inadequate for analyzing inter-organizational trust. While comparing with inter-personal trust this chapter surveys existing work on inter-organizational trust addressing the complementary and contradictory concepts, as well as different practices in various disciplines. The chapter then presents a characterization of trust and trust relationships as addressed in VBEs and identifies three main challenges related to trust studies.

This chapter has been published, for the most part, as a book chapter in: Methods and Tools for Collaborative Networked Organizations [Msanjila & Afsarmanesh 2008b].

2.1 Introduction

Trust has been widely studied, most importantly as a component of relationships among individuals and organizations. In Section 2.2, we present a survey of existing and reported research work on trust among such individuals and organizations. The survey first discusses differences between aspects of inter-personal and inter-organizational trust and subsequently discusses in detail the concepts related to trust among individuals. In Section 2.3, we introduce the characterization of inter-organizational trust in VBEs. In that section, we present concepts which either complement (such as security, reputation, etc.) or contradict (e.g. risks, privacy, etc.) aspects of inter-organizational trust. In that section, we also introduce fundamental aspects of organizational trustworthiness, namely those of a technological, structural, economical, social, and managerial nature. In Section 2.4, we present fundamental aspects necessary to guide organizations for deciding on the type of trust-related data, which are needed in the VBE and shall be sufficient to enable them trust other organizations. In that section, we also address different kinds of evidence of validity for trust related data of organizations. In Section 2.5, we briefly introduce fundamental steps proposed to guide establishmet of inter-organizational trust relationships in VBEs.

2.2 Traditional practices on trust

As a subject, trust has gained increased attention and has been examined in both research and practice. The challenges related to inter-personal trust date far back and correspond with the beginnings of human life. This section first examines the differences between inter-personal and inter-organizational trust, and then focuses on inter-personal trust.

2.2.1 Inter-personal versus inter-organizational trust

Many researchers have indicated that trust is an important issue in smoothening inter-personal and inter-organizational relationships. However, research work conducted to address inter-organizational trust has focused on theoretical evaluations [Currall & Judge, 1995]. Nevertheless, in the current information society some studies have addressed trust from a practical standpoint and have produced fundamental empirical evidence on the creation of trust among actors [Smith & Barclay, 1997]. Even so, until today there is still no actual agreement on the exact nature and definition of the trust with respect to its conceptualization, perception, preference and measurement (Section 1.3). To address trust in research satisfactorily, understand the effects of trust in different types of partnerships, and enable acceptable results for all stakeholders, it requires the involvement of communities and other institutions from heterogeneous domains [Smith & Barclay, 1997].

A fundamental difference between inter-personal trust and inter-organizational trust relate to their antecedents [Msanjila & Afsarmanesh, 2007d]. Inter-personal trust is defined at the level of the individual and it represents the extent to which a person places trust in another person. It has been observed that although inter-organizational trust and inter-personal trust differ in a number of aspects, they share the aspects of time in relation to the ***temporary and dynamic nature of trust*** [Ratnasingam, 2003]. For example, ***time*** can influence the decision on the trust related data, considering aspects such as validity, sources and mechanisms applied for its collection, which are needed to create trust among actors. Thus, time is a key aspect to consider when analyzing and modeling trust relationships among organizations as addressed in Section 4.3.1. Table 2.1 presents a summary of comparisons of complexity of trust among individuals and organizations.

Table 2.1: Complexities of trust among individuals and among organizations.

Trust among individuals	**Trust among organizations in VBEs**
The creation of trust is traditional and proven	The creation of trust is emerging and unproven
Mechanisms for assessing the level of trust are known and informal	There is lack of mechanisms for assessing the level of trust and formal ones are needed
The assessment applies opinions of others	The assessment is based on rational data
The trust related data and their sources are known and are proven	The trust related data and their sources are difficult to define and need verification
Does not necessarily need tools for supporting related processes	Needs tools due to the urgency for processing a large amount of data
Trust criteria are mostly known and static	Trust criteria are not known and are dynamic
Less interferences in establishing trust relationship	Other stakeholders must be involved while establishing trust relationships

A basic or essential level of trust is required for smoothening inter-organizational cooperation. An established climate of trust that is internalized in organizational behavior and supported by mutual belief is necessary for collaborative efforts between partner organizations [Cosimano, 2004]. Optimal gains from a network can be achieved through collaboration that is facilitated by inter-organizational trust, such as reduced costs, greater achievement speed, and an improved ability to handle complexity of different activities. Furthermore, trust influences an organization's long-term strategic plans, collaborative market performance and loyalty. Trust also broadly influences organizational relationships, commitment, cooperation, functional conflict, uncertainty, the propensity to leave, and acquiescence [Msanjila & Afsarmanesh, 2008a].

The difficulty in the conceptualization of trust among organizations is extending a phenomenon that is inherently at an individual level, to an organizational level. These difficulties can produce confusion in relation to the creation of inter-organizational trust.

2.2.2 Trust among individuals

The theory on origins of inter-personal trust [Cosimano, 2004; Lahno, 2001] has mainly proceeded along three main fronts: (1) explaining differences among the individual propensity to trust, (2) understanding diverse dimensions of trustworthy behavior, and (3) suggesting different levels of trust development.

- *Individual propensity to trust:* Trust among individuals is regarded as a generalized expectancy that assumes people may be relied on. This expectancy is a function of the degree to which trust has been honored by that individual's history of past social interactions. Recent work has suggested that both the characteristics of the trustees involved in trust relationships and their level of trust vary with time [Msanjila & Afsarmanesh, 2008a]. As further addressed in Section 5.4, the computed trust level of an organization is a relative value depending on the applied set of trust criteria, other involved organizations, and interpretation of trustworthiness scores by the trustor organization, as addressed below.
    - *Applied set of trust criteria* depends on the preference and perception of the trustor organization on trust, depending on the objective for establishing inter-organizational trust relationships. Trust objective might vary with time which means the preference and perception of trustor organizations on trust might also vary with time.
    - *Number of involved organizations* depends on the objective of the collaboration that indicates the needed collective competencies and resources owned by selected organizations. The availability of these competencies and resources might vary with time. Furthermore, if the involved organizations change then the optimal values of trust criteria that are used to compute the comparative values might also change (see Section 5.4.1). This in turn might cause changes in the levels of trust in organizations.
    - *Interpretation of trustworthiness* score depends on a number of issues such as the trust objective, risks associated with the collaboration, previous experience of the trustor, etc. which also vary with time.
    - *Applied trust related data* is based on the performance of an organization both within the VBE in collaboration with other organizations and from individual organization's projects. As organizations continue participating in different activities their performance data is collected and thus their trust related data is updated which means it changes with time. This implies that their trust level will also be continuously evolving with time.
- *Dimensions of trustworthy behavior:* Trust among individuals can be grounded into the evaluation of three main specific characteristics, namely their ability, integrity and benevolence [Cosimano, 2004]. Furthermore, the more a trustor observes and/or identifies

these three characteristics in a trustee, the more likely the trustor’s level of trust in that trustee will grow [Msanjila & Afsarmanesh, 2007a], as addressed below.

- o *Ability* typically refers to the trustee’s knowledge, skill, or competency. This dimension recognizes that establishing trust relationships depends on the trustee being capable of performing properly and meeting the expectations of the trustor.
- o *Integrity* refers to the degree to which the trustee adheres to principles that are acceptable to the trustor. This dimension leads to trust, based on the consistency of past actions, communication credibility, commitment to standards of fairness, and the congruence of the trustee’s word and deed.
- o *Benevolence* refers to the trustor’s assessment of how concerned the trustee is about the trustor’s welfare, in order to either advance the trustor’s interests, or at least not to impede them. Here, the trustee’s intentions and motives are the most central issues. For example, honesty and open communication, the delegation of decisions, the sharing of control, and so on, all act as an indication of a person’s benevolence.

- *Different stages of trust development:* Early theories on trust have described it as a uni-dimensional phenomenon that simply increases (or decreases) the magnitude and strength of a relationship [Ishaya & Mundy, 2004]. Recent approaches suggest that trust builds in continuous and sequential stages. Therefore, trust may grow with time to 'higher' levels (or diminish to lower levels); moreover, it can become stronger and more resilient. When defined by *calculus-based trust (CBT) and identification-based trust (IBT)* trust can be dynamic [Ishaya & Mundy, 2004], as is discussed below.

During the early stages of a relationship between two individuals, the level of trust is mainly *calculus-based*. In other words, the trustor (with the help of trust experts) can carefully calculate the trustee’s likely level of trust in a given situation. This also depends on the environment’s rewards for being trustworthy and deterrents against untrustworthy behavior, as these encourage more trustworthy behavior. Over time, *calculus-based trust (CBT)* can grow as individuals are able to improve their reputation and assure the stability of their behavior by behaving consistently, e.g. meeting deadlines, fulfilling promises, and so forth. CBT is largely a cognitively-driven trust approach, grounded in judgments about the trustee’s predictability and reliability [Castelfranchi & Falcone, 2000]. However, once actors come to a deeper recognition of each other through repeated interactions, they become more aware of each others’ shared values and goals. This allows their trust relationship to grow and reach a higher and more qualitative level.

When trust between the trustor and trustee evolves to its highest level, the function is called the *identification-based trust (IBT)* [Settle, 1998]. At this stage trust has grown to the point that the actors have internalized each other's desires and intentions. They understand what the other actor really cares about and, therefore, each actor is in fact able to act as an agent for the other. Trust at this advanced stage is also enhanced by a strong emotional bond between the actors, based on the sense of shared goals and values. So in contrast to the CBT, the IBT is more emotionally -driven, grounded in perceptions of inter-personal care and concern, and a mutual need [Lahno, 2001].

2.2.3 Trust in different disciplines

Trust is a key concept addressed by research in many disciplines and it is gaining importance in the emerging information society. In this sub-section we present the reported research on perceptions of trust in five different disciplines, namely sociology, economics, psychology, politics and computer science.

In sociology, trust is defined through reputation and previous interactions among individuals. Furthermore, the ways and reasons by which reputation for trustworthiness is established or destroyed are being studied in social trust relationships. Not only will the perceivers of reputation have access to information which the reputation holder does not control, but also the manner in which both types of information are interpreted is not straightforward [Good, 1988]. Therefore, individuals wish to have complete information about the people with whom they deal before dealing with them [Dasgupta, 1988].

In economics, decisions about trust are similar to decisions about taking risky choices. Individuals are assumed to be motivated to establish trust relationship with each other in order to either maximize the expected gains, or minimize the expected losses from their transactions [Josang & Lo Presti, 2004]. The critical factor with respect to trust in economic studies is the risk management related to trust relationships. Trust in psychology is related to beliefs. A trusting behaviour occurs when an individual believes that there is an ambiguous path; the result of which could be good or bad [Morgan & Hunt, 1994]. The occurrence of the good or bad result is contingent on the actions of another person. If the individual chooses to go down that path, he makes a trusting choice.

In politics and digital governments, trust is related to truth telling. It is important for digital government, to maintain high standards of truth telling and to avoid being associated with poor reputation and thus loosing the trust of the public [Sztompka, 1999]. Trust in governments and politics is essential in order for the governments and the related political parties to remain in power. However, several other factors are also identified as influential on the level of trust governments have towards their citizens, such as reputation, performance, accountability, commitment, and so on [Sztompka, 1999].

In computer science, trust has been mainly associated with security, privacy and reputation. Establishing trust among interacting systems that are developed based on the service oriented architecture depends on their compliance to the set of communication policies. These policies provide regulations that must be met by a system to be trusted [Blaze, et al., 2009]. Generally, when an environment is secure, it is easier to establish trust relationships among the systems' users, and equally if a user respects the privacy of others in relation to their personal data and sensible information he can be regarded as trustworthy [Seigneur & Jensen, 2004]. Reputation is being used for managing trust in systems that are developed using multi-agent technology; therefore, in multi-agent systems the trustworthiness of a trustee represented by an agent "*b*" is assessed by a trustor represented by an agent "*a*", using the reputations witnessed by the trustor (or trustor's friends) or certified by the trustee's friends [Huynh, et al., 2004].

None of the existing studies have adequately addressed *trust among organizations*, particularly within collaborative environments such as VBEs [Msanjila & Afsarmanesh, 2006b]. Among other reasons, this inadequacy is due to the fact that the collaborative networked organization (CNO) is itself a newly emerging scientific discipline [Camarinha-Matos & Afsarmanesh, 2005], and thus demands innovative approaches and mechanisms to support its necessary establishment and operation. Also, the collaboration for which the establishment of trust is required is not at the level of individuals since it is dealt with traditionally, but at the level of which the involved participants are only organizations, as is further discussed in Section 2.3.

VBE members may constitute organizations that operate in different domains or disciplines. The member organizations might differently perceive trust, e.g. according to their trust objectives their perceptions might be influenced by a number of aspects related to what is believed to be important for their businesses and future goals. We address inter-organizational trust in VBEs considering a wide variety of the above aspects, taking into account how those aspects are characterized in various disciplines as some of which are briefly addressed in this section. Large volume of aspects from different disciplines is analyzed later in this thesis and classified into five "points of view" that are referred to as trust perspectives, further addressed in Section 2.3.6 and in Chapter 3. For instance, the elements of trust addressed above from the politics and digital governments discipline constitute a part of the managerial perspective of our proposed model, while the psychology and sociology aspects are related to social and managerial perspectives, and the computer science aspects are related to technological perspective, etc.

2.3 Trust among organizations in VBEs

The emerging preparatory co-working environment (or 'VBE'), as described in Chapter 1, is characterized by some features that have never been practiced before. In this section we address these emerging practices and the research results that have been achieved on trust among organizations involved in VBEs.

2.3.1 Importance of creating trust between organizations in VBEs

VBEs are characterized as multi-actor environments, in which each actor organization is autonomous, and has interests and goals that might contradict those of others. A catalyser for the enhancement of cooperation between member organizations in VBEs is the establishment of trust relationships, which is why past research states that trust is the most salient factor for cooperation networks in achieving the network objectives [Morgan & Hunt, 1994]. Trust relationships between organizations are more important for large VBEs where direct personal contact are more difficult to achieve by all, while they shall operate under pressure from the global economy, the increasing value of information, and the mounting uncertainties surrounding their businesses [Msanjila & Afsarmanesh, 2007a]. Several advantages can be gained once trust relationships between member organizations have been properly established and managed in the VBE. Following are some example advantages gained by establishing trust relationships between organizations in VBEs:

- Facilitating the achievement of common goals through information exchange, knowledge sharing, tools sharing, and so forth, between member organizations.
- Enabling the member organizations to cope with uncertain or incomplete information.
- Easing the process of creating and launching VOs and smoothing the partner selection processes.
- Accelerating the contract negotiation process between selected VO partners.
- Encouraging the member organizations to avoid opportunistic behaviour during collaboration.
- Achieving the competitive advantage, through reduction of governance internalization (acquisitions) tasks, and thus the transaction costs, as addressed in Sections 1.2.2, 1.2.3, and 3.3.2.
- Enabling open communication and thus reducing conflicts between member organizations.

2.3.2 Antecedents of trust between organizations in VBEs

Trust antecedents are cardinal elements that may have a positive or negative impact on the effectiveness of the established trust relationships among organizations. Three trust antecedents are identified for organizations in this thesis, namely the *shared values, the previous interactions,* and *the practiced behaviors*. Strengthening of these antecedents shall be aimed by all VBE member organizations as well as the VBE administration.

Shared values: Shared system of values occur when the trustor organization and the trustee organization have a common understanding on important issues that might influence the creation of trust towards each other, such as their missions, goals, policies and interpretations of right or wrong [Morgan & Hunt, 1994]. Shared values can range from business objectives to internal management processes and approaches. In business environments, it is more difficult to have shared values between two competing organizations than between two organizations that are complementing each other [Clay & Strauss, 2000]. Typically, when two organizations have a common understanding/perception and/or belief in a set of values they both feel secure in the knowledge that there will be no unexpected results during their cooperation/collaboration. It is therefore easier to establish a trust relationship under such conditions. As an aspect of preparedness, the VBE must ensure that member organizations establish shared values with other organizations within the VBE. In a VBE shared values among member organizations can be achieved through the following approaches among others:

- Establishing and maintaining a definition of common VBE value system
- Enhancing and maintaining transparency by the VBE administration
- Performing joint activities among member organizations within the VBE
- Establishing a common or interoperable ICT-I for all organizations in the VBE.

When member organizations achieve some level of shared values with each other then the process of establishing trust relationship between them can be easier accomplished [Msanjila & Afsarmanesh, 2007d].

Previous (fruitful) interactions: Previous (fruitful) interactions between the trustor organization and the trustee organization - either directly or indirectly (through other intermediate organizations) – may enhance the effectiveness of established trust relationships. These time-related interactions can be formal such as the formal exchange of information, knowledge or expertise. Interactions can also involve individuals who work within the two organizations either technical or social. Even though sometimes there may be no current business-oriented interactions, yet the existence of previous informal interactions may smoothen the establishment of trust relationship among organizations.

Member organizations of the VBE have the possibility and are encouraged to interact with each other. Interactions can be achieved through different approaches, among others:

- Inviting representatives of other VBE member organizations to attend organizational general meetings as observers
- Organizing workshop and inviting presenters from other VBE member organizations
- Supporting the sharing of information on public issues of the VBE member organizations through the portal which is maintained by the VBE management system (VMS).

Practiced ethical and/or moral behaviours: Practiced ethical and/or moral behaviours basically refer to the opposite of *opportunistic behaviour*. Opportunistic behaviour means taking immediate advantage - unethically - of any circumstance that may generate possible benefit. Traditionally, opportunistic behaviour in competitive markets seemed natural because the typical focus of organizations in such environments was on the acquisition of customers, without regard for long-term relationships with other organizations. In collaborative networks however, organizations must rather cooperate in order to best serve the same customers.

Opportunistic behaviour has therefore a negative impact on the effectiveness of trust relationships among organizations. It mainly derives from transaction cost literature and is defined as *seeking self-interest with guile* [Mukherjee, 2003]. Here we refer to opportunistic behaviour as an *ungentle action that might be taken by VBE member organizations for the purpose of benefiting themselves* ***unethically****, more than others (e.g. quitting the collaboration once they have made a large gain, or when they expect the risks of the collaboration to become a threat).*

2.3.3 Main related challenges in trust studies for VBEs

In relation to the analysis of trust in VBEs, we have identified three main challenges that must be well-addressed in order for trust to be realized and met by VBE member organizations, VBE administration and external stakeholders. These are as follows:

Main related challenge 1- Causality: a major challenge for the analysis of trust is its causality. The future trustworthiness of an organization is "causally" related to its role and behavior at present, and actions it has performed as well as events it has caused in the past. Therefore, a part of trust engineering in VBEs is intended to support decision-making about the present and future trustworthiness of organizations, while the information needed for this estimation can mostly be derived from the past.

Main related challenge 2- Transparency and fairness: one more challenge for the assessment of the level of trust in organizations is the transparency and fairness for all stakeholders. Each step taken for entire process of assessing the level of trust must be clear and transparent for all involved organizations. For fairness, the steps taken and approaches used for an assessment of the level of trust must be accompanied with some formal reasoning, and also the information used for the assessment must be accredited and/or certified to avoid personal (subjective) judgment and biases.

Main related challenge 3- Complexity: another challenge for trust analysis in VBEs is the way in which the complexity of the multi-objective, multi-perspective, and multi-criteria nature of inter-organizational trust is handled. As discussed in this thesis, trust is not a single concept that can be applied to all cases of trust-based decision making. Measurements of level of trust are subject to both the purpose of the trust relationships, and the specific actors involved. Every case is different and requires the employment of specific trust criteria in order to assess the level of trust.

2.3.4 Boundary characteristics of rational and subjective trust

Subjective trust is the most adopted and practiced form of trust for smoothening interactions among individuals. However, nowadays collaboration among organizations has become a fundamental approach for co-working in business, such as joining initiatives and efforts for the purpose of enhancing competitive power in the market. Applying subjective trust concept is difficult here as it lacks a reasoning approach and/or mechanism for results of the assessment of level of trust in organizations [Msanjila & Afsarmanesh, 2007a]. As a result, rational trust analysis is currently gaining in popularity [Castelfranchi & Falcone, 2000].

Subjective trust is created on the basis of qualitative data and is opinion-based. Some fundamental sources of information for creating subjective trust among parties include experience and knowledge of trustors on trustees, recommendations of third parties on trustees, previous interactions, trustees' reputations, and so forth.

Rational trust (objective trust) is created on the basis of quantitative data and is fact-based. The main source of trust related data is the organizational performance which is accumulated in the past from different activities in which it participated, both in collaboration with other partners, and as an individual organization. Rational approaches for assessing the level of trust in organizations employ formal mechanisms, such as mathematical equations, which in turn provide some formal reasoning of the resulting level of trust [Msanjila & Afsarmanesh, 2007a].

Subjective trust and rational trust also differ with respect to the "*boundaries*" that are applied. The real challenge here relates to a definition of where these boundaries start and end for daily interactions among actors, for both subjective trust and rational trust.

Boundaries for subjective trust: Boundaries for subjective trust can be discussed in relation to the transitive and propagatory nature of trust among involved actors. Subjectively, trust transitivity means, for example, that if "Alice" trusts "Bob" and "Bob" trusts "Eric", then "Alice" trusts "Eric". This assumes that Bob actually tells Alice that he trusts Eric, which is called a *recommendation*. In social and individual interactions, in which subjective trust is mostly practiced, trust can be assumed to be transitive. This is because trust among individuals participating in these interactions is mostly created on the basis of other people's opinions. The opinions of these people, who trust a specific individual, are used to create trust with a new trustor. Thus, subjective trust is transitive.

It is common to collect advices from several sources in order to be better informed when making decisions. In other words, it is also common to collect several recommendations in order to convince a trustor, such as for job application, of the trustworthiness of a trustee. When the trustor has different sources of recommendations from which he or she can create trust for the certain trustee, a specific characteristic of trust transitivity emerges, namely *parallelism*.

Since subjective trust is transitive, the most complex issue concerns the point at which the propagation starts to diminish and lastly stops. This point defines the trust boundary, yet it is not clear which factors may indicate it. As such, even the trust boundary itself from one trustor to another is subjective.

Boundaries for rational trust: It can be shown that trust is not transitive for "objective-specific" collaborations and transactions, for which the rational trust is mostly needed to be practiced. For example, the fact that Alice trusts Bob to look after her child, and that Bob trusts Eric to fix his car, does not imply that Alice trusts Eric to look after her child, or to fix her television. This is because "trust objectives" in these two cases differ. Rational trust is created on the basis of facts and the application of formal mechanisms, in which different cases will have different preferences. As such, the value of the level of trust in this case is not absolute and cannot be transferred to different cases, which is why rational trust is more suitable than subjective trust for smoothening organizations' specific objective collaborations. Therefore, rational trust is not transitive.

Rationally, a trust boundary does not exist, since trust is created on the basis of preferred perspectives. Different trustors may prefer different perspectives in order to trust the same trustee. In other words if the same set of trust criteria is preferred for all trustors, the same level of trust shall be achieved, regardless of the trustor. Therefore, rational trust does not propagate among involved actors and thus all trustors shall trust their respective trustees on the basis of their own preferred perspective.

2.3.5 Main concepts related to inter-organizational trust

Trust is related to different concepts and these relations either complement (such as trust and security, reputation, co-working) or contradict (such as trust versus risks, privacy, and so on.) its perceptions among actors. This section discusses trust in relation to five concepts, namely: (a) trust versus risks, (b) trust and security, (c) trust versus privacy, (d) trust and reputation, and (e) trust and organizational virtual co-working.

a) Trust versus risks

Risk is a concept that denotes a potential negative impact to an asset or some characteristics of a value that may arise from present processes or future events. In everyday usage, "risk" is often used synonymously with the probability of a known loss. Many definitions of risk depend on a specific application and situational contexts. Frequently, risk is considered as an indicator of threat. It can be assessed qualitatively or quantitatively. Qualitatively, risk is considered proportional to the expected losses which can be caused by an event and to the probability of the same event. The harsher the loss and the more likely the event, the greater the overall risk. Measuring risk is often difficult; the probability is assessed by the frequency of past similar events, which in fact is difficult to link to the future. Trust and risk are negatively related. When there is a high chance that certain risks may arise in a certain environment it is very difficult for an organization to trust other organizations in that specific environment. Moreover, when organizations trust each other they tend to relax and rely on one another based on the assumption that risks may not arise. However, this attitude may in time increase the chance of risks arising due to new changes inside each organization.

Different types of risks may arise while organizations are collaborating in order to achieve their common goals. Below are six example types of risks related to organizations that shall be considered when aiming to reduce the severity of their impact on inter-organizational trust relationships in the VBE.

- ***Strategic risks:*** Several different strategic risks may be associated with operating in various types of business or industry domains. These include risks arising from acquiring business opportunities, changing customers, changes in customers' demands, changes in operating environments, and emerging innovative results from research and development. Organizational strategies must be flexible enough to accommodate such changes. Rigid strategies can result in risks, such as the failure of an organization to properly integrate and collaborate with other organizations in VOs as a result of unacceptable or outdated strategies.
- ***Operational risks:*** Operational risks may exist as a result of direct or indirect loss that has been caused by for example inadequate or failed internal processes, employees' behaviour that might compromise security of information management system, etc. An organization's failure to achieve the agreed results due to internal problems endangers the success of the entire consortium to achieve its common goals. Therefore, operational risks that may arise for both the organizations and the consortium must be properly addressed.
- ***Legal and cross-border risks:*** These are risks that may exist due to changes of rules, regulations and laws imposed by governments or local authorities. Usually business organizations have limited influence on the make-up of regulations and rules, for instance, only through lobbing but not direct involvement in the process. The organizations involved in a VBE might in addition be subjected to different regulations, e.g. for different sectors or in different countries. Changes in regulations in a country where one

of the member organizations is located might for example create risks for their cooperation with other organizations located in different countries. This is especially an issue when laws and regulations in the two countries contradict.

♦ ***Financial risks:*** VBEs have to deal with financial risks to sustain the collaboration among member organisations. There are various types of financial risks, among others, they include: credit, liquidity, transactions, interest rate and currency exchange rates.

♦ ***Reputation risks:*** Reputation risks are related to an organization's image and instability as a result of negative opinions, either from other member organizations in the VBE, or from the public. Poor reputation affects an organization's ability to establish new trust relationships with other organizations, or to continue with existing trust relationships. Reputation risk exposure must be properly dealt within an organization and may require exercising caution in dealing with customers and the community.

♦ ***Technology related risks:*** Current risks surrounding ICTs, such as network failures, lack of qualified human resources and insufficient skills, lack of network security, hacking, viruses, etc., have the potential of a greater negative impact on an organization than ever before, since collaboration and cooperation are both facilitated by computer networks. Additional risks posed by technologies might include lack of privacy, unauthorized information access, increased complexity of applied technologies and so on.

In traditional business investments, greater risks are associated with higher expected returns. In organizations, tradeoffs in relation to risks are about the returns on investment that will be obtained once a specific risk has been accepted and the outcome of taking this risk has been favorable. However, cooperation between organizations in the VBE may not provide an immediate return. The economical benefits of cooperation between member organizations include an increase in their chances of acquiring better and more opportunities as well as involvement in VOs responding to opportunities brokered with other organizations.

In practice, trust and risks are inversely related - when one increases there is a high chance that the other will decrease. Therefore, if risks existing in a certain VBE environment increase then organizations operating in this environment will feel at risk and will hardly establish trust in other organizations. Similarly, if organizations trust each other to a great degree then they will feel that risks are unlikely to arise during the course of collaboration (e.g. minimal possibility of occurring an opportunity behavior) and thus do not pay attention to the need for preparing themselves against risks.

Considering the style of virtual co-working in VBEs, organizations may interact with others without ever meeting face-to-face, thus enhancing fears about some potential risks, such as those discussed above. One strategy that organizations can assume as a means to avoid risks associated with collaboration is being reluctant in engaging in such trust relationships with other organizations. However, such a strategy can cause problems with respect to sharing resources, knowledge, competency, and information which are necessary for facilitating collaborations in VBEs. Cooperation in the VBE and collaboration in VOs are the only potential styles of co-working that have demonstrated to be suitable for member organizations in these environments. Establishing trust relationships between participating organizations has proven to be an amenable facilitator that eases cooperation between organizations in the VBE as well as their collaboration in configured VOs. However, a challenging issue for VBE administrators is how to convince organizations to establish and commit to their established trust relationships despite the existing risks. In the VBE, member organizations are encouraged to trust others in order to smoothen their collaboration through the following strategies:

- Enhancing the sense of togetherness and safe feelings among organizations in the VBE by promoting the culture of sharing day to day information, useful knowledge, etc., through the common storage and retrieve portal called "*bag of assets*" [Afsarmanesh, et al., 2008].
- Defining and applying a comprehensive set of "*working and sharing*" principles that can also provides guidelines on how to share any kind of loss caused by collaborative business among organizations due to emerged risks during the collaboration [Romaro, et al., 2008].
- Defining and encouraging use of proper *value systems* in the VBE that will also provide a set of performance indicators for measuring performance of organizations, which in turn provide data to be used as input to the computation of the trust level of organizations.
- Define *rewarding strategies and build reward mechanisms* to encourage good behavior and high achievements for organizations in collaborative activities.

b) **Trust and security**

Inter-play between trust and security can be examined from different aspects. The two most popular aspects that are also discussed here are: in respect to management systems and in respect to technologies owned by and available to organizations.

✦ ***Trust and security for management systems***

Until a few years ago, enhancing the security of systems that are used for the management of information, resources, stored knowledge, available skills, and so forth, was the fundamental approach used to enhance trust among collaborating organizations. Since this time and even currently, the situation has changed dramatically. New security regulations, significant security, privacy incidents, and so on, are no longer enough to guarantee smooth operations for business organizations on markets that currently present continuously increasing turbulent conditions [Grandson & Sloman, 2000]. Consequently, it is now fundamental that the search for solutions and a balance between trust and security in relation to the ICT systems and the facilitated businesses now involves both business organizations and ICT industries.

From a business perspective, security mainly concerns the management of risks and, in this case, with respect to ICT-facilitating tools. Current markets are characterized by turbulent conditions, including scarce resources, lack of knowledge and skills, volatile business opportunities, changing and emerging unique customer requirements. Therefore, enhancing the security of the ICT systems and managing the related risks do not fully guarantee the success and survival of an organization in the current market.

An ICT system can provide the right level of security whether or not it keeps the risks for business at an acceptable level. Potential losses due to malicious acts by disgruntled employees, hackers, unauthorized users, and so on, are central to each risk. Whether a risk is acceptable or not is a business decision and is not only influenced by the state of the ICT system, but also by many more different factors relating to the system, such as the behavior of other partners, changes in business requirements, and so on [Msanjila & Afsarmanesh, 2007c]. The description of a security level and the demonstration that an ICT system meets this level are fundamental challenges in computer science, and specifically in relation to the newly emerging needs of management to build inter-organizational trust. It is more challenging in the current climate as organizations have to collaborate together in order to acquire and respond to opportunities. This collaboration needs geographically distributed support from ICT systems. The level of security that is enough to support the creation of inter-organizational trust in such an environment is still unclear and it is difficult to define.

The security of an ICT system alone is not sufficient for smoothing cooperation and collaboration among organizations, and thus guaranteeing the necessary success and survival. As a result, security boundaries among organizations are fast becoming increasingly less stringent. Therefore, trust propagation that is based on the security of an ICT system is decreasing and becoming rationally specific. Applications that used to run on dedicated servers now are running on virtual environments, sharing infrastructure with others, and using widely-distributed physical resources [Rabelo, et al., 2006]. This makes the process of creating inter-organizational trust with the application of system security even more difficult.

As a result of amplification of problems related to the security of ICT systems, risks associated with businesses supported with ICT systems, market turbulences, and so forth, certain other approaches for smoothing co-working environments - such as VBEs - are needed and must be considered. Managing trust among organizations, by applying rational mechanisms for assessing level of trust and creating trust, has emerged as a promising approach for achievement of the required smoothening [Msanjila & Afsarmanesh, 2007a]. In our approach, systems (Trust Management systems) are suggested as a means to support organizations in the performance of tasks related to creating trust of their organization in others. A number of processes also need to be supported with tools in order to provide the required services for the management of trust among organizations, as discussed in Chapter 6.

c) **Trust and security in relation to owned and experienced technologies**

There has been a misconception about trust and security, and roles that technology plays in this binomial for setting/facilitating collaboration. Most people tend to believe that trust is merely the result of security - when security exists, actors can trust each other - but researchers have observed that this notion does not represent the entire picture [Rousseau, et al., 1998]. Trust is a wider concept and its link with security is not linear [Msanjila & Afsarmanesh, 2007c]. Technology can effectively provide security; for example, every step of an online transaction has one or more procedures for transmitting users' data safely, such as using cryptography and protocols technologies. However, this does not represent trust. Security-driven approaches for creating trust among organizations have led to a bias entitled "*the double illusion of 100% safe*" [Weth & Bohm, 2006].

It is said that technology is always deceptive: it is safe until it is violated. Every secure environment will soon become insecure, because technical innovation occurs in both the positive area of security protocols and the negative area of hacking processes. Organizations that use security of environments that are enhanced by technology as the only means of trusting others might face difficultly when unexpected problems occur, such as the hacking of software [Grandison & Sloman, 2000]. This is the first illusion.

Imagine for a moment that a secure environment has been obtained. Organizations are able to act freely and confidently because they are protected by technology. However, this is not a trust-building atmosphere because the importance of trust increases when there is a chance that certain risks may increase [Rousseau, et al., 1998]. An environment depicted with hard technology protection deteriorates trust building: organizations feel the security but not necessarily trust. This is the second illusion.

d) **Trust versus privacy**

At the individual level, privacy can be seen as a fundamental human right. Similarly, organizations are now facing problems related to privacy and, more specifically, with respect to confidential data and strategies. Different legislative and technological mechanisms have been proposed to enhance the privacy of organizational data in the world of computers. Protection depends on whether privacy is seen as a right, which should be protected by laws; or a need, which should be supported by devices [Msanjila & Afsarmanesh, 2007c]. From the point of view of privacy and considering the co-working among organizations, there is an inherent conflict between trust and privacy: the more knowledge a first entity gains about a second entity, the more accurate the results will be of the level of trust assessment. Nevertheless, the more knowledge is gained about the second entity, the less privacy is left to this entity [Seigneur & Jensen, 2004]. The contradiction of enhancing level of trust in organizations, while at the same time enhancing their privacy, is a challenge for further research.

e) **Trust and reputation**

Reputation concerns general opinions (more technically, a social evaluation) of the public toward a person, a group of people, or an organization. It is an important factor in many domains, such as business, online communities or social status. Reputation is known to be a ubiquitous, spontaneous and highly efficient mechanism of social control in natural societies. It is a subject which is being studied in disciplines such as social, management and technological sciences. Furthermore, reputation acts on different levels of agency, namely individual and supra-individual. At the supra-individual level, it focuses on groups, communities, collectives and abstract social entities (such as firms, corporations, organizations, countries, cultures and even civilizations) and it affects phenomena at different scales, from everyday life to relationships between nations. There are two kinds of reputation: *witnessed reputation* and *certified reputation.*

Witnessed reputation [Huynh, et al., 2004] refers to the reputation-related information that is collected by the trustor, or the trustor's associated organizations (friends). In this case, the trustor organization or its associated organizations observe characters of the trustee organization to decide its trust level. In VBEs, where organizations collaborate virtually, the adaptation of this approach is hardly feasible.

Certified reputation [Huynh, et al., 2004] refers to the reputation-related information that is collected by the trustee organizations and made available to the trustor organization. The trustee organization can provide information such as a detailed organization profile, recommendation letters, accreditation documents, auditing results, etc., to the trustor organization in order to enhance its trust level. The trustee organization can also request its friend/authorized organizations to provide positive information (e.g. accreditation document) to the trustor organization in order to enhance its trust level. The main problem of this approach is that there is high risk of user-biased information, which endangers the success of the resulting trust relationships. The validation of such information is also difficult since, in practice, bad reputations are usually hidden.

The management of an individual's reputation involves recording a person's actions and the opinions of others about those actions. These records can then be made available in order to allow other people (or agents) to make informed decisions on trusting that person. A reputation management system, particularly as applied in multi-agent technologies, which use pre-programmed criteria for reputation management, facilitates the process of supporting cooperative behaviour over selfish behaviour. Reputation has been applied in different disciplines to study relations between entities and their trustworthiness.

f) Trust and virtual co-working among organizations

The emerging economy is knowledge-based and without borders, and competition exists among both local and national organizations on how to learn faster and organize more flexibly so as to take advantage of the "technology-enabled" market. Within this new economy, ICTs are ubiquitous. They have transformed geographically separated locales into a "global village" for information sharing, organizational interactions, and an exchange of economical value. Technology, and in particular ever-expanding digital bandwidth, has resulted in the creation of new economy forms of intangible, knowledge-based capital, the value of which now exceeds that of the physical capital that once dominated old economies (Afsarmanesh & Camarinha-Matos, 2005). Whereas business models for the old economy emphasized tasks and roles organizationally, business models for the new economy focus on self-organizing: teams, companies, industry-based clusters, or CNOs. Organizations have realized that by virtually co-working, such as in CNOs, they can enhance their chance of jointly meeting the opportunities presented by the continuously changing requirements of "innovation-demanding" opportunities more effectively (Camarinha-Matos & Afsarmanesh, 2006). There are three questions that need to be addressed when considering technology in relation to virtual co-working (Msanjila & Afsarmanesh, 2007c):

- *i)* What are the distinguishing factors that separate ICT-enabled collaboration in physical setting from virtual setting?
- *ii)* Can previous findings on physical collaboration help us to understand the characteristics of emerging virtual collaborations?
- *iii)* How does the creation of trust differ for physical collaborations and for virtual collaborations?

Innovative organizations that employ technology to facilitate collaborative projects are the hallmark of the new economy (Camarinha-Matos & Afsarmanesh, 2006). Such collaborations can range from arms-length information sharing to highly inter-dependent and geographical dispersed joint projects. In large VBEs, organizations cooperate/collaborate with others that sometimes are physically unknown to them. These organizations must trust each other in order to work together effectively. Basically, in the current innovative-based economy, trustees must possess technologies which can facilitate virtual co-working.

Moreover, the current economy demands the ability to acquire and possess competitive information and knowledge. Technologies are playing a great role in efficiently achieving such organizations' goals. The number of domains where technical artifacts are filtering into communications and relationships is increasingly growing, and now include computer supported interactions, computer supported co-work, e-commerce, etc. These are a few examples of this trend. In relation to technology, the importance of trust is twofold: (1) it can be seen as trust towards technical systems (i.e. with electronic payments), and (2) trust in technologies as mediators of interactions between organizations. Thus, when setting up technologically-related collaboration, organizations that possess the required technologies are judged to be technologically trustworthy.

2.3.6 Different aspects of trust in organizations - applied to the proposed approach

Most reported research results have addressed trust among organizations with a consideration of only a few aspects and in most cases with the application of only a single point of view, e.g. financial aspects. In our research we have identified five independent trust perspectives that comprehensively cover fundamental aspects which can be considered by trustor organizations, namely, technological, structural, economical, social, and managerial as further discussed in Chapter 3. It should be noted that for different trust establishment objectives, only some of these perspectives may be relevant as exemplified in Chapter 1. This section briefly describes these five perspectives, and a discussion of their related aspects follows in the Section 3.3.

i) Technological aspect of inter-organizational trust

The current new economy is a knowledge-based economy without borders, where competition now lies not only in acquiring business, but also in acquiring and owning technology for the purposes of communication and the delivery of products/services. Technology can play two roles: (1) facilitating collaborations among organizations in a collaborative consortium, acting as a communication infrastructure; and (2) applying in production for use as resources (e.g. machines, computers, etc.). Thus organizations possessing technologies, which thoroughly address these two technological roles, will be judged to be trustworthy. A number of technologically-related aspects of inter-organizational trust have already been described in the previous section (Section 2.3.3) of this chapter, namely in relation to security, privacy, risks, and so forth. Aspects of technological perspective are discussed in Section 3.3.

ii) Structural aspect of inter-organizational trust

As an organization grows in size, geographical scope (coverage), and capabilities (competences and expertise), etc. its structural performance improves. It enhances thus its capability to transform, collaborate and cooperate, its structural trustworthiness. This perspective is further discussed in Chapter 3 in an elaboration of the approach used to analyze inter-organizational trust.

iii) Economical aspect of inter-organizational trust

Today's technologies and volatility of opportunities have encouraged organizations to start investigating and deploying values of trust that can be achieved through economical successes. Globalization has changed the old rules of competition and continuous innovation has become a strategic priority [Blomqvist, 2005]. With current advances of information and communication technologies (ICTs), it is difficult for organizations to keep information about their business strategies and investment plans confidential. At the same time, government policies aim to encourage collaboration between organizations [Assimakopoulos & Macdonald, 2002], which in turn requires extensive sharing of economical data. While organizations are not willing to let their competitors access their potential business data and thus are only looking for advanced mechanisms to enhance their privacy, new forms of collaborative networks, such as VBEs and VOs, encourage openness and sharing. Challenging issues here relate to selecting trustworthy partners with which to share such strategic economical information. The challenge remains of which information to make accessible and of finding a level of accessibility that is acceptable for all stakeholders. Below are the key economical elements for the creation of trust among organizations in VBEs [Msanjila & Afsarmanesh, 2006a]: (1) Collaborative ***economical success and survival*** of organizations in a VBE depends on the amount of trust between them, (2) the possibility of finding ***scarce resources and lacking knowledge*** owned by other partners depends on the intensity of trust among involved organizations, (3) trust among organizations reduces the frequency of the occurrence of ***financial risks*** such as by discouraging opportunistic behavior, and (4) trust among organizations enhances the ***interoperability*** between business processes at different organizations. Based on an economical perspective, trustors need to access economical data for assessing level of trust that will persuade them to create trust for trustees. Aspects related to this perspective are discussed in Section 3.3.

iv) Social aspect of inter-organizational trust

An accurate definition of social trust is difficult to establish. However, it has been encapsulated as an ongoing motivation of social relations that form the basis for interactions. At the individual level, social trust can entail perceived honesty, objectivity, consistency, competency, and fairness; all of which foster relationships among individuals that must be maintained by the sustained fulfillment of these elements [Boslego, 2005]. A decision to trust on the basis of a social perspective has been described by several trust experts as a "risk judgment", which is a form of cooperation that has no immediate payoff or benefit, and one which involves a gamble that trusted parties will act as expected [Good, 1988]. Aspects of social trust are not universal, but vary across cultures, contexts, countries, and so on.

While people may trust their relatives, co-workers, classmates, friends, and even their friends' friends, the puzzle of social trust is the idea of trusting strangers. The difficulty a person encounters in trusting a stranger is similar to that which an organization faces when it needs to trust another completely unknown organization with which it has previously interacted. The only basis on which social trust other organizations can be judged is that organization’s social performance and status, which may be influenced by their ethnic or cultural group, the characteristics and values of the society in which they were registered and are currently operating, their past experiences and interactions, and - more broadly - the historical tradition of their society [Msanjila & Afsarmanesh, 2006a].

The practical challenge concerns the actions to be taken once social trust has been broken. Should organizations with many racial, religious, and ethnic problems resign themselves to low levels of trust, or can trust be somehow re-engineered? Social trust is a good public phenomenon that should be maximized, and is thus non-excludable, non-rivalrous, and does not result in direct profit, but benefits organizations and society indirectly. Consequently, it must be re-engineered whenever is needed.

In VBEs, organizations must enhance their trust from the society in which they are operating. Social trust for an organization is very important as a way to maintain moral acceptance from the society in which it is operating its business. For social trust, internal achievements of the organization receive little attention in comparison with its external social achievements. Aspects of social perspective are discussed in Section 3.3.

v) Managerial aspect of inter-organizational trust

The need for flexible and responsive organizations has been widely publicized in today’s technologically-enabled and competitive market. In order to support this flexibility, a shift has taken place to new organizational structures and processes. Organizations in this century cannot remain static. They must constantly respond to dynamic environments. What is more, they must also learn to take a proactive stance, even creating changes. To be in a static mode may mean that organizations will be left eating the dust of their competitors when markets and technologies advance [Msanjila & Afsarmanesh, 2007c].

The changes, uncertainties, and complexities that characterize today’s greatest challenges in business and in particular in those performed in virtual world, also present challenges to managers at all levels. Responding to changes in external environments requires ever-vigilant managers. Managers must be flexible in order to effectively promote flexibility in their organizations. The necessary flexibilities include the flexibility to manage and compete for VBE rewards, the ability to flexibly and collaboratively plan, flexibility in collaborative problem solving, technological flexibility, and flexibility in addressing VBE politics [Msanjila & Afsarmanesh, 2006a].

Although the palpability of trust is known to organizations in VBEs, it still proves difficult to create. VBE administration cannot be successful without acquiring trust within those organizations that the administration is managing, whether at the level of the organization or at the level of the VBE. There are two possibilities from which a trustor can create trust to a trustee, based on managerial aspects:

- Trustors can trust trustees only focusing on current tasks or roles and specifically on aspects of managerial *competency* to fulfill those particular roles or tasks. This kind of trust is referred to as *situational-based rather than relational-based.* For example, business organizations trust credit card companies to handle the financial transactions that taking place all over the world using their cards. However, these business organizations can hardly trust credit card companies to train their employees on financial management. This *competence-based trust* is rationally developed and needs certified evidences. It can emerge quickly and it does not require previous interactions.
- Trustors can also trust trustees by assessing and evaluating their *motivations.* This kind of trust takes much longer to develop because both actors must be able to *understand and experience each other's intentions.* The difficulty here is that managers might have self-interests that may lower the trust of their organizations. This kind of trust needs rational data that is based on the previous performance of managers.

For some purposes, trustors may consider the managerial history of trustees as the primary element when assessing their level of trust. In this manner, trust assessment is based on how well trustees have behaved professionally and how well power has been used in management positions in past networks, such as in VOs. Aspects of managerial perspective are discussed in Section 3.3.

2.4 Characterization of trust related data for organizations in VBEs

In addition to achieving high performance in order to enhance their trustworthiness, organizations in VBEs must be able to provide evidence of validity for their trust related data (performance data expressed in terms of trust criteria as addressed in Chapter 3). In this section we address the classification of trust related data needed to support creation of trust among organizations and we also propose some sources of evidence of validity for this kind of data.

2.4.1 Classification of data for creation of trust among organizations

Organizations' perceptions of trust correspond with both the nature of the purpose of its application as well as with the actors involved. For each specific practice in which a particular group of organizations is involved, trust is interpreted and perceived differently. Organizations therefore may need different kind of information – here referred to as trust-related-data – to trust others depending on the following aspects:

- ***Who:*** Collaborations among organizations in VBEs are characterized as goal-oriented. Inter-organizational trust relationships provide a fruitful basis for achieving common or compatible goals in such collaborations. Organizations will trust other actors on the basis of the role these actors will play in helping to achieve the common goals. For example, in virtual organizations the roles that can be assumed are that of coordinator or partner. Each role might need different kinds of information to enable a certain organization to trust the organization that is seeking trust. Thus the term "who" as applied here is related to the specific role an organization will play within a collaborative consortium.

- ***When:*** In this thesis, the proposed approach for assessing level of trust requires the application of an organization's past performance data as the fundamental input data. The word "past" here is of subjective nature: it is not clear how long into the past the performance data needs to be covered to be sufficient for the organizations that give trust. The preferred time of the collection and provision of information will differ between the organizations that give trust (trustor) and organizations that seek trust (trustee). Consequently, the information that needs to be provided to organizations may vary and differ with time.
- ***What:*** This refers to the information that will be provided to each organization that is participating in the concerned relationship of trust. It is not easy to define in advance the specific type of information that each organization might need in every trust relationship due to the variation of organizations' perceptions in the specific context and preferences on what they think is important to give their trust.
- ***How:*** The validity of the information is influenced by the authenticity of both its sources and the applied mechanisms/tools for data collection and provision. It can be argued that in circumstances in which information sources and data collection mechanisms are highly trustworthy the information provided has high validity.
- ***Why:*** The information that is provided to a specific organization will also depend on the reason why it is requested. Here, this refers to the main trust objective and related sub-objectives for establishing the trust relationship between organizations.

2.4.2 Types of validity evidence for trust related data

Information made available to a VBE by an organization in order to assess its level of trust must be supported by satisfactory evidence of validity. This section proposes two types of evidence that can be used by organizations to examine and assure the validity of their trust related data, namely: ***certified evidence and witnessed evidence***.

i) Certified evidence

The validity of information in this category is based on well-defined and agreed standards that the information must meet. The validation is usually performed by authorized organizations. In light of the need illustrated in this thesis for the validation of the trust related data of organizations, we suggest the following five sources of certified evidence:

(a) *Accreditation:* Accreditation is defined as an independent act of granting recognition to an organization as proof that the respective organization meets and maintains the specified standards. In the health sector, for example, accreditation is an independent external review process that assesses the quality of healthcare services in order to encourage better performance and assure the public of the quality of the services provided by the organizations [Lichiello & Turnock, 2002]. Accreditation standards are traditionally set at what are considered to be the minimum achievable and allowed levels. Accreditation is traditionally practiced to assess the *quality and cost of business processes and their related products/services*.

(b) *Financial rating:* Financial rating (credit rate) is a published ranking that is based on a detailed financial analysis. As a rule, credit bureaus perform the financial analysis, which is based in general on the financial history of an organization and in particular on its ability to meet payment obligations. VBE member organizations must validate their financial record and have it approved by authorized organizations that are legalized to perform the financial related analysis. Approval is thus sought for aspects including *credit score, solvency, profitability ratios, bankruptcy prediction, etc.*

(c) *Patent:* A patent is a set of exclusive rights granted by an authorized party to an organization for a fixed period of time in exchange for the regulated or public disclosure of a certain device, method, or process which is new, inventive, and industrially applicable. Patents granted to organizations could be used as evidence of performance data.

(d) *License:* License is an official or legal permission to do or own a specific item. A license can be a document, plate, or tag that is issued as proof of official or legal permission to own something or carry out an activity (e.g. a business license). The issue of a license with intellectual property rights, such as a copyright or trademark is a proof of permission to use, reproduce, or create an instance of the licensed work. Therefore, licenses can also be used to attest the information provided by an organization.

(e) *Certificate and awards:* A certificate is an official document that proves the accomplishment of a certain achievement. For example, a business registration certificate warrants the formal existence of an organization. In computing and in particular computer security and cryptography, the word certificate generally refers to a digital identity certificate, also known as a public key certificate. An award is something given to a person or organization to recognize excellence in a certain field. Such proof can also be used as a means to validate the information provided by an organization.

ii) Witnessed evidence

This type of evidence constitutes a certain form of documentation that is generated by third parties and that is subjective by nature. So although this type of evidence provides some proof of accuracy it can be argued that the degree of validity is less than certified evidence. Such witnessed evidence may include information obtained from: (1) Public channels, (e.g. magazines, newspapers) and (2) Private channels, (e.g. recommendations).

Although these types of evidence are not as strong as certified evidence, when certified evidence is lacking they can provide some degree of validity of the provided information. Clearly, the validity level increases if the channels used (the news sources or the person providing the recommendation) are publicly recognized. For example, reputable news media put extra effort into discovering the truth about the story they report, although their report can only focus on certain aspects of the story and they do not guarantee the provision of comprehensive coverage. Similarly, a letter of recommendation from party A about party B only shows a limited number of party B's qualifications as party A only knows party B to a certain extent.

2.5 Characterization of trust relationships among organizations in VBEs

One important strategy that is necessary for VBEs is to focus on organizational preparedness to enhance their chances of participating in VOs. Organizational strategies must therefore properly address the notion of collaboration with other business partners. As addressed in Chapter 1, in addition to acquiring resources, knowledge and competencies, a crucial aspect of the preparation process involves establishing trust relationships with potential business partners in order to smoothen possible collaboration. There are two kinds of trust relationships between organizations that can be established in VBEs, namely:

- *Short-term trust relationships:* established to facilitate co-working between organizations that will exist for a relatively short period of time, e.g. collaborations in VOs.
- *Long-term trust relationships*: established to facilitate co-working between organizations that will exist for a relatively long period of time, e.g. cooperation in VBEs.

Consideration of a large number of specific fundamental aspects is necessary when addressing trust between organizations in VBEs. As described in Chapters 3, 4, 5, and 6, inter-organizational trust is characterized as a multi-objective, multi-perspective, and multi-criteria subject. It is a challenging task to comprehensively cover all these specific fundamental aspects of inter-organizational trust and thus use them to facilitate the establishment of trust relationships between organizations. A single specialized approach, such as based on reputation of organizations, security of systems, etc., cannot adequately cover all fundamental aspects of trust that need to be considered while establishing trust relationships between organizations in VBEs. Accordingly, a generic but comprehensive and structured approach must be designed that will support the realization of inter-organizational trust relationships in VBEs.

A number of specific steps must be taken into account in order to characterize the planned relationships and prepare the involved organizations on a number of essential aspects in establishing their goal-oriented trust relationships. In order to effectively establish trust relationships between organizations in VBEs applicable to different domains, we propose the following four steps, each addressed further in next chapters. The first three steps focus on guiding involved organizations to prepare themselves in relation to trusting one another for the purpose of facilitating the intended collaboration. The following are the four proposed steps:

Step 1: Assessment of level of trust in organizations as further addressed in Chapter 5 and Chapter 6,

Step 2: Validation of trust level results based on the analysis of evidence of validity of the trust related data for organizations as further addressed in Section 2.4,

Step 3: Presentation of levels of trust in organizations and related trust concepts as easy and understandable as possible to involved organizations as further addressed in Chapters 3, 4, 5 and 6.

Step 4: Creation of trust between organizations to support the launching of the intended trust relationships by providing sufficient information based on a number of trust aspects as addressed in Section 2.4, and Chapters 3 and 6.

2.6 Chapter discussion and conclusion

This chapter has presented a survey on existing practices and reported research results on trust. It has surveyed inter-personal trust and has used results as a means of comparison with the basic concepts of inter-organizational trust. In addition, it has presented perceptions of trust experienced and applied in different disciplines and domains.

The chapter has also introduced the characterization of inter-organizational trust in VBEs and it has presented fundamental concepts which either complement (such as security, reputation, etc.) or contradict (e.g. risks, privacy, etc.) inter-organizational trust. It also introduces primary aspects of organizational trustworthiness, namely those of a technological, structural, economical, social, and managerial nature. The chapter ends by presenting the characterization of trust related data and inter-organizational trust relationships in VBEs.

A key contribution of this chapter in this thesis is the characterization of the main challenges related to trust studies, namely: (i) the causality relations between trust and a wide variety of related aspects (see further details addressed in Chapters 3 and 5), (ii) the need to enhance transparency and fairness in relation to the analysis of inter-organizational trust and measurement of performance of organizations which in turn provides fundamental input data to the evaluation of trustworthiness of the organization (see further details in Section 3.3.3), and (iii) characterization of a large set of trust elements that must be considered in building models and mechanisms for assessing the level of trust in organizations (see Sections 2.3.5 and 2.3.6, and Chapters 3, 4 and 5).

The next chapter (Chapter 3) further extends the concepts presented in Section 2.3.6 by presenting an approach which is applied for identifying and characterizing trust elements for organizations.

Chapter 3

Identification of trust elements for organizations

Trust is not a single concept that can be applied to all cases for trust-based decision-making. Its measurements depend on both the purpose of establishing a trust relationship and its specific involved actors. The assessment of trust level of organizations may consider a series of trust criteria. The level of trust in organizations is complex and can neither be measured with the single value of a single parameter, nor interpreted with a single metric. In our approach, trust level of an organization is measured rationally in terms of quantitative values of a number of related trust criteria. One key challenge related to the characterization of trust in VBEs is the identification of measurable trust criteria for organizations. This chapter presents an approach for identifying and characterizing the trust elements. The chapter also provides a general comprehensive set of trust criteria for organizations identified by applying the proposed approach and validated by the existing industrial VBE networks.

This chapter contains material previously published in two articles, of which one appeared in the International Journal of Production Research [Msanjila & Afsarmanesh, 2007a], and the other appeared in the international journal of software [Msanjila & Afsarmanesh, 2008d].

3.1 Introduction

One important aspect of characterizing trust in VBEs is the identification of trust elements for various organizations. In our study we found that trust elements for organizations are not at the same level of abstraction or measurability (are not equivalent); differences in abstraction indicate their hierarchical relations. Figure 3.1 visualizes the hierarchical relations among trust elements. We define trust elements as follows.

> ***Trust elements** represents a set of types (classes) defined in the thesis, each encapsulating certain aspects related to measuring trust. These elements are hierarchically inter-related from the abstract (non measurable) ones representing the root of the hierarchy to the real measurable ones which represent the lowest (leaf nodes) in the hierarchy, and that together they characterize both trust and trust-relationships in VBEs. Trust elements form the base for identifying the data needed for assessment of trust level of organizations [Msanjila & Afsarmanesh, 2007c].*

Some trust elements defined in the literature related to organizations are *subjective* (*opinion-based)*, such as the recommendations, polling, voting, and so on. Opinion-based trust elements are not related to measurable facts about organizations, which consequently makes it difficult to support them with formal reasoning mechanisms while assessing level of trust [Weth &

Bohm, 2006]. However, in a different approach a number of performance-based trust elements can be identified for organizations. Namely, with a different approach some *rational* (fact-based) measurements for trust elements of organizations can be defined as addressed in this chapter that are supported with formal mechanisms such as mathematical formulas to assess organization's trustworthiness. In the Section 3.2 we present an approach for identifying such trust elements for organizations. The presented approach also supports the analysis of inter-relations (impact and causal influence relations) among these measurable trust elements. Finally, in Section 3.3 we present a general set of trust elements for organizations.

3.2 HICI: An approach for identifying trust elements for organizations

The HICI approach proposed by this thesis constitutes three stages, each one focusing on a specific task related to the identification and characterization of trust elements for organizations. The first stage called the ***Hierarchical analysis stage***, further addressed in Section 0, focuses on the identification of types of trust elements and classifying them into a generalization hierarchy based on their level of measurability. The second stage called the ***Impact analysis stage***, further addressed in Section 3.2.2, focuses on the analysis of the impact on the trust level of the organization caused by changes in values of trust criteria. The third stage called the ***Causal Influence analysis stage***, addressed in Section 3.2.3, focuses on the analysis of causal relations between trust criteria and other VBE environment factors as described in Section 3.2.3. To enhance the presentation of the HICI approach below we present the base definitions of four fundamental terms applied in the classification of trust elements as shown in Figure 3.1.

Trust objective: *is the purpose for which the establishment of a trust relationship among the involved organizations is required. Examples of trust objectives include the following: for inviting an organization to join a VO, for appointing or selecting an organization as the VO coordinator, for an organization to decide to join VBE, and so forth.*

Trust perspective: *represents the specific "point of view" of the trustor on the main aspects that must be considered when assessing the trustee's level of trust. The trust perspectives help the trustor organizations in deciding what information related to trustee organizations should be considered primarily, or secondarily, etc., and made available to them in order for them to create the required level of trust.*

Trust requirements: *represent the essentials (cardinals) that characterize and guide on how the respective trust perspective shall be realized. Thus, trust requirements are the fundamental cardinals that guide or suggest what must be met in order for the respective trust perspective to be realized. For instance, "financial stability" is an example requirement that must be met, to support establishing trust based on the economical perspective; similarly, "compliance with community standards" is a requirement for trust related to social perspective, and "stability in management" is a requirement for managerial perspective.*

Trust criteria: *represent the measurable trust elements that characterize each respective trust requirement. Therefore, the values of each organization's trust criteria can be used to make a rational (fact-based) judgment on whether the respective trust requirement is met. Each trust criteria has its own related value structure that defines the acceptable structure for its data, such as the scalars, vectors, arrays, list of strings, and so on. Furthermore, such value structure also defines the metric to be used to scale the specified data. The only source of data for trust criteria is the respective trustee's organization. Therefore in each*

VBE, member organizations shall submit data related to their trust criteria, and keep them up-to-date. Data related to the trust criteria of organizations will be used in the VBE for different purposes related to trust management.

In order to enhance the presentation of the HICI approach, in Table 3.1 we introduce an example set of trust elements for two different trust perspectives. A complete set of the trust elements defined for VBE organizations is presented in Section 3.3. In relation to the establishment of different kinds of trust relationships between organizations, we have identified three trust objectives addressed in details in Section 3.3, and five trust perspectives where each trust perspective is characterized by a number of trust requirements, which in turn are characterized by a number of trust criteria. These are later addressed in details in Section 3.3 and more specifically in Figure 3.6.

Table 3.1: Examples of trust elements

Trust perspective	Trust requirements	Trust criteria	Acronym
Structural	Structural strength	Size of an organization	SZ
		Competencies	CP
		Personnel experts	EP
	Business strength	Centers	CT
		Workload allocation	WA
		Geographical coverage	GC
		Joint ventures	JV
Economical	Capital	Cash	CC
		Physical capital	PL
		Material (operational) capital	MC
	Financial stability	Cash in	CI
		Cash out	CO
		Profit/Loss	PO
		Operational costs	OC
	VO -Collaboration based financial stability	Cash in	VCI
		Cash out	VCO
		Profit/Loss	VPO
	Financial standards	Auditing standards	AS
		Auditing frequency	AF

Table 3.1 includes subordinate trust elements identified for the organizational structural perspective, as well as the economical perspective related to measuring an organization's trustworthiness. The elements in this table are later used within the examples in this chapter. The example set of trust elements as shown in Table 3.1 are related to and characterize a specific trust objective of *creating trust in organizations for inviting them to participate in a VO* as further addressed in Section 0. For example, geographical coverage is one characteristic criterion representing the business strength requirement at the structural perspective of an organization necessary to evaluate its trustworthiness.

3.2.1 First Stage: Hierarchical Analysis

The hierarchical relations defined in HICI among the trust elements represent their inter-relations from a highly abstract element as the root node (e.g. trust objective – 1) to all its subordinate measurable elements at the leaf nodes (e.g. trust criteria – 1.1.1.1). We have identified five levels of abstraction (L1 to L5) for representing the hierarchical relations among trust elements. As such trust-relationships are established as a means for involved organizations to achieve a specific trust objective. Trust objectives characterize the reason why trust relationships must be established when addressing the creation of trust among member organizations in the VBE. In our classification of trust elements for organizations, trust objectives represent the first level (L1) of the abstraction hierarchy, as shown in Figure 3.1.

❑ A ***trust objective*** is characterized by a number of trust perspectives (e.g. structural perspective, economical perspective, etc.). A trust perspective represents a “point of view” on what trust and trust relationships mean to a trustor, therefore a trust perspective indicates the primary aspects preferred by a trustor, in order for him to trust a trustee. In our classification of trust elements, trust perspectives represent the second level (L2) of the abstraction hierarchy.

❑ A ***trust perspective*** is characterized by a set of trust requirements (e.g. for structural perspective requirement, it can be structural strength, and business strength). A trust requirement also refers to what details related to each trust objective the trustor believes must be met by the trustee organization before trust is created and realized on the basis of the preferred perspective. For example, in our classification of trust elements the trust requirements represent the third level (L3) of the abstraction hierarchy.

❑ A ***trust requirement*** is characterized by a set of trust criteria (e.g. for structural strength requirements the trust criteria include: size of an organization, personnel experts, etc.). Trust criteria are the only real measurable elements from the organizations environments. In order to facilitate their measurement, each trust criterion is specified together with its value structure that defines the magnitude and meaning (SI-Unit) of the possible values. In our classification, trust criteria and value structures represent the fourth (L4) and fifth (L5) levels of the abstraction abstract.

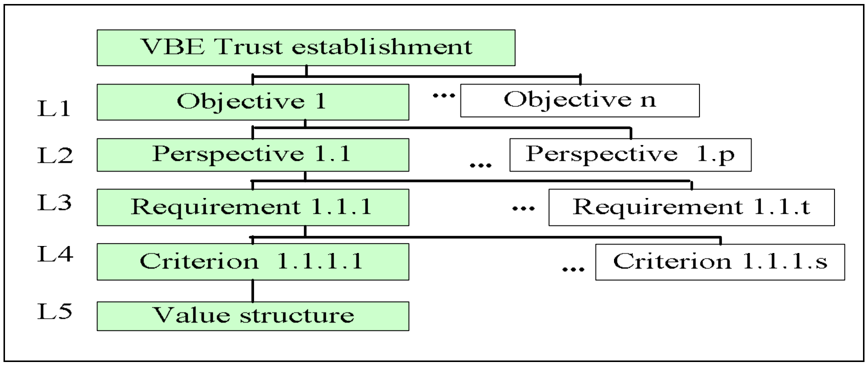


Figure 3.1: General view of hierarchy of trust elements for VBE trust establishment
This figure shows a classification of trust elements in a generalization hierarchy based on their level of measurability, as described earlier in this section.

The first stage of the HICI approach can also be applied to customize the identified trust elements to meet specific characteristic of a VBE environment. This aspect is addressed in Section 5.4 in a discussion on the formulation of mechanisms for assessing organization’s trust level. Although each trust criterion only occurs at one trust requirement and at one trust perspective, it does not mean that the trust criteria are totally independent. Inter-relations do exist among some trust criteria and even between different trust perspectives as a result of the existence of “intermediate factors” as discussed in Section 3.2.2.

3.2.2 Second Stage: Impact Analysis

A rational (fact-based) assessment of the level of trust in organizations is essentially based on information about their past performance. However, trust criteria that constitute the basis for measurement of level of trust, do not exactly match the ***performance indicators*** typically defined and applied for measuring the performance of organizations. Research in the past has not addressed the "*direct*" representation of needed organization's performance in terms of related trust criteria. By means of impact analysis of trust criteria factors, here referred to as "*intermediate factors*", our approach makes it possible to identify the relationship between trust criteria and some trust related performance indicators. Simultaneously, trust criteria are influenced by the so-called "*known factors"* in the VBEs, as discussed below.

Known factors represent a set of domain/application dependent factors that indirectly influence the outcome of measurements of level of trust in the involved organizations. Each domain/application, such as business, manufacturing, medical, and so on, is affected by both the VBE's internal factors (e.g. the minimum wage per hour for all organizations within the VBE), as well as the VBE's external factors relating to environment / market / society in consideration of the VBEs scope both geographical and area wise. For example: (1) certain pre-existing regulations or standards (e.g. regional tax subsidies in a given market), (2) an environment's norm and practice (e.g. minimum number of competencies required for each organization to become a VBE member), or (3) the current state of the market/society (e.g. regional availability of raw material or a market consumption capacity of products/services), etc. These factors indirectly influence the level of trust. For each VBE, its specific known factors are identified during the customization of its generic trust management system (Chapter 5) based on specific domain/application of the VBE. Consequently, the main source of data for the known factors related to the VBE is its administration itself that knows about both its internal and external environments. The data about known factors should also be kept up-to-date by the VBE administration.

Intermediate factors represent the factors that play an intermediary role in relating the VBE's known factors to its organizations trust criteria. In principle, both trust criteria and known factors do influence each other. Their influences are twofold, consisting of causal and impact influences. However, these influences are not direct, but occur through some intermediate factors. In Section 3.2.3 the analysis of causal influences among the trust criteria and known factors is represented diagrammatically in the so-called causal diagram. Based on the results of this causal analysis, the influence relations are used for the derivation of mathematical equations, which formally show relationships between trust criteria and known factors, through specific intermediate factors. These equations are further used to calculate the values for each intermediate factor in relation to every organization, and thus acting as a means of partial trust level assessment for the organizations in VBEs. Consequently, unlike the trust criteria and known factors for which the data is respectively assigned by the organization and the VBE administration, the intermediate factors must be calculated through these equations. Namely, if needed, the only way that the value of an intermediate factor can be improved is either through the changes in the values of the organizational trust criteria, or changes in the known factors of the VBE that can be decided internally within the VBE, since these are the only controllable factors that influence the intermediate factors.

For example as shown in Figure 3.2, consider the intermediate factor "organizational expenditure", which is influenced by the two trust criteria of size (from a structural perspective) of an organization referring to the number of employees, the operational cost (from an economical perspective) referring to the minimum wage of employees acceptable at the VBE. Changing the expenditure of an organization can be achieved by changing the values of the two above stated trust criteria.

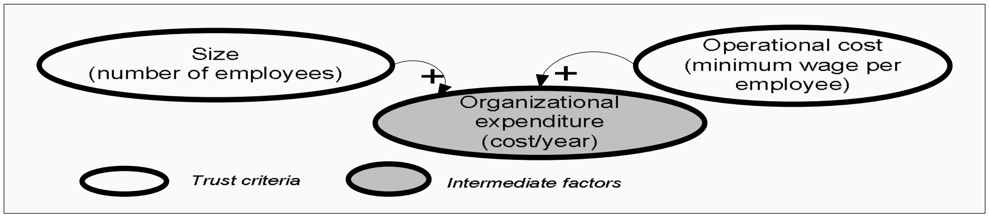


Figure 3.2: Example relation between trust criteria from different trust perspectives
This figure exemplifies how the causal influences between trust criteria and intermediate factors can be analyzed and diagrammatically represented.

Intermediate factors are identified through the *impact analysis* which is the main focus of the second stage of the HICI approach as presented in this Section 3.2.2. Impact analysis enables both the identification of intermediate factors and an analysis of their relations to trust criteria and to the performance of organizations.

In order to further describe this concept, consider an example related to *structural perspective* as presented in Table 3.1. Using an empirical study of the organization's domain that is validated by domain experts, we have identified a set of trust criteria and intermediate factors that we apply to show the example of impacts analysis. Figure 3.3 shows how changes in values of trust criteria (i.e. size of an organizations [SZ], organizational competency [CP], personnel experts [EP], of the structural strength requirement, and the trust criteria centers [CT], Workload allocation [WA], geographical coverage [GC], and joint ventures [JV] for business strength requirements) can create impact on the intermediate factors (i.e. social capital [SC], connections [CN], common context [CC], and production capacity [PC]), that can in turn directly affect the improvement of the performance of organizations in relation to its structural perspective, and thus influencing its trust level.

To further describe the impact analysis, consider an example in Figure 3.3 addressing how the changes in values of the trust criteria "size" of an organization can produce impact on its trust level through the intermediate factor "social capital" as is detailed out below. As defined in this thesis, the size of an organization increases when the number of employees increases. The increase of size of an organization creates an impact on the organization's social capital through the connections of its individual employees [Putnam, 1995]. Social capital here refers to the aggregation of the actual or potential resources which are linked to possession of a durable network (of individuals), representing more or less institutionalized relationships of mutual acquaintance and recognition [Bourdieu, 1983]. When the social capital increases it will improve the structural performance of the organization, such as related to increasing in chances of acquiring opportunities through the use of its employees' durable network within the society. In turn, the structural performance of an organization increases then its trust level will also rise. Section 5.4.5 further addresses the aspects presented in this figure in more details. Two more specific examples of impact relations (examples 3.1 and 3.2) are provided below in this section.

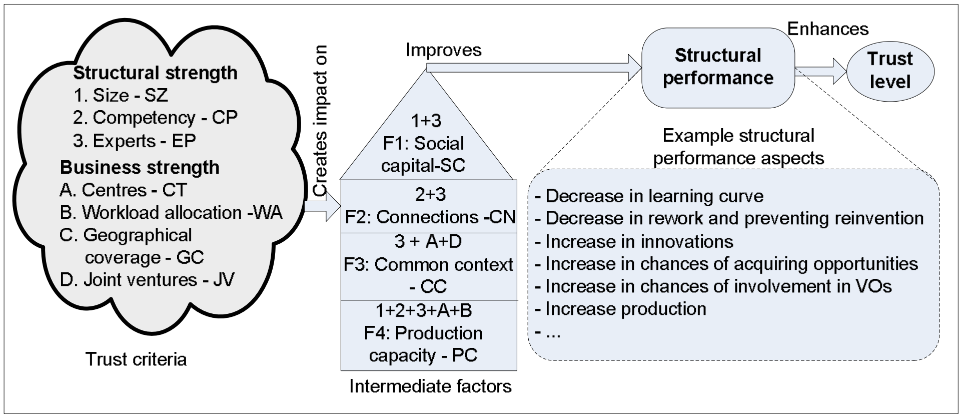


Figure 3.3: Analysis of the impact of trust criteria on performance for structural perspective

This figure shows the relation between trust criteria and organization's trust level through the defined intermediate factors (as also exemplified in example 3.1 and 3.2 below), which in turn provide means for expressing performance data (e.g. structural performance) of organizations in terms of trust criteria. The figure also presents a number of example performance aspects for the structural perspective.

Here "*Workload allocation or WA*" refers to the *maximum level* to which an employee of a certain organization can produce. The level of workload varies according to the specific domains, business environments, legal systems, and so on. For example, the workload of doctors in medical organizations is typically measured in terms of "the number of patients to which a single doctor can attend per day", while the workload of employees in a business organization is typically measured in terms of "the number of hours that each employee must spend at work", similarly in manual production/processing businesses, this may be measured in terms of the amount or number of items produced or processed per day, and so forth.

Example 3.1: Consider an organization, for example a research center, that increases the number of its employed experts (EP); it is shown here how this increase can improve the level of trust in this organization. Usually, employees do maintain their connections. For example, email communication with their academic colleagues who may be employed in other organizations, etc. Therefore, when an organization employs new experts, through these experts it indirectly expands its connectedness to other organizations, even including potential customers (CN in the middle of Figure 3.3). At the same time, through these experts some common context on interests may develop among different organizations (CC in the middle of Figure 3.3); with the aim, for example, of finding solutions to certain common problems. Furthermore, the connections and common context serve as a way to enhance the communication between organizations both directly and indirectly. If common context and connections among organizations exist then unnecessary rework and reinventions can be avoided, as well as learning curves can be reduced, both achieved through sharing of new ideas and information between organizations. The result of this will be an improvement in the structural performance of the organization and consequently an increase in its level of trust.

Example 3.2: A second example represents how the SZ, CP, EP, CT, and WA trust criteria as shown in Figure 3.3 influence the production capacity (PC) of an organization. Basically, if an organization grows in size (number of employees), increases the number of its centers (e.g. production centers), enhances its competencies, or acquires more experts, it will - assuming the employees can highly be exploited (such as for supporting manufacturing production) - in turn enhance its production capacity. This will then also directly improve its performance, which will result in an increase in its level of trust.

Results from impact analysis assist the VBE actors with their understanding of relations between trust criteria, performance, and level of trust. In short, when the rational trust level of an organization is decreasing or falls below the acceptable level, a number of performance aspects, such as the level of its production, innovation, acquisition of opportunities, etc., shall be analyzed in order to support discovering which aspects of the organization are getting weaker. Through the analysis, in turn, the related trust criteria whose change of values has impacted the performance aspects through intermediate factors can also be identified. Therefore, with impact analysis as presented in this section it is possible to identify certain trust criteria for which the values need to be improved in order to enhance the level of trust in an organization.

3.2.3 Third Stage: Causal Influence Analysis

The level of trust in an organization is causally related to past recorded events and actions taken or caused by the respective organizations. These relations are not direct or straightforward and in most cases there is a lack of fundamental comprehensive data, which is necessary to reason (or support reasoning) about them. Therefore, in order to analyze these relations and build a good understanding about the causal influences of past performance on current or future level of trust, we need to apply approaches which support reasoning with partial and or incomplete data.

Causal analysis, as applied in the discipline of System dynamics and/or systems engineering, and specifically related to structural modeling of causally related factors, supports the evaluation of relations between factors for which quantitative data may be incomplete or missing [Iriondo, et al., 2003, Parnell, et al., 2008]. This analysis then provides the means to qualitatively represent and reason about the continuous aspects of the world, such as the space, time, quantity, and so on. Furthermore, it is an “approximate” reasoning approach, which supports an analysis and even its argumentation with insufficient information [Greenland & Brumback, 2002]. In this study, we adopt and apply causal reasoning and analysis to examine the causal influences among trust criteria, known factors and intermediate factors.

Causal analysis supports the study and analysis of influence of inter-relationships between different factors in an environment. Causal modeling and causal sketching, which are special aspects of causal reasoning, are predominantly used for sequences of reasoning where the sequences are characterized by keywords such as ‘leads to’, ‘influences’, ‘causes’ on one hand, and ‘if-then’, ‘when-then’, ‘on-then’, ‘as-then’ or ‘supposing-then’, on the other hand [Akkok, 1998; Hovmand, 2003]. Typical examples are statements such as “when the accelerator is depressed, the speed increases” or “as more fuel flows into the engine, the speed increases” or “the amount of fuel flowing influences the speed”. This approach has been in the past used in population growth modeling, the modeling of decision-making processes, the modeling of policy analysis processes, to name but a few [Msanjila & Afsarmanesh, 2008c]. In VBEs, causal reasoning can be effectively used for the analysis of:

- Social networking side-effects that can be experienced by partners due to their participation in a VO, configured to respond to a specific brokered business opportunity (i.e. side-effects of business opportunity),
- Influences of different VBE administrative decisions on the general VBE’s performance,

- Inter-relations between the measurable trust criteria, influencing the trust level of organizations.

For this thesis the focus is on the last usage. Nevertheless, understanding the essentials of a given causal model requires adequate amount of knowledge in the field and the context within which it is being developed [Akkok, 1998]. The causal modeling approach (as shown in Figure 3.4) does not provide standard-building blocks or factors that are typically considered for modeling. Therefore, factors that are included in a certain causal model vary widely from one model to another and depend mainly on (1) the modeler, (2) the problem addressed, (3) the application domain, and (4) the stakeholders.

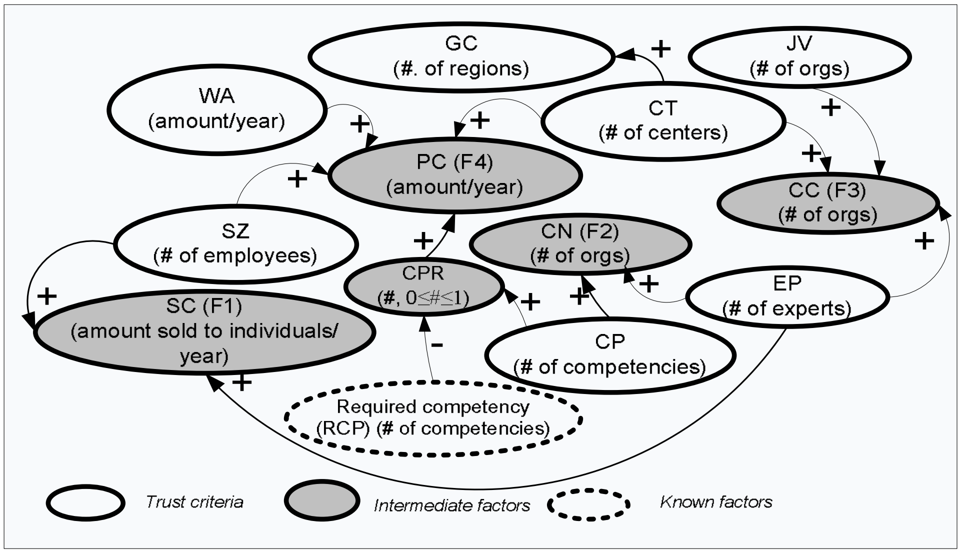


Figure 3.4: Causal influences between trust criteria for structural perspective

Where CPR represents competency ratio and RCP represents required competency in the VBE and all other parameters are defined earlier in Section 3.2.2, and also represented in Table 3.1 and Figure 3.3. This figure shows a qualitative analysis of causal influences between measurable parameters for the structural perspective, namely, the associated trust criteria (size, workload allocation, competencies, experts, centers, joint ventures, and geographical coverage), known factors (required competencies) and intermediate factors (social capital, competency ratio, connections, common context, and production capacity). As an example, please note in Figure 3.4 that the intermediate factor CPR (competency ratio) is positively influenced by one trust criteria CP (competency) and negatively influenced by one known factor RCP (required competency).

For an assessment of the level of trust in different organizations in VBEs, in the third stage of the *HICI approach*, we first use causal analysis and reasoning to understand influences among the measurable elements of trust, organizations' activities, and the environments; and then we use it as a means to identify their behavioral influences on the level of organization trust. For example, in order to analyze whether the behavioral changes of one specific trust criterion, causally influences the changes of several other specific trust criteria. Also, since the assessment of an organization's level of trust depends on the values of these trust criteria, changes in these values will also causally influence the variation in the organization's trust level.

Usually, causal relations between different trust criteria are not direct, rather through some defined intermediate factors. A causal diagram can be developed to *diagrammatically* *represent the results of the causal analysis among different factors and the qualitative reasoning on the behavior of a trust system*, based on its measurable trust elements whose values are continuously changing [Msanjila & Afsarmanesh, 2006a]. Figure 3.4 shows the relations between some trust criteria in the *structural perspective*, diagrammatically represented in a causal diagram. We have used causal diagram for representing the causal inter-relationships among trust criteria, intermediate factors and known factors and how they causally influence each other. A plus sign (+) on an arrow indicates that the increase or decrease of the source (first) factor respectively causes an increase or decrease in the destination (second) factor. On the contrary, the minus sign (-) indicates that the increase or decrease in the first factor respectively leads to a decrease or increase in the second factor [Kirkwood, 1998].

The results of these causal analyses are applied to the formulation of mathematical equations [Byne, 2006] that constitute the base for our developed mechanism for assessing the level of trust in organizations, as further discussed in Chapter 5.

3.3 Trust elements related to organizations in VBEs

In order to study the requirements for trust in VBEs, to model them as well as to validate and verify the approach of HICI, and to identify general trust elements for organizations participating in VBEs, three approaches are considered and applied as follows.

Approach A: State of the art study and other research

As a research area, VBEs are newly defined collaborative environments addressed within the last five years. Inter-organizational trust in VBE as one of the fundamental VBE research topics still lacks the needed research. As a result, there is little in the literature to start with and against which to compare and validate our new multi-criteria approach for analyzing inter-organizational trust. However, some limited research is performed related to the identification of "trust criteria" for systems or agents, but either in very specific domains such as health [Rolfe, 2006], or for some very specific applications such as the multi-agent systems, network certificate systems, internet applications, and so on, [Zhang, 2005]. In view of these facts, we opted for the other following two approaches (B and C), in order to examine the innovative aspect of the HICI approach.

Approach B: Expert based requirement analysis and validation

By means of questionnaires, we have collected data from experts relating to their judgments on the validity and applicability of our identified trust elements, as well as rating the innovative features of the HICI approach. The results of these questionnaires, which were conducted during the trial sessions of our system (the trust management system) in the context of the ECOLEAD project are presented in Section 6.6.2.

Approach C: Empirical based requirement analysis and validation

Several industrial running VBE networks were consulted in order to validate the identified set of generic trust elements in practice. We mostly focused our analysis on innovative aspects and potential applications of the trust elements identified by applying the HICI approach in real life businesses. Again, the consultation was achieved through a set of questionnaires that were completed by the industrial VBE networks (Annex C) which participated through the ECOLEAD project.

On the basis of the above three approaches, we have identified the following three categories of trust objectives for establishing trust among organizations in VBEs:

- Trust of a VBE member organization to another VBE member organization,
- Trust of a VBE member organization to the VBE administration organization, and
- Trust of an external stakeholder organization to the VBE.

These trust objectives are first introduced below and then in following sub-sections they are further discussed including their subordinate trust elements. Furthermore as addressed in Chapters 5 and 6, a detailed implementation of the Trust Management system (TrustMan) is achieved for the first category of trust objectives required to create trust among the VBE member organizations.

a) *Creating trust among VBE member organizations:*

The main aim of establishing and promoting trust relationships between VBE member organizations is to enhance the efficiency and success of both their cooperation within the VBE, as well as their potential collaboration in VOs that will be configured within the VBE environment. Further to the achievement of VBE member organizations, the main aspects that influence the level of trust a VBE member organization has towards other VBE member organizations is mainly its past performance in activities within the VBE, and from its participation in configured VOs. In addition, other aspects that may influence an organization's level of trust include its roles, reputations, membership level at the VBE, and so on. The subordinate trust elements for this trust objective are addressed in Section 3.3.1.

b) Creating trust of the VBE member organization to the VBE administration:

Trust of a VBE member organization towards the VBE administration enhances the chance of the member organization remaining loyal to the VBE, increases its willingness for active involvement in the VBE, and encourages the respective VBE member organization to invite and bring other valuable organizations into the VBE. Among the main issues that influence the creation of trust in member organizations towards the VBE administration are found to be: successes in managing the VBE environments, a VBE's successes in external markets and recognitions achieved through VBE's marketing and branding, the transparency of the administration procedures and rules, the transparency and efficiency of procedures used for measuring the performance of member organizations, the frequency of and support for collaboration opportunities brokerage, and an equal opportunity for all VBE member organizations to get involved in potential VOs. The subordinate trust elements for this trust objective are addressed in Section 3.3.2.

c) Creating trust of external stakeholders to the VBE:

A VBE must be trusted by its external stakeholders, including invited organizations and customers. On the one hand, invited organizations must be convinced that the VBE environment is trustworthy for their businesses and, in addition, that they will benefit more than they would if they were to work individually. On the other hand, customers that create business opportunities in the market (to which VBE can respond by creation of VOs) must recognize and trust the VBE in order to accept its proposed bid. Consumers (end users of VBE results) also need to trust the VBE in order to decide positively on purchasing or accepting the VBE's products and services that have been produced / provided through VOs. The subordinate trust elements for this trust objective are addressed in Section 3.3.3.

3.3.1 Trust elements for creation of trust between organizations

There are *five potential trust perspectives* [Msanjila & Afsarmanesh, 2006b] that a trustor organization can assume, or choose from, for representing its "primary aspects" as a means to assess the level of trust in a trustee organization. These perspectives constitute the so-called "*trust perspective pentagon*" (Figure 3.5), where the detail inside this figure is represented in Figure 3.6. When a VBE organization needs to trust another VBE organization, five trust perspectives to be measured may be of interest or concern to the trustor organization, with the base assumption of their independence these perspectives include: Structural (STP), Economical (ECP), Technological (TEP), Managerial (MGP), and Social (SOP).

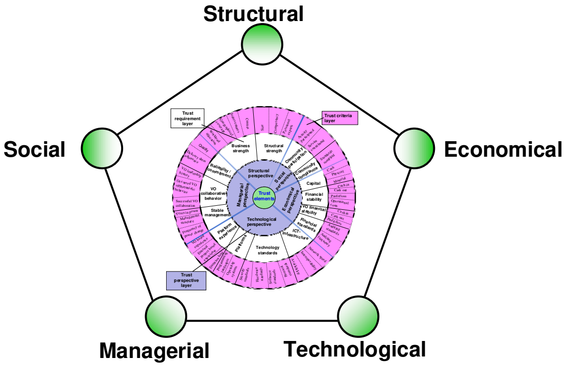


Figure 3.5: Trust perspectives pentagon for trust relationships between VBE members
The descriptions of these elements are provided in the paragraph above and further classification is provided in Figure 3.6.

In the Trust Management (TrustMan) system developed and addressed in this dissertation (later in Chapter 6), trust related data is stored and managed in a database. The TrustMan system provides functionalities and services for supporting different actors in the VBE, in order to perform tasks related to the management of trust among organizations in a VBE, including trust level assessment, trust relationship establishment, and trust creation. These functionalities require some assistance from domain/trust experts while being applied during the operation stage of the VBE life cycle. The TrustMan system is discussed in more detail in Chapter 6.

The assessment of level of trust in a VBE member organization occurs in three different cases. Firstly (case 1), for each VBE membership applicant, its *"base" trust level* needs to be assessed in order to be accepted as a member of the VBE. The base trust level is the minimum threshold value of trust level, which allows a member organization to keep operating in the VBE. Secondly (case 2), periodic assessment of the base trust level for all VBE member organizations is necessary, in order to control and preserve the trust balance at an acceptable level within the VBE. Tertiary (case 3) is when *specific trustworthiness* evaluation is requested by a trustor for certain "specific" purpose, such as for inviting a VBE organization to participate in a VO, or for appointing an organization to become VO coordinator, and so on. In such cases the trustworthiness of the organization must be assessed for that specific purpose [Msanjila & Afsarmanesh, 2007a].

In Section 3.2 we analyzed the causal influences among the trust criteria for the structural perspective as an exemplification of the HICI approach. The trust criteria and related customizations of trust perspectives are also used as an example in Chapter 5 for the formulation of mechanisms for assessing the level of trust in organizations. Trust criteria, their unit of measurement and their related causal analysis result for all five trust perspectives mentioned above are further described in Table 3.2, Table 3.3, Table 3.4, Table 3.5, and Table 3.6.

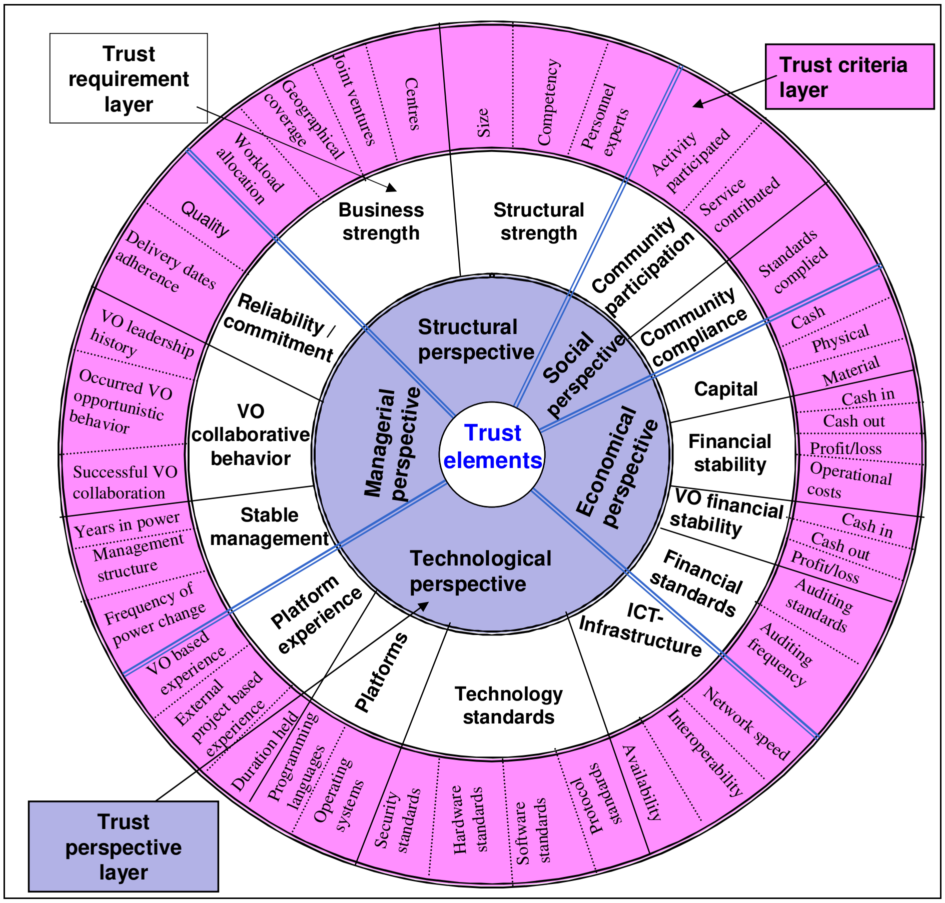


Figure 3.6: The wheel of general trust elements for VBE member organizations

The descriptions of these elements are provided in Table 3.2, Table 3.3, Table 3.4, Table 3.5, and Table 3.6. The classification of layers is based on the levels of measurability of trust elements as shown in Figure 3.1.

For the first two cases above (assessing base level of trust for a potential VBE member and a VBE member organization), the assessment of level of trust is based on a so-called set of *base trust criteria*. This set of base trust criteria is identified by the VBE administrator usually a priori to the establishment of the VBE, is announced to all VBE member organizations for transparency reasons, and is used for the assessment of their base level of trust.

For the third case, the evaluation of specific trustworthiness will be based on the so-called set of *specific trust criteria* identified by the trustor organization. Both the specific and the base trust criteria represent a subset selected among the list of *general set of trust criteria (VBE pool of trust criteria)*. Figure 3.6 shows the set of general trust criteria in the form of a wheel representing the three layers of trust perspectives, trust requirements, and trust criteria. As such, it illustrates the general trust criteria identified for VBE member organizations in respect to trust requirements and trust perspectives. Please note that, whenever needed, the general set of trust criteria for a VBE can be updated or extended by the domain experts with the help of trust experts. Please also note that the base trust criteria usually constitute a subset of the general set of trust criteria, as selected by the VBE administrator for this purpose. The selection of trust criteria made by the VBE networks that have been used to demonstrate our results is presented in Section 6.6.2.

A. Trust criteria subordinated to social perspective

Trust in an organization related to social aspects is needed to maintain the organization's moral acceptance within the market and within the society. In Section 2.3.6 we addressed the social aspects of trust in relation to establishing collaboration between organizations. Figure 3.6, among others, presents a set of trust criteria related to the social perspective. Table 3.2, presents the description for each trust criteria of the social perspective.

Table 3.2: Description of trust criteria related to social perspective

Trust criteria	Description
Activities participated ***(AP,** measured in: # of activities)*	Societies in which organizations operate their businesses do have some activities that enable each specific society to achieve certain goals that maintain smooth continuity. Such activities may include: voluntary cleaning of the surroundings, voluntary participation in emergencies (such as providing support to people on earthquake disaster), voluntary support for sporting events, etc. Although participating in these activities does not directly influence the performance and profit of organizations, it enhances the social trust of the community. This encourages the society to support the organization and thus sustain its continuity, for example, by purchasing its products/services, supporting its operations, and so on.
Services contributed ***(SC,** measured in: # of services)*	Various services are needed within a society to maintain the balance of life in the community and ensure the survival of the society such as related to the provision of health, education, etc. Organizations can enhance their trust on the basis of social aspects by supporting, contributing and facilitating the realization of such services. For example, contributing to disabled schools, providing support for students' transport, contributing to the purchase of medicine for outbreaks of diseases, etc.
Complied Standards ***(CS,** measured in: # of standards)*	Every society maintains certain standards with which each organization operating within the community must comply. Common ones include: environmental standards, financial standards, cultural standards, etc. Such standards can influence the organization's trustworthiness in the eyes of the society and compliance with these standards shows how organizations perceives themselves as part of and belonging to the respective society.

B. Trust criteria subordinated to economical perspective

A large set of trust criteria related to economical perspective needs to be considered to support the creation of trust in organizations to smoothen their collaboration. In Section 2.3.6 we introduced the economical aspect of inter-organizational trust. We also show in Figure 3.6 the trust criteria for the economical perspective in Section 3.3. Below in Table 3.3 we present a description for each trust criterion for the economical perspective.

Table 3.3: Description of trust criteria related to economical perspective

Trust criteria	Description
Cash capital (CC, *measured in: Euros)*	In finance and accounting, capital refers to financial wealth especially that is used to start or maintain a business. In economics, capital refers to the physical assets that are used in relation to labor and other inputs in order to produce products and services. In business, the term capital refers to the money that is available for investment. Here, we refer to cash capital as the amount of money available to an organization that can be or has been invested in its businesses.
Physical capital (PL, *measured in: Euros)*	In general, physical capital refers to any non-human asset made or adopted by humans (excluding money) and then used in production. Often, it refers to economic capital in some combination of infrastructural capital and natural capital, such as machinery, equipment, buildings and land, acquired by an organization and applied in its businesses.
Material (Operational) capital (MC, *measured in: Euros)*	Otherwise known as working capital, this refers to current assets minus current liabilities. Operational capital is a measurement of the number of liquid assets an organization has and those it can use in order to build its business. In general, companies that have a high operational capital can be more successful as they have the power to improve their operations.
Cash in stability (CI), cash out stability (CO), and profit/loss *(all three criteria measured in: Euros):*	Cash in refers to the amount of money that is received as a result of the daily business conducted by an organization. Cash in stability refers to the balance of the money that flow into the organization at a given period of time and the opposite of this is the *cash out stability,* which refers to the balance of the money that flow out of the organization. The difference between the cash in and the cash out gives the *profit/loss (net gain)* of the organization.
Operational costs (OC, *measured in: Euros)*	Operational costs are the daily expenses that an organization incurs in order to maintain its operations and thus these costs are usually subjected to specific opportunities.
VO cash in (VCI), VO cash out (VCO) and VO related profit/loss *(all three criteria measured in: Euros)*	These are similar to cash in, cash out and profit/loss respectively as described above, however, these refer specifically to achievements with respect to participations in VOs.
Auditing standards (AS, *measured in: # of standards)* ***and auditing frequency (AF,*** *measured in: # of times per year)**:***	an audit is an evaluation of an organization's financial performance that is carried out by competent, independent, and unbiased professionals known as *auditors*. The aim of an audit is to make an independent assessment based on a management's representation of their financial transactions using the organization's financial statements. The audit is also a means to ensure that the operational effectiveness of the internal accounting system is in accordance with approved and accepted accounting standards, statutes, regulations, or practices. Auditing frequency refers to the number of times that auditing must be done in certain period such as in one, two of five years.

C. Trust criteria subordinated to technological perspective

There are a number of trust criteria that organizations must examine and consider when seeking to enhance their technological related trustworthiness as shown in Figure 3.6. Below, in Table 3.4, we describe the trust criteria related to the technological perspective.

Table 3.4: Description of trust criteria related to technological perspective

Trust criteria	Description
Network speed (Broadband) (NS, *measured in: megabytes per second)*	In computer networks this refers to the rate of data transfer supported by a network connection such as the internet, local area network, etc. In order for organizations to match the need for fast and efficient communication, as well as the rapid exchange of information, they must possess and maintain reasonable bandwidth for their computer network.
Interoperability (IB, *measured in: # of systems)*	With respect to software, the term interoperability is used to describe the capability of different systems to exchange data via a common set of procedures, and to read and write in different formats and use different protocols. Organizations must possess interoperable systems and technologies to facilitate the setup of collaborations.
Availability (AV, *measured in: % of time)*	Refers to the proportion of time that a system is in a functioning condition. Systems and computer networks of an organization that participate in collaboration must advocate high availability.
Protocol supported (PS, *measured in: # of protocols)*	Refers to a set of guidelines that are used to guide communication between organizations through the use of an ICT infrastructure. Several communication and computing protocols are being used in today's world. Organizations are now confronted with heterogeneous protocols and must therefore be prepared to comply with as many of these as possible.
Software standards (SS, *measured in: # of standards)*	Standards enable heterogeneous software to interoperate. Organizations must ensure that their systems are developed based on established standards and must conform with as many of these as possible.
Hardware standards (HS, *measured in: # of standards)*	Unless applied in hardware, these standards are able to limit interoperability among technologies such as machines and other equipments. Organizations must be careful when purchasing hardware components or when manufacturing those components. They must conform to the available and specified hardware standards in order to optimize communications and collaboration with other organizations.
Security standards (SC, *measured in: # of standards)*	These standards are becoming more fundamental due to the fact that sensitive information is now frequently exchanged on the internet and stored on computers that can be accessed remotely. Security standards in relation to organizational systems have become fundamental to organizations to guarantee both the confidentiality and the privacy of stored and exchanged information.
Operating systems (OS, *measured in: # of operating systems)*	An operating system (OS) is a software program that manages the hardware and software resources of a computer. An OS performs basic tasks, such as controlling and allocating memory, prioritizing the processing of instructions, controlling input/output devices, facilitating networking and managing files. Operating systems have an important role in relation to both external communication and data sharing between

Trust criteria	Description
	organizations. Thus, organizations shall be prepared to apply any standard OS whenever it is a requirement for setting up the collaboration.
Programming languages (PL, *measured in: # of languages)*	A programming language is an artificial language that is intended to be used for controlling the behavior of a machine (often a computer). Like human languages, programming languages use syntactic and semantic rules to define meaning. They facilitate communication relating to the task of organizing and manipulating information, and many of these provide a way to accurately express algorithms. Programming languages adopted by organizations influence the chance to share and exchange technical and programming information, such as programming codes, with other organizations.
Experience in applying the technology in VOs (VO projects – VP, *measured in: # of projects per year)*	Technology can most broadly be defined as the material entities created by the application of mental and physical effort to nature in order to achieve certain values. An organization can demonstrate their capabilities related to using specific technology by showing its past experience with that technology in applying it in previous collaboration.
External project applied (EP, *measured in: # of projects per year)*	Organizations also participate individually in other businesses. For example, each organization may perform its daily activities serving its customers using the technologies it owns. The experience gained in such activities – once proved – can be used to show its experience with such technologies.
Duration held (YH, *in: # of years)*	This refers to the number of years that an organization has owned and has been using a certain technology.

D. Trust criteria subordinated to managerial perspective

A number of trust criteria related to the managerial perspective are shown in Figure 3.6. Below, in Table 3.5, we provide a description for each trust criterion.

Table 3.5: Description of trust criteria related to managerial perspective

Trust criteria	Description
Management structure (MS, *measured in: # supported structure)*	Various types of management structures are currently practiced in different kinds of organizations. The decision as to which management structure to implement is mainly linked to the purpose of an organization's existence and the nature of its business processes. In the literature, management structure is in fivefold, namely: simple structure, machine bureaucracy, divisionalized form, professional bureaucracy, and adhocracy. See further description in [Mintzberg, 1992]
Years in power (YP, *measured in: # of years)* ***and frequency of power change (FP,*** *measured in: # of years per term)*	The number of years a manager can stay in power in an organization depends on many factors, such as the nature of organization (business, educational, government, etc.), surrounding society (culture, country rules, etc.), the operating rules of the organization, etc. The frequency of power change influences: the level of experience that can be attained by managers, the possibility of exchanging power and the chance of learning from each other's leadership. Business organizations need highly experienced administration and therefore, allowing the managerial team

Trust criteria	Description
	to remain in power for a relatively long period is highly preferable.
***Opportunistic behavior (opportunistic occurred – OO,** measured in: # of opportunistic events)*	Refers to an ungentle action taken by an organization for the purpose of benefiting unethically more than others (e.g. quitting the collaboration once the organization has achieved its own goals or if the risks are expected to arise). In competitive environments, this seems natural because the focus of organizations is to acquire customers without considering long-term relationships with others. In collaboration, however, organizations must collaborate with others in order to jointly respond to opportunities. Therefore, opportunistic behaviour in collaborations is discouraged.
***Successfully VO collaborations (SV,** measured in: # of projects)*	An organization can improve in relation to both its experience and its performance by participating in as many VOs as possible. The trustworthiness of organizations is assessed to support the selection of the most trustworthy organizations to invite into the VO. This indicates that an organization which frequently participates in VOs has been assessed trustworthy by different trustors.
***VO participation as organizer/leader (VL,** measured in: # of projects led)*	Previous VO participations as a leader indicate that the organization has been perceived trustworthy by other VO partners. Organizations are encouraged to participate in collaborative activities as leaders or organizers in order to enhance their managerial trustworthiness.
***Quality of products/services achieved (QA,** measured in: # of projects)*	The quality of products and services that each organization delivers to customers for each project not only ensures customer loyalty, but may influence the decision made by those customers to accept offers that the organization makes on future occasions. Therefore, organizations must ensure that they produce products or provide services that meet the quality demanded by the customers.
***Adherence to delivery dates (AD,** measured in: # of projects)*	Organizations should make sure that they adhere to delivery deadlines for each project agreed by the customers.

E. Trust criteria subordinated to structural perspective

The structural perspective is in detail described in Section 3.2 and its subordinate trust criteria are shown in Figure 3.6. Trust criteria for this perspective are described below.

Table 3.6: Description of trust criteria related to structural perspective

Trust criteria	Description
***Size of an organization** (measured in: # of employees)*	Refers to the number of people employed by the organization. Increase in number of employees indicates the availability of human resources that can be allocated when collaboration opportunities are brokered. The readiness of organizations to quickly act on emerging opportunities due to the availability of human resources enhances the structural trustworthiness of the organization.
***Geographical coverage** (measured*	Refers to the number of regions, such as cities, zones, states, countries and continents, in which an organization operates its businesses. As the

Trust criteria	Description
in: # of cities)	coverage increases, the organizations enhance their connections with others, which may ease the establishment of the trust relationships that are needed to smoothen the intended collaboration.
Competences *(measured in: # of different competencies)*	Competency influences the performance of an organization and it is currently a fundamental requirement for collaboration. An organization that possesses a number of different competencies has a better chance of sharing and complementing competencies with other organizations. This can lead to daily interactions between organizations which in turn enhances their trustworthiness.
Personnel expertise *(measured in: # of experts in organization's businesses)*	Refers to the available personnel skills and knowledge in different areas/domains that can be applied in emerging collaboration opportunities. As an organization acquires more experts, its structural trustworthiness improves, which may lead to more invitations to participate in VOs.
Joint ventures *(measured in: # of organizations)*	Refers to other partners, such as agents, alliances, and so on which are able to represent the organization in its business. Such joint ventures are now common, for example, among flight companies, where passengers who buy tickets from a different company may find themselves flying with another company. These types of joint ventures indicate a certain level of reliability of the company in its businesses and also in its trust with respect to previous cooperation.
Centres *(measured in: # of centres)*	Refers to the number of offices, service delivery points, production centres, branches, etc., of an organization. The number of centres indicates how distributed the organization is and how easily it can deliver products/services to its customers.
Workload allocation *(measured in: # of specified unit)*	Refers to the *maximum level* that an employee of a certain organization can be exploited. The level of workload varies depending on the domain, business environment, legal system, and so forth. E.g. the workload of doctors in medical organizations is typically measured in terms of "the number of patients to which a single doctor can attend in a day", while the workload of employees in a business organization is typically measured in terms of "the number of hours that each employee must be at work". Similarly in the manual production/processing businesses, this can be measured in terms of the amount or number of items produced per day.

3.3.2 Trust elements for creation of trust from members towards the VBE administration

The trust of a VBE member organization towards the VBE administration must be created and maintained in order to enhance the interests and loyalty of the member with respect to the VBE establishment, a trust which in turn also increases its active involvement in VBE's activities. In this thesis we have identified four trust perspectives that together represent the primary aspects of this trust objective and can be used to create trust in a VBE member organization towards a VBE administration (Figure 3.7) where the detail inside this figure is represented in Figure 3.8 [Msanjila & Afsarmanesh, 2007a]. As such, the approach suggests that the VBE member organization should be able to access the necessary information related to these four trust perspectives. Figure 3.8 shows the general trust criteria for trust between the VBE member and the VBE administration.

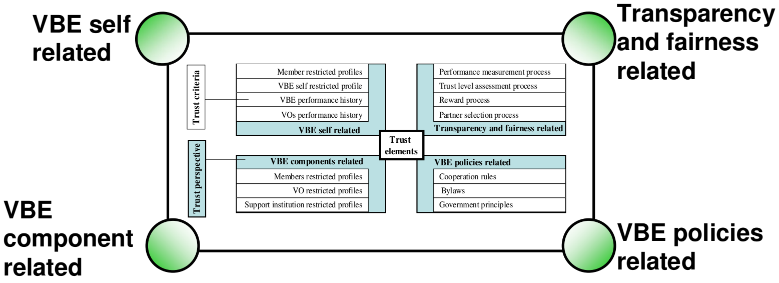


Figure 3.7: Rectangle of trust perspectives for trust in members to the administration
The descriptions of these elements are provided below and further classification is provided in Figure 3.8.

Furthermore, a VBE member organization needs to be convinced that the VBE administration is trustworthy in order to join and remain active in the VBE. For example, since VBE member organizations continuously compete to win an opportunity to participate in VOs that are configured within the VBE, they must be convinced that the VBE administration is impartial and that the selected member organizations for each VO are chosen on the basis of their qualifications. Below we address four trust perspectives for this trust objective and provide the subordinate trust elements under each trust perspective as shown in Figure 3.8.

i) ***VBE policy related perspective:*** VBE policy addresses the plan of action that guides VBE decisions and activities. Policies can be understood as political, management, financial, and administrative mechanisms for reaching explicit goals. For VBE environments, the main aspects related to trust, and the policies that must be accessible to member organizations are illustrated in Figure 3.8.

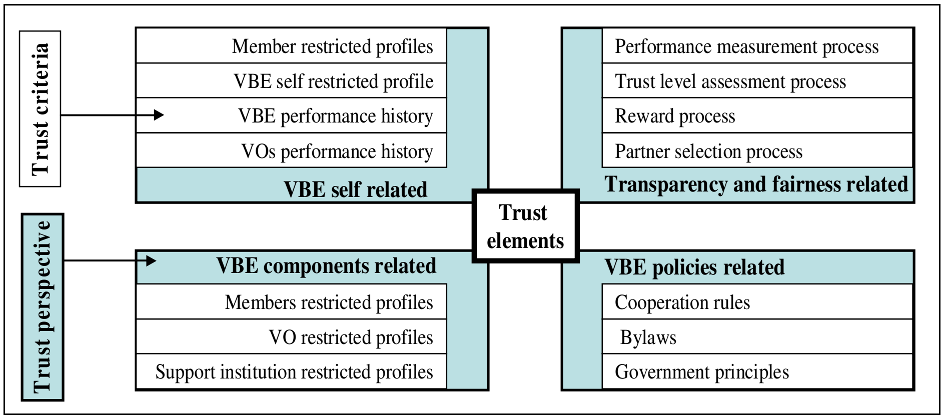

Trust criteria
Trust perspective
Member restricted profiles
VBE self restricted profile
VBE performance history
VOs performance history
VBE self related
Performance measurement process
Trust level assessment process
Reward process
Partner selection process
Transparency and fairness related
Trust elements
VBE components related
Members restricted profiles
VO restricted profiles
Support institution restricted profiles
VBE policies related
Cooperation rules
Bylaws
Government principles

Figure 3.8: Rectangle of trust elements for trust in members to the administration
This figure shows a classification of trust criteria per perspective for the objective of creating trust from members to the administrator as described in this section.

ii) ***Transparency and fairness related perspective:*** A VBE administration must be transparent and fair to all VBE member organizations. In particular with respect to some of the main transparency issues that are sensitive here and refer to the steps taken or activities performed during the entire process of assessing the level of trust in member organizations and measuring their performance, which in turn is a key source of trust related data. Fairness refers to the fact that as much as possible should constitute a formally unified reasoning mechanism and approach in relation to the decisions made in the VBE, and that all aspects are as "rational (fact-based)" as possible. For this purpose, information about trust elements (Figure 3.8) must be accessible by all VBE members.

iii) ***VBE component related perspective:*** The VBE component-related perspective refers to the components that constitute the VBE. The main component of the VBE is its member organizations and its VOs. Another component of the VBE constitutes the supporting institutions. A VBE member organization that wants to assess the trustworthiness of the VBE and its administration will need the information related to the VBE structure and its components. The organization can be provided with information for three trust elements for this perspective, as represented in Figure 3.8.
iv) ***VBE-self related perspective:*** When it comes to trusting the VBE, member organizations must also be provided with information that will serve to build a positive picture of the VBE as a whole. Here the relevant information needs to address the performance of VOs and other information about VBEs that are restricted for its members, as in Figure 3.8.

3.3.3 Trust elements for creation of trust from external stakeholders towards the VBE

This section addresses another main VBE trust objective, namely the creation of trust between external stakeholders and the VBE. By external stakeholders we refer to the two kinds of actors, namely a potential organization that aims to become a VBE member, and a customer that aims to either buy VBE products or recommend the VBE for a bid made for a collaboration opportunity. There are two ways that lead to an organization becoming a member in the VBE. Firstly, when the respective organization finds the VBE an essential environment for its businesses, and thus submits an application for membership. In this case, in addition to other assessments such as competency compliance, the new membership applicant will be assessed to analyze whether it meets the required base trust level. This manner of becoming a VBE member and the required trust level assessment is addressed in Chapter 5. Secondly, when a VBE identifies gaps, such as the necessary competencies, it might search for some external competent organizations in the market to invite. Therefore, the process of such an organization becoming a VBE member is initiated by the VBE itself by means of invitation. Nevertheless, in both cases organizations will need to create trust for the VBE and its suitability for their businesses.

Similarly, customers must also be supported to trust the VBE establishment. The VBE operates in a common market where there might be other competitor VBEs and even individual powerful companies. To pursue the customer to either buy VBE products or recommend the VBE for a collaboration opportunity, the customer must be convinced about the trustworthiness of the VBE. To support the achievement of this trust objective, we identified three trust perspectives in our research that external stakeholders can assume as primary aspects when building trust in the VBE. External stakeholders must be provided with information based on preferred trust perspectives as shown in Figure 3.9 where the detail inside this figure is represented in Figure 3.10.

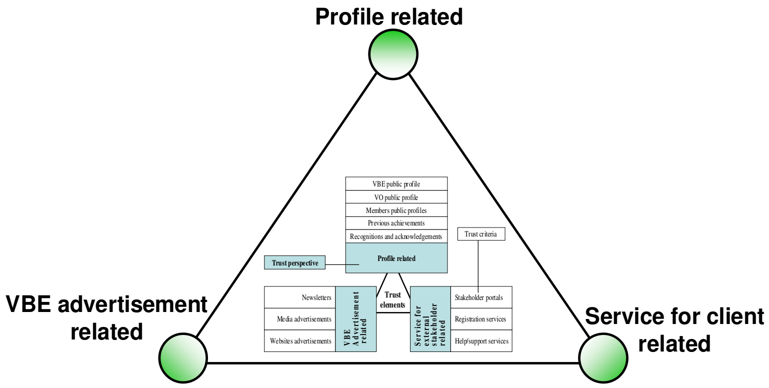


Figure 3.9: Triangle of perspectives for creating trust of external stakeholders to the VBE
The descriptions of these elements are provided in following paragraphs and further classification is provided in Figure 3.10.

Therefore, in order to accept the invitation to join or decide to apply for membership, the organization will need to trust the VBE. Moreover, in order to select the VBE (e.g. when a customer wants to provide a tender or needs to accept the VBE for a business opportunity), customers will need to trust the VBE. We recommend providing these external stakeholders with the information related to the three specific trust perspectives described below, and also summarized in Figure 3.10:

i) ***Profile related perspective:*** This information will enable the external stakeholder to understand the constituents of the VBE and its related competencies. It includes: (1) VBE public profile including list of members and list of VOs, (2) VO public profile including partners and VO performances, (3) VBE members' public profiles, (4) Previous VBE/VO product/service recognitions, and (5) Specific previous VBE/VO achievements.

ii) ***VBE advertisement related perspective:*** As in the normal business world, VBEs will also advertise their products and services (offered through VOs) to the market. Information on advertisements that are usually made can indicate the capability of the VBE to support its members for business opportunity brokerage and also its capability to reach its customers. Such information can include the following: (1) Copy of advertisements in the media, (2) Link of advertisements in websites, and (3) Newsletters.

iii) ***Service for client related perspective:*** An external stakeholder, such as a customer, can be convinced to trust the VBE on the basis of the availability of services that it needs and the quality or comprehensiveness of the support that will be provided when acquiring these services. This includes: (1) Member or customer portal, (2) Membership or customer registration functions and (3) Help or support services.

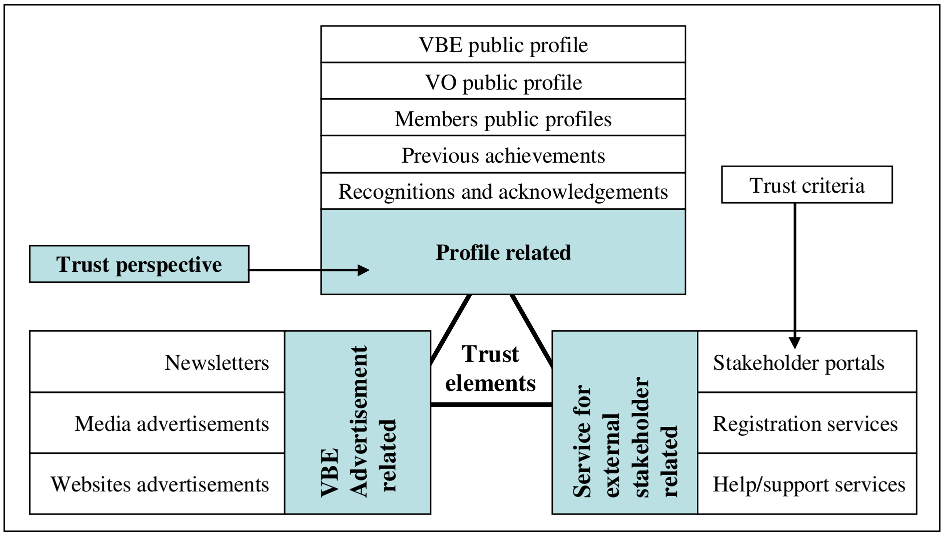


Figure 3.10: Triangle of elements for trust in external stakeholders to the VBE

This figure shows a classification of trust criteria per perspective for the objective of creating trust from external organizations to the VBE as described in this section.

3.4 Chapter discussion and conclusion

This chapter presents the HICI approach, which is used to identify trust elements for organizations. HICI constitutes three stages that address: the identification and characterization of trust elements, analyzing the impact of relations between trust elements and the performance of organizations (and thus addressing their levels of trust), and analyzing the causal influences between the trust criteria, the known factors and the intermediate factors.

By involving industrial VBE networks at the requirement analysis stage as well as applying the HICI approach, we were able to identify and characterize a set of general trust elements. A set of generic trust elements for organizations is presented in this chapter. These trust elements are categorized into their three respective main trust objectives as characterized by applying the HICI approach, namely for the building trust from: (1) a member organization towards other member organizations, (2) a VBE member organization towards the VBE administration, and (3) an external stakeholder towards the VBE and its administration.

This chapter has thus addressed two main research questions introduced in Section 1.5. It addressed the main research question MRQ1 by presenting the approach for identifying and analyzing trust elements for organizations. It addressed MRQ3 by introducing concepts regarding a multi-criteria-based approach for assessing level of trust in organizations. It further addressed MRQ3 by presenting the causal analysis approach which is applied to formulated mathematical equations. The formulated equations are further applied to the development of mechanisms for assessing trust level of organizations (Chapter 5). In Chapter 7 an integrated overview is presented of how all research questions of Section 1.5 are addressed in this thesis.

In response to the research questions as mentioned in the above paragraph, this chapter provides two key contributions of this thesis, namely: (i) the proposition of the systematic approach (HICI) for identifying, characterizing and analyzing trust elements for organizations, and (ii) the presentation of the comprehensive general set of trust criteria for organizations. We have also addressed the characterization of performance data in terms of trust criteria, which is the main input data to the assessment of trust level of organizations (see Section 3.2.2). Based on this characterization it is possible to identify specific trust criteria whose values must be improved to enhance the trust level of a particular organization. The modeling of classes for the identified trust elements is presented in the next chapter (Chapter 4). The analysis of inter-relations among trust criteria in terms of causal influences, whose results provide a base for the formulation of mechanisms for assessing trust level of organizations, is presented in Chapter 5.

Chapter 4

Conceptual modeling of trust elements

The perceptions, preferences and interpretations of trust differ among the organizations, as addressed before, depending on their purposes for establishing trust relationships with others. As a result, different organizations consider different aspects when analyzing trust in other organizations. Thus a large number of aspects must be properly specified and modeled to comprehensively cover the trust objectives of organizations. In addition to a survey of existing work related to modeling trust, this chapter analyzes and proposes three specific modeling formalisms (namely, record-based, object-based, and ontology-based formalisms) that best represent trust relationships among organizations and presents some examples.

This chapter has been partially published in the International Journal of Technology Transfer and Commercialization [Msanjila & Afsarmanesh, 2007b].

4.1 Introduction

Considering the key role that trust plays in facilitating collaboration within VBEs, understanding the base concepts relating to inter-organizational trust is necessary for creating successful collaborative networks of organizations. This chapter examines conceptual modeling of trust relationships between organizations, which fundamentally contribute to creating a common understanding of inter-organizational trust among its different actors. In Section 4.2 we first present a survey of related research on trust models and subsequently, in Section 4.3, we address the conceptual modeling of trust relationships between organizations that assist us with characterizing inter-organizational trust. In Section 4.3.1 we present the main trust parameters applied in developing models of inter-organizational trust relationships. In Sections 4.3.2, 4.3.3, and 4.3.4 we present three modeling formalisms that are applied in this thesis to model different aspects of trust, namely: *object-based conceptual formalism, record-based conceptual formalism and ontology-based conceptual formalism*, respectively.

4.2 Related trust models in research and development

Research on trust is characterized by a substantial diversity in disciplinary background, methodologies, models, and definitions. These differences result mainly from different actors' perceptions of what it means to trust. By the same token as the differences in interpretation of trust, diversity also exists among the current trust models developed by these same researchers. Several examples of trust models are discussed below, and although they are originated and applied in environments different from VBEs, each one presents some aspects that are related to the VBEs:

i) An integrated model of trust in e-commerce

Electronic commerce, commonly known as ***e-commerce***, refers to buying and selling of products or services over electronic systems such as the Internet and other computer networks. A wide variety of commerce is conducted in this way, spurring and drawing on innovations in a number of business aspects including: electronic money transfer, supply chain management, internet marketing, online transaction processing, electronic data interchange, inventory management systems, automated data collection systems, etc. Modern e-commerce typically uses the World Wide Web, at least at some point in the transaction's lifecycle, although it can encompass a wider range of technologies, such as e-mail as well. A large percentage of e-commerce is conducted entirely electronically for virtual (non-physical) items, such as access to premium content on a website, issuing electronic tickets for flights, etc. However, other e-commerce transactions may also involve the transportation of physical items to buyer in some way once the ordering and payment are accomplished electronically.

Past research has pointed out a number of challenges that need to be addressed in order to facilitate the full realization of e-commerce. Some few challenges to exemplify here are: authentication of users with their specific and unique identification and role, assurance of the privacy of involved actors, support for online negotiation, management of online payments, personalization of e-commerce services, establishment of suitable infrastructures, creation of support software, etc. [Keen, 1999]. In addition to these challenges, one more key challenge, related to research addressed in this thesis, is the establishment of trust among actors involved in the e-commerce transactions. In fact transactions taking place in e-commerce are similar to the business processes conducted and/or supported in VBEs, in the sense that they are both handled virtually and in distributed environments. Thus the concepts of trust among actors involved in e-commerce transaction and in particular, the e-commerce related trust models can be fundamental input to understanding and modeling inter-organizational trust.

To support the understanding of trust among actors in e-commerce and its related transactions, Kini and Choobineh [1998] have developed a theory that provides a strong theoretical foundation for a set of evaluating factors influencing trust related behaviour. This model is based on the fundamental assumption that trust in an online system is a function of the following four dimensions (as also shown in Figure 4.1): (1) characteristics of the person making the e-commerce transaction, (2) the online system itself that supports the required transactions, (3) the task for which the system is being used, and (4) trust related information and its source environment.

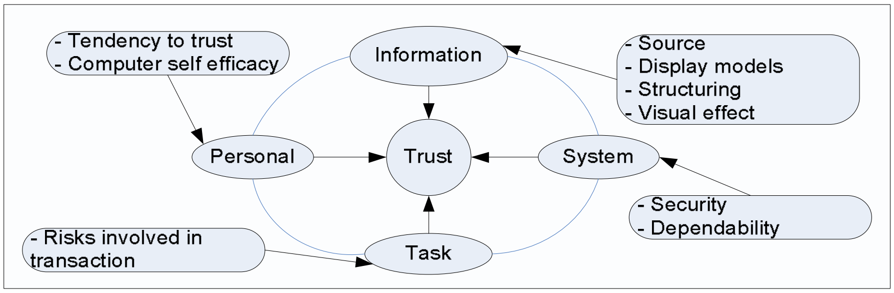


Figure 4.1: An integrated model of trust for E-commerce application

Based on concepts as presented by Kini and Choobineh [Kini & Choobineh, 1998] this figure shows the influence of four e-commerce related factors and their related aspects on the process of creating trust among actors, as discussed in the following paragraphs.

As shown in Figure 4.1, all four of these dimensions influence the creation of trust between the partners involved in the e-commerce transactions. In their study, Kini and Choobineh [1998] proposed that it is the ***personal*** characteristics of an individual which determine his/her readiness to trust. Other researchers who have studied individuals' trusting behavior also contend that the readiness to trust is shaped by specific developmental and social-contextual factors [Lee & Turban, 2001]. In this model, this readiness characteristic is called *Tendency To Trust* (TTT). This research demonstrated that people with a high TTT are more willing to trust others when confronted with new situations.

To further understand the TTT in relation to specific transactions, it is important to study the kinds of ***task*** that necessitate trust, and to focus on means of fostering and developing trust in these tasks in order to ensure that *e- commerce systems* can be developed for a wide range of applications.

The sensitivity of a ***task*** being executed using the e-commerce technology might make the creation of trust among e-commerce actors difficult. For example, whether the task needs to be accomplished completely online or some physical processes are needed. Also, the gains expected by actors and the risks that can emerge by handling the task using e-commerce technologies, as compared to other approaches such as physical transactions, might influence the decision of an e-commerce actor to trust others.

The characteristics of the ***system*** with which the user interacts play a critical role in the development and preservation of trust between participating partners in e-commerce-based transactions. Several studies have shown that security is a main factor in the success or failure of online businesses [Msanjila & Afsarmanesh, 2007c]. Other important factors that influence the creation of users' trust in the online system are their perceptions of the dependability and reliability of the system itself.

The ***information*** which needs to be exchanged to support e-commerce transactions has an important role in realizing the required trust among e-commerce actors. The content of information which needs to be exchanged among e-commerce actors must be as accurate, valid, up-to-date and complete as possible. Furthermore, the reputation of the environment where the information is collected *(source's environment)* and usability of environment where the e-commerce actors access the information *(online system interfaces)* might influence the decision of actors to trust others. For example, the usability of the system influences the willingness of customers to in detail read the online advertisements of products and services and thus decide on which provider to trust. The environment presented by the system – user interfaces - should be correctly perceived and understood by users in relation to the presentation and structuring of the information. Therefore, visualization and display models are critical issues that must be taken into account in order for the information to be successfully exchanged among e-commerce actors. The effects of system's user interfaces should be studied in order to guide the design and implementation of suitable interfaces. In particular, it is important to identify whether different presentation modes, such as websites based on frames, multimedia, dynamic/static website, and so on, affect the creation of trust among e-commerce actors using online systems.

The external environments –surrounding environments such as the competitor markets – might also influence the creation of trust between actors by providing them with complementing or contrasting information. It also contributes to the overall perception of the reliability, security, privacy, dependability, etc. of a system supporting the e-commerce transactions. It is important also to understand whether trust in a system can be manipulated by providing information on possible external impacts relating to relevant aspects of the system.

Relevance to our research: As described earlier in this section, the virtual and distributed nature of e-commerce transactions is similar in the way business processes are handled and supported in VBEs. In relation to the work addressed in this thesis, the approach for characterization of elements that are included in the e-commerce trust model, as exemplified here, is relevant and complementary. Specifically, concepts presented in this model are applied in our model to analyze a number of trust related aspects among organizations in VBEs, as addressed below:

- *Trust related information to be exchanged among organizations*: We have applied the concepts presented by this model to analyze the content of information that is needed to be provided to a trustor organization in order to trust a trustee organization. Applying the knowledge gained through learning this model we have characterized the content of organizational data related to trust on the basis of five aspects, namely: "*why", "what", "when", "how" and "who"* as further addressed in Section 2.4. We have also applied the concepts presented by this model to analyze the need for information to be accurate, valid, up-to-date and complete for the purpose of enhancing the effectiveness of the process for creating inter-organizational trust.
- *Technological aspects supporting organizational collaboration*: We have considered the concepts presented by this model to analyze the influence of technology (related to technological perspective – see sections 2.3.6, 3.3.1 and 5.5) such as information systems, on the process of creating trust among organizations. The success of creation of trust between collaborating organizations is influenced by a number of various aspects related to the technological perspective. Information and communication systems that are applied by an organization or by the VBE to facilitate the collaboration among organizations can influence the decisions made by those partners about trusting each other. System related aspects, such as security, privacy, reliability, etc., unless handled properly by the VBE and by organizations can negatively influence decisions made by organizations to provide their trust related data to the VBE administrator or the trustor organization. So, there will be a lack of trust related data and as a result organizations will face difficulty in trusting each other.

ii) A trust model for inter-organizational network effectiveness

This trust model has been proposed as a means to support and provide guidelines, and act as a driver, to organizations that are participating in cooperation/collaboration networks [Ahuja, 2000]. The aim of this model is to increase the chance of an organization for achieving their common or compatible goals, and thus improving the effectiveness of their collaborative network. The focus of this model is on how inter-organizational networks can benefit from and influence strategic resource acquisition (Figure 4.2). This proposed model addresses factors relating to the structural and relational dimensions of social capital built between organizations in a collaborative network. On the basis of this model, organizations can analyze the effectiveness of their network in relation to the following:

- *How collaboration among organizations influences the potential for achieving common goals.*
- *How achievements of common goals improve the network's effectiveness.*
- *How trust affects organizations' collaboration especially in relation to sharing and exchanging information, resources, etc.*
- *What are the relations between network performance and individual organization's performance?*

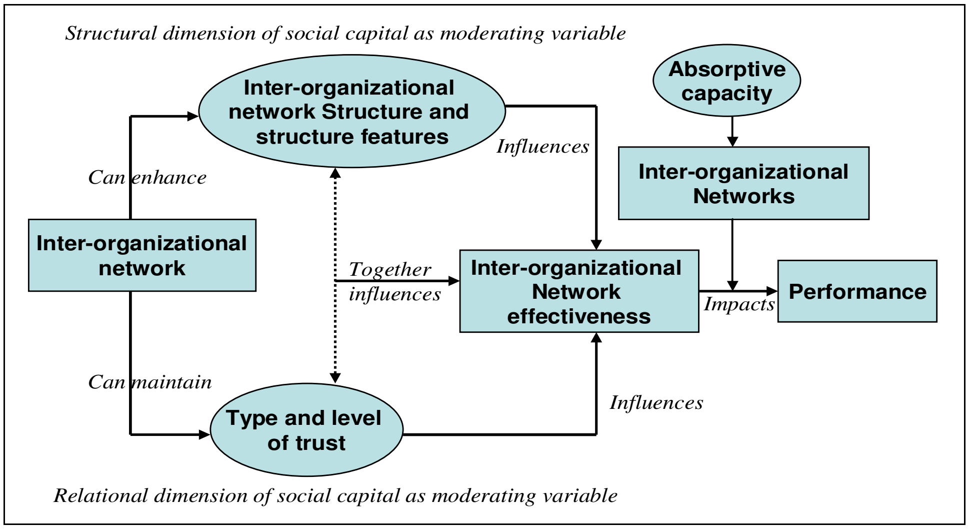

Structural dimension of social capital as moderating variable
Inter-organizational network Structure and structure features
Absorptive capacity
Influences
Inter-organizational Networks
Can enhance
Inter-organizational network
Together influences
Inter-organizational Network effectiveness
Impacts
Performance
Can maintain
Influences
Type and level of trust
Relational dimension of social capital as moderating variable

Figure 4.2: Conceptual model for trust and network effectiveness

Based on the concepts presented by Ahuja [Ahuja, 2000], this figure shows the inter-relations between trust and organizations' performance and other related aspects.

A collaborative network can ultimately enhance the performance of its individual organizations by supporting different forms of collaboration which best fit the needed response to acquired opportunities. For example, an organization's innovative capabilities are positively impacted by both direct and indirect forms of well-established communication with other organizations. This communication enables knowledge sharing between the cooperating or collaborating organizations and the opportunity for them to provide each other with complementary skills [Msanjila & Afsarmanesh, 2007a]. These different forms of collaboration and their specific transactions reflect different organization configurations in collaborative networks [Ahuja, 2000].

Researchers have explored the impact of collaborative network configurations, focusing on the number of involved organizations and the hierarchies in making decisions, on outcomes and effectiveness of their collaborations [Human & Provan 1997; Gloor, et al., 2008]. The results indicated that the level and range of performances achieved by organizations in networks might be influenced by the number of involved organizations and the manner of their involvement. For example, a network with large number of member organizations has high chance of internally constituting a large set of competencies and thus is able to quickly and efficiently respond to emerging business opportunities. The results also indicated that in a flat network in which decisions are collaboratively made (decentralized network) there is high chance of making acceptable and effective decisions by all involved organizations.

Although communication between organizations alone can represent a significant level of sharing and exchanging resources, this does not guarantee the actual transfer or exchange of strategic resources in the network. There are three fundamental barriers that encumber the transfer of strategic resources among organizations in the network [Szulanski, 1995; Hurmelinna-Laukkanen & Blomqvist, 2007]:

- the receiver's lack of absorptive capacity;

- causal ambiguity within the interactions;
- a weak relationship between the source and the receiver.

It was observed that trust helps to overcome all three of these barriers and that it also encourages an important condition for the exchange of resources to occur, namely the *motivation* [Ahuja, 2000]. Without trust, organizations will be reluctant to share resources due to the fear of possible risks that might arise, such as the opportunism from other collaborating organizations. This model implies that the level of trust affects the number and level of resources that can be exchanged. It also implies that the level of trust is related to the difference between the number of resources that organizations are willing to transfer and the amount that they are actually able to transfer. Consequently, the effectiveness of the collaborative network is dependent on the level of trust from its member organizations. This indicates that the amount of resources acquired through inter-organizational networking is related to the balance of trust levels between organizations.

Relevance to our research: As proposed earlier in this thesis (Section 3.2.2), the main input data to the assessment of the trust level of an organization is its performance data. The performance of the VBE as a whole and its configured VOs, represent the collective performance of all VBE involved organizations. Different aspects presented in this model which influences the performance of both – the network and the member organizations – such as the absorptive capacity of organizations, causal ambiguities within the interactions, the willingness to exchange and share resources, etc. - are of particular importance for our model of trust.

We have considered the concepts presented by this model to better understand how VOs need to be configured, and especially related to constituent partners that are selected from the VBE, to enhance the chance of optimizing the performance of both individual organizations as well as the VO itself, which in turn will enhance their trust level. As such, a VO should be configured constituting the set of most trustworthy partners in the VBE for each specific trust objective, as described in Section 6.4.2 (see Service 2) and Section 6.6.1 (see Module 6). As presented by this model, strong trust among organizations has positive impact on the effectiveness of their collaboration and their individual organization’s performances, which in turn shows that there is a causal feedback between trust in an organization and its performance in collaborative activities (as described in Section 3.2.2).

iii) FIRE: Trust model for open communities

An open community is a group of people that primarily interact via communication media, such as letters, telephone, email or Internet rather than face to face; for social, professional, educational or other purposes. If the mechanism applied to support the interactions among actors is a computer network, such as the Internet, then the community is called *an online community*. The ability to interact with like-minded individuals instantaneously from anywhere on the globe has considerable benefits, such as possibility to acquire knowledge from any place in the world. But these open communities have bred some fear and criticism mostly due to their virtual nature. It has been stated that these communities can serve as dangerous networking or hunting grounds for online criminals, such as identity thieves and stalkers, with children particularly at risk [Sharratt & Usoro, 2003]. Of particular interest to our research is how the trust of the involved actors is assessed, analyzed and assured. One source of information needed to analyze and understand trust of actors in open online communities is the reputation of each actor.

FIRE - an acronym that is created from first two letters of the word '**fi**des', which is Latin for ‘trust’, and the first two letters of the word ‘**re**putation’ - is a reputation-based model of trust that has been proposed as a means to support a common understanding of trust between actors in open communities [Huynh, et al., 2004]. It provides an explicit representation of uncertainties, yet is only used to add weight to different nodes (actors) during the complete trust integration (creation) phase. It also employs a very simple approach for the aggregation of reputation information. The modelers enhance the performance of their model by separating different types of trust and reputation, but they do not reach the level represented in the trust model. The FIRE trust model integrates the following four different types of trust and reputation aspects (addressed in Section 2.3):

- *Interaction trust* resulting from past experience of direct interactions,
- *Role-based trust* defined by various role-based relationships between the actors,
- *Witness reputation* built from reports of witnesses about an actor's behaviour,
- *Certified reputation* built from third-party references provided by the actor itself.

The inter-relation between trust and reputation is not clear in this model and in particular, how the data on reputation is manipulated while analyzing trust of actors. Therefore, the function of evaluating trust may fail to account variations of reputation when the reliability of the actor's behaviour changes with time.

Relevance to our research: Although the trust model for open communities addresses the trustworthiness of individuals, the nature of the environment in which this model is applied have some similar characteristics to those of the VBEs – mainly, its virtual collaboration nature. Therefore different aspects related to analyzing trust of individuals in open communities, who can virtually interact without physically knowing each other, are relevant input for studying trust among the VBE member organizations, as addressed in Sections 2.2.

iv) Taxonomy-based trust model for supporting an understanding of multi-agent systems (MAS)

In recent years there has been a significant growth in the field of multi-agent systems in both research and practice. As applied to collaborative networks, an agent represents an organization rather than an individual or a system. One challenging issue in this field relates to the provision of support, which is necessary to facilitate cooperation between different agents and is fundamentally related to a computation of their reputations. Several researchers addressing MAS have discussed this challenge and suggested a number of reputation models that appear in the literature offering solutions to this problem. However, most of these solutions introduced specific concepts, terminologies and specific ways to represent reputation models and manipulation mechanisms [Korba & Song, 2003]. Consequently, it is difficult to achieve a "hypothetical understanding" of reputation evaluation among agents using different reputation systems [Pinyol et al., 2007]. To address this problem Pinyol et al., [2007] have proposed a trust model based on ontology (taxonomy) that aims to support agents to achieve the required level of common understanding of trust and, in particular, the mechanism they use for assessing reputations. A number of characteristics are considered for this purpose and included in the ontology, as illustrated in Figure 4.3. The key elements which the model examines are an agent's belief and its social evaluation, which are affected by a number of other subordinate elements, as shown in Figure 4.3. The model proposes a fundamental solution that can be implemented for exchanging the results of social evaluations of agents using different reputation models within the same multi-agent system paradigm.

Relevance to our research: Supporting the VBE member organizations within a network in achieving common understanding on concepts related to their trust, is as important as the creation of the trust itself. The taxonomy based model is developed to support agents with achieving common semantics on related reputation based systems. This model and its constituent concepts are consider in our research to understand how the concepts of inter-organizational trust need to be classified, and later on to be presented to organizations for the purpose of enhancing their understanding of trust concepts as applied in the VBE environment as further addressed in Section 4.3.4.

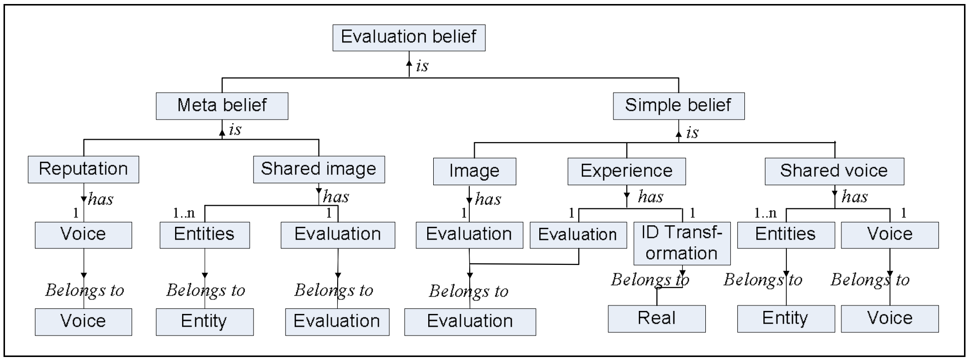


Figure 4.3: The taxonomy, membership relations, and components of evaluation of belief [Pinyol et al., 2007]

Based on the concepts presented in [Pinyol et al., 2007] this figure shows the examination of agent's belief and social evaluation and their subordinate elements for supporting common understanding among agents.

v) Federation for Identity and Cross- Credentialing Systems (FiXs)

This trust model is developed by FiXs [www.fixs.org]. The Federation for Identity and Cross-Credentialing Systems (FiXs) is a coalition of commercial companies, government contractors, and non-profit organizations whose mission is to establish and maintain a worldwide, interoperable identity and cross-credentialing network. This network is built on enforced security, privacy, trust, standard operating rules, policies, and technical standards. The FiXs network verifies and authenticates the identity of personnel seeking to enter the U.S. military installations and other government-controlled areas, as well as the commercial sites tied to the network. FiXs provides a trusted mechanism for federated identity infrastructure within and between public and private sector organizations with accuracy through the application of a so-called "Federated Trust Model". The network services supported by the trusted mechanism can be accessed worldwide, in remote or fixed environments, wired or wireless, and in real-time. A key component to the network integrity is its strong credential authentication and revocation processes, as governed by the FiXs operating rules.

The Federated Trust Model defines an underlying foundation that guides the common operating rules and legal procedures of the Federation of Identity and Cross-Credential Systems. It enables all participants and advisors to keep their existing security systems and policies intact, while strengthening their credentialing processes, in order to achieve balanced levels of trust within a shared infrastructure. The model is based on the concepts of community trust and brokered trust (Figure 4.4) [FiXs, www.fixs.org].

Relevance to our research: The trusted mechanism that supports organizations' access to network services, and the trust model which defines the common operating rules and legal procedures for collaboration, are the fundamental concepts applied to the establishment of trust among interacting actors who use the federated identity infrastructure. VBE Member organizations are typically in geographically dispersed locations. Therefore, the concept of federation introduced in this trust model helped us to understand and learn about how the analysis of trust among organizations can be performed when considering the need for interoperability among their systems. As such, the interoperability aspect of organizations is analyzed, considering the level by which the organizations' information systems meet the following elements of the VBE: formulated policies, operating rules, security guidelines, specified architectures, etc. Furthermore, these concepts are applied in the thesis for better understanding of the need for sharing and exchanging information and knowledge between VBE member organizations and the influence of the results of these processes on inter-organizational trust relationships as addressed in Sections 2.4 and 2.5.

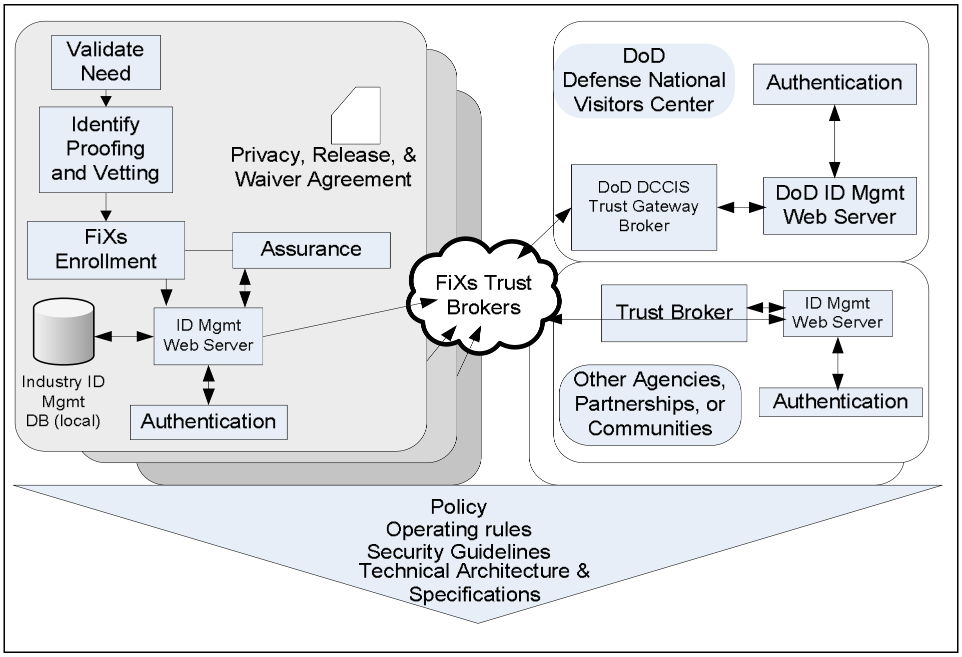

Validate Need
Identify Proofing and Vetting
FiXs Enrollment
Assurance
Privacy, Release, & Waiver Agreement
ID Mgmt Web Server
Industry ID Mgmt DB (local)
Authentication
FiXs Trust Brokers
DoD Defense National Visitors Center
Authentication
DoD DCCIS Trust Gateway Broker
DoD ID Mgmt Web Server
Trust Broker
ID Mgmt Web Server
Other Agencies, Partnerships, or Communities
Authentication
Policy
Operating rules
Security Guidelines
Technical Architecture & Specifications

Figure 4.4: Trust model for the Federation of Identity and Cross-Credential Systems

Based on the concepts presented in www.fixs.org, this figure shows components of a model supporting coalition of commercial companies, government contractors, and non-profit organizations whose missions are to establish and maintain a worldwide, interoperable identity and cross-credentialing network.

vi) Direct: A trust model for the VO creation process

This model is based on reputation and is applied in the process of VO creation [Avila-Rosas & Luck, 2005]. As such, the potential partner organizations will decide to accept or reject an invitation for the VO on the basis of each other's reputations. The model also eases the process of assessing and selecting the most suitable set of network member organizations for a VO. The reputations are assessed on the basis of personal and mediated experiences by applying certain reputation systems. Information on reputations is based on what one party has said about another party over time, and the history of the interactions of these parties with others [Lucas, 2005].

Reputation systems have been addressed by a number of research and development projects. These systems are used in various applications, among others, in e-commerce to assess the trust of buyers/sellers, and in collaborative environments to assess trust of potential partners. As implemented in various systems, *reputation* is a function of the cumulative positive and non-positive ratings/opinions for an actor over the recent periods (weeks, months, years) related to how it is known and perceived by others [Resnick & Zeckhauser 2000].

Reputation systems are applied to analyze the collected reputation data and provide results about the subjective trustworthiness of actors for a particular purpose.

Despite the obvious usefulness of reputation and related concepts for collaboration, such as in supporting exchanging and transferring knowledge between organizations [Lucas, 2005], there are still some existing conceptual gaps in the current developed and applied models. Resnick and Zeckhauser [Resnick & Zeckhauser, 2000] have pointed out the so-called "*Pollyanna*" effect in their study of a larger set of reputation systems. In relation to this effect, it has been observed that there is disproportionately positive feedbacks from users and rare negative feedbacks which in turn makes the results from the analysis in most cases biased and do not represent the actual true picture [Rao, 2006].

Relevance to our research: One fundamental strategic goal of the VBEs is to support their member organizations to rapidly and efficiently configure VOs in response to brokered opportunities. A fundamental indicator for potential VO partners (organizations) is their trust level. As proposed in this thesis the main input data to the assessment of organizations' trust level is a set of their measurable fact-based data e.g. in relation to their performance (as addressed in Section 3.2.2). However, in some cases the performance data of organizations might not be up-to-date or some measurable data might be missing / incomplete. In such case, the organizations' reputation can be applied instead to indicate their actual trustworthiness subjectively. Thus our research has benefited from the presented concepts in this model as a fundamental input to understanding the process of complementing the rational analysis of trust in potential VO partners with some subjective trust analysis, if and when it is needed as addressed in Sections 2.3.4 and 2.3.5.

4.3 Modeling of trust relationships between organizations - The proposed approach

In order to accurately model trust relationships between organizations and to represent their related components, we have chosen to base the definition of our model of trust on the following three formalisms [Msanjila & Afsarmanesh, 2007b].

- *Ontology-based models* of trust relationships between organizations: to support organizations achieve and maintain common understanding about the fundamental concepts of inter-organizational trust.
- *Object-based models* of trust relationships between organizations: to address cardinalities of relationships between trust elements, which are used for the implementation of functionalities of the TrustMan system.
- *Record-based models* of trust relationships between organizations: to provide a rough relational database schema, and thus applied to the design of the database for organization's trust related data.

Although the models resulted by applying these three modeling formalisms constitute some similar parameters, each of these three models of trust relationship between organizations is developed to cover certain specific aspects and support our research in achieving different purposes related to development of organizational trust management system, as further addressed in Chapter 6.

A priori to modeling trust relationships between organizations, we have to identify and classify trust aspects and factors that need to be included in the models. A challenge is that of ensuring that the model incorporates and covers all basic and advanced concepts as perceived in the targeted domain through requirement analysis with the users of the environment. As such, each designed conceptual modeling is correct and complete, while clearly not unique for representing the addressed concepts, entities, characteristics and their inter-relationships.

4.3.1 Main trust parameters for modeling trust relationships between organizations

Trust parameters that need to be included in the conceptual model of trust relationship between organizations have been divided into five main groups, namely: the *trust actors, time, level of trust, trust relationship, and trust elements*. Considering the brief definitions of these parameters as presented in Chapters 1 and 3, below we provide formalized descriptions for each parameter in order to enhance the understanding of the models of trust relationships among organizations, as presented later in this chapter.

i) *Trust actors: Trustor and Trustee:* The two parties in the trust relationship, namely the trustor organization and the trustee organization, are important when defining, modeling, and creating trust in collaborative networks. In general, a variety of factors might be required by different trustor organizations for assessing the level of trust in the same trustee organizations, even if the trustors have the same "objective" in establishing trust relationships. Therefore, it is important that both the trustor organization and trustee organization are distinctly represented in the model of their trust relationship.

ii) *Time: Past, Present and Future:* A trust relationship (and its intensity) between two organizations is an issue of time, which may differ today or tomorrow from how it was yesterday. In other words, an organization's level of trust is not static and may vary depending on changes in the set of trust criteria, the values of the trust criteria, involved trustor organizations, specific ratings of trust level, and so on. All of these factors, which have the potential of influencing changes in an organization's level of trust, are time sensitive. Thus time is an important factor, and must be properly addressed when modeling trust relationships between organizations in VBEs.

iii) *Trust level:* Trust level refers to the intensity of the level of trust for a trustee organization in a trust relationship, on the basis of an assessment of the values for a set of necessary trust criteria. Therefore, the trustee's level of trust is an important aspect to consider for each trust relationship between two actors. Accordingly, this aspect is considered in the model of trust relationship between organizations.

iv) *Trust relationship:* Generally, a relationship is a state of connectedness between people or organizations, or is a state involving a mutual association between people or parties. Trust relationship here refers to the state of connectedness between a trustor and a trustee, the intensity of which is characterized and based on the level of trust. In our modeling approach, trust relationship is the primary parameter of the trust model.

v) *Trust elements:* One important aspect of characterizing trust in VBEs is the identification of trust elements for various organizations. As addressed in Chapter 3, we have found that trust elements considered for organizations are not at the same level of abstraction and/or measurability. Through requirement analysis with users we have identified a wide range of trust elements as presented in Section 3.3. The identified trust elements are hierarchically-related, from abstract (non measurable) ones which represent the root and other high level nodes, to the measurable ones which represent the lowest leaf nodes in the hierarchy. Together these elements characterize the trust and trust relationships for organizations and their classifications represent the fundamental concept of inter-organizational trust, and in particular related to the assessment of trust level of organizations. Therefore, the models of trust relationship between organizations must also capture and include all these aspects further as described in Section 4.3.2.

4.3.2 Object-based conceptual modeling formalism

In recent years, object-oriented modeling (OOM) has become the de-facto standard in early phases of software development in research environments. The current state-of-the-art for conceptual modeling is dominated by Unified Modeling Language (UML) which has been initiated and further stimulated by industry [Maciaszek, 2007]. With UML, Modeling can develop three kinds of models, namely the *static models, structural models, and transitional models*. In some cases the concepts represented in static models and structural models are combined to produce a more comprehensive design model. OOM constitutes the following seven modeling constructs:

- *Objects:* These are entities that have state and attributes, and they provide services when initiated, instantiated and executed. Modelers who are interested in making blocks as a way of representing the problem domain and specifically address the requirements analysis mostly use object concepts.
- *Classes:* These constructs provide a way to categorize objects with similar attributes or services. Classes form an abstraction hierarchy through 'is_a' relationships.
- *Attributes:* These are used to represent an object's state. Modelers use attributes as a means to specify the type, visibility and modifiability of each function and procedure in the class.
- *Relationships:* These define how one object is related to another object. Relationships can be classified as '*is_a'* classification relations, '*part_of'* relationships, and as having '*associations*' between classes.
- *Methods (functions and procedures):* These are the operations that all objects in a class can perform in order to provide the targeted output of the object when called on to do so by other objects.
- *Message Passing:* Provide a means for objects to invoke services that are provided by other objects.
- *Use Cases/Scenarios:* Provides a description on the sequences of messages exchanged between objects in order to facilitate the execution of a specific service.

The main aim of developing the model of a trust relationship between organizations, by applying object-based formalism, is to represent applied trust elements as objects that provide users with proper ways of studying cardinality of a relationship between objects modeled to represent those elements. For example, defining the cardinality of the relationship between an object which is representing a trust criterion and another object which representing a trust perspective. Figure 4.5 shows an objective-based model of trust relationship between organizations. In Figure 4.5, TR represents the trust relationships, TRO represents the trustor organization and TRE represents the trustee organization. Detailed definitions of the parameters defined in this model are introduced in Sections 1.3.2 and 3.2.

Understanding of relations among trust elements and the possibility to model these elements as objects, capturing the cardinality of the relationships among the objects, assist the developers in the process of implementing organizational trust management systems. As addressed in Chapter 6 modules developed for supporting the computation of trust level of organizations, using the TrustMan system, are implemented as objects in Java programming language.

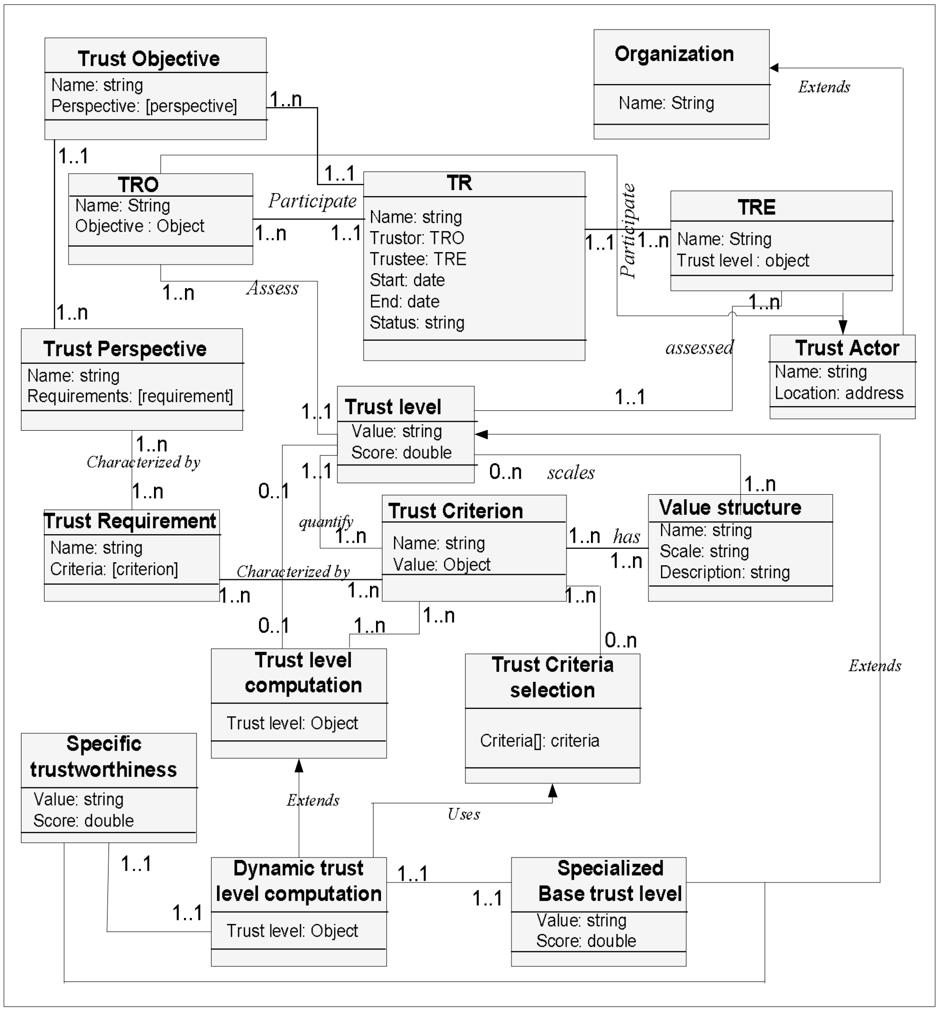


Figure 4.5: Object-based model of trust relationship among member organizations

In this model, TRO refers to trustor organization, TRE refers to trustee organization and TR refers to trust relationship. This model shows classes and their inter-relationships representing various aspects of inter-organizational trust as characterized in the thesis.

Therefore, the object-oriented model of the trust relationships between organizations is used to guide developers with the implementation of functionalities of the TrustMan system. The modules developed on the basis of this object-oriented model are also applied to classify the functionalities, on the basis of cardinalities of relationships among their implemented classes, into sets of integrated services.

4.3.3 Record-based conceptual modeling formalism

This formalism can be used to model trust relationships between organizations as records as inspired in the approaches for relational data modeling. In this modeling formalisms, a trust relationship (TR) is modeling as a record constituting five attributes, namely: trustor organization (TRO), trustee organization (TRE), trust level of the trustee organization (TL), start date and status (equation (4.1)). The ***status*** indicates whether the TR is past, present or planned for future

$$TR = [TRO, TRE, TL, start\_date, status] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4.1)$$

Trust level of the trustee (TL) is also modeled as a record constituting three attributes, namely: the trust perspective preferred by the trustor organization (perspective), the trust requirements for each preferred trust perspective, and trust criteria for each trust requirements (equation (4.2)).

$$TL = [Perspective, (requirements, (criteria))] \ldots\ldots\ldots\ldots\ldots\ldots(4.2)$$

Furthermore, the trust criterion is modeled as a record of its value structure and value metrics (equation (4.3)).

$$Criteria = [value\_structure, value\_metric] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4.3)$$

The three equations (4.1 to 4.3) together make the set of records constituting the record-based trust model for a single trustor organization to single trustee organization in a single trust relationship. If the respective trustor organization has multiple trust relationships with the same trustee organization, the attributes TL, start-date and status of the TR record (equation (4.1)) become repeating attributes. Repeating attributes are closed by parentheses and separated by commas. The representation of repeating attributes takes into account the fact that, although the actors are the same, it is possible that at different times there may be a different level of trust for each trust relationship between the trustor organization and trustee organization. While records for TL and criteria remain the same, the TR record changes as shown in (4.4).

$$TR = [TRO, TRE, (TL, start\_date, status)] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4.4)$$

Furthermore, it is possible for a trustor organization to have many trust relationships with different trustee organizations (equation 4.5).

$$TR = [TRO, (TRE, TL, start\_date, status)] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4.5),$$

A single trustee organization can also have at different times many trust relationships with different trustor organizations (equation 4.6). Moreover, these TR can have dissimilar intensity due to different levels of trust in the participating actors.

$$TR = [TRO, (TRE, (TL, start\_date, status))] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4.6)$$

When the trustee organization has multiple trust relationships with different trustor organizations, the inverse of the records in equation (4.5) and (4.6) apply as shown in equations (4.7) and (4.8).

$$TR = [TRE, (TRO, TL, start\_date, status)] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4.7),$$

$$TR = [TRE, (TRO, (TL, start\_date, status))] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4.8)$$

A formalized record-based representation of trust relationships between actors when a trustor organization is simultaneously a trustee organization and probably with relation to different trustee organizations and trustor organizations respectively needs to be modeled. For this case, the following *record-based model* of trust relationship between organizations is developed, as presented in a diagrammatic form in Figure 4.6. Figure 4.6 shows four nodes N1 to N4, and their trust related relationships, in which they may act as either a trustor or a trustee. In Figure 4.6 it is shown that the trustor TRO-1 has two trust relationships, one with the trustee TRE-2 and the other with the trustee TRE-3. However, the trustee TRE-2 is also the trustor as TRO-2 and it has two different trust relationships with the trustee TRE-4.

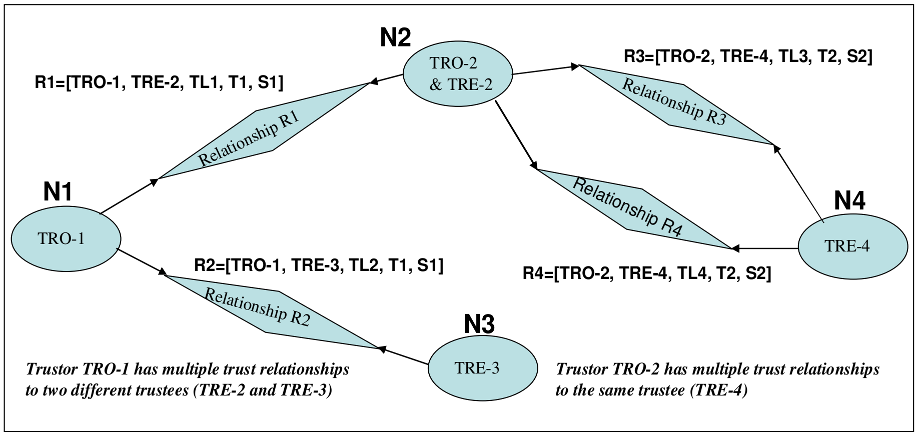

N2
TRO-2
& TRE-2
R1=[TRO-1, TRE-2, TL1, T1, S1]
Relationship R1
R3=[TRO-2, TRE-4, TL3, T2, S2]
Relationship R3
N1
TRO-1
Relationship R4
N4
TRE-4
R2=[TRO-1, TRE-3, TL2, T1, S1]
R4=[TRO-2, TRE-4, TL4, T2, S2]
Relationship R2
N3
TRE-3
Trustor TRO-1 has multiple trust relationships
to two different trustees (TRE-2 and TRE-3)
Trustor TRO-2 has multiple trust relationships
to the same trustee (TRE-4)

Figure 4.6: Relationship-based model of multiple participations among organizations

Where TL represents trust level of the trustee organization, T represents time (start date), and S represents status of the relationship (past, present, future). This is a model of trust relationships among organizations in which the involved trustors and trustees are involved in more than one interaction at the same time.

One of the most challenging and central tasks in managing the process of trust between organizations is managing the data that is required to support the assessment of the organizations' level of trust. A traditional approach for managing structured data is through maintaining a database. The main objective of data modeling in databases is to provide a data structure that adequately represents the real world and that can be processed efficiently by database management systems. Developing services supporting the management of data is an important part of the processes for managing inter-organizational trust. As a result, trust related data must also be correctly modeling and structured using some systems in order to enhance the effectiveness of its exploitation.

Most existing databases and database management systems follow a relational approach. In order to enhance the interoperability and sharing of data that is managed by the TrustMan system with the existing/legacy databases, the database that we developed also adopted the relational approach. Therefore, in our design and implementation of the system for managing trust related data for organizations, we have used the record-based models of trust relationship between organizations addressed above to define relational database schemas detailing the required records (types) and respective attributes (columns). Namely, based on the classification of trust elements as presented in Section 3.2, we have designed three different schemas: *schema for general data related to trust elements, schema for general organizational data, and schema for trust related data of organizations* (as further defined and addressed in Section 6.5.4).

4.3.4 Ontology-based conceptual modeling formalism

In information sciences and engineering, ontology refers to 'an explicit specification of a conceptualization', 'a theory or a system of concepts/vocabulary used as building blocks for information processing systems', and 'a representation of semantics of terms and their inter-relationships'. A VBE environment is characterized by its dynamic characteristics, such as its environmental features, objectives, member organizations, etc. New ontologies for VBEs will continuously emerge and existing ones will evolve. Development of a trust related ontology will also undergo the same life cycle processes [Afsarmanesh & Ermilova, 2007].

The effectiveness of an assessment of level of trust and the acceptability of its results is greatly influenced by the common understanding of trust between its involved parties, including trustor organizations, trustee organizations, VBE administrator organization, and other stakeholder organizations. One approach for supporting establishment of such an understanding of trust is by providing these parties with an ontology describing the concepts and terms used for the various elements, features, principles, mechanisms and software tools [Afsarmanesh & Ermilova, 2007a]. For the specific purpose of supporting such common understandings on trust, we have developed an ontology-based model of trust relationship between organizations classifying the taxonomical relations between trust elements (Figure 4.7). This ontology is described for VBE environments and included within the *Ontology Discovery and Management System* (ODMS) developed with the ECOLEAD project [Afsarmanesh et al. 2008].

Concepts related to the level of trust in organizations, inter-organizational trust relationships, different trust elements, and so on must also be understood well by all of the actors within a VBE. Therefore, the ontology-based models for trust relationships between organizations are also applied to the implementation of the TrustMan system.

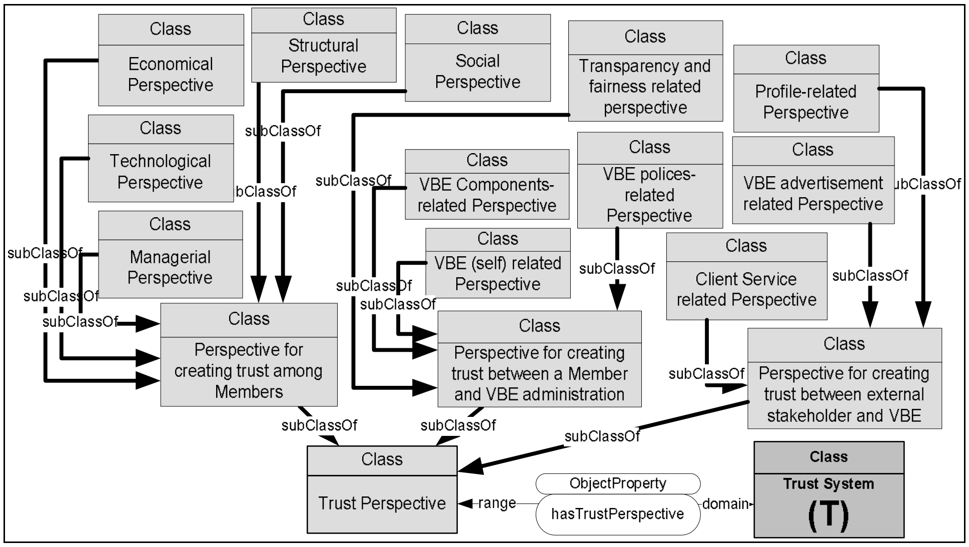

Class
Economical Perspective
Class
Structural Perspective
Class
Social Perspective
Class
Transparency and fairness related perspective
Class
Profile-related Perspective
Class
Technological Perspective
Class
VBE Components-related Perspective
Class
VBE polices-related Perspective
Class
VBE advertisement related Perspective
Class
Managerial Perspective
Class
VBE (self) related Perspective
Class
Client Service related Perspective
Class
Perspective for creating trust among Members
Class
Perspective for creating trust between a Member and VBE administration
Class
Perspective for creating trust between external stakeholder and VBE
Class
Trust Perspective
ObjectProperty
hasTrustPerspective
range
domain
Class
Trust System
(T)
subClassOf
subClassOf
subClassOf
subClassOf
subClassOf
subClassOf
subClassOf
subClassOf
subClassOf
subClassOf
subClassOf
subClassOf
subClassOf
subClassOf
subClassOf

Figure 4.7: Ontology-based model of trust relationship between organizations

This figure shows the taxonomy inter-relationships among various concepts and aspects representing the classes of trust elements that characterize trust relationships among organizations.

4.4 Chapter discussion and conclusion

This chapterhas addressed the conceptual modeling of trust relationship between organizations as a means to contribute to the characterization of inter-organizational trust. It has presented three kinds of conceptual modeling formalisms, namely: *object-based, record-based and ontology-based formalisms,* where each one is also exemplified with some models for trust relationships between organizations.

Object- oriented paradigm assists system developers in addressing the complexity of a problem domain by considering the problem not as a set of functions that can be performed but primarily as a set of related and interacting objects. The modeling task therefore consist of specifying for a specific context, those objects (or the class that the objects belong to), and their respective set of properties and methods, shared by all object members of the class. This modeling approach also supports the analysis of cardinalities of relationships between the objects. On the basis of these concepts, an object-based model of trust relationship between organizations is applied in this thesis to designing and implementing modules/functionalities of organizational Trust Management System, as further addressed in Chapter 6.

Relational databases are the most commonly used type of data storage in research and practice. This is due, in large part, to the fact that the simplicity of their storage and access principles offers users greater efficiency. Also, the table-like structures map easily to most real-life data formats, such as forms and spreadsheets. Record-based models of trust relationship between organizations, developed on the bases of the concepts in relational data modeling, are presented in this chapter. These proposed models are applied here in designing a relational database schema for data related to trust in an organization. The designed schema is applied in developing a database for the TrustMan system as described in Section 6.5.4.

Effectiveness of assessment of the level of trust in an organization and the acceptability of its results is greatly influenced by the common understanding of trust concepts between its involved parties. Such parties in VBEs include: trustor organizations, trustee organizations, VBE administrator organization, and other stakeholder organizations. One approach for supporting the establishment of such understanding of trust concepts is by providing these parties with an ontology describing these concepts and the terms used for various trust elements, mechanisms for assessing trust level, and applied functionality offered by the software tools used for this purpose. This chapter has presented an ontology-based model of trust in VBEs between the participating organizations and other actors, in order to achieve a common understanding regarding these fundamental trust concepts.

In this chapter, we have addressed the main research question MRQ2. We have presented models of trust relationships between organizations that can be used to provide knowledge to different actors, in order to help them achieve better understanding of trust, such as gaining insight on trust related concepts, designing a database schema, or understanding relations among objects representing trust elements. An integrated overview of how all posed questions in this thesis that are addressed by different chapters is presented in Chapter 7.

Inter-organizational trust plays a key role in facilitating collaboration within VBEs. Therefore, better understanding of the concepts related to inter-organizational trust is necessary for creating successful collaborative networks of organizations. This chapter proposes models of trust relationships among organizations, constituting their related trust elements and inter-relations. As such, the chapter provides the stakeholders in VBEs' research and practice with a set of models to enhance the understanding and characterization of inter-organizational trust, as addressed in the thesis. These developed models are applied to the design and development of the organizational trust management system (TrustMan system) presented in Chapter 6.

Chapter 5

Mechanisms for assessing trust level of an organization

In order to "rationally" assess the level of trust in an organization, a series of fact-based criteria about organizations shall be considered. Mechanisms applied for assessing the level of trust in organizations can apply some or all of these criteria to reflect the purpose for which the trust is to be established. Proper mechanisms should exist to support dynamic selection of specific subsets of these criteria. As such to measure the level of trust in organizations, customizable mechanisms need to be developed. This chapter presents a mathematical approach for assessing the level of trust in organizations and introduces formal mechanisms for customization of the input criteria to the mathematical model of trust assessment.

This chapter constitutes mainly material that has been previously published in the International Journal of Production research [Msanjila & Afsarmanesh, 2007a].

5.1 Introduction

Designing and developing *rational (fact-based) mechanisms* for assessing the level of trust in organizations is of particular importance to large and very large VBEs, in which all member organizations are not usually familiar with one another. This chapter presents a conceptual model in terms of mathematical equations. The model is applied to develop rational (fact-based) mechanisms for supporting an objective trust analysis in VBEs. That is to say, developed mechanisms are used to assess the level of trust in organizations. The model, and thus its related mechanisms for assessing the level of trust in an organization comprise measurable trust elements, namely trust criteria, known factors and intermediate factors.

The remaining part of this chapter is organized as follows: related work on the assessment of the actors' level of trust in different kinds of collaboration is presented in Section 5.2; basic concepts relating to level of trust in an organization are presented in Section 5.3 with particular focus on the concept of the comparativeness of trustworthiness; and in Section 5.4 the mathematical model for developing mechanisms to assess the level of trust in organizations is explained.

5.2 Traditional approaches addressing assessment of trust in organizations

In the past, and in most current modus operandi, assessment of the level of trust in individuals and organizations has been subjective, since it has used data such as opinions on the reputation of trustees. However, attempts have been made by different researchers addressing the assessment of the level of trust in individuals and organizations to use objective approaches. In such cases some sort of measurable data were applied to estimate the level of trust in each actor. The fundamental weakness of these suggested approaches is however that the sources of used data and the categorization of the parameters that are used as trust criteria are not properly characterized and difficult to rationally measure. These approaches can be categorized into two groups as addressed below, namely that which provides "probability values" as the final calculated results, and that which provides "expectation values" as the final calculated results.

As discussed in Section 1.3, trust is mostly regarded in both research and practice as the *probability* perceived by a trustor that a trustee will do something [Gambetta, 1988]. Applying mathematical definition, the probability of the occurrence of x is calculated as:

$$P(x) = \frac{No(x)}{No(\cup)}$$

Where P(x) refers to probability that x will occur, No(x) refers to the number of times x can occur and No(U) refers to the number of all possible occurrences.

Some other researchers have described the assessment of the level of trust in actors as expectation of occurrence [Rousseau et al., 1998; Mayer et al., 1995]. Applying mathematical definition for the expectation that x will occur, it can thus be calculated as:

$$E[x] = \sum_{\forall i} P_i * x_i$$

Where P_i refers to the probability that x_i will occur, E[x] refers to the expectation of x.

For expectation, also a key concept in the formula is once again the probability. It is however difficult to compare values of probability related to two or more actors (such as organizations) which may represent their different levels of trust. It is also difficult to reason on the suitability of assessment results for a specific objective, such as selecting potential partners for configuring a VO. The VO might need specific capabilities, such as the financial or technological capabilities and experience, and so on; and these do not lend themselves to reasoning through the use of general probability values.

However, a probability-based assessment works well when trust is regarded as a subjective aspect. It is easier to count opinions that supported the positive reputation of trustees and thus use these to calculate their trustworthiness as probability values. In such practices, the need to formally reason about results assessment is not important. Today, formal mechanisms for assessing the level of trust in organizations are needed to support making formal reasoning on results.

As addressed in Section 2.2.3, the notion of trust itself has been differently interpreted and perceived in the various disciplines that apply this concept in daily practice. Based on their interpretation and perception, trustors in these disciplines prefer to use different kinds of trust elements when assessing the level of trust in trustees. Similarly, the approaches and mechanisms that are employed to manipulate the collected data also differ. In order to exemplify these approaches and mechanisms, we have surveyed several traditional approaches that have been used to assessing the level of trust in: individuals, actors within an online business, as well as individual members within online social communities, as addressed below.

o ***Measuring individuals' level of trust:*** Traditionally, assessing the level of trust in one individual has been carried out on the basis of the opinions of other individuals and, in particular, on information concerning the reputation of the trustee himself/herself. There are different purposes for which individuals may decide to assess the level of trust in their respective trustee a priori to interacting with them. In order to illustrate this, we have studied the assessment of individuals' trust level for the following purposes: admission in higher learning education, the selection of suitable job applicants, the creation of a personal friendship network, and so forth. It was observed that in all of these processes the reputation data of trustees is used as a key source of information in assessing the level of trust. The aspects related to the assessment of the level of trust in individuals are in details addressed in Sections 2.2.2 and 2.2.3.

o ***Measuring the individual's level of trust in an online business:*** It is currently becoming common practice for business processes – such as the selling and buying of products and services – to take place online e.g. the e-commerce. In such a business environment, sellers and buyers interact with each other to complete all necessary transactions virtually, without ever meeting face-to-face. It is thus a challenge for both sellers and buyers to trust each other and subsequently commit to either deliver products and services, or pay for the required products and services. There are traditional approaches that use subjective data which support the creation of trust between these actors. For example, sellers may use their reputation data as recommended by previous customers to convince new buyers. This information is usually made available online at the seller's website. The aspects of trust in e-commerce are addressed in Sections 4.2.

o ***Measuring the individual's level of trust in online social networks:*** Establishing and expanding a personal social network has traditionally been used as a key way to keep up-to-date on different events that take place in one's society [Dasgupta, 1988]. It has also been used as a fundamental approach to quickly gain the trust in a new social network member based on that person's popularity (and thus possesses a large social network of his/her own). These networks are established for different purposes, including sharing knowledge and accessing online entertainments. Nowadays, such networks are established and managed online. Trust between individual members has demonstrated to be a fundamental aspect in facilitating network survival and existence [Preece, 2004]. Therefore, reputation data has proven to be the key source of information when assessing the individuals' level of trust and applying results to the creation of inter-personal trust.

The three approaches presented above highlight the current practice related to trust, which in fact reflects difficulty that exists in carrying out a quantitative assessment of the level of trust in actors, so instead of using reputation data (opinions). Therefore, no quantitative trust criteria data exists. In addition to this, research has realized that it is also difficult to formulate formal measurement mechanisms, such as mathematical equations, to manipulate such data in order to formally assess the level of trust in actors such as organizations. These practiced approaches do not satisfy the need for trust establishment in business-based collaborations, such as needed for VOs, which need to effectively provide a quantitative assessment of the level of trust in organizations within the VBE.

In our research, trust in VBEs is characterized as a multi-objective, multi-perspective and multi-criteria subject. The main source of trust related data is the quantitative measured performance of organizations, expressed in terms of trust criteria. Formal mechanisms, namely mathematical equations, are formulated in order to support the measurement of the level of trust in organizations and reasoning on results. In the remaining part of this chapter, we present an approach for the formulation of the formal mechanisms used for the assessment of the level of trust in an organization.

5.3 Concepts related to assessment of trust

The aim of measuring the level of trust in VBE's member organizations is to support two general purposes, namely, (1) the controlling and monitoring of the balance of the **base level of trust** in member organizations, and (2) evaluating the **specific trustworthiness** of an organization for a specific trust objective. For the rational assessment of the *base level of trust* in organizations, a minimum set of trust criteria, the so-called *base trust criteria* can be defined to be applied. The VBE administrator decides on this set of base trust criteria during the time when the VBE is being established, from a pre-defined general larger set of trust criteria, i.e. the VBE's **pool of trust criteria**, covering all aspects of the five different organizational perspective of trust. This pool of criteria is presented in Section 3.3.1 and Figure 3.6. All organizations in the VBE must provide their trust related "data" for the set of **base trust criteria**. The base trust level represents the minimum acceptable level of trust in each organization in the VBE and to control the balance of trust among member organizations. Furthermore, for each specific objective and purpose, evaluation of the *specific trustworthiness* of organizations becomes necessary. Here, a set of **specific trust criteria** shall be applied, which can be dynamically selected from the pool of VBE trust criteria by the trustor organization, to meet different specific trust objectives he/she may have at the time. Mechanisms are needed to support both the dynamic selection of specific trust criteria, as well as the application of selected criteria to rational evaluation of specific trustworthiness of organizations. Development of these mechanisms is discussed in Chapter 6.

5.4 Measuring and assessing organization's trust level

This section addresses the measurement and rational assessment of the level of trust in an organization in the VBE. We first present the need for assessing this trust level and then describe the base concepts regarding the comparative/relative nature of the assessed trust level. Second, we present the mathematical approach applied to formulate generic mechanisms for assessing trust level of an organization. Finally, we introduce an example VBE, to analyze some complex aspects that can emerge while formulating the mechanisms for assessing trust level of an organization and how they can be handled. This section also presents some corrective measures for mechanisms used for the assessment of the trust level of organizations, so as to record the variations in the preferences of trustors related to their specific set of trust criteria.

5.4.1 Need for trust measurement in VBEs

Requirement analysis and empirical studies identify that establishing trust between organizations is amenable for a smooth management of VBE networks and an antecedent for VBE's effective operational continuity. To ensure that every organization in the VBE meets the minimum established trust threshold, indicators need to be developed and applied to establish a grading and ranking scheme for trustworthiness of an organization. The proposed indicators in this thesis, as described in earlier chapters, comprise what we suggest as an organization's *"trust level or trustworthiness"*. Among others, following represent the main needs for assessing the trust level of organizations in the VBEs:

- ***As a strategy to enhance cohesion among member organizations within the VBE:*** The assessment of the base trust level of an organization in the VBE and particularly, when applying for VBE membership can be perceived as an examination which every organization must qualify in order to enter and remain within the VBE. This may positively influence the cohesion among member organizations and their perceptions that they together belong to a group of trustworthy organizations. As a result, VBE member organizations will perceive as operating in a controlled risk environment.

- ***As a measure for management of the VBE:*** A key activity for a VBE administrator is to ensure that member organizations meet all VBE membership requirements necessary to assure successful VBE continuity. Among others, such requirements include: possessing required competency, achieving good performance, maintaining proper ICT infrastructure for collaboration, and abiding to the VBE working and sharing principles. These aspects are considered and covered by the base set of trust criteria as presented in Section 3.3. Thus assessing trust level of each member organization in the VBE will enable the VBE administrator to have a general but complete picture about how the VBE requirements are met by each organization. Assessing the base trust level of member organizations in the VBE can thus be applied as one of the management measurement by the VBE administrator. Thus assessing the base trust level of organizations within the VBE indicates how the VBE is prepared to compete in the market and in acquiring business opportunities, which are key aspects for its effective future continuity.
- ***As an indicator for establishing objective-specific collaboration:*** When a few organizations in the VBE need to be selected for participation in a specific collaboration, such as in a VO, their evaluated trustworthiness for the specific objective of the VO needs to be measured. The selection of the most fit partner for each task considers the measurement of its trust level. These measurements indicate how trustworthy each member is when compared to other organizations.

As seen from the above examples about the need for assessing trust level of an organization in the VBE, a wide range of trust criteria may be considered while evaluating organization's trustworthiness. Trust in VBEs is characterized by considering a wide variety of aspects that together comprehensively support the rational measurement of trustworthiness of organizations. As such, trust is not a single concept that can be applied to all cases for trust-based decision-making and its measurements depend on both the purpose of establishing a trust relationship and its specific involved actors. Trust level of an organization can be measured rationally in terms of quantitative values of related trust criteria e.g. based on an organization's past performance. The level of trust in an organization is complex and can neither be measured with single value of a single parameter, nor interpreted with a single metric. Nonetheless, an organization's level of trust can be specified on the basis of the values for a set of related trust criteria.

Understanding and interpreting the level of trust in an organization, described and formulated in terms of values of a set of trust criteria, will be complex and difficult to grasp for most decision-makers in organizations, such as managers and directors, if they are not trust experts and do not have sufficient knowledge in both mathematics and computer applications. Thus, the trust level of organizations must be presented in a format that is as understandable as possible to the expected users while not loosing its semantics.

This thesis proposes that the level of trust in organizations should be represented and expressed in terms of a set of qualitative values, and these values can only represent comparative levels of trust in different organizations in a VBE for a specific given trust purpose, and not as absolute levels. A set of "qualitative values" are designed for the level of trust in an organization to be presented to the decision makers that include: *Strongly more trustworthy, More trustworthy, Average trustworthy, Less trustworthy, and Strongly less trustworthy*. As an example, the comparative qualitative values of the trust level of four organizations (ORG-1 to ORG-4) in a VBE are graphically represented in Figure 5.1. This representation is referred to as the "***Trust-Meter***". As shown in this figure, considering selected criteria, ORG-3 is "more trustworthy" that others.

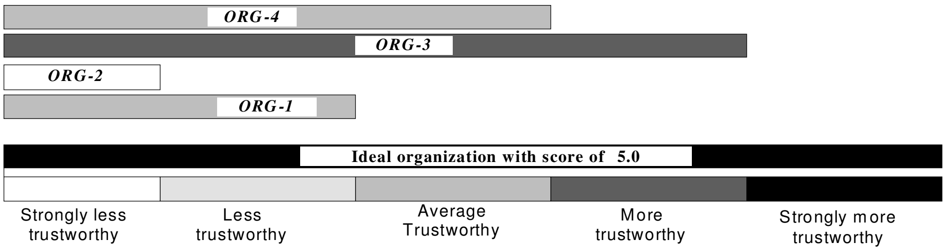


Figure 5.1: A trust-meter for presenting comparative level of trust in organizations

As further addressed below, this figure shows how the level of trust can be compared relatively for a number of involved organizations.

As such, in our approach the trust level of an organization is not an absolute value rather it is computed as a relative value depending on the following aspects:

- ♦ ***Involved organizations:*** While assessing the trust level of an organization, its relative score for each trust perspective is computed by comparing the organization's value for each applied trust criterion against the optimal value of that specific criterion, among the all involved organizations. The general equation below exemplifies how the relative score for the economical perspective (S_{ECO}) is computed from the values for its different criteria and the maximum value for those criteria in the VBE.

$$S_{ECO} = f\left(\frac{capital}{\max capital};\frac{financial\_stability}{\max financial\_stability};\frac{VO\_stability\_stability}{\max VO\_based\_stability};\frac{financial\_compliance}{\max financial\_compliance}\right)$$

Thus if some organizations join or leave the collaboration then there is a possibility that optimal values of some trust criteria may change. As a result the value for trust scores may change nevertheless, the relative scores of different organizations remain a good indicator for comparing the trust level of organizations. This illustrate that the trustworthiness of an organization is relative on the basis of involved organizations at the time of the computation.

- ♦ ***Applied set of trust criteria:*** In our approach the trust level of organizations is measured in terms of those trust criteria which are preferred and selected by respective trustors, depending on their: trust objectives, trust preferences and trust perceptions. Thus the relative nature of trust level of an organization also depends on these three aspects. As examples, the pool of trust criteria that were preferred and selected by different VBE administrators for experimenting the TrustMan system at their industrial VBEs, are presented in Table 6.3 of Section 6.6.2.

- ♦ ***Grading and interpreting scores for the trust level:*** In our approach, the score for the trust level of an organization is given in a range of zero "0" (representing the lowest score) and five "5" (representing the highest score). The intermediate ranges (namely, between 0 and 5) and their specific interpretation and meaning depend on the rating/grading of these scores as preferred by the trustor organization. Table 5.1 shows an example of two possible differences in setting the meaning to the range of scores assigned to different measurements of trust levels by different trustors. Thus the relative nature of trust is also dependent on the interpretation of computed scores by the specific trustor organization.

Table 5.1: Illustration of differences in grading the trust level of an organization

Trust level	**Preferred range for 1st trustor**	**Preferred range for 2nd trustor**
Strongly less trustworthy	$0 < score \leq 1$	$0 < score \leq 1.5$
Less trustworthy	$1 < score \leq 2$	$1.5 < score \leq 2.5$
Average trustworthy	$2 < score \leq 3.5$	$2.5 < score \leq 3.5$
More trustworthy	$3.5 < score \leq 4.3$	$3.5 < score \leq 4.5$
Strongly more trustworthy	$4.3 < score \leq 5$	$4.5 < score \leq 5$

Please note that for the classification of different comparative levels of trust in organizations when specific ranges are not specified as exemplified in Table 5.1, the *lowest resulted value* will be assigned to the category of "*Strongly less trustworthy*" and similarly the *highest resulted value* to the category of "*Strongly more trustworthy*" and the other categories represent a uniform distribution of these two values.

5.4.2 Proposed trust assessment mechanisms

The score for the trust level of an organization is computed as a weighted generalization (e.g. averaging) of scores attained by the organization on the basis of specifically designated trust perspectives. With the base assumption, as addressed earlier in Chapter 3, about the independence of the five trust perspectives, the generic formula is given below.

$$S_{TL} = Average([w_{TEP} * s_{TEP}],[w_{STP} * s_{STP}],[w_{SOP} * s_{SOP}],[w_{ECP} * s_{ECP}],[w_{MGP} * s_{MGP}])$$

Here, "S_{TL}" refers to the relative score for the trust level of an organization. The TEP represents technological perspective, STP represents structural perspective, SOP represents social perspective, ECP represents Economical perspective, and MGP represents managerial perspective of trust in organizations.

Furthermore, "*S*" (also defined further below) refers to the score that an organization acquires from the manipulation of its related values in each trust perspective and for the selected set of trust criteria for that perspective. Also, "W" refers to the weight specified for each trust perspective by each respective trustor organization. When weights are not specified, the Trust Management (TrustMan) system (see Chapter 6) will assume uniform ones for all perspectives designated by the trustor organizations. The sum of these weights must always be equal to one and each weight must range between zero and one.

Similarly, the score for each individual trust perspective, such as STP, will be calculated as a weighted average of scores reached by an organization for each of the trust requirements in that trust perspective. For example, for the structural perspective will be calculated as follows,

$$S_{STP} = Average([w_{STS} * s_{STS}],[w_{BSS} * s_{BSS}])$$

Here, "*STS*" refers to structural strength and "*BSS*" refers to business strength, which together constitute the trust requirements of the structural perspective (Figure 3.6).

The *weighted average of the intermediate factors related to each requirement* also applies to the calculation of the score for that requirement. While a number of generic intermediate factors that will be applied to all VBEs are identified a-priori to a VBE's establishment, and their respective formulas are predefined, in some case more specific intermediate factors might need to be identified and defined during the customization of the generic TrustMan system for one specific VBE domain and/or application, as further exemplified in Section 5.4.5.

The TrustMan system developed for the management of trust in VBEs, provides services for supporting the assessment and measurement of the level of trust in an organization (addressed in detail in Chapter 6), calculating these scores using a pre-defined set of mathematical formulas. These formulas are derived from the causal analyses, such as those diagrammatically represented in the causal diagrams of Figure 3.4, Figure 5.2 and Figure 5.5. Causal diagrams define and depict the inter-relations between **trust criteria, intermediate factors** and **known factors**. While the trustee organizations (VBE member organizations) will provide values for trust criteria, and the values of known factors are already known from the VBE environments, *mathematical formulas must be derived for calculating the values of the intermediate factors.* Based on the calculated values of intermediate factors, the respective trust *scores* can be determined for each organization, in relation to each designated trust perspective of the trustor. Furthermore, the final *comparative trust level* of an organization will be calculated based on the combination of these perspective-based trust scores.

In Section 5.4.3 we present the approach applied to derive formulas for intermediate factors, which greatly influence the calculation of organization's perspective-based trust level. In Section 5.4.5 we apply this proposed approach to derive mathematical equations for a specific example VBE.

5.4.3 Developing mechanisms for assessing trust level of organizations

The proposed mechanism for assessing the trust level of an organization uses mathematical relations. The equations are formulated using the results from the analysis of causal relations between trust criteria, known factors and intermediate factors. To present our approach for formulating the required equations we use the causal diagram shown in Figure 3.4 in Section 3.2.3, that figure is repeated below as Figure 5.2 for reader's convenience.

For the formulation of mathematical equations, based on the results of a causal analysis, the plus sign (+) on an arrow in the diagram translates either to an arithmetic addition or to a multiplication. The minus sign (-) translates either to an arithmetic subtraction or to a division. The selection of appropriate arithmetic operator for the equation is done depending on the semantics of each trust criterion as well as the metric that scales it [Kirkwood, 1998; Ge et al., 2004]. Also, the selection of the correct arithmetic operator considers the *balance of the dimensions*, and when complex relations are involved, *dimensional analysis* can be applied (as for example addressed in mathematics, physics, chemistry, and engineering to check the plausibility of derived equations and computations) [Barenblatt, 1987]. When several criteria (C1 to Cn) influence an intermediate factor (Ft), the *value-metric* of Ft is used to determine how the *value metrics of the C1 to Cn* must be inter-related with each other to produce the Ft.

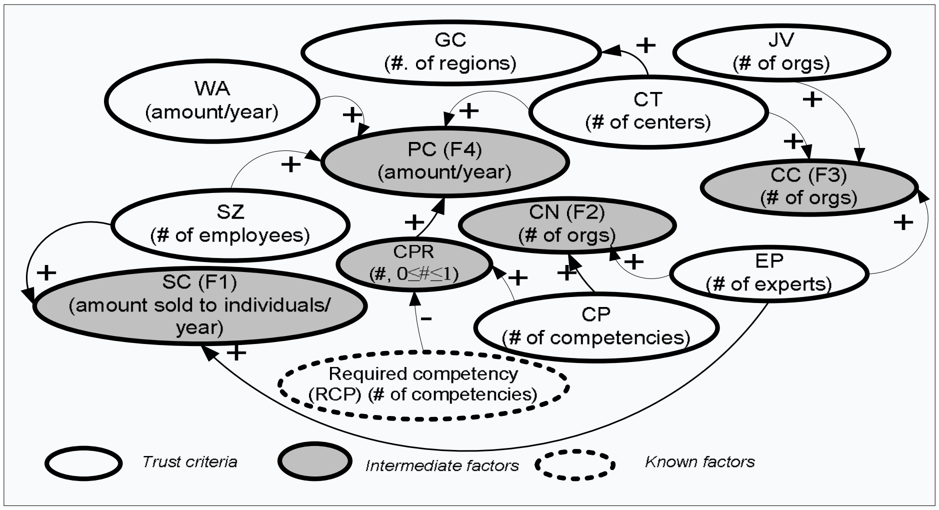


Figure 5.2: Causal influences between trust criteria for structural perspective

This figure is repeated from Figure 3.4 *in Chapter 3, where CPR represents competency ratio and RCP represents required competency in the VBE and all other parameters are defined earlier in Section 3.2.2, and also represented in Table 3.1 and Figure 3.3. This figure shows a qualitative analysis of causal influences between measurable parameters for the structural perspective, namely, the associated trust criteria (size, workload allocation, competencies, experts, centers, joint ventures, and geographical coverage), known factors (required competencies) and intermediate factors (social capital, competency ratio, connections, common context, and production capacity). As an example, please note in Figure 3.4 that the intermediate factor CPR (competency ratio) is positively influenced by one trust criteria CP (competency) and negatively influenced by one known factor RCP (required competency).*

Further, in developing equations for each intermediate factor, all arrows directed towards the respective intermediate factor are considered towards developing its equations [Byne, 2006; Pearl, 1998]. Therefore, the formula for each intermediate factor will be developed in terms of both the criteria and the known factors influencing it, and thus pointing towards it. Clearly, it is feasible that intermediate factors also influence each other but there will be no cycle, in which case the formula of one intermediate factor may be considered as a known factor within the other formula.

Below we present the formulation of generic equations for one trust perspective, namely the structural perspective. Specifically, to present our approach we develop mathematical equations for one intermediate factor – Production Capacity (PC) – as shown in Figure 5.2 for which we use the results of related analysis of causal relations. The derivation of mathematical formulas for the other four trust perspectives, namely: the technological, social, economical and managerial perspectives are presented in Section 5.5.

Example 1: Developing an equation for Production capacity (PC)

We refer here to PC as the amount/number of products/services that an organization can produce and/or provide during a specific period of time. As shown in Figure 5.2 three trust criteria directly influence the behavior of PC, namely: size of the organization (**SZ**)**,** which refers to the number of employees per organization's centre; the workload allocation (**WA**) of employees**,** which refers to the standard amount/number of products/services that a fully qualified employee is able to process in a specified period of time; and organization's centres (**CT),** which refers to the number of branches/offices at different places supporting the production/provision of products/services. PC is also influenced by another intermediate factor, namely the competency ratio (**CPR),** which refers to the ratio of the number of competencies that an organization can offer to the total number of required competencies in the VBE. The arithmetic equation, which relates these four factors to the processing capacity (PC), is represented in the equation below.

$$PC = SZ * WA * CPR * CT$$

Furthermore, each organization has a certain number of competencies that it offers to the VBE. Also the number of competencies required in each VBE is known. Therefore, CPR refers to the competency ratio of the organization and considering the metrics of those factors that influence it as shown in the causal diagram (Figure 5.2), it can be mathematically represented as follows:

$$CPR = \frac{CP}{RCP}$$

Where CP refers to the number of competencies of an organization offered to the VBE, RCP refers to the total number of required competencies in the VBE. Substituting the equation of CPR in the equation of PC generates:

$$PC = SZ * WA * \frac{CP}{RCP} * CT \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \textbf{(5.1)}$$

By definition, in calculus, the derivative of a parameter "y" with respect to another parameter "x" measures the rate of change of y with respect to x. Therefore, in order to capture the rate of change of every intermediate factor (such as the PC) for the analysis of variation of the trust level of an organization in time durations, we simply apply the above rule. *Assuming all the parameters in the arithmetic equation are continuous in respect to time*, the derivative of equation (5.1) with respect to the time parameter "t" represents the rate of change for each of the trust criterion (or for the known factor) with respect to time, in relation to the rate of change of PC, also with respect to time, as shown in equation (5.2). The derivative equation is used for the analysis of evolution of the level of trust in an organization (such as determining whether the level of trust is increasing, decreasing or uniform) at a certain point in time.

$$\frac{d}{dt}PC = \left(WA*\frac{CP}{RCP}*CT\right)\frac{d}{dt}SZ + \left(SZ*\frac{CP}{RCP}*CT\right)\frac{d}{dt}WA + (SZ*WA*CT)\frac{d}{dt}\left(\frac{CP}{RCP}\right) + \left(SZ*WA*\frac{CP}{RCP}\right)\frac{d}{dt}CT \cdots \textbf{(5.2)}$$

Moreover, in order to capture the accumulation of values of all parameters over time for intermediate factors, such as the PC, we have applied integral calculus. To apply the integral calculus we have *assumed that all parameters in the arithmetic equation are continuous with respect to time*. Capturing accumulation of values of intermediate factors will support the analysis and computation of average scores for trust level of an organization over a certain interval of time, such as computing its average trust level during the period of its involvement in a VO. In calculus, the integral of a function is an extension of the concept of summation, which in fact provides the accumulation of the first parameter with respect to the second parameter. The process of finding integrals is called integration. The process is usually used to find a measure of totality such as area, volume, mass, and so forth, when its distribution or rate of change with respect to some other quantity, such as *position* or *time,* is specified.

Therefore, the integral of equation (5.2) in this respect provides the accumulation for PC, which also represents the total amount of products that can be produced by the organization during a given period of time such as from t_1 to $t_{2,}$ as shown in equation (5.3).

$$\int_{t1}^{t2} PC = \int_{t1}^{t2}\left(WA * \frac{CP}{RCP} * CT * SZ\right) + \int_{t1}^{t2}\left(SZ * \frac{CP}{RCP} * CT * WA\right) + \int_{t1}^{t2}\left(SZ * WA * CT * \frac{CP}{RCP}\right) + \int_{t1}^{t2}\left(SZ * WA * \frac{CP}{RCP} * CT\right) \ldots\textbf{(5.3)}$$

The integral equations are used in our study to analyze the averaged accumulation of score for the trust level of an organization in a specific time interval. This enables to get a picture on how the trustworthiness of an organization has been changing accumulatively and thus on the basis of this picture we can predict the future trend of trust level of the organizations.

5.4.4 Corrective measures for assessing trust level

In the TrustMan system as presented in Chapter 6, a list of formulas that formally define inter-relations between trust criteria, intermediate factors, and known factors, are applied for the implementation of mechanisms for assessing the level of trust in each organization. When a trustor designates/selects a number of trust criteria within a trust perspective, the related predefined formulas that constitute these criteria will be invoked. However, in some cases the predefined formulas might also include some other trust criteria that are not selected by the trustor. In such situations, mechanisms are implemented in the TrustMan system to automatically eliminate (nullify) the effects of refused (not selected) trust criteria within predefined formulas, thus ensuring that accurate comparative arithmetic results are obtained for all involved organizations. For example, if a refused (not selected) trust criterion in the equation is related to one selected trust criterion or a known factor with an addition (+) sign or a subtraction (-), then a value of 0 will be assigned to it. Moreover, if the refused trust criterion in the equation is related to one selected trust criterion or a known factor with a multiplication (*) or a division (/), then a value of 1 will be assigned. With this approach the influences of the refused (not selected) trust criteria will be avoided on the final comparative results.

However, values for all selected trust criteria must be a-priori available from all organizations in the VBE and whose trustworthiness is being assessed. Namely, the trustworthiness of any organization for which its values for all selected trust criteria are not available will not be calculated that may in turn result the loss of opportunity for organizations. The TrustMan system identifies such missing values and notifies the trustor as well as the VBE management about the faulty organizations and incomplete values for their trust criteria.

Furthermore, the use of the different kinds of equations presented in Section 5.4.4 may differ. These equations can be used for assessing the level of trust in an organization at a specific point in time, such as the current time. However, it becomes more complex when the level of trust in an organization needs to be assessed on the basis of a large amount of data gathered during a relatively long-period of time in the past. The complexity of an assessment also increases when level of trust in an organization needs to be forecasted for a relatively long-period of time in the future. Simulation can be applied in such special cases, which involves the use of differential equations (such as equations 5.2, 5.3) in order to build the simulation models.

5.4.5 Setting up and customization of organizations trust assessment system for VBEs

Every VBE belongs to a general VBE domain (such as the manufacturing, health, tourism, etc.), and it further represents a specific application area(s) within that domain (e.g. production of clothing, or elderly support services). In order to further present our approach for assessing the level of trust in an organization and go to the low level of addressing trust criteria, we use the example of a VBE that specializes in perishable products. In particular, we address a VBE that specializes in the processing, production, and preservation of perishable food, and further on the specific application area of processed fish products (see example 5.1). In this sub-section, we apply the concepts of HICI approach that was presented in Section 3.2, in order to develop a tailored trust management system for a specific VBE.

Following is a replicable approach with a set of activities that shall be performed to achieve this purpose for each VBE:

- Selecting a set of trust criteria from the generic set of potential trust criteria, to be included within the specific VBE's pool of trust criteria (see "a" below)
- Analyzing the impact of the selected trust criteria and the VBE-generic intermediate factors, on the trust level of organizations in this VBE (see "b" below)
- Analyzing causal influences between the selected trust criteria in the pool, the intermediate factors (both the VBE specific and the generic ones) and the known factors specific to this VBE (see "c" below)
- Formulating equations using the results of the causal analysis, and apply these equations to the development of mechanisms for assessing trust level of organizations in this VBE (see "c" below).

a) Selection of trust criteria from VBE-generic set of trust criteria to form the "VBE's pool of trust criteria"

In VBEs, trustor organizations assess the level of trust in trustee organizations on the basis of specific trust objectives and their preferred perspectives for trust establishment. In Section 3.3 we identified three generic categories of trust objectives for VBEs. The first category of trust objectives, namely "creating trust between organizations", is used in VBEs for any of the following reasons:

- Acceptance of a new organization's membership application in the VBE
- Invitation of potential VBE members to participate in a VO
- Periodic control of the level of trust in VBE member organizations.

To meet the assessment of trust level of organizations such trust objectives, may apply different sets of trust criteria, which will be subsets of the VBE's pool of criteria. Consider the example 5.1 which represents a VBE case used in this chapter to exemplify our approach.

Example 5.1:

Consider an example case of a VBE that specializes in the production and preservation of perishable food, and especially in processed fish products. This specific example is supposed to be focused on fish processing and work in two geographic zones. The first zone *(local center)* is where the fishing is carried out, and where the organizations which do the pre-processing are located. The second zone *(international center)* is a neighboring country in which the international export of smoked, canned, and frozen fish products is carried out, and where the organizations that carry out the final processing steps and marketing are located. The processing activities at the local center include: cleaning fish, cutting off heads, clearing fins, removing entrails, intermediate packaging, etc. The activities at the international center include: removing bones, cutting fish into pieces, smoking, canning, freezing, and packaging according to specific customer demands, preservation treatments, marketing, etc.

Here, the VBE administrator needs to select some trust criteria from the **generic set of trust criteria** as presented in Section 3.3 to include within this **VBE's pool of trust criteria**. The VBE administrator will go through all trust perspectives, in the general set of trust criteria, selecting the preferable trust criteria for the VBE. Each VBE's pool of trust criteria constitutes all trust criteria that are applicable in the VBE for assessing the base trust level as well as for evaluating specific trustworthiness of organizations by different trustors in the VBE. To give examples, in this section, we focus on *structural perspective*. The VBE administrator shall subsequently select specific trust requirements for further realization of the structural perspective. For example, in this case, the *structural strength* and *business strength* requirements would be chosen (see Figure 5.3). Following this selection of trust requirements, the VBE administrator will select preferred trust criteria for each trust requirement. For instance, for the structural strength requirements, trust criteria such as *size*, *competency*, and *number of experts*; and for the business strength requirements, trust criteria such as *centers* and *workload allocation* will be selected. Lastly, the VBE administrator will decide on the *value structure* for each trust criterion.

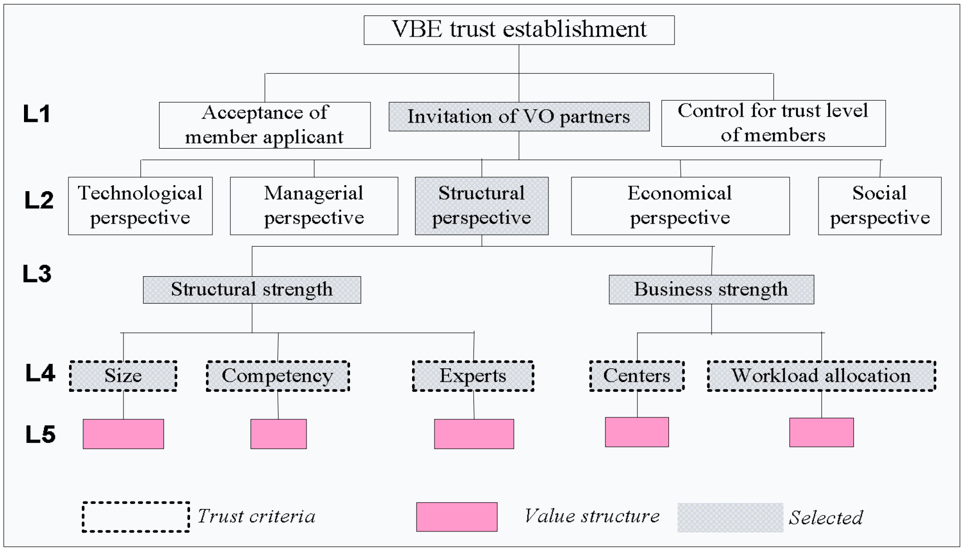


Figure 5.3: A systematic selection of trust criteria

As a part of a customization of the TrustMan system, this figure shows that for the specific trust objective of "invitation of VO partners" (at L1) the VBE administrator has selected the structural perspective (at L2) and in turn both structural strength and business strength (at L3), as well as five trust criteria (at L4) together with their value structure (at L5). Please see the complete set of trust criteria, requirements and perspectives in Figure 3.6.

Using the HICI approach presented in Section 0, Figure 5.3 illustrates this systematic selection of preferred trust criteria. The selection of trust criteria follows the hierarchical analysis that represents the first stage of the HICI approach as presented in Chapter 3.

b) VBE-generic analysis of impact of trust criteria and intermediate factors on trust level of organizations

Impact analysis represents the second stage of the HICI approach as addressed in Chapter 3. Using the impact analysis approach we have defined four intermediate factors – F1 to F4, namely, processing *capacity, connections, common context and social capital* – that are influenced by the five trust criteria that are selected as shown in Figure 5.3, i.e. *size, competency, experts, centers, and workload allocation*. Figure 5.4 shows the impact analysis for the selected trust criteria and their respective intermediate factors.

Please note that many more intermediate factors (i.e. F5 to F16) are further identified with the help of experts during the analysis of causal influences between trust criteria and intermediate factors, as shown in Figure 5.5. The interpretation and explanation of the components addressed in Figure 5.4 are presented in Section 3.2.2.

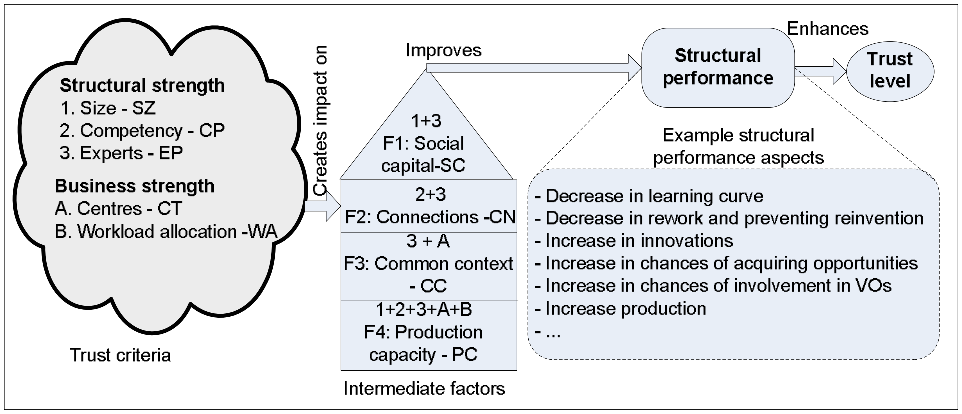


Figure 5.4: VBE-generic impact analysis of the selected trust criteria for the structural perspective

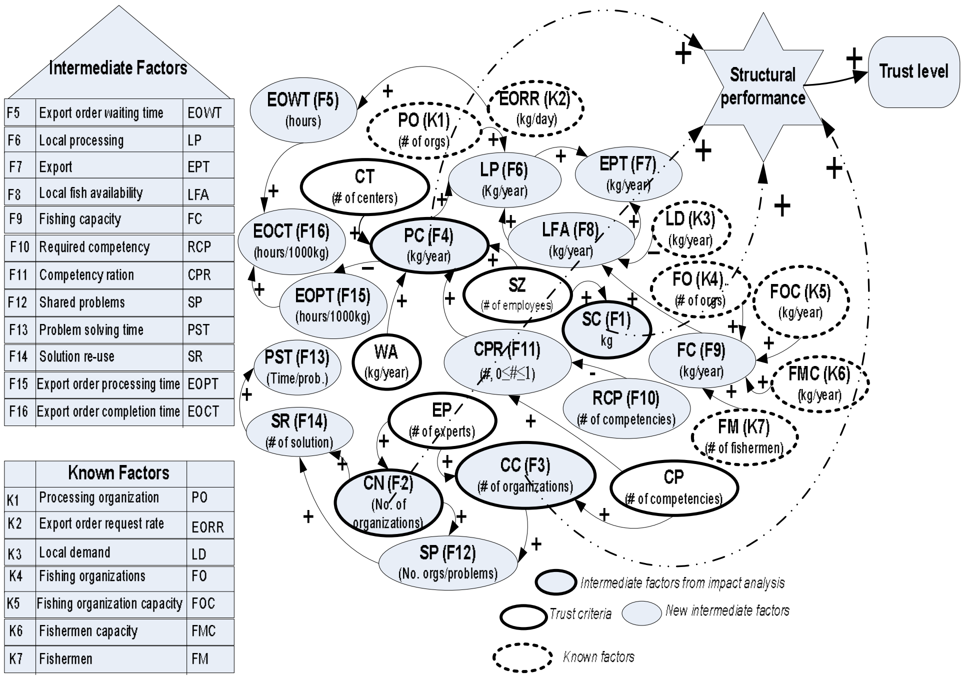
This figure represents a customization of the generic impact analysis for the structural perspective as shown in Figure 3.3. The analysis is done by defining intermediate factors to link selected trust criteria and certain performance aspects. The links indicate how changes of values of trust criteria can create impact on the trust level of organizations. Note the two examples (3.1 and 3.2) in Section 3.2.2 describing this figure.

c) Analysis of causal relations between trust criteria, known factors and intermediate factors in a specific VBE

To effectively assess the level of trust in organizations, inter-relations between trust criteria, known factors and intermediate factors in the VBE environment must be analyzed and well understood. This means that a priori to formulating mathematical equations, which will be used for developing mechanisms for assessing organization's trust level, the scope of the TrustMan system must be analyzed and specified. Specifying the scope of a system is a main concern in the process of systems development due to the continuous changing of system requirements related to users and operational environments. The challenge here is "how do define the scope of the trust management system?" Response to this challenge is not straightforward, because the trust management system is a part of the VBE management system, namely a part of a set of systems that together manage the VBE environment [Maciaszek, 2007]. These systems interoperate by exchanging information and invoking services from each other.

In order to specify the scope of the TrustMan system we therefore need to know the context in which it operates, such as in our case each specific VBE environment. We need to specify the elements that can be considered inside that environment (internal factors) and thus need to be modeled and implemented. We also need to specify elements that can be considered as outside the system (external factors) that require to be analyzed to provide some understanding about any needed interaction between the TrustMan system and the external environment.

Specification of the scope of the TrustMan system is done through classifying its known factors and intermediate factors as shown in the causal diagram illustrated in Figure 5.5, into the internal factors – those that must be included in the equations – and the external factors – those that are considered outside the system and do not need to be included in the equations. For this purpose, both known factors and intermediate factors are analyzed to examine the intensity of their influence on each other, so that they may be divided into those that should be inside the system, and those that should be regarded as external factors. External factors (both known and intermediate) are those factors that while still influencing the system, have an influence which is assumed to be uncontrollable both by the system and its users.



Intermediate Factors		
F5	Export order waiting time	EOWT
F6	Local processing	LP
F7	Export	EPT
F8	Local fish availability	LFA
F9	Fishing capacity	FC
F10	Required competency	RCP
F11	Competency ration	CPR
F12	Shared problems	SP
F13	Problem solving time	PST
F14	Solution re-use	SR
F15	Export order processing time	EOPT
F16	Export order completion time	EOCT

	Known Factors	
K1	Processing organization	PO
K2	Export order request rate	EORR
K3	Local demand	LD
K4	Fishing organizations	FO
K5	Fishing organization capacity	FOC
K6	Fishermen capacity	FMC
K7	Fishermen	FM

Figure 5.5: Customized causal relations between trust criteria, intermediate factors, and known factors

The analysis considers the selected trust criteria, VBE generic intermediate factors, VBE specific intermediate factors and the known factors. This figure shows an extended and customized causal diagram for the measurable parameters associated with the structural perspective as addressed in this section. Some examples describing this follow below.

Following the division of such external factors and internal factors, the derivation of formulas subsequently focuses *only on intermediate factors that are classified to be inside the system.* Therefore, specifying the system's scope enables a reduction in the number of formulas that have to be derived for intermediate factors, while preserving the expected functionalities and the effectiveness of those parts of the system that can be controlled.

With the help of experts in the field and survey of past research, some inter-relations between pre-defined "general" trust criteria (see Figure 5.2) can be developed a-priori to the establishment of any VBE as exemplified in Section 3.3. However, with the help of trust experts, this generic model of inter-relations may be later customized to different specific VBE domain/application (e.g. as shown in Figure 5.5), and/or it may be required to dynamically define additional new intermediate factors for these inter-relations. In this section, all the intermediate factors and known factors specified in Figure 5.4 are considered to be inside the system.

While customizing and formulating the VBE pool of trust criteria, the inter-relations between trust criteria, known factors, and intermediate factors, as well as the causal influences these have on each other, must be carefully analyzed and modeled. Please note that during customization, further to the identification of new intermediate factors, a number of known factors may be also identified. Known factors represent elements for which their values are known within the VBE environment; for example, the number of required competencies per organization in the VBE (RCP) which can be a generic known factor for any VBE, or the number of fishing organizations (FO) which is a specific known factor for the fish processing VBE.The list of known factors (K1 to K7) is represented in Figure 5.5 for the fish processing VBE. Figure 5.5 illustrates a causal diagram that represents both a set of additional intermediate factors (F5-F16) and a set of known factors (K1 to K7) that are involved in the influence relations between the trust criteria, intermediate factors and known factors. Please note that the metrics for values are represented inside parenthesis in each oval, which are needed and are used in the definition of formulas.

As described in Section 3.2.3, in the causal diagram a plus sign (+) on an arrow indicates that the increase or decrease of the source (first) factor respectively causes an increase or decrease in the destination (second) factor. On the contrary, the minus sign (-) indicates that the increase or decrease in the first factor respectively leads to a decrease or increase in the second factor. As shown in Figure 5.5, for example, "competency ratio" – CPR (intermediate factor) is positively influenced by "competency" –CP (trust criteria) and negatively influenced by "required competency" – RCP (known factor). The CPR positively influences the "production capacity" – PC (intermediate factor). PC is also positively influenced by: "workload allocation" – WA, "size" of the organization– SZ, and "production centers" – CT, which are all trust criteria. The PC itself is known factor that positively influences the structural performance of the organization. Lastly, the structural performance positively influences the trust level of the organization.

For the sake of illustration, we will derive mathematical equations for four intermediate factors. We will derive equations for processing capacity –PC (F4), export order completion time –EOCT (F16), export order processing time –EOPT (F15) and export order waiting time –EOWT (F5) to exemplify *different level of sophistication* needed for the developed formulas. Namely, with the *dimensional analysis* applied to PC (see example 1 in Section 5.4.3), it needs the multiplication and division for equation (5.1). For EOCT (example 3), it needs only addition. However, the examples 4 and 5 require more complex analysis of the inter-relationships among the trust criteria, known factors, and the intermediate factors for which the use of queuing theory is needed to derive the required formulas.

Example 2: Developing an equation for processing capacity (PC)
We refer here to PC as the amount of fish (expressed in kilogram, or kg) that an organization can process during a specified period of time. Three trust criteria directly influence the behavior of PC, namely: *size of the organization (**SZ**), which refers to the number of employees; the workload allocation (**WA**), which refers to the standard amount of fish that a fully qualified employee is able to process in a specified period of time; and processing centers (**CT**), which refers to the number of processing centers at different places. PC is also influenced by* one other intermediate factor, namely *the competency ratio (**CPR**), which refers to the ratio of the number of competencies that an organization can offer to the total number of competencies required in the VBE.*

The equations for the example 1 have been formulated as shown in equations (5.1, (5.2) and (5.3) in Section 5.4.3. Considering that the same parameters are also applied here in the example 2, having the same causal relations, the equations for PC in this case are the same as those formulated in example 1. The equations for all other intermediate factors except the "*export order processing time"* – EOPT, and "*export order waiting time*" – EOWT as shown in Figure 5.5 can be formulated following the same approach that is presented in Section 5.4.3. In some cases, the influencing relations of known factors and trust criteria to an intermediate factor are too complex to represent mathematically using direct arithmetic operands and operators, due to the fact that their dimensions cannot be directly balanced. The dimensions of the involved factors in some relations (e.g. influences directed to EOWT and EOPT) cannot directly balance in the equation, due to some specific complex behavior, e.g. statistical behavior, exponential behavior, etc. Furthermore, there are also a number of other aspects (such as waiting time, service rate, etc.) that need to be addressed applying specifically defined mathematical theories, such queuing theories, exponential distribution, Poisson distribution, etc. For the examples 4 and 5 presented below, we use queuing theory to derive equations for the two intermediate factors, namely, EOPT and EOWT. But, below we first present example 3 whose results are later used in examples 4 and 5.

Example 3: Developing equations for export order completion time (EOCT)
Similar to example 1, the respective three equations namely, arithmetic equations, derivative equations, and integral equations for EOCT are generated as follows:

$$EOCT = EOWT + EOPT \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\textbf{(5.4)}$$

$$\frac{d}{dt}EOCT = \frac{d}{dt}EOWT + \frac{d}{dt}EOPT \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\textbf{(5.5)}$$

$$\int_{t1}^{t2}(EOCT) = \int_{t1}^{t2}(EOWT) + \int_{t1}^{t2}(EOPT) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\textbf{(5.6)}$$

Where the **EOWT** (export order waiting time) is the time that an order is queued and waiting (delay) before the processing of fish can start, the **EOPT** (export order processing time) is the time required to process a specified amount of fish for a given order. These two intermediate factors are addressed below in examples 4 and 5.

Examples 4 & 5: Developing equations for export order waiting time (EOWT) and export order processing time (EOPT)

For these two intermediate factors, we need to apply the ***Queuing theory*** to formulate their respective equations. The Queuing theory [Adan & Resing, 2001] can be simply stated as the mathematical study of waiting in lines (or queues). This theory enables the mathematical analysis of several related processes, including arriving at the (end of the) queue, waiting in the queue, and being served by the server(s) at the front of the queue. This theory guides the derivation and calculation of several performance measures, including the average waiting time in the queue or system, the expected number of entities that are waiting or receiving services, and the probability of encountering the system in certain states, such as empty, full, having an available server, or having to wait for a certain time before being served. Queuing theory is generally considered as a branch of operations research, as a result it is often used when making business decisions about resources needed to provide services. In order to illustrate the underlying principle of the Queuing theory a priori to addressing our example, we examine the M/M/1 queuing system (also known as Markovian Systems) [Adan & Resing, 2001]. Such a system is defined as a system that supports a *multiple number of arrivals* (λ) that are measured as an average number of arrivals based on specified probability distribution, a *multiple number of elements in the queue*, and a *single server* with a service rate (μ) that is measured as the average time needed to serve a single element based on the specified probability distribution. According to the Queuing theory definitions and, in particular, the Markov model, the arrival rate follows *Poisson distribution* with mean λ , and the service rate follows the *exponential distribution* with mean μ . Three main performance parameters are identified in the Queuing theory, namely *response time* (RT), *queuing time* (QT) and *service time* (ST). These parameters are mathematically defined as follows:

$$ST = \frac{1}{\mu}, \qquad QT = \frac{\lambda}{(\mu - \lambda) * \mu}, \qquad \text{and} \qquad RT = \frac{1}{\mu - \lambda}$$

Relating our example to the Queuing theory, we assume that there will be no limitation on the number of export orders received by an organization and that as many orders as possible may wait for processing. We refer to EOPT as the time that an organization will need in order to process a specified amount of ordered fish. We refer to the EOWT as the average time that an export order will wait in queue (delayed) from the time when it was received to the time that the processing of fish begins. Applying Queuing theory we can conclude that the three intermediate factors – EOPT, EOWT, and PC – are statistically related. Comparing with performance indicators applied in the Queuing theory, EOPT is similar to the *service time*, EOWT is similar to the *queuing time*, and PC is similar to the *service rate*. The export requests received by a certain organization to be processed are distinct. Thus both the export order request rate (EORR) and the PC follow the *Poisson distribution*. The EOPT follows the *exponential distribution* since it measures the time required to process a certain amount of fish for a single order. Based on the Queuing theory definitions, the equations for EOPT and EOWT are shown in equations (5.7a) and (5.8a). For this case, EORR is similar to the arrival rate in the Queuing theory. The differential equations for EOPT and EOWT are shown in equations (5.7b & 5.7c) and (5.8b & 5.8c) respectively.

Equations for EOPT:

$$EOPT = \frac{1}{PC} \text{........(5.7a);} \qquad \frac{d}{dt} EOPT = \frac{d}{dt}\left(\frac{1}{PC}\right) \text{......(5.7b);} \quad \int_{t1}^{t2} (EOPT) = \int_{t1}^{t2} \left(\frac{1}{PC}\right) \text{......(5.7c)}$$

Equations for EOWT:

$$EOWT=\frac{EORR}{(PC-EORR)PC}\text{............(5.8a);}\qquad \frac{d}{dt}EOWT=\frac{d}{dt}\left(\frac{EORR}{(PC-EORR)PC}\right)\text{..........................(5.8b)}$$

$$\int_{t1}^{t2}(EOWT)=\int_{t1}^{t2}\left(\frac{EORR}{(PC-EORR)PC}\right)\text{..(5.8c)}$$

Analysis of the causal relations between these intermediate factors in the causal diagram (Figure 5.5) shows that PC is negatively related to EOPT, which proves the fact that a minus sign can be represented as a division in the mathematical equation as shown in equation (5.7a). EORR is positively related to EOWT, but in the equation (5.8a) its representation is a very special case. Although it is in the quotient part of the equation (5.8a), the EORR is negated in the quotient, which indicates that it is in fact positively related to the EOWT.

Export order completion time (**EOCT**), as addressed in example 3, is in principle the sum of EOPT and EOWT, which match the relations as indicated in the causal diagram in Figure 5.5, and also as described in the Queuing theory. Therefore, equation (5.9a) shows the EOCT represented in an alternative equation for equation (5.4), with different parameters. Its respective differential equations are shown in equations (5.9b) and (5.9c).

$$EOCT=\frac{1}{PC-EORR}\text{...(5.9a);}\quad \frac{d}{dt}EOCT=\frac{d}{dt}\left(\frac{1}{PC-EORR}\right)\text{...(5.9b)}\quad \int_{t1}^{t2}(EOCT)=\int_{t1}^{t2}\left(\frac{1}{PC-EORR}\right)\text{...(5.9c)}$$

5.5 Analysis of causal influences among trust criteria

In this section, we analyze the causal influences among the trust criteria, the known factors and the intermediate factors for each trust perspective. The results of the causal analysis are then applied to formulate mathematical equations to support the development of mechanisms for assessing level of trust in organizations. In this section, three kinds of mathematical equations are formulated for each intermediate factor. Each equation supports the analysis of different aspects of the inter-organizational trust as follows:

- ***Arithmetic equations***: These equations support the evaluation of trust level of an organization at a certain point in time. For example, they are used to compute trust level of organizations at the day that a selection of partners to join a VO is made.
- ***Derivative equations***: These equations support the analysis of evolution of the trust level of an organization at certain in point in time. For example, they are used to support examining whether the trust level of each selected VO partner is increasing, decreasing or uniform at the time selection of partners is made. The derivative equations are formulated by differentiating the arithmetic equations and for this purpose all parameters in each arithmetic equation, as addressed in Sections 5.5.1, 5.5.2, 5.5.3 and 5.5.4, are assumed to be continuous in respect to time.
- ***Integral equations***: These equations support the analysis of the average of the trust level scores of an organization for a certain interval of time by providing the possibility to capture the accumulations of trustworthiness scores in that period. For example, they are used to support the analysis of the average trust level of an organization for an entire period of its involvement in the VO. The integral equations are formulated by integrating the arithmetic equations and for this purpose all parameters in each arithmetic equation, as addressed in Sections 5.5.1, 5.5.2, 5.5.3 and 5.5.4, are assumed to be continuous in respect to time. Thus the integration of arithmetic equations is performed with respect to time.

5.5.1 Social perspective

As described in Section 3.2, the analysis of causal relations among trust criteria involves identifying both the intermediate factors and the known factors. Trust criteria related to social perspective are presented in Section 3.3.1 and in detail described in Table 3.2. For the this trust perspective, one intermediate factor was identified – *social acceptance (SAC)* – and three known factors, namely (1) *Societal activities (SA),* (2) *Services needed (SN),* and (3) *Societal standards (SS).* Figure 5.6 represents the causal influences between the trust criteria, known factors and intermediate factors.

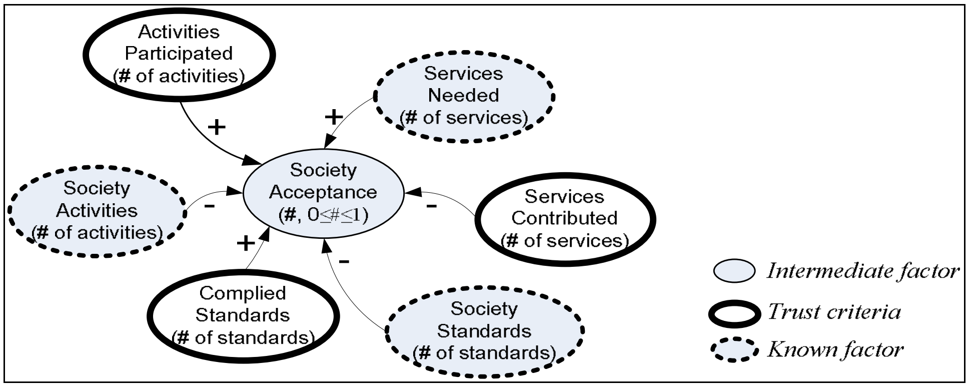

Activities Participated (# of activities)
+
Services Needed (# of services)
+
Society Activities (# of activities)
-
Society Acceptance (#, 0≤#≤1)
-
Services Contributed (# of services)
+
-
Complied Standards (# of standards)
Society Standards (# of standards)
Intermediate factor
Trust criteria
Known factor

Figure 5.6: Causal influences between trust criteria for social perspective

This figure shows a qualitative analysis of causal influences between measurable parameters for the social perspective, namely, its associated trust criteria, known factors and intermediate factors.

As addressed in Section 5.4.3, results of the causal analysis are applied to the formulation of mathematical equations. The equations are derived by relating an intermediate factor, as the subject of equation, to the trust criteria and known factors. Using the acronyms of trust criteria presented in Table 3.2, below are the arithmetic, differential and integral equations for social acceptance (measured in: # *in a range of* $0 \leq \# \leq 1$*)*:

$$SAC=\frac{1}{3}\left(\frac{AP}{SA}+\frac{SC}{SN}+\frac{CS}{SS}\right); \quad \frac{d}{dt}SAC=\frac{d}{dt}\left[\frac{1}{3}\left(\frac{AP}{SA}+\frac{SC}{SN}+\frac{CS}{SS}\right)\right]; \quad \int_{t1}^{t2} SAC = \int_{t1}^{t2}\frac{1}{3}\left(\frac{AP}{SA}+\frac{SC}{SN}+\frac{CS}{SS}\right)$$

5.5.2 Economical perspective

A number of trust criteria related to the economical perspective are presented in Section 3.3.1 and in detail described in Table 3.3. Figure 5.7 visualizes the causal influences (in a causal diagram) between trust criteria, known factors, and intermediate factors related to economical perspective. Using the acronyms of trust criteria which are presented in Table 3.3, below we present the mathematical equations derived for intermediate factors of the economical perspective as shown in Figure 5.7.

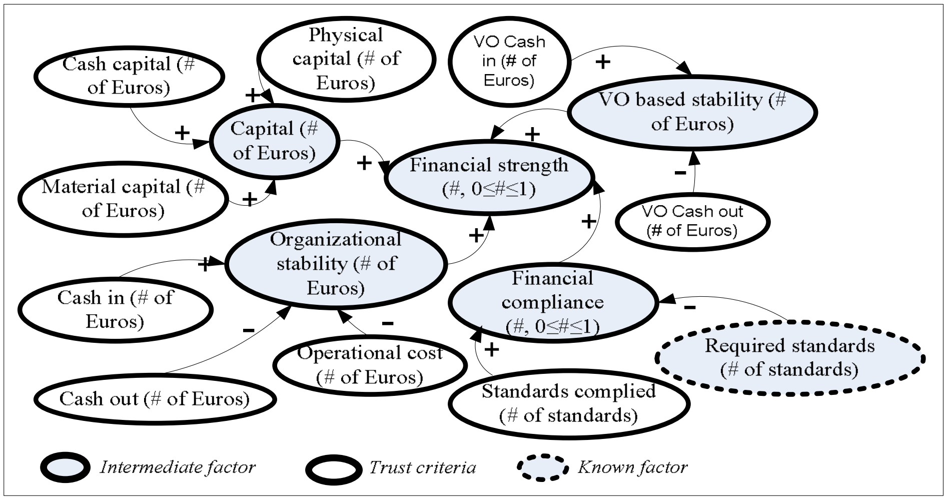

Cash capital (# of Euros)
Physical capital (# of Euros)
VO Cash in (# of Euros)
VO based stability (# of Euros)
Capital (# of Euros)
Financial strength (#, 0≤#≤1)
Material capital (# of Euros)
VO Cash out (# of Euros)
Organizational stability (# of Euros)
Financial compliance (#, 0≤#≤1)
Cash in (# of Euros)
Required standards (# of standards)
Operational cost (# of Euros)
Standards complied (# of standards)
Cash out (# of Euros)
+
+
+
+
+
+
+
+
+
+
-
-
-
-
Intermediate factor
Trust criteria
Known factor

Figure 5.7: Causal influences between trust criteria for economical perspective

This figure shows a qualitative analysis of causal influences between measurable parameters for the economical perspective, namely, its associated trust criteria, known factors and intermediate factors.

***(1) Equations for capital (CA,** measured in: Euros)*

$$CA = CC + PL + MC$$

$$\frac{d}{dt}CA = \frac{d}{dt}CC + \frac{d}{dt}PL + \frac{d}{dt}MC$$

$$\int_{t1}^{t2}(CA) = \int_{t1}^{t2}(CC) + \int_{t1}^{t2}(PL) + \int_{t1}^{t2}(MC)$$

***(3) Equations for organization stability (OS,** measured in: Euros)*

$$OS = CI - CO - OC$$

$$\frac{d}{dt}OS = \frac{d}{dt}CI - \frac{d}{dt}CO - \frac{d}{dt}OC$$

$$\int_{t1}^{t2}(OS) = \int_{t1}^{t2}(CI) - \int_{t1}^{t2}(CO) - \int_{t1}^{t2}(OC)$$

***(2) Equations for VO based stability (VS,** measured in: Euros)*

$$VS = VCI - VCO$$

$$\frac{d}{dt}VS = \frac{d}{dt}VCI - \frac{d}{dt}VCO$$

$$\int_{t1}^{t2}(VS) = \int_{t1}^{t2}(VCI) - \int_{t1}^{t2}(VCO)$$

***(4) Equations for financial compliance (FA,** measured in: # in range of* $0 \le \# \le 1$*)* where RS (*measured in: # of standards*) refers to required standards

$$FA = \frac{AS}{RS}\ ;\ \frac{d}{dt}FA = \frac{d}{dt}\left(\frac{AS}{RS}\right)$$

$$\int_{t1}^{t2}(FA) = \int_{t1}^{t2}\left(\frac{AS}{RS}\right)$$

***(5) Equations for financial strength (FS,** measured in: # in range of* $0 \le \# \le 1$*)*

As explained in Section 3.2, when the intermediate factor (source factor) influences another intermediate factor (destination factor), the source factor is assumed as a known factor and its equation can be applied to the equation of the destination factor. For example, as shown in

Figure 5.7 the intermediate factors: capital, organizational stability, financial acceptance are perceived as known factors when formulating equations for the financial strength. Therefore, the arithmetic, differential and integral equations for financial strength (FS) can be formulated as shown below.

$$FS = \frac{1}{2}\left[\left(\frac{OS+VS}{CA}\right)+FA\right]; \quad \frac{d}{dt}FS = \frac{d}{dt}\left(\frac{1}{2}\left[\left(\frac{OS+VS}{CA}\right)+FA\right]\right); \quad \int_{t1}^{t2}(FS) = \int_{t1}^{t2}\left(\frac{1}{2}\left[\left(\frac{OS+VS}{CA}\right)+FA\right]\right)$$

For the implementation of the equation for financial strength (FS) some necessary restrictions/assumptions need to be defined to ensure the correctness of the results that shall be computed using the equation. The following assumptions need to be implemented using some decision mechanisms such as using logical operations or selection mechanisms:

- If $FS \geq 1$ then the value of FS becomes 1 and it will be automatically assigned a score of 5 for the financial trustworthiness. In this case it indicates that the respective organization whose trustworthiness is being computed is making a healthier profit than its capital.
- If $FS < 0$ then the value of FS becomes zero and it will be automatically assigned a score of zero for the financial trustworthiness. In this case it indicates that the respective organization whose trustworthiness is being computed is making a financial loss in its businesses.

5.5.3 Technological perspective

A number of trust criteria related to technological perspective are presented in Section 3.3.1 and in detail described in Table 3.4. The results of the analysis of the causal influences between trust criteria, known factors and intermediate factors related to the technological perspective are shown in Figure 5.8. The following are the acronyms for known factors of the technological perspective.

Required interoperability	RIB	Required software standards	RSS
Required network speed	RNS	Required protocol standards	RPS
Required availability	RAV	Required experience	REP
Required security standards	RSC	Required operating systems	ROS
Required hardware standards	RHS	Required programming languages	RPL

Using the acronyms of trust criteria which are presented in Table 3.4, below we present mathematical equations formulated for six intermediate factors related to technological perspective.

***(1) Equations for experience gained (EG,** measured in: # of projects)*

$$EG = (VP + EP) * YH$$

$$\frac{d}{dt}EG = \frac{d}{dt}[(VP + EP) * YH]$$

$$\int_{t1}^{t2}\left(\frac{d}{dt}EG\right) = \int_{t1}^{t2}([(VP + EP) * YH])$$

***(2) Equations for ICT acceptance (IA,** measured in: # with range of* $0 \leq \# \leq 1$*)*[1]

$$IA = \left(\frac{AV}{RAV} + \frac{NS}{RNS} + \frac{IB}{RIB}\right) * \frac{1}{3}$$

$$\frac{d}{dt}IA = \frac{d}{dt}\left(\frac{AV}{RAV} + \frac{NS}{RNS} + \frac{IB}{RIB}\right) * \frac{1}{3}$$

$$\int_{t1}^{t2}[IA] = \int_{t1}^{t2}\left[\left(\frac{AV}{RAV} + \frac{NS}{RNS} + \frac{IB}{RIB}\right) * \frac{1}{3}\right]$$

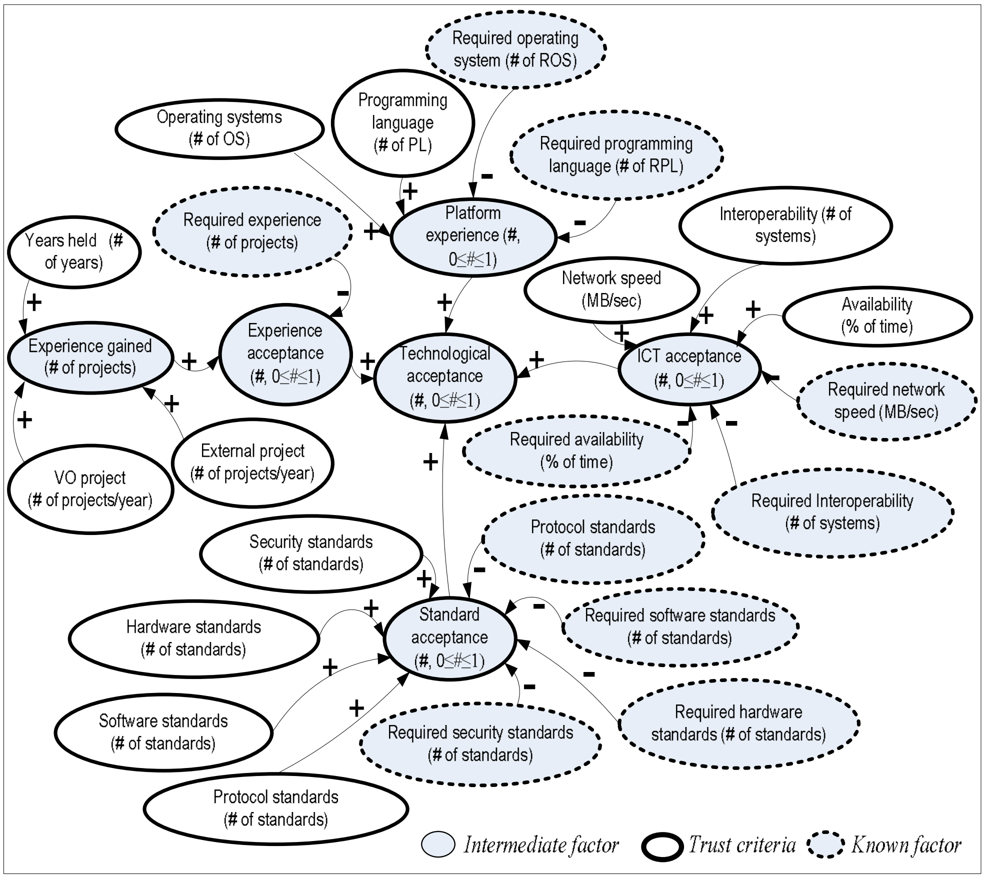

Required operating system (# of ROS)
Programming language (# of PL)
Operating systems (# of OS)
Required programming language (# of RPL)
Required experience (# of projects)
Platform experience (#, 0≤#≤1)
Interoperability (# of systems)
Years held (# of years)
Network speed (MB/sec)
Availability (% of time)
Experience gained (# of projects)
Experience acceptance (#, 0≤#≤1)
Technological acceptance (#, 0≤#≤1)
ICT acceptance (#, 0≤#≤1)
Required network speed (MB/sec)
Required availability (% of time)
External project (# of projects/year)
VO project (# of projects/year)
Required Interoperability (# of systems)
Protocol standards (# of standards)
Security standards (# of standards)
Standard acceptance (#, 0≤#≤1)
Required software standards (# of standards)
Hardware standards (# of standards)
Required hardware standards (# of standards)
Software standards (# of standards)
Required security standards (# of standards)
Protocol standards (# of standards)
Intermediate factor
Trust criteria
Known factor

Figure 5.8: Causal influences between trust criteria for technological perspective

This figure shows a qualitative analysis of causal influences between measurable parameters for the technological perspective, namely, its associated trust criteria, known factors and intermediate factors.

***(3) Equations for experience acceptance (EA,** measured in: # with range of* $0 \leq \# \leq 1)^{1}$

$$EA = \frac{EG}{REP}$$

$$\frac{d}{dt} EA = \frac{d}{dt}\left(\frac{EG}{REP}\right)$$

$$\int_{t1}^{t2} (EA) = \int_{t1}^{t2} \left(\frac{EG}{REP}\right)$$

***(4) Equations for standard acceptance (SA,** measured in: # with range of* $0 \leq \# \leq 1)^{1}$

$$SA = \left(\frac{SC}{RSC} + \frac{HS}{RHS} + \frac{SS}{RSS} + \frac{PS}{RPS}\right) * \frac{1}{4}$$

$$\frac{d}{dt} SA = \frac{d}{dt}\left(\frac{SC}{RSC} + \frac{HS}{RHS} + \frac{SS}{RSS} + \frac{PS}{RPS}\right) * \frac{1}{4}$$

$$\int_{t1}^{t2}\left(\frac{d}{dt} SA\right) = \int_{t1}^{t2}\left(\left(\frac{SC}{RSC} + \frac{HS}{RHS} + \frac{SS}{RSS} + \frac{PS}{RPS}\right) * \frac{1}{4}\right)$$

[1] For the implementation of these equations some necessary assumptions need to be made in order to ensure that the final value of the intermediate factor is always between 0 and 1 inclusive. Thus if the computed value is greater than 1 then the intermediate factor is automatically assigned a value of 1. This indicates that the organization has performed better than the threshold which is set in the VBE.

***(5) Equations for platform experience (PE,** measured in: # with range of* $0 \leq \# \leq 1$*)*[1]

$$PE = \left(\frac{OS}{ROS} + \frac{PL}{RPL}\right) * \frac{1}{2}$$

$$\frac{d}{dt}PE = \frac{d}{dt}\left(\frac{OS}{ROS} + \frac{PL}{RPL}\right) * \frac{1}{2}$$

$$\int_{t1}^{t2}(PE) = \int_{t1}^{t2}\left(\left(\frac{OS}{ROS} + \frac{PL}{RPL}\right) * \frac{1}{2}\right)$$

(6) Equations for technological acceptance (TA**, measured in: # with range of* $0 \leq \# \leq 1$)***

$$TA = \frac{SA + IA + PE + EA + EG}{5}$$

$$\frac{d}{dt}TA = \frac{d}{dt}\left(\frac{SA + IA + PE + EA + EG}{5}\right)$$

$$\int_{t1}^{t2}\frac{d}{dt}(TA) = \int_{t1}^{t2}\left(\left[\frac{SA + IA + PE + EA + EG}{5}\right]\right)$$

5.5.4 Managerial perspective

A number of trust criteria related to managerial perspective are presented in Section 3.3.1 and in detail described in Table 3.5. The results of the analysis of causal influences between trust criteria, known factors, and intermediate factors related to the managerial perspective are shown in Figure 5.9.

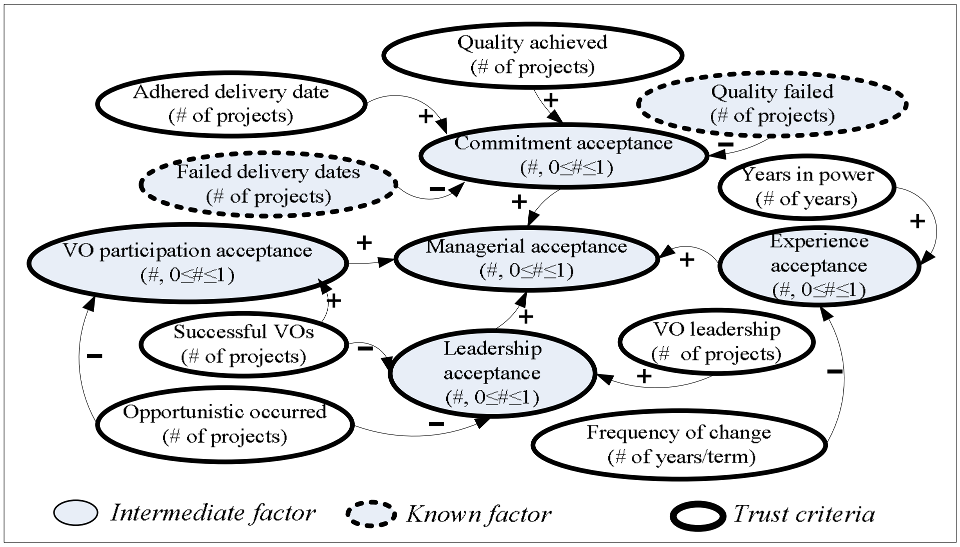

Quality achieved (# of projects)
Adhered delivery date (# of projects)
Quality failed (# of projects)
Commitment acceptance (#, 0≤#≤1)
Failed delivery dates (# of projects)
Years in power (# of years)
VO participation acceptance (#, 0≤#≤1)
Managerial acceptance (#, 0≤#≤1)
Experience acceptance (#, 0≤#≤1)
Successful VOs (# of projects)
Leadership acceptance (#, 0≤#≤1)
VO leadership (# of projects)
Opportunistic occurred (# of projects)
Frequency of change (# of years/term)
+
−
Intermediate factor
Known factor
Trust criteria

Figure 5.9: Causal influences between trust criteria for managerial perspective

This figure shows a qualitative analysis of causal influences between measurable parameters for the managerial perspective, namely, its associated trust criteria, known factors and intermediate factors.

We have applied the results of the causal analysis to formulate mathematical equations for the intermediate factors as shown in Figure 5.9. For the managerial perspective, we have identified two known factors, namely, the failed delivery dates (FD, *measured in: # of projects*) and the quality failed (QF, *measured in: # of projects*). Using the acronyms of trust criteria presented in Table 3.5, below we present the equations for the intermediate factors related to managerial perspective.

(1) VO participation acceptance (VA) where the sum of OO and SV represents the total number of VOs.

$$VA = \frac{SV}{OO + SV}$$

$$\frac{d}{dt}VA = \frac{d}{dt}\left(\frac{SV}{OO + SV}\right)$$

$$\int_{t1}^{t2}[VA] = \int_{t1}^{t2}\left[\left(\frac{SV}{OO + SV}\right)\right]$$

(2) Leadership acceptance (LA) where the sum of OO and SV represents the total number of VOs.

$$LA = \frac{VL}{OO + SV}\ ;\ \frac{d}{dt}LA = \frac{d}{dt}\left(\frac{VL}{OO + SV}\right)$$

$$\int_{t2}^{t1}[LA] = \int_{t1}^{t2}\left[\left(\frac{VL}{OO + SV}\right)\right]$$

(3) Commitment acceptance (CP) where the sum of AD and FD as well as QA and QF represents the total number of projects that the organizations provided services (participated).

$$CP = \left(\frac{AD}{AD + FD} + \frac{QA}{QA + QF}\right) * \frac{1}{2}$$

$$\frac{d}{dt}CP = \frac{d}{dt}\left[\left(\frac{AD}{AD + FD} + \frac{QA}{QA + QF}\right) * \frac{1}{2}\right]$$

$$\int_{t2}^{t1}(CP) = \int_{t2}^{t1}\left(\left[\left(\frac{AD}{AD + FD} + \frac{QA}{QA + QF}\right) * \frac{1}{2}\right]\right)$$

(4) Experience acceptance (EA)[1]

$$EA = \frac{YP}{FP}\ ;\ \frac{d}{dt}EA = \frac{d}{dt}\left(\frac{YP}{FP}\right);\ \int_{t1}^{t2}[EA] = \int_{t1}^{t2}\left(\frac{YP}{FP}\right)$$

(5) Managerial acceptance (MA)

$$MA = \frac{CA + VA + LA + EA}{4};\ \frac{d}{dt}MA = \frac{d}{dt}\left(\frac{CA + VA + LA + EA}{4}\right);\ \int_{t1}^{t2}[MA] = \int_{t1}^{t2}\left[\left(\frac{CA + VA + LA + EA}{4}\right)\right]$$

Implementation of mathematical equations in TrustMan system

The mechanisms introduced for assessing the trust level of organizations are implemented in the TrustMan system using the mathematical equations presented in this chapter. As addressed in Chapter 6, the TrustMan system provides two integrated services particularly designed to support the measurement of the trust level of organizations, namely, services for the *assessment of the base trust level of VBE member organizations (Service 1)* and for the *evaluation of specific trustworthiness of VO partners (Service 2)*. As such, these services support the analysis of trust in organizations only at specific points in time. For these two services, all related mechanisms for assessing the level of trust in organizations are implemented applying the arithmetic equations. The current implementation of TrustMan system addresses and meets the VBE requirements identified in Chapter 1. Our further research on advanced support systems for VBEs aims at the development of decision support systems based on the analysis of evolution of trust level of organizations. This in turn will require the implementation of the differential equations as addressed in this chapter.

5.6 Chapter discussion and conclusion

As presented in this chapter about the need for assessing trust level of an organization in the VBE, a wide range of trust criteria may be considered while evaluating organization's trustworthiness. Trust in VBEs is characterized as a multi-objective, multi-perspective and multi-criteria subject. Trust is not a single concept that can be applied to all cases for trust-based decision-making [Msanjila & Afsarmanesh, 2006a], and its measurements depend on both the purpose of establishing a trust relationship and its specific involved actors. Trust level of an organization can be measured rationally in terms of quantitative values of related trust criteria e.g. based on an organization's past performance. The level of trust in an organization is complex and can neither be measured with single value of a single parameter, nor interpreted with a single metric. Nonetheless, an organization's level of trust can be specified on the basis of the values for a set of related trust criteria.

Understanding and interpreting the level of trust in an organization, described and formulated in terms of values of a set of trust criteria, will be complex and difficult to grasp for most decision-makers in organizations, such as managers and directors, if they are not trust experts and do not have sufficient knowledge in both mathematics and computer applications. Therefore, the trust level of organizations must be presented in a format that is as understandable as possible to the expected users while not loosing its semantics. This thesis proposes that the level of trust in organizations should be represented and expressed in terms of a set of qualitative values, and these values can only represent comparative levels of trust in different organizations in a VBE for a specific given trust purpose, and not as absolute levels.

Therefore, this chapter has addressed the main research question (MRQ3) and its related sub-questions (SRQ3.1, SRQ3.2, SQR3.3 and SQR3.4). We have presented how the level of trust in an organization can be measured. The chapter has also addressed MQ1 by presenting an approach for developing mechanisms to assess trust level of an organization. In Chapter 7 an integrated view on how all the questions in this dissertation are addressed is presented.

In conclusion, this chapter introduces a mathematical model for organizations' trust assessment, and a replicable approach for customization of the general trust management system for each specific VBE. It has also addressed the formulation of mechanisms for assessing the level of trust in an organization. These mechanisms are formulated by applying mathematical equations which are derived from the results of analysis of causal influences between trust criteria, known factors and intermediate factors. Therefore, the chapter has presented a mathematical approach to generate formal mechanisms for assessing an organization's level of trust. The assessment of the level of trust in an organization might differ in terms of the possible comprehensiveness depending on the time the results will be applied (e.g. forecasting trust level) and the amount of data that need to be applied (e.g. large volume of data from many past years). To address these different levels of complexities three kinds of equations – *arithmetic, derivative, and integral* – are proposed and exemplified.

The mechanisms for assessing trust level of organizations as presented in this chapter, the models of trust relationships as presented in Chapter 4 and set of trust elements as presented in Chapter 3 constitute a key input concepts to the development of the organizational trust management system (TrustMan system) as presented in the next chapter (Chapter 6).

Chapter 6

Development of trust management system for VBEs

One obstacle to the configuration of VOs as well as the management of VBEs has been the difficulty in assessing the trust level of involved organizations. The assessment of trust level of organizations has been performed manually by trustors and in ad hoc manners, which is both time consuming and hardly produces accurate results. Consequently, formation of collaborative initiatives in form of temporary consortiums such as VOs has become more challenging and organizations are reluctant to work with each other. This chapter presents the development of services constituting the trust management system which is designed to support the management of trust among organizations reqiored for VO creation in the VBE.

The content of this chapter constitutes materials from three published articles, which appeared in the International Journal of Software [Msanjila & Afsarmanesh, 2008d], in lecture notes in computer science [Msanjila & Afsarmanesh, 2007e] and in the International Journal of Production Research [Msanjila & Afsarmanesh 2009].

6.1 Introduction

This chapter presents the development of the **Trust Man**agement (TrustMan) system. It addresses the analysis, specification, architectural design and implementation aspects related to different steps for its system development. The TrustMan system is designed to assist the management of the VBEs (as addressed in Chapter 1), by handling tasks related to control and assessment of trust level of organizations within the VBE. TrustMan system is a subsystem of the so-called VBE management system (VMS), as further addressed in Section 6.2.

The remaining of this chapter is organized as follows: Section 6.2 presents the VBE management system and introduces its main subsystems. Section 6.3 introduces the main concepts relating to the TrustMan system and presents aspects regarding the implementation of mechanisms for assessing the level of trust in organizations. Section 6.4 presents the analysis and specification of the TrustMan system through its *potential users and their requirements, as well as proposed functionalities and services*. Section 6.5 presents the design of the TrustMan system and provides its "*interoperability architecture"* and its *"four-layer componential architecture*". Section 6.6 addresses the implementation of the TrustMan system and its adaptation to industrial VBE networks. Lastly, Section 6.7 presents some conclusions and a summary of the concepts addressed in this chapter.

6.2 VBE management system

Collaboration among autonomous and geographically dispersed organizations is a process increasingly facilitated by advances in computer networks, support services, and related technologies. Collaboration among different sites is important for facilitating and leveraging various activities in societies, such as those related to innovation, scientific research, emergency and disaster management, and so on. As a result of intense research and development in this area, new specialized management systems for collaborative networks are now being developed. One challenging task in this process is the development of a system providing services for the management of the collaborative networks, such as the VBEs.

The management system in collaborative networks is a collection of services and functionalities supporting the framework of processes and procedures used by stakeholders during its life cycle, which ensures that the network can operate smoothly fulfilling all required tasks to achieve its objectives [Afsarmanesh et al., 2008]. The VBE management system shall perform the administrative tasks including the assignment of partner responsibility, maintaining a schedule for activities to be performed, as well as providing a set of tools to facilitate the implementation of actions and such scheduled activities; thus creating a productive and smooth VBE environment. Such a system is here referred to as the VBE management system (VMS). Thus the VMS serves the purpose of assisting the VBE administration in performing its tasks related to the management of the VBE, and its successful progression towards achieving its objectives.

6.2.1 VMS base concepts and motivation

Collaborative Networks (CN) have been established as an emerging new scientific discipline (Camarinha-Matos & Afsarmanesh, 2005). A number of specific forms of CNs can be currently observed in business practices and society. However, as new forms of CNs are emerging, innovative solutions are required to address the many challenges faced by collaborating partners, and in particular within VBEs.

A number of VBE networks (or similar such networks that share some characteristics with the VBEs) now exist world-wide, including the SwissMicroTech (Switzerland), the HELICE (Spain), the CeBeNetwork (Germany), and the IECOS (Mexico) (see their description in Annex C). Management activities of these VBE networks can be facilitated with certain semi-automated tools and services that aim to enhance the efficiency of performing VBE activities, such as reducing the required resources, time and costs. However, the existing management systems in currently operational VBEs are limited and do not properly support their requirements capturing all characteristics of VBEs. One such characteristic is the involvement of organizations which are heterogeneous in many aspects (e.g. their structural, componential, functional and behavioral aspects), and autonomous in their decision making, systems of values, and interests in the market and society (Afsarmanesh, et al. 2007). A number of sub-systems need to be developed for the VMS, as described in the next section. For example, the VMS is aimed to assist the VBE administration with performing the following tasks:

- Managing the profiles and competencies related to the VBE member organizations, to VOs, and to the VBE itself
- Management and discovery of the ontology for the VBE environment
- Assessing, managing and balancing the trustworthiness of the organizations in the VBE
- Collecting/managing information related to the performance of organizations within the VBE
- Supporting the acquisition of new members and managing the VBE member structure
- Managing the collective assets (data, best practices, software, etc.) in the VBE and VO
- Supporting the processes of decision making based on some collected data in VBEs.

It is necessary to note that the need for addressing the above specific VMS components is identified through extensive requirement analysis and road-mapping work carried out in previous research relating to the EC-funded project VO-map (Camarinha-Matos, Afsarmanesh, 2003). The fundamental requirement analysis and road-mapping results were achieved together, and/or in consensus with a large group of field experts involved in this initiative, and were further validated and approved by the CN community of experts, including academic, research and industry visionaries.

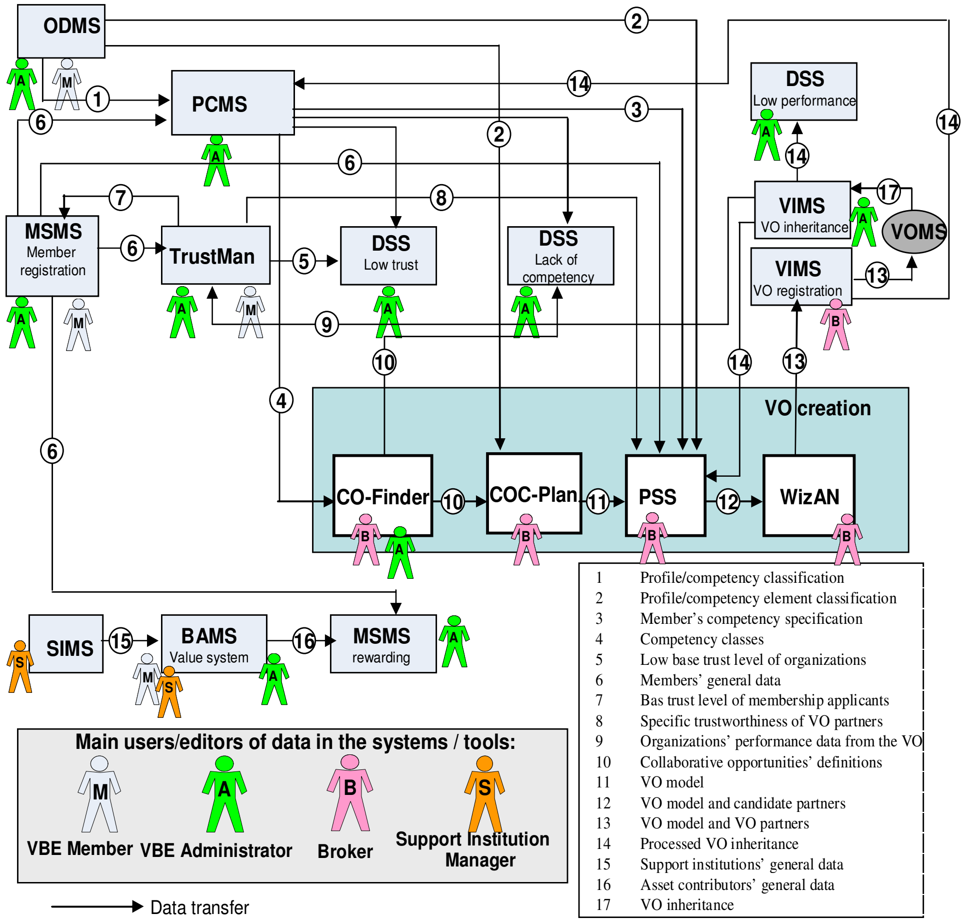
6.2.2 VMS subsystems

As characterized and developed for VBEs in the ECOLEAD project (as addressed in Section 1.7), the VMS constitutes a number of subsystems, as shown within Figure 6.1, and briefly summarized in subsequent paragraphs. Please note that Figure 6.1 also expounds the required interactions between these subsystems. The VMS system developed in ECOLEAD constitutes the following seven main subsystems, (Figure 6.1) [Afsarmanesh, et al., 2008]: (i) VBE Membership and Structure Management System (MSMS), (ii) Profile and Competency Management System (PCMS), (iii) Ontology Discovery Management System (ODMS), (iv) Trust Management system (TrustMan), (v) Decision Support System (DSS), (vi) VO Information Management System (VIMS), and (ii) VO Creation Services (VCS)

i) ***VBE Membership Structure Management Systems:*** Acquisition and registration of new member organizations in VBE networks is particularly related to assessing their suitability in the VBE. Collection and analysis of the applicants' information as a means to ascertain their suitability in the VBE has proved particularly difficult. This subsystem provides services which support the integration, accreditation, disintegration, rewarding, and categorization of members within the VBE. In particular, it addresses functionalities for registration and rewarding of members, and management of their roles and rights.

ii) ***Profile and Competency Management Systems:*** Due to the dynamics of VBEs, caused by the daily changes in customers' demands and all other aspects of the market and society, a VBE must have the needed data to be able to quickly analyze its members' competencies against emerging opportunities. The high level of dynamism in medium and large size VBEs means that the VBE administration is unable to obtain and analyze up-to-date competency information on all of its members. There is thus a need for ICT-based submission and processing procedures for members' profiles and competencies. PCMS provides services that support the creation and maintenance of profiles and competencies of all VBE member organizations, of the collective VBE competencies, and of the VOs registered within the VBE.

iii) ***Ontology Discovery Management Systems:*** In order to systematize all VBE-related concepts, a generic/unified VBE ontology needs to be developed and managed. The ODMS system provides services for the manipulation of VBE ontologies, which is required for the successful operation of the VBE and its VMS. The services designed for ODMS aim to achieve the following main objectives: (1) providing a common understanding of the VBE-related concepts for all VBE actors, (2) facilitating the reusability of knowledge that has been accumulated in one VBE with that of another VBE, (3) providing the formal classification of the knowledge for VMS subsystems (e.g. competency) in order to facilitate the knowledge processing in VBEs by software, and (4) supporting knowledge interoperability both intra-VBE (to support varied forms of collaboration), and inter-VBEs (through sharing of the unified models of knowledge).



1	Profile/competency classification
2	Profile/competency element classification
3	Member's competency specification
4	Competency classes
5	Low base trust level of organizations
6	Members' general data
7	Bas trust level of membership applicants
8	Specific trustworthiness of VO partners
9	Organizations' performance data from the VO
10	Collaborative opportunities' definitions
11	VO model
12	VO model and candidate partners
13	VO model and VO partners
14	Processed VO inheritance
15	Support institutions' general data
16	Asset contributors' general data
17	VO inheritance

Figure 6.1: VMS components and their related interactions

This figure shows the sub-systems constituting the VMS as well as the information which might be exchanged between these components of the VMS as described in this section.

iv) ***TrustMan system:*** The TrustMan system is designed to support the VBE administrator and other stakeholders in the VBE with handling tasks that relate to both balancing the levels of trust in organizations in the VBE as well as assisting with the assessment of organizations for VO partner selection process. The TrustMan system is addressed in the remaining sections in this chapter.

v) ***Decision Support Systems:*** Decision-making within enterprises has been challenging. The decision making process in a VBE needs to involve a number of actors whose interests may even be contradictory. The DSS has three components that support the following operations related to decision-making within a VBE: Warning of an organization's lack of performance, Warning related to the VBE's competency gap, and Warning of an organization's low level of trust.

- The *tool for the lack of performance warning* supports the VBE administrator to analyze the progressive performance of member organizations, and to send a warning message to a specific organization when its performance has fallen beyond a certain specified threshold.
- The *tool for competency gap analysis* is designed to support the VBE administrator in discovering weak points and missed opportunities due to a lack of competencies needed in the market/society, but missing in the VBE. It is based on two important elements: (1) the definition of the VBE's strategic competency plan, and (2) an analysis of the missed collaboration opportunities in the market. The strategic competency plan targets the expected VBE competencies to reflect on the actual competencies available in the VBE at a certain point in time. The aim of this analysis is however to compare the required competencies in the market versus those available in the VBE. This approach enables the missing competencies in the VBE to be identified, which facilitates the definition of the measures that need to be taken in order to acquire and attract these competencies.
- The *tool for low trustworthiness level warning* supports the VBE administrator in managing and balancing the levels of trust in organizations by analyzing their progressive trustworthiness. This tool provides a scheduled calculation of the trust level by executing the service for assessing trustworthiness of organizations, provided by the TrustMan system. Based on progressive results, this tool will send a warning message to organizations whose trust level has fallen beyond the specified threshold.

vi) *VO Information Management Systems:* We can deduce from the underlying concepts of VBEs and VOs, the benefits for a VBE of incorporating experiences from previous VOs into the creation of new ones. Developing thorough processes and guidelines on how to use this information in the process of VO creation is dependent on the VO Creation Framework. However, the management and provision of VO related data is subject to the VIMS. Thus, the functionalities supported by VIMS provide mechanisms for storing information about newly created VOs and dissolved VOs within the VMS data-structure.

VO-related information will be needed by the VO planner as a repository of experiences with certain partners and combinations of partners in the past. The VO initiator will need this information as input in the decision on which of the two or more competing partners are to engage in the VO. The VIMS comprises the functionalities of (i) the Registration of Created VOs Service, and (ii) the Management of VO Inheritance Information

vii) *VO Creation Services:* The potential to rapidly form a VO, when triggered by an identified business collaboration opportunity and specially tailored to the requirements of that opportunity, is the emerging solution – particularly for SMEs – and a survival mechanism in face of market turbulence (Camarinha-Matos, et al., 2005). The same approach is, however, spreading and also becoming appealing in non-business-oriented domains and contexts. Nevertheless, agility in the configuration of VOs as mission/goal-oriented collaboration networks necessitates an a priori preparedness of organizations, which takes time and effort and is nowadays supported through the pre-existing VBE.

Providing services for supporting the configuration of a VO, when an opportunity is brokered is now amenable, considering the current market trends and requirements. VO creation services support the opportunity brokers and VO planners with handling the tasks related to the configuration of new VOs. In ECOLEAD these services are provided through the following four tools:

- *Collaboration Opportunity Identification and Characterization (coFinder)*: This tool assists the opportunity broker to identify and characterize a new Collaboration Opportunity (CO) in the market/society that will trigger the formation of a new VO within the VBE. A collaboration opportunity might be external, initiated by a customer and brokered by a VBE member that is acting as a broker. Some opportunities might also be generated internally, as part of the VBE's development strategy.

- ♦ *CO characterization and VO's rough planning (COC-plan)*: This tool supports the planner of the VO with developing a detailed characterization of the CO needed resources and capacities, as well as with the formation of a rough structure for the potential VO, therefore, identifying the types of required competencies and capacities needed from organizations that will form the VO.
- ♦ *Partners search and suggestion (PSS)*: This tool assists the VO planner with the search for and proposal of one or more suitable sets of partners for VO configurations. The tool also supports an analysis of different potential VO configurations in order to select the optimal formation.
- ♦ *Contract negotiation wizard (WizAN)*: This tool supports the VO coordinator to involve the selected VO partners in the negotiating process, agreeing on and committing to their participation in the VO. The VO is launched once the needed agreements have been reached, contracts established, and electronically signed.

6.3 Trust management system

Establishment of trust relationships between organizations has proven to enhance the cooperation among organizations involved in VBEs and their collaboration within the VOs. However, the main obstacles in establishing trust relationships, as described in the previous chapters stems from the lack of a common definition for trust and trust elements. Consequently, the assessment of organizations' level of trust and the creation of trust between organizations are quite challenging. In practice, organizations individually evaluate the trustworthiness of others both manually and in an ad hoc manner, which is both time consuming and highly unlikely to produce accurate results. This section presents an approach and a system for Trust Management, which assists the management of VBEs, and is a part of its VMS. Based on the multi-criteria and customizable trust models presented in Chapters 4 and 5, this chapter defines a TrustMan system that on one hand combines the introduced models and approaches, and on the other hand provides services for supporting processes related to the management of trust between organizations within VBEs.

6.3.1 Mechanisms for assessing trust level of organizations

Perceptions of trust have corresponded with both the nature of the purpose of its application, as well as the actors involved. Thus, the purposes for establishing trust differ among different practices. For each specific practice in which a particular group of actors is involved, trust is interpreted and perceived differently. In this thesis, trust aspects for VBEs are classified into five perspectives: Technological (Tech), Social (Soc), Structural (Str), Managerial (Man), and Economical (Eco), as described in detail in Chapter 3. Furthermore, in order to address the differences in trust perceptions, a rational trust level assessment approach is required for VBEs to both assist the measurement of trust level of organizations and reasoning of the results, as addressed in Chapter 5.

In order to "rationally" assess the level of trust in organizations, a series of fact-based trust criteria are applied, as addressed in Chapter 5. Using an empirical study of running VBE networks, as well as a survey of past research, our research has identified a substantial number of measurable criteria (trust criteria) that act as indicators of trust assessment [Msanjila & Afsarmanesh 2007c], as further described in Chapter 3. It has also revealed that the influence of a trust criterion on the level of trust can be either positive or negative, depending on its behaviour in the environment. Furthermore, the behaviour of each trust criterion changes over time and causally influences other criteria. Causal influences can be studied by applying concepts from system dynamics [Kirkwood, 1998], and the results of a causal analysis can be visually represented in a so-called "*causal diagram*". Such results can also be translated into mathematical equations that reflect the inter-relations among trust criteria [Msanjila & Afsarmanesh 2007c]. The formulated equations comprise the base for the mechanisms that have been designed in the TrustMan system for assessment of the level of trust in organizations [Msanjila & Afsarmanesh 2007a]. As implemented in the TrustMan system, basically, mechanisms to calculate the final comparative trust score for an organization is formulated as the computation of an average of weighted scores of all trust perspectives (equation 6.1) where the weight is between 0 and 1, and the total weights applied for all parameters is 1. The following abbreviations are used in all subsequent equations: **TL** (trust level), **S** (score), **per** (trust perspective, i.e. Tech, Soc, Str, Man, and Eco, all described in Section 3.3), **IF** (intermediate factor), **W** (weight), and **Avg** (average).

$$TL = Avg[(W_{Tech} * S_{Tech}),(W_{Soc} * S_{Soc}),(W_{Str} * S_{Str}),(W_{Man} * S_{Man}),(W_{Eco} * S_{Eco})] \ldots (6.1)$$

The weights of parameters used in the equations are dynamically specified by the trustor organization depending on its trust objective during the assessment of trust level (See section 6.6.1, Module number 11). If these weights are not specified by the trustor then the TrustMan system assumes uniform weights for all parameters in each equation. The score for each trust perspective is calculated as a weighted average of the score for all intermediate factors as shown in equation (6.2).

$$S_{per} = \frac{1}{n}\sum_{i}^{n} W_{IF_i} * S_{IF_i} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (6.2)$$

Where "n" refers to the number of defined intermediate factors for the trust perspective

The score for the intermediate factors is calculated as a function of trust criteria and known factors as shown in equation (6.3). These equations are formulated from the results of causal analysis as addressed in Chapter 5.

$$S_{IF} = f[trust\_criteria, known\_factors] \qquad \ldots\ldots\ldots\ldots\ldots\ldots (6.3)$$

6.3.2 Approach for developing the TrustMan system

Development of TrustMan system follows standard phases of the software life cycle, including: (1) system analysis, (2) system design, (3) system implementation, (4) system operation and (5) system maintenance as described in [Maciazsk, 2007]. These phases [Maciazsk, 2007] are normally performed sequentially, where the output of each phase, is used as the input to the next phase, as visualized in Figure 6.2 and briefly addressed in this section:

+ ***Phase 1 – System analysis:*** This phase focuses on aligning business processes with system processes when developing services to support potential tasks. Analysis related tasks are performed by two types of experts, namely, the *business analyst* and the *system analyst*. In this phase the first task is the identification of *potential users* of the system as well as *activities/processes (user requirements)* that need to be supported with services. Next, the identified user requirements which need some automated solutions (services) are used during the process of *system specification* to capture *functionalities and services, input data and output data*. Finally, results are documented in a so-called *system requirement document* which is the output of this phase and input to the next phase. The analysis and specification of the TrustMan system is addressed in Section 6.4.

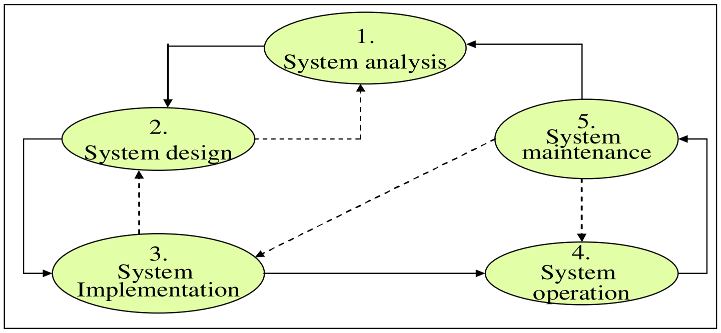


Figure 6.2: Phases in the Software life cycle

Based on the concepts in [Maciaszek, 2007] this figure shows the tasks which were performed during the development of TrustMan system.

+ ***Phase 2 – System design:*** This phase focuses on designing models and architectures of the intended system. Tasks related to system designing performed by the *system designer* are: (1) Defining internal components of the system, (2) Defining components supporting external interactions, (3) Developing the system architecture and (4) Designing user interfaces for human and remote-system users. The output of this phase is a well documented "*system design*" presenting system architectures and models. The document is used as input to the next phase to guide the implementation of functionalities and services. The design of TrustMan system is addressed in Section 6.5.

+ ***Phase 3 – System implementation:*** This phase focuses on the implementation of the system including: installing the platforms and coding of custom-written components. Development related tasks that are performed by the *system developer* are: (1) Coding the required modules and components, (2) Testing developed components, (3) Validating and verifying functionalities, (4) Compiling the system by integrating the separately developed components, and (5) Deploying the system to the real running environment. The output of this phase is the developed system (prototype) and its documentation which together are used as input to the next phase (system operation). The implementation of TrustMan system is addressed in Section 6.6.

+ ***Phase 4 – System operation:*** This phase focuses on handing the system (or take ups when the system is a prototype) to the customer (potential users) ready for running the system at the business site. At early stages of this phase all parties participated in the entire process of developing the system are involved, namely: *the developers, the system analysts, the business analysts and the customers (users).* If some faults happen while the system is operating then the next phase – system maintenance – starts. The operation (the take-ups) of TrustMan system is briefly addressed in Section 6.6.

+ ***Phase 5 – System maintenance:*** This phase focuses on the modification of the system, among others: to correct some faults, to improve performance, or to adapt the system to a changed environment or changed requirements. When a major modification is needed such as implementing a new functionality whose design already exists the third phase (system implementation) is repeated. If there is no design for the needed major modification or a new system need to be developed then the software life cycle is re-started. This phase is realized by commercial and business systems and not by prototypes. Prototypes are developed for the purpose of testing or verifying some features of a concept or commercial system that might be developed in the future. Therefore, the TrustMan system did not undergo this phase because it is developed as a prototype. Nevertheless all new requirements that emerged during the trial and take-up phases of “TrustMan prototype” by industrial VBEs were addressed accordingly, and thus this prototype has gone through some needed maintenance.

6.4 Analysis and specification of the TrustMan system

This section addresses the analysis and specification stages of TrustMan system by: identifying and classifying its potential users, and defining the roles and rights of each user. The section also addresses the specification of functionalities and services of the TrustMan system.

6.4.1 Specification of system users and user requirements

Identification of users of the TrustMan system is based on the analysis of potential stakeholders for the three general trust objectives, as presented in Section 3.3, regarding the creation of inter-organizational trust within the VBE, namely:

♦ *Trust between VBE member organizations:* This trust objective addresses the assessment of the level of trust in organizations and the establishment of their trust relationships for different purposes, such as smoothing cooperation in the VBE, and enhancing collaboration in VOs. The potential stakeholders for this trust objective are: VBE administrator, VO planner, VBE member organizations, and VBE membership applicants. Requirements for the organizations related to this trust objective are described in Table 6.1.

♦ *Trust between a VBE member and the VBE administration:* This trust objective addresses the creation of trust in a VBE member organization towards the VBE administration, as a means to: enhance the commitment of the member to the VBE, ease managerial tasks, attract new member organizations to the VBE, and so forth. The potential stakeholders for this trust objective are: VBE administrator, VBE member organizations, and VBE membership applicants. The user requirements for the organizations related to this trust objective are described in Table 6.1.

♦ *Trust between external stakeholders and the VBE:* This trust objective addresses the creation of trust in external stakeholders towards a VBE, i.e. organizations that have been invited to become members or customers that wish to provide opportunities. The potential stakeholders for this trust objective are: VBE administrator, and external stakeholders (customers and invited organizations). User requirements for the organizations related to this trust objective are described in Table 6.1.

Five user groups are classified on the basis of these three general trust objectives. This classification is based on: each group’s respective user requirements that need to be supported by the system, the rights for each user within the system, and the roles that these users will play in addressing a specific trust objective. These five User Groups (UG1 to UG5) and their respective user requirements are presented in Table 6.1.

Table 6.1: Identification and classification of users of the TrustMan system

User group	User roles & rights	User requirements (UR)
UG1: VBE administrator	Highest administrative rights and can view, execute, modify all services	1. Assessing the trustworthiness of membership applicants and VBE member organizations. 2. Defining, authorizing and assigning rights to other users. 3. Supporting other users, such as the VO planer, in evaluating the specific trustworthiness of trustee organizations for certain purposes. 4. Managing the trust related data in the system.

User group	User roles & rights	User requirements (UR)
		5. Updating the list of trust criteria in the system.
UG2: VO planner	Limited administrative rights and can view and execute some services	6. Viewing the trust criteria that are used in the system. 7. Selecting specific trust criteria from the VBE pool of trust criteria. 8. Applying the selected trust criteria to evaluate specific trustworthiness of potential VO partners.
UG3: VBE member	Normal user rights and can manipulate its own records	9. Accessing its base trust level records 10. Updating its trust related data 11. Viewing the trust criteria that are used in the system.
UG4: Membership applicant	Basic user rights and can submit trust related data	12. Submitting trust related data as a requirement to the analysis of its membership application
UG5: External stakeholders	Guest rights and can access public information only	13. Supporting customers to analyze trust of VBEs and thus trusting those VBEs for purchasing their products and services. 14. Supporting invited organizations that want to become members in the VBE to analyze the trust of that VBE in relation to their businesses and possible benefits. 15. Supporting guests to access the basic information related to trust of the VBE.

In addition to the above identified and classified users of TrustMan system, another potential user is the *trust expert*. This is a specialized user which needs TrustMan functionality to support tuning the TrustMan system to match the requirements, such as the introduction of new trust criteria, disabling some refused trust criteria from the general set of trust criteria for VBEs, etc. Figure 6.3 summarizes and visualizes the user rights and administrative relations.

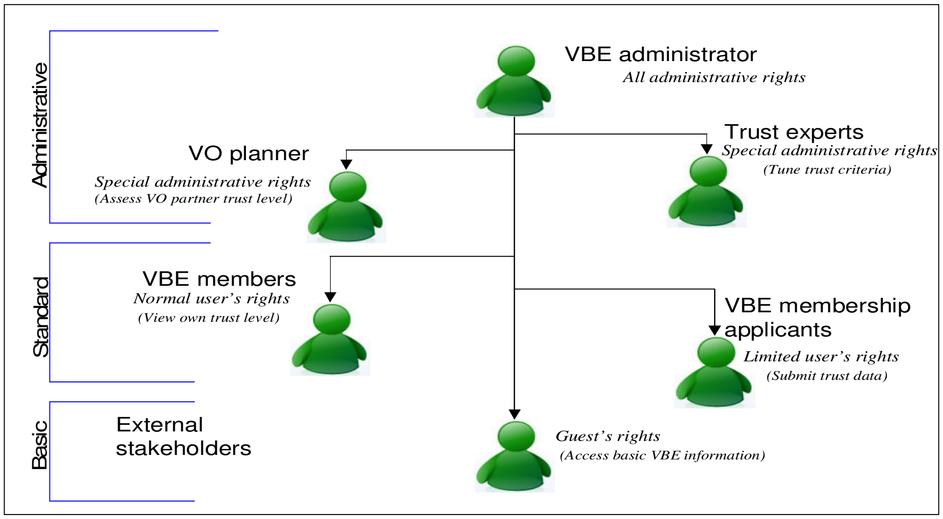


Figure 6.3: User rights hierarchy accessing TrustMan system

These classifications represent different groups of user organizations with the same access rights. The hierarchy also represents access rights to the trust information that decreases downwards.

6.4.2 Specification of functionalities and services

In this section we address the specification of functionalities and services that shall be provided by TrustMan system. These specifications are based on the analysis and classification of user requirements as presented in Section 6.4.1.

A. Specification of required functionalities for the TrustMan system

Design of the TrustMan system, as addressed in Section 6.5, is based on the service oriented architecture (SOA) and in particular the web service technology. Accordingly, the specified functionalities are referred to here as services (referred to as "S" in table below). The system provides seven integrated services as described in Table 6.2 to support all user requirements as presented in Table 6.1.

Table 6.2: Specified services of the TrustMan system

S	Service name and description
S1	For assessing the base trust level of organizations: This service supports the assessment of trust level of an organization applying the set of base trust criteria, for two main purposes, namely: supporting the periodic assessment of base trust level of member organizations and supporting the one-time assessment of base trust level of a membership applicant. This is mainly a VBE administrative service and it is accessed by the VBE administrator. The service also supports member organizations' assessment of their own base trust level. This service addresses user requirements 1 and 9 (Table 6.1).
S2	For evaluating the specific trustworthiness of organizations: This service supports the trustor organization (VBE administrator, or VO planner) to evaluate the specific trustworthiness of an organization for a specific trust objective, such as inviting a VBE member to participate in a VO, appointing a VBE member to become a VO coordinator or the VBE administrator. The evaluation of specific trustworthiness can be done at any point in time, such as the current time. Furthermore, the evaluation can be used to forecast trustworthiness for future collaborations. This is an administrative service and is thus accessed by the VBE administrator and the VO planner. This service addresses user requirements 3, 6, 7 and 8 (see Table 6.1).
S3	For establishing trust relationships between organizations: This service supports an organization, based on its user rights, to access trust related data and decide regarding the suitable information to provide to other organizations in order to create trust. The challenge here concerns the provision of required information to create trust between organizations aimed at supporting the establishment of trust relationships. Therefore, it is related to five aspects, namely: "who", "when", "why", "what" and "how" (as further addressed in details in Section 2.4). However, certain information that is stored in the system might be too strategic; as a result of which the owner organizations will be unlikely to allow it to be publicly accessed. In order to support this requirement, the access to trust related information is categorized as: (1) Public access – any organization inside or outside the VBE may access the information, (2) Restricted access – any VBE member organizations may access the information, and (3) Protected access – only the VBE administrator and the owner organization itself may access the information. This is a semi-administrative service that can be accessed by the VBE administrator and VBE member organizations. This service addresses user requirements 5, 6, 9, and 11 as shown in Table 6.1.
S4	For managing trust related data: This service supports three kinds of users, namely:

S	Service name and description
	VBE membership applicants, VBE member organizations, and the VBE administrator, for different purposes. The VBE membership applicant will use this service to submit its own trust related data in order to facilitate the evaluation of its qualifications to join the VBE. The VBE member organizations will use this service to update their own trust related data. The VBE administrator will use this service to manage all trust related data in the system, i.e. to ensure that it is up-to-date, valid and extracted from a reliable source. It service addresses requirements 4, 5, 10, 11, and 12 (see Table 6.1).
S5	For creating trust in the VBE: This service supports external stakeholders (customers and invited organizations) to create trust to the VBE establishment for different purposes. The external stakeholders need to access information that will persuade them of the trustworthiness of the VBE in relation to their businesses. The service also helps customers to build trust in the VBE in order facilitate business transactions, such as opportunity bids, payment procedures, and so forth. This service addresses user requirements 13, 14, and 15 as shown in Table 6.1.
S6	For managing the assessment mechanisms: As shown in Section 6.3.1, the equations applied for the development of mechanisms for assessing level of trust in an organization incorporate some weights for the included trust criteria and the known factors. These weights may be changed from time to time when it is necessary. This service assists the VO planner, VBE administrators and trust experts in adjusting these weights when necessary. This service addresses the user requirements 2, 4, 6, 7, and 8 (see Table 6.1).
S7	For analyzing an organization's trust-level history: This service supports VBE administrator to track the history or evolution of trust level of an organization. It has a mechanism that triggers the service for assessing base trust level for all organizations in the VBE periodically (such as every six-months). The service then stores the results in the TrustMan database, the user can retrieve both the trust level history of specific organizations for a given period of time, and/or perform some analyzes such as identifying the weak or strong organizations. As presented in Section 6.2.2 this service is invoked by DSS (Decision Support System) tool which is a subsystem of VMS. Further analysis of the evolution of trust level of an organization is supported by DSS.

B. Specification of input data and its sources:

The input data used in the process of assessing trust level of organizations are the values of defined trust criteria for the organizations. The main sources of input data (organizational data related to trust) as addressed in this thesis are twofold: *(1) Data submitted by each VBE membership applicant* and *(2) Performance data of organizations gathered by VBE in relation to the organizations' participations in VOs and other VBE related activities.*

C. Specification of output data and its presentation:

The output produced by the services for assessing trust level of the organization and evaluating its specific trustworthiness is the "level of trust" expressed qualitatively, using the scales provided by the Trust-Meter, as shown in Figure 5.1. Qualitative representation of trust level of an organization is based on the interpretation of scores computed by the TrustMan system (as exemplified in Table 5.1), namely: the Strongly less trustworthy, Less trustworthy, Average trustworthy, More trustworthy and Strongly more trustworthy.

6.5 Designing the TrustMan system

Based on the specification of services presented in Table 6.2, this section presents the design of the TrustMan system, addressing its two architectures, namely: *the interoperability architecture*, and *the four-layer componential architecture*. It also presents the design of its user interfaces and the database.

6.5.1 Interoperability architecture of the TrustMan system

TrustMan system is one of the subsystems constituting the VBE management system (VMS) as presented in Section 6.2. In order to provide the required services accurately and comprehensively, the TrustMan system interacts with others sub-systems as shown in Figure 6.4 for four main purposes, namely *(a) acquiring the trust related data, (b) providing results of the trust level assessment, (c) accessing basic services provided by the ICT-Infrastructure (called ICT-I),* and *(d) supporting human user access.* The interoperability architecture of TrustMan system is designed to guide developers in implementing the needed modules for supporting these four kinds of interactions. Please note that the internal components of the system (the area indicated with dashed line in Figure 6.4) are discussed in Section 6.5.2.

External interactions, as further described below, are supported by a number of internal components of TrustMan system that are grouped into three categories, namely the component for: *(1) User right control, (2) Services choreography, and (3) Results provision.*

- The components for *user right control* provide functionalities for authorizing users (both human and system users) that wish to access the TrustMan system. For the authorized users, these components also provide functionalities for classifying the services on the basis of the user rights as well as providing access to those services that each user is allowed to view or execute (such as public, restricted or administrative services).
- The components for *services choreography* provide internal mechanisms and/or functionalities to organize the order and time for the execution of a number of services in response to each received user's request.
- The components for *results provision* organize and provide proper responses to requests received by the system, such as returning specific results for the successful requests, or returning negative response for the rejected requests.

As described earlier in this section, the TrustMan system supports four types of external interactions, indicated as (a), (b), (c) and (d) in Figure 6.4, as are described below.

(a) Interactions for assisting the acquisition of trust related data

Two sub-systems, namely the *Membership Structure Management System (MSMS)* and the *Performance Data related Management System (PDMS)*, interact with the TrustMan system for the purpose of submitting trust related data as addressed below.

- Interaction with MSMS: One fundamental piece of information needed by the VBE administration in order to decide whether to accept a VBE membership applicant organization is its base trust level. The MSMS interacts with TrustMan system so as to facilitate the applicant's submission of the trust related data.
- Interactions with PDMS: Organization's data related to trust must be kept up-to-date and thus needs to be continuously updated. The PDMS interacts with the TrustMan system to assist the VBE member organizations with updating the trust related data on the basis of the organizational performance that is gathered in relation to their participation in

different activities. The PDMS constitutes a set of information management systems that support the management of VO related information and inheritance, and the VBE activities related performance data.

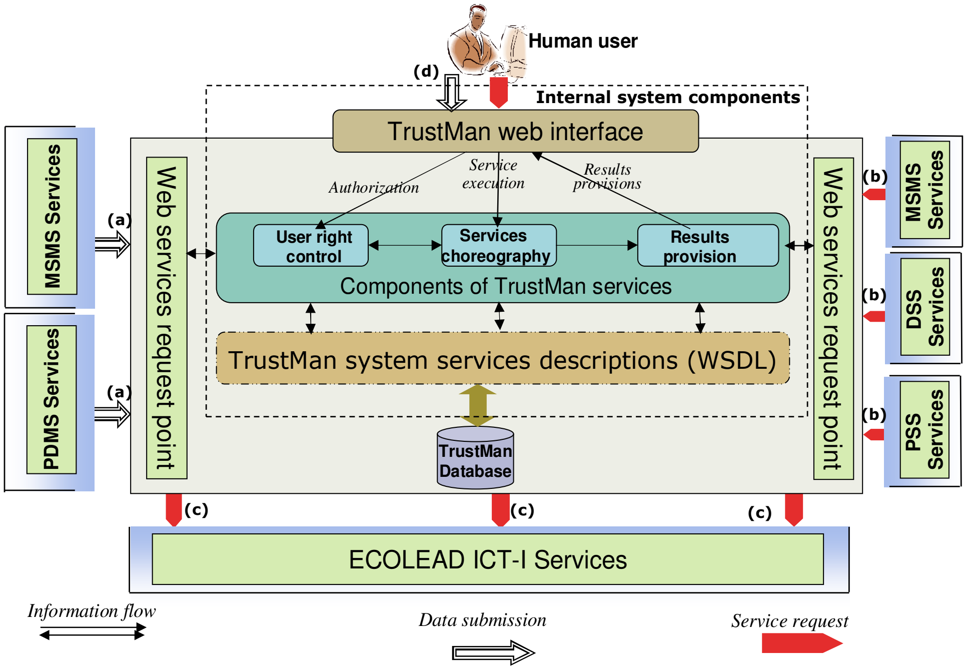


Figure 6.4: Interoperability architecture of TrustMan system

This figure shows other sub-systems of the VMS that will interact with the TrustMan system. It also indicates different purposes of interactions (with arrows) as described below in this section.

(b) Interactions related to accessing organizations' records of trust level

Three VMS subsystems invoke the services provided by the TrustMan system, namely: *Membership Structure Management System (MSMS), Decision Support System (DSS),* and *Partner Search and Suggestion (PSS), as addressed in Section 6.2.1.* These VMS subsystems need to invoke some services provided by the TrustMan system in order to access the information about organizations' level of trust. The level of trust in an organization is used as input by the client systems to provide the required services to their respective users.

- MSMS will invoke the service for assessing the base trust level of an organization in order to support the VBE administrator analyze whether the applicant organization meets the required minimum level of trust in an organization within the VBE.
- DSS supports the VBE administrator to analyze the evolution of the level of trust in an organization for a past period of time. In order to support the analysis of the evolution of organization's level trust, the DSS periodically invokes the services provided by the TrustMan system for assessing the organization's base trust level. Therefore, these organizations whose trust level is continuously deteriorating can be alerted and advised on how to enhance their trustworthiness.

- PSS supports the VO planner to select suitable VO partners among the VBE members. One key activity during the selection of such VO partners is the evaluation of their specific trustworthiness. The PSS interacts with the TrustMan to support the VO planner with evaluation of the specific trustworthiness of VO partners.

(c) Interactions related to accessing services provided by ICT Infrastructure

In order to effectively provide the required services, the TrustMan system invokes some basic services that are provided by the ICT Infrastructure (ICT-I), namely: the service for *data access* and the service for *security management* [Rabelo, et al., 2006].

- The service for data access supports the TrustMan system to manage performance data in its database, such as the related interactions with MSMS and PDMS for data acquisition.
- The service for security management supports the TrustMan system in the authentication of user services and in particular, the remote user services. It involves authenticating the source networks, corresponding security certificates, and so on that are necessary to maintain the required security.

(d) Interactions related to accessing the TrustMan system by human users

Interactions between human users and the TrustMan system are facilitated and achieved through the web interface. A web interface is designed to facilitate the interactions needed by human users based on the access rights as illustrated in Figure 6.3.

6.5.2 The four-layer componential architecture of the TrustMan system

Four-layer componential architecture of the TrustMan system adopts the standard definitions for web service technology. Thus it addresses the classification of internal components (system modules) into four layers. The components of TrustMan system, as shown in Figure 6.5, are classified into these four main layers, namely: the *presentation layer, the process layer, the description layer,* and *the message layer,* as described below.

(a) Layer 1: Presentation layer

This layer deals with the delivery of information from the process layer to the web interface in a format that is readable by humans. The layer also handles the transformation of data submitted by human users to the format that is acceptable by various modules at the process layer addressed below [Field & Hoffner, 2003].

The TrustMan system manages and deals with some sensitive information that in most cases the VBE member organizations may consider as proprietary, such as strategic business data. The designed web interfaces that facilitate the accessibility of information, as well as the execution of various supported services, are classified based on the user rights as addressed in "*service S3*" in Table 6.2, namely: the *public interface, the restricted interface* and *the protected interface*. Comparing against the components as classified in the interoperability architecture as shown in Figure 6.4, the following holds:

- The modules for the public interface belong to the group of "results provision" components in the interoperability architecture.
- The modules for the restricted and protected interfaces constitute components that belong to both the "user control components" (associated with user rights and roles), as well as the "services choreography" components (associated with classifying records of trust level of an organization) in the interoperability architecture.

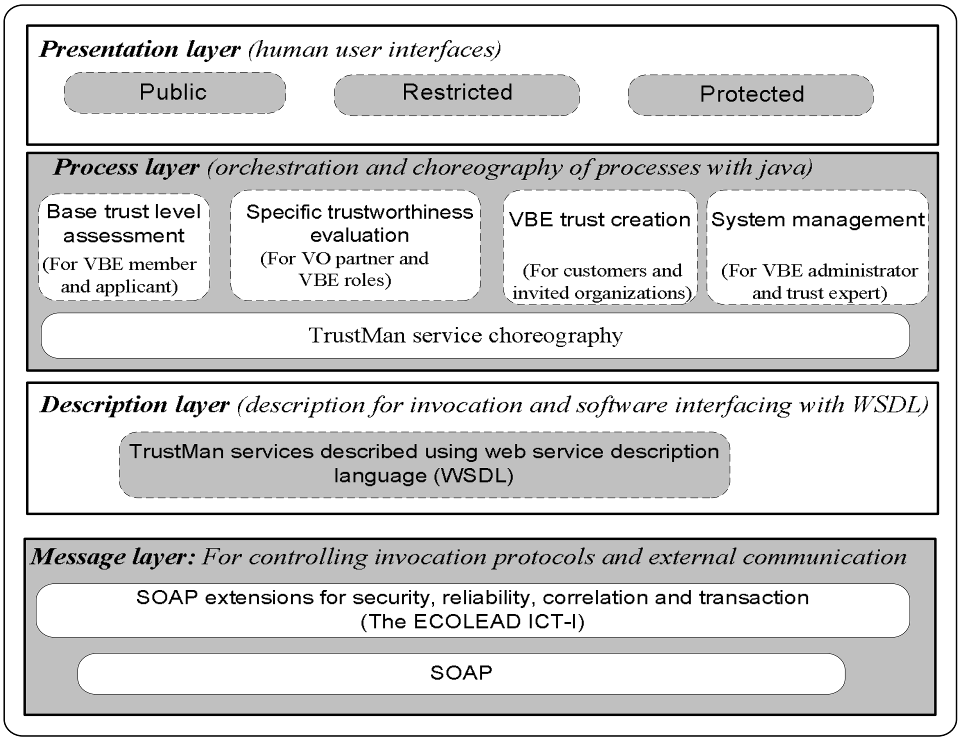

Presentation layer (human user interfaces)
Public
Restricted
Protected
Process layer (orchestration and choreography of processes with java)
Base trust level assessment
(For VBE member and applicant)
Specific trustworthiness evaluation
(For VO partner and VBE roles)
VBE trust creation
(For customers and invited organizations)
System management
(For VBE administrator and trust expert)
TrustMan service choreography
Description layer (description for invocation and software interfacing with WSDL)
TrustMan services described using web service description language (WSDL)
Message layer: For controlling invocation protocols and external communication
SOAP extensions for security, reliability, correlation and transaction (The ECOLEAD ICT-I)
SOAP

Figure 6.5: Four-layer componential architecture of the TrustMan system

This figure shows at the high-level the internal components of the TrustMan system and their relations based on service oriented architecture (SOA) layer classification as addressed in this sub-section.

(b) Layer 2: Process layer

The process layer is responsible for defining the logic of the invocation of various processes (modules) that need to be executed concurrently in order to provide the requested service. The process scheduling constitutes *orchestration and choreography processes.*

Orchestration refers to the logic (the sequence and flow) of the execution of various functions within one system process [Papazoglou & Georgakopoulus, 2003]. For example, in java programming this refers to the logic of the execution of functions within one object. Figure 6.6 illustrates a number of orchestrations within different single services, such as the order of execution of various actions/functions within (inside) the "*trustworthiness computation service*".

Choreography represents the logic that will be followed in order to execute various modules, including invoking other services in order to provide an integrated service [Peltz, 2003]. As a means to exemplify this, the choreography of an integrated service for evaluating the specific trustworthiness of an organization is shown in Figure 6.6.

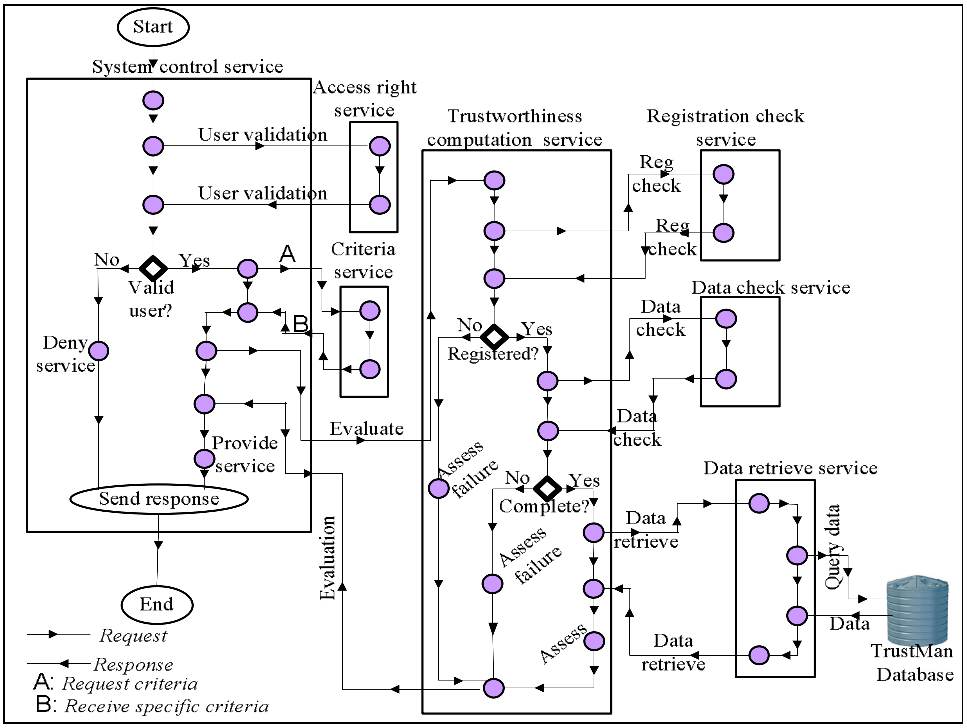


Figure 6.6: The choreography of a service for evaluating specific trustworthiness

This figure shows the order of invocations of a series of services, in order to accomplish the evaluation of specific trustworthiness of organizations as addressed below.

This figure (Figure 6.6) shows the choreography of a set of services constituting the process of evaluating specific trustworthiness of an organization (as further explained below), and thus represents a part of the architecture of processes in TrustMan system. Consider the case of a user starting to evaluate the "specific trustworthiness" of a member organization in the VBE. The TrustMan system will first validate whether the user has the right to access the TrustMan system and the specific requested service. Once positively validated, the user will be granted the access. Then the service for selecting relevant trust criteria is invoked. Once the specific set of trust criteria is selected and submitted to the system, the service for computing trustworthiness will be invoked. The system then checks whether the organization whose specific trustworthiness needs to be evaluated is registered and its trust related data is available and complete in the system. When positive response is received from the services which check the registration and completeness of data, the data related to the organization will be retrieved and its specific trustworthiness will be evaluated. Lastly, the evaluation result is sent to the user. If at any stage a failure occurs then the process is terminated and the user receives a negative response with notifications about hints to the error, for example, the system may state that the organization is not registered in the VBE (Figure 6.6).

As shown in Figure 6.5 the components of TrustMan system at its process layer are classified into four groups, each providing one or more services, as addressed in Table 6.1, namely: (1) Components for base trust level assessments, which comprise service S1, (2) Components for specific trustworthiness evaluation, which comprise service S2, and S7, (3) Components for trust creation, which comprise services S3 and S4, and (4) Components for system management, which comprise e services S5 and S6. Process layer is the only layer which constitutes the services that are scheduled and executed to respond to the requests sent by users. Therefore, all components in this layer belong to "service choreography" components in the interoperability architecture as shown in Figure 6.4.

(c) Layer 3: Description layer

Description layer deals with the provision of the grammatical specifications of the services provided by the TrustMan system, to support the external invocations by remote systems. The description of a service applies "*web service description language*" (WSDL) to detail the following four fundamental parts:

- *Public interface:* Describes the public operations that are visible to external parties and thus can be invoked.
- *Data type information:* For all messages related to requests and responses, it describes the variables that need to be passed in order to access a specific service.
- *Binding information:* Related to the transport protocol, it defines the protocols necessary to access the service and facilitates external communication.
- A*ddress information:* For locating the specified service, it describes the server location and how it can be discovered in the UDDI.

This layer represents similar aspects to the service description part in the interoperability architecture, as shown in Figure 6.4.

(d) Layer 4: Message layer

The message layer defines the protocols for communication among systems and exchanging information across the network so that a receiving server/client may be able to interpret it [Peltz, 2003]. The standard applied communication protocol for web services is SOAP (Simple Object Access Protocol). Besides the standard SOAP protocol, additional mechanisms can be added to improve the security, reliability, adaptability, and so forth, of the system. At present, the ECOLEAD ICT-I mentioned in Figure 6.5 that is developed by the ECOLEAD project provides a set of necessary features (such as security control, network certificates authentication, etc.) that smoothen the interactions between different ECOLEAD systems (including VMS that has TrustMan as a subsystem) that support collaborations among organizations [Rabel, et al., 2006].

6.5.3 Design of user interfaces of the TrustMan system

This section addresses the design of two interfaces for the TrustMan system to support the two types of users, namely: human users and system users.

(i) ***Interface for human users:*** Access to the TrustMan system by human users is achieved through a web interface developed as prototype and is controlled by three main parameters: user-name, password, and user-role. The user name refers to the user's unique identification in the system. The password is created by the respective user during the first login. In addition to authorizing the user, these parameters serve to identify which type of information and/or services may be accessed with the current login details and the specific roles of the user. Thus the same user can access various parts of the system with a single sign on.

(ii) ***Interface for remote-system users:*** TrustMan system provides services that can be called by other systems by means of invocation based on the SOAP (simple object access protocol [Rhody, 2002]). Figure 6.7 presents the service invocation and interactions needed for an organization to update its trust related data at TrustMan system with information at its local repositories. The TrustMan system applies a certain level of security across the network, such as the authentication of source network, as also provided by the ECOLEAD ICT infrastructure [Rabelo, et al., 2006]. The invocation request is expected to receive a local authentication certificate, as shown in step 1 in Figure 6.7, and if access to the requested service is granted by the TrustMan system control then a positive response is sent. If it is not granted then a negative response is sent. The interface supporting remote invocations of the TrustMan services is through WSDL interface at the description layer [Kreger, 2003].

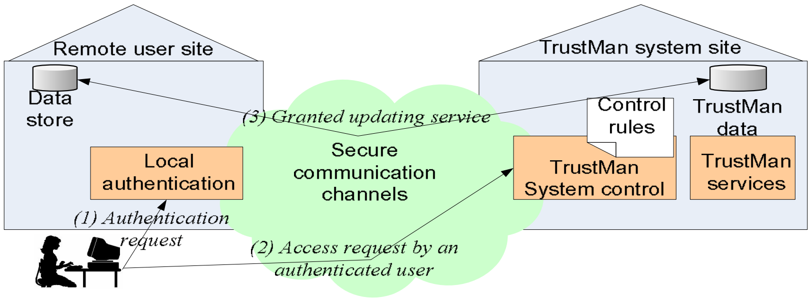


Figure 6.7: External invocation for TrustMan system

This figure shows the steps controlled by the TrustMan system for updating trust related data from a remote user site.

6.5.4 Design of database schema for the TrustMan system

In Chapter 4 we presented a record-based model of trust relationships between organizations. This model is used here to support designing a database schema for the TrustMan system as shown in Figure 6.8. We categorize the data applied in the analysis of inter-organizational trust into three groups, namely, *organizational trust related data, data related to trust elements, and the basic data about the organization.*

- *Organizational trust related data:* This information constitutes the values of trust criteria for each organization. This information indicates primarily the organization's performance data expressed in terms of trust criteria and is used as the main input data for the services that assess the level of trust in an organization. Figure 6.8 shows an object-oriented model representing the database schema for the organizational trust related data.

- *Data related to trust elements:* This information constitutes a list and descriptions of trust elements, namely of the trust perspectives, trust requirements and trust criteria.

- *Basic data about organization:* This refers to the information that is necessary to accurately describe each physical organization or virtual organization. For physical organizations, this information may constitute the name, legal registration details, address, and so on. For virtual organizations, this information may constitute the VO coordinator details, launching and dissolving dates, involved partners, the customers, and so on.

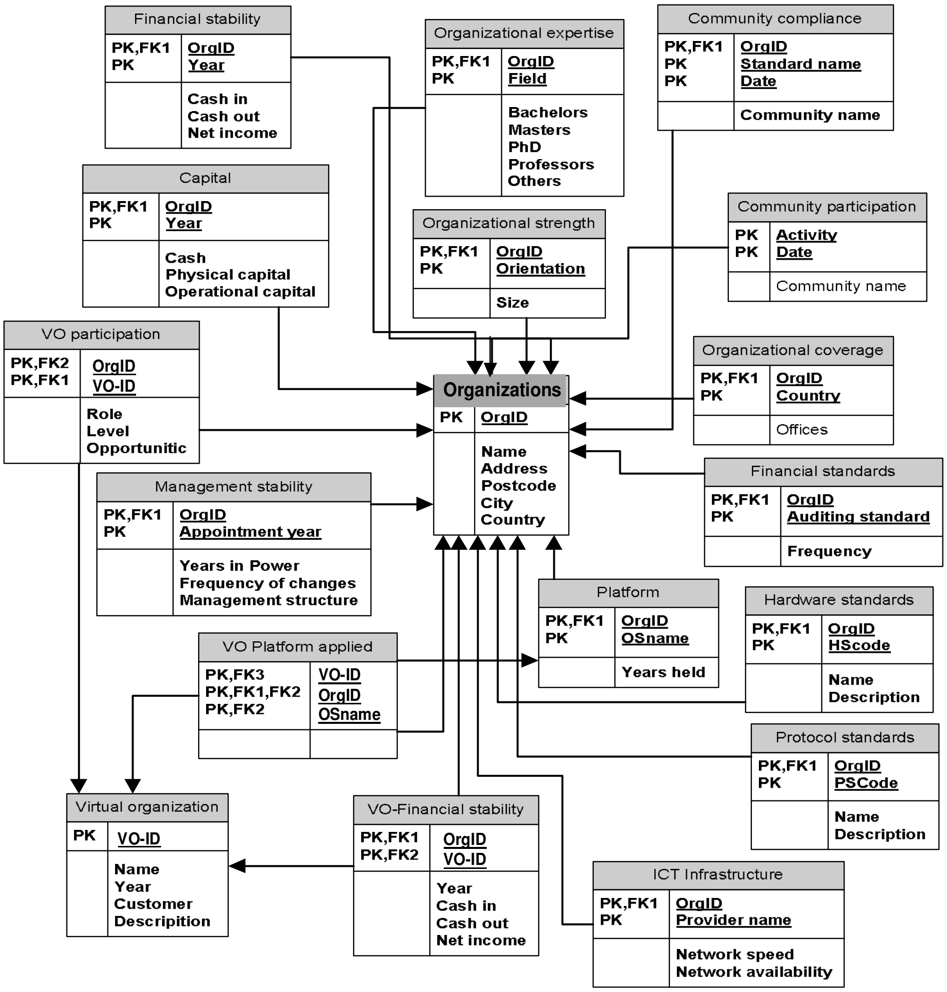


Figure 6.8: Object-oriented schema for TrustMan system database

This figure shows a schema applied for the development of the relational database for the TrustMan system, to support the storage and management of organizational trust related data. The following short forms are applied to the Figure 6.8:

PK:	Primary key	HS:	Hardware standard	VO-ID:	VO-identification
FP:	Foreign key	OS:	Operating system	PS:	Protocol standard
OrgID:	Organization identification				

6.6 Implementation and operation of the TrustMan system

According to [Ozcan et al., 2006], a well developed system is supposed to be: (a) generic enough to be *replicated* in different targeted environments, (b) *adaptable* enough to meet the general (common) user requirements in each specific targeted environment, and (c) *customizable* enough to meet the needs of each specific user in the environment. These three indicators, namely, ***replicability, adaptability and customizability*** are discussed below in relation to the development of the TrustMan system.

(a) Replicability of the TrustMan system to different VBEs

Replicability refers to the ability of a system to support its own duplication for the purpose of deploying it in new environments without changing the characteristics or supported processes. Replicability of a system is analyzed considering its "core part" (sometimes known as the kernel or the central engine) that does not change when it is deployed in different environments. The TrustMan system is replicable considering the following aspects:

- *General set of trust criteria*: The mechanisms for assessing the trust level of organizations form the core part of the TrustMan system. These mechanisms are developed considering all trust criteria for organizations involved in the VBE so far identified as indicated in Figure 3.6 in Section 3.3. Thus any VBE can install the TrustMan system to meet its requirements related to management of inter-organizational trust.

- *Developed mechanisms for assessing trust level of organizations*: The mechanisms for assessing the level of trust in organizations rely on mathematical equations. The equations are formulated based on causal influence analysis between *trust criteria, generic known factors* and *generic intermediated factors*. Thus the mechanisms for assessing trust level of organizations implemented in the TrustMan system are also *generic*. Therefore, the TrustMan system can be replicated and deployed to different VBEs without the need to re-formulate the equations or re-develop the mechanisms for assessing trust level of organizations.

In relation to *Adaptation* and *customization*, the TrustMan system allows meeting the requirements of specific VBEs through its mechanisms for disabling or enabling features within the system. In this way the TrustMan system assures adaptability and customizability.

(b) Adaptability of the TrustMan system to different VBEs

In our approach, a series of trust criteria is applied for assessing the level of trust in an organization. Each VBE may, however, apply a different "*pool of trust criteria*", which constitute the trust criteria that are selected by the VBE administrator from the generic set of trust criteria for all VBEs, during the establishment of the VBE. This selection of trust criteria depends on the preferences and perceptions of trust of the VBE administrator and the specific requirements of the VBE in relation to the management of inter-organizational trust. Furthermore, these preferences and perceptions might also be subject to the day-to-day changes that happen over time. In order to handle such situations, the TrustMan system must not only be replicable but also easily adaptable. We have addressed these aspects in the TrustMan system by implementing modules 9 and 10 (Figure 6.9) as addressed below.

(c) Customizability of the TrustMan system to different VBEs

A number of features need to be customized in order to ensure that the TrustMan system meets the requirements of each specific VBE. In practice, the customization of a system involves the reconfiguration of its user interfaces, user rights, external interoperability points, and so on. These aspects are generic to every system and therefore also considered in the customization of the TrustMan system. However, a unique feature of the TrustMan system, which is addressed below, is the customizability of the mechanisms for assessing the level of trust in organizations to meet the requirements of each user.

The mechanisms implemented in the TrustMan system for assessing the level of trust in organizations are designed on the basis of mathematical equations. As presented in Section 6.3.1, each mathematical equation constitutes a number of trust criteria and known factors. Each trust criterion and known factor is further related to others (trust criteria and known factors), as part of an operand in the equations, by means of a specified weight that indicates the preferences of the environment. The values of these weights (between 0 and 1, and their sum equals 1) might need to be further refined in order to meet the specific preferences of every trustor. The TrustMan system supports the customization of such weights in the implemented equations for two main purposes, namely: for supporting the assessment of base trust level of organizations and for supporting the evaluation of specific trustworthiness of potential VO partners. We have addressed these aspects in the TrustMan system by implementing module 11 (Figure 6.9) as addressed below.

The remaining of this section describes modules, functionalities, mechanisms and user interfaces developed for TrustMan system. In addition, it presents the trials aimed at examining the applicability of the TrustMan system performed through take-ups at different running industrial VBE networks.

6.6.1 Implementation of the TrustMan system

Services provided by the TrustMan system are developed in the Java language. A number of components (classes) are implemented and classified into modules. Each module constitutes a number of components (classes) that when executed provide a complete functionality e.g. each service as presented in Table 6.2. Figure 6.9 shows the modules (modules 1 to 11) constituting the TrustMan system, whose functions are further presented in this section. The description of each module is provided below:

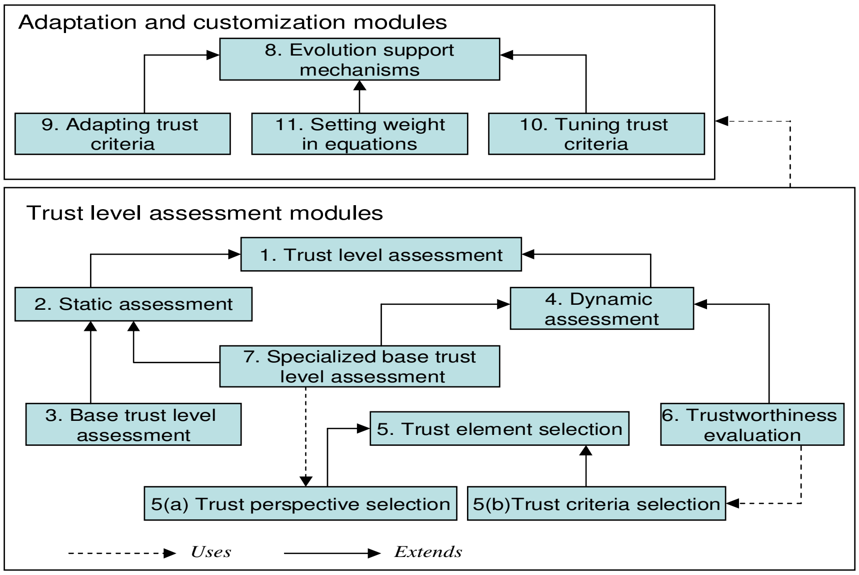

Adaptation and customization modules
8. Evolution support mechanisms
9. Adapting trust criteria
11. Setting weight in equations
10. Tuning trust criteria
Trust level assessment modules
1. Trust level assessment
2. Static assessment
4. Dynamic assessment
7. Specialized base trust level assessment
3. Base trust level assessment
5. Trust element selection
6. Trustworthiness evaluation
5(a) Trust perspective selection
5(b)Trust criteria selection
Uses
Extends

Figure 6.9: A global view of the modules in the TrustMan system

This figure shows groups of implemented components of the TrustMan system, categorized into modules and the relations among those modules. The functionalities supported by each module included in this figure are described below, specified by its corresponding numbers in the figure.

1. *Module for trust level assessment:* It consists of a number of classes which provide basic algorithms for assessing an organization's level of trust. The classes implement generic algorithms for computing various measures of levels of trust in organizations. For example, the mechanisms for computing the scores for intermediate factors, based on mathematical equations as presented in Chapter 5, are implemented in this module.

2. *Module for static assessment of trust level:* The classes in this module extend the classes in module 1; reusing the implemented generic algorithms. These classes provide algorithms for assessing the level of trust in organizations on the basis of a static (fixed or pre-defined) set of trust criteria such as a set of base trust criteria.

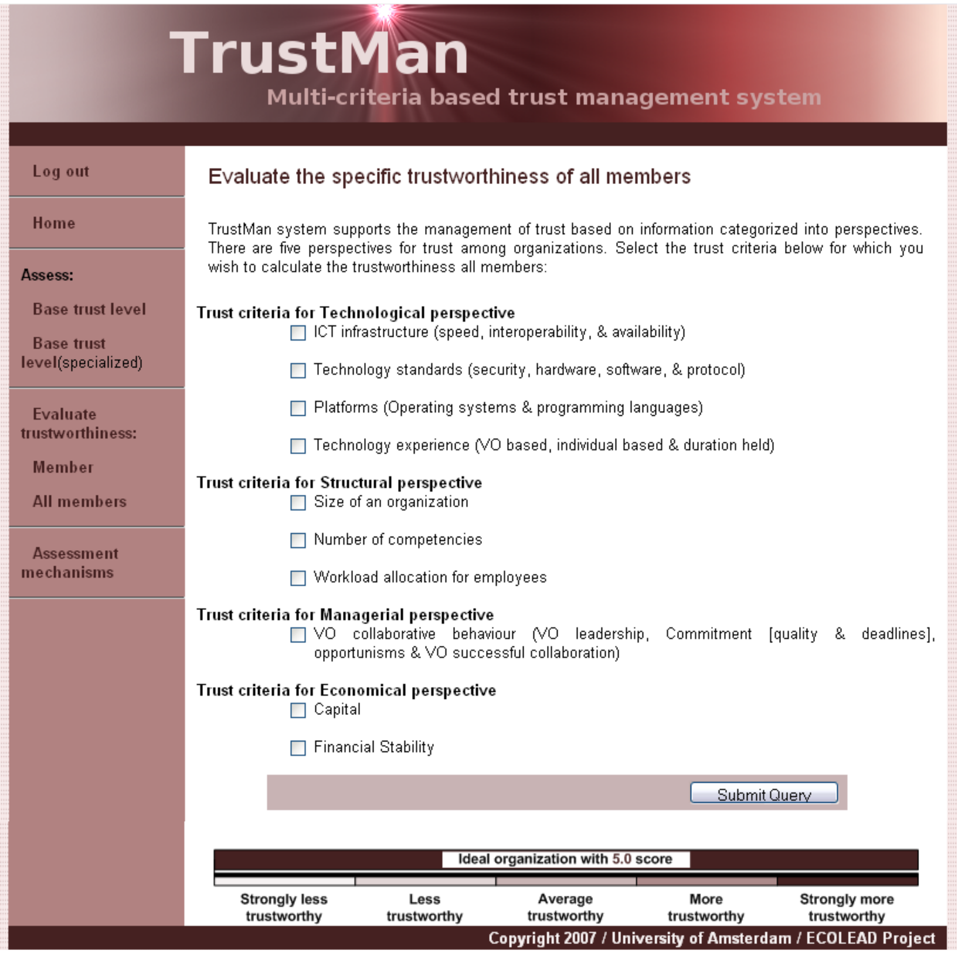
3. *Module for base trust level assessment:* The assessment of base trust level applies the set of base trust criteria selected by the VBE administrator during the establishment of the VBE. In addition to reusing mechanisms implemented in module 2, this module consists of mechanisms for rating various computed scores, such as the *score* per trust perspective as described in Chapter 5. This module also supports the generalization of level of trust in an organization into one category, as defined in the Trust-Meter which is shown in Figure 5.1.

4. *Module for dynamic assessment of trust level:* The classes in this module extend the classes included in the module for trust level assessment (module 1). This module provides additional mechanisms that are applied to assess an organization's level of trust on the basis of a dynamic set of trust criteria, e.g. set of trust criteria for evaluating specific trustworthiness of VO partners (Chapter 5). In this case, the trust criteria to be applied for the assessment are selected by the user, and automatically applied in the assessment of level of trust of an organization.

5. *Module for selection of trust elements:* This module constitutes classes that provide algorithms for selecting trust criteria to support the evaluation of specific trustworthiness of an organization. As such, its operations are inherited by the classes in the modules for selecting perspectives (5a) and in modules for selecting criteria (5b).

6. *Module for trustworthiness evaluation:* This module supports the assessment of specific trustworthiness of organizations applying a set of trust criteria selected by the trustor to meet the requirements of a specific VO. Since the selection of trust criteria is dynamically performed, this module reuses mechanisms implemented in the module for dynamic assessment of trust level (module 4) for computing trust level of organizations. The classes in this module also extend the classes in the module for selecting trust elements (module 5) for the purpose of reusing the implemented mechanisms to dynamically acquire the preferred set of trust criteria. Figure 6.10 shows a web interface implemented in the TrustMan system that supports the selection of trust criteria.

7. *Module for the assessment of specialized base trust level:* The classes in this module support the assessment of base trust level of organizations that are invited to join a VBE for a specific role. The role of such invited organizations may for example be to fill certain gaps within the VBE, such as to provide missing competencies in the VBE. Thus, each invited organization will need its base trust level to be assessed vis-à-vis its business specializations and competencies. The classes in this module extend the classes in the module for dynamic assessment to reuse the algorithms for selecting trust perspectives. When the trust perspective is selected, all preferred trust criteria in that perspective are applied to the assessment of trust level of the invited organization. Therefore, the classes in this module also extend the classes in the module for static assessment of trust level (module 2) to reuse the implemented mechanisms for assessing base trust level when the perspective is known.


TrustMan
Multi-criteria based trust management system
Log out
Home
Assess:
Base trust level
Base trust level(specialized)
Evaluate trustworthiness:
Member
All members
Assessment mechanisms
Submit Query

Evaluate the specific trustworthiness of all members

TrustMan system supports the management of trust based on information categorized into perspectives. There are five perspectives for trust among organizations. Select the trust criteria below for which you wish to calculate the trustworthiness all members:

Trust criteria for Technological perspective

□ ICT infrastructure (speed, interoperability, & availability)

□ Technology standards (security, hardware, software, & protocol)

□ Platforms (Operating systems & programming languages)

□ Technology experience (VO based, individual based & duration held)

Trust criteria for Structural perspective

□ Size of an organization

□ Number of competencies

□ Workload allocation for employees

Trust criteria for Managerial perspective

□ VO collaborative behaviour (VO leadership, Commitment [quality & deadlines], opportunisms & VO successful collaboration)

Trust criteria for Economical perspective

□ Capital

□ Financial Stability

Ideal organization with 5.0 score

Strongly less trustworthy	Less trustworthy	Average trustworthy	More trustworthy	Strongly more trustworthy

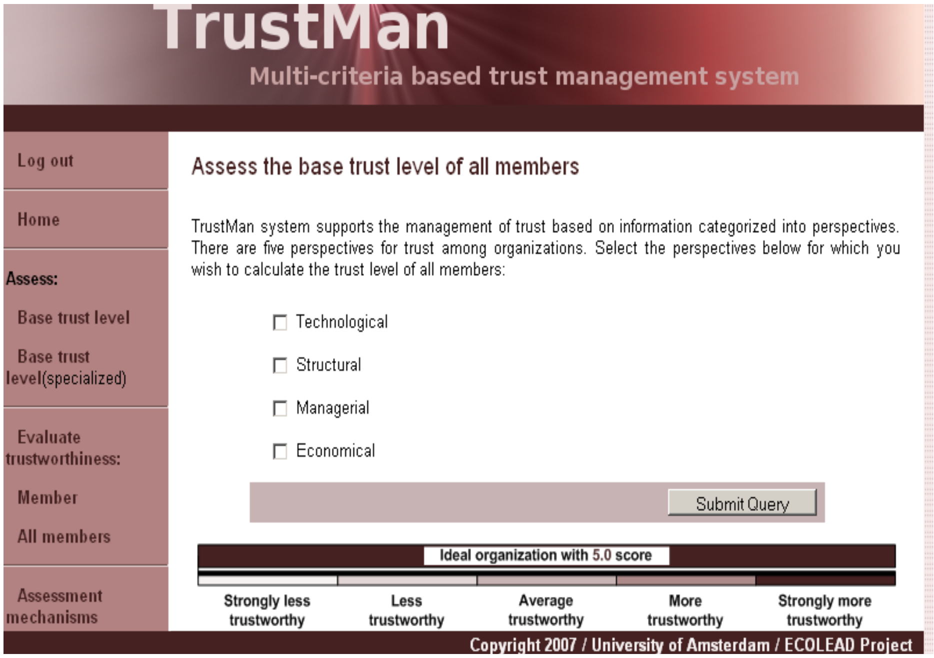
Copyright 2007 / University of Amsterdam / ECOLEAD Project

Figure 6.10: Web interface for selection of trust criteria to evaluate specific trustworthiness

This figure shows a screenshot of the user interface supporting the trustor with selecting specific set of trust criteria, related to evaluation of the trustworthiness of potential VO partners.

8. *Module for evolution support mechanisms:* This module is composed of classes that support the adaptability and customizability of the TrustMan in different VBEs.

9. *Module for adapting trust criteria:* The adaptation of the TrustMan system is enhanced by facilitating the possibility to change the applied set of trust criteria, without modifying any implemented mechanism. Although the entire set of general trust criteria is supported in the system, only the selected trust criteria for the VBE's pool are applied in the assessment of organization's level of trust in each VBE. "*Logical operations*" are implemented in the module as a way to support the changes of the set of preferred trust criteria for each VBE. Figure 6.11 shows an interface of the TrustMan system indicating four trust perspectives whose trust criteria were preferred and selected by IECOS VBE network during the take-up (see Table 6.3).


TrustMan
Multi-criteria based trust management system
Log out
Home
Assess:
Base trust level
Base trust level(specialized)
Evaluate trustworthiness:
Member
All members
Assessment mechanisms
Submit Query
Ideal organization with 5.0 score
Strongly less trustworthy
Less trustworthy
Average trustworthy
More trustworthy
Strongly more trustworthy
Copyright 2007 / University of Amsterdam / ECOLEAD Project

Assess the base trust level of all members

TrustMan system supports the management of trust based on information categorized into perspectives. There are five perspectives for trust among organizations. Select the perspectives below for which you wish to calculate the trust level of all members:

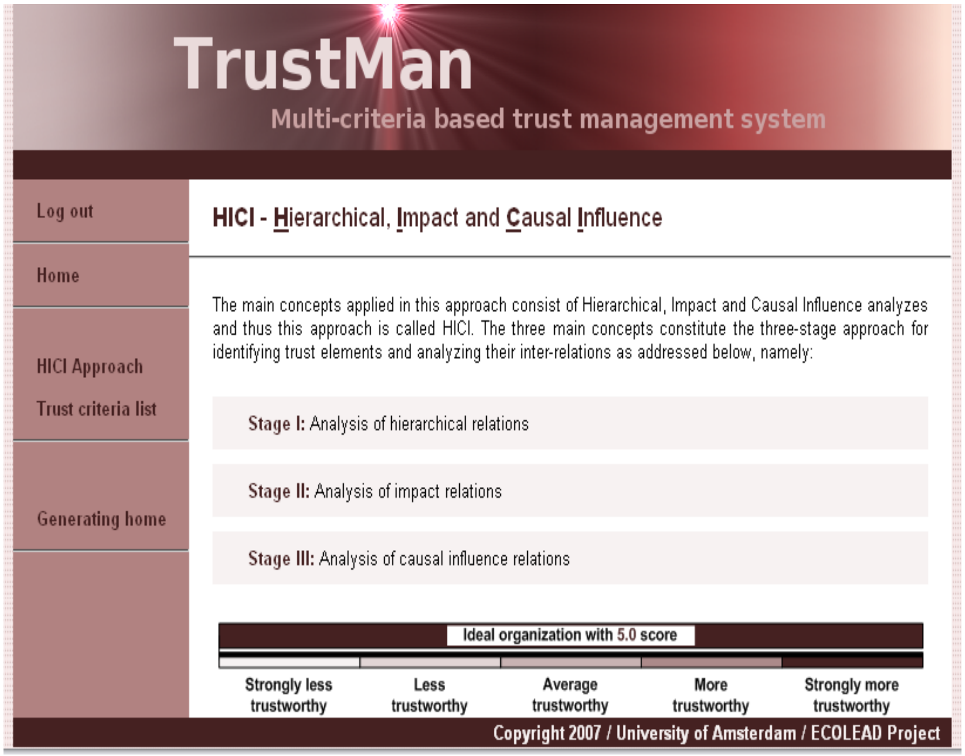
- □ Technological
- □ Structural
- □ Managerial
- □ Economical

Figure 6.11: Trust perspectives included in VBE pool of trust elements

This figure shows a screenshot of the user interface displaying the four trust perspectives selected by one VBE network, whose associated trust criteria are included in this VBE's pool of trust criteria.

10. *Modules for tuning the set of trust criteria:* The set of trust criteria applied in the TrustMan system may need to be tuned due to changes of certain conditions within the VBE environment which may lead to the need for adding new emerging trust criteria such as the emergence of a completely new trust objective. The TrustMan system provides guidelines based on HICI approach (as presented in Chapter 3) to support identifying sets of new trust criteria, which can then be used to further tune the system. Figure 6.12 shows an interface for accessing the guidelines based on HICI approach for tuning trust criteria.

11. Module for setting weights in equations: Customization of weights in mechanisms for assessing the base trust level of organizations is done based on the preferences of the VBE administrator. The weights here are assumed to be valid for a relatively long period. They will not change until the VBE undergoes an evolution. The evolution can for example be extending the VBE with introduction of a new market focus, which in turn will require selecting new set of base trust criteria. The customization of weights in mechanisms used to evaluate the specific trustworthiness of potential VO partners is done based on the preferences of the VO planner. The weights assigned to trust criteria and known factors are assumed to be short-term and only valid for each individual VO. This configuration of weights is supported by this model shown in Figure 6.9.


TrustMan
Multi-criteria based trust management system
Log out
Home
HICI Approach
Trust criteria list
Generating home
Ideal organization with 5.0 score
Strongly less trustworthy
Less trustworthy
Average trustworthy
More trustworthy
Strongly more trustworthy

HICI - Hierarchical, Impact and Causal Influence

The main concepts applied in this approach consist of Hierarchical, Impact and Causal Influence analyzes and thus this approach is called HICI. The three main concepts constitute the three-stage approach for identifying trust elements and analyzing their inter-relations as addressed below, namely:

Stage I: Analysis of hierarchical relations

Stage II: Analysis of impact relations

Stage III: Analysis of causal influence relations

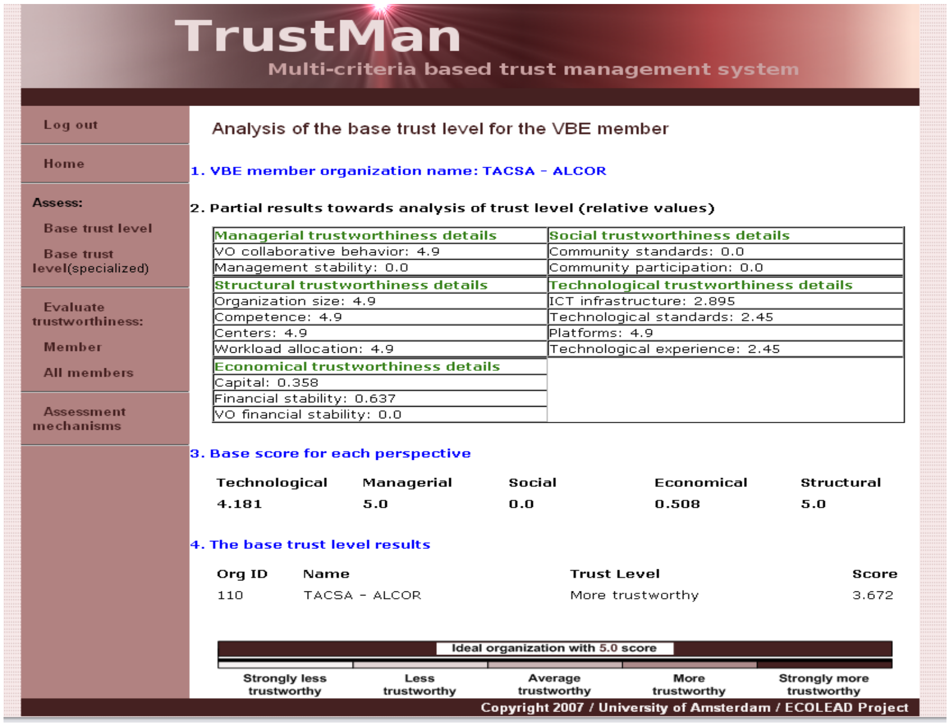
Copyright 2007 / University of Amsterdam / ECOLEAD Project

Figure 6.12: Information about HICI approach in the TrustMan system

This figure shows a screenshot of the user interface with links (stage I to III) to the information on the HICI approach addressed in Section 3.2.

Another important aspect supported by the TrustMan system is the customization of the user interfaces. Users can set their preferences, for example, related to how the system should display results of the assessment of trust level. The interface may be for example to display detailed results including score of each intermediate factor (as shown in Figure 6.13). Alternatively, the final results of the trust level of organizations (see Figure 6.15).

The last aspect supported by the TrustMan system in relation to customization is setting up the ranges of scores for trust level and their interpretation. This is of particular importance for the evaluation of specific trustworthiness of organizations because the sensitivity of processes that VO partners may participate differs among brokered opportunities. Consequently, VO brokers may set a different range of scores for the same level of trust in organizations as shown in Table 5.1. Therefore, the TrustMan system supports user to define these ranges and their interpretation while evaluating the trustworthiness of organizations.


TrustMan
Multi-criteria based trust management system
Log out
Home
Assess:
Base trust level
Base trust level(specialized)
Evaluate trustworthiness:
Member
All members
Assessment mechanisms
Ideal organization with 5.0 score
Strongly less trustworthy
Less trustworthy
Average trustworthy
More trustworthy
Strongly more trustworthy
Copyright 2007 / University of Amsterdam / ECOLEAD Project

Analysis of the base trust level for the VBE member

1. VBE member organization name: TACSA - ALCOR

2. Partial results towards analysis of trust level (relative values)

Managerial trustworthiness details	Social trustworthiness details
VO collaborative behavior: 4.9	Community standards: 0.0
Management stability: 0.0	Community participation: 0.0
Structural trustworthiness details	**Technological trustworthiness details**
Organization size: 4.9	ICT infrastructure: 2.895
Competence: 4.9	Technological standards: 2.45
Centers: 4.9	Platforms: 4.9
Workload allocation: 4.9	Technological experience: 2.45
Economical trustworthiness details	
Capital: 0.358	
Financial stability: 0.637	
VO financial stability: 0.0	

3. Base score for each perspective

Technological	Managerial	Social	Economical	Structural
4.181	5.0	0.0	0.508	5.0

4. The base trust level results

Org ID	Name	Trust Level	Score
110	TACSA - ALCOR	More trustworthy	3.672

Figure 6.13: Detailed presentation of the trust level of an organization

This figure shows a screenshot of the user interface displaying detailed analysis results for an organization from the service for assessing the base trust level.

6.6.2 Take-ups of the TrustMan at running industrial VBE networks

The applicability and relevance of the TrustMan system was tested by four running industrial VBE networks, namely: IECOS (Mexico), CebeNetwork (Germany), SMT (Switzerland) and ISOIN (Spain) (see their description in Annex C). The testing of the TrustMan system followed three steps: (A) Setting up the VBE pool of trust criteria and deploying the TrustMan system, (B) Managing inter-organizational trust using the TrustMan system, and (C) Analyzing the improvements on the performed processes and the gained benefits.

A. Setting up the VBE pool of trust criteria and deploying the TrustMan

In addition to reconfiguring the user interfaces, user rights, external interoperability points, and so on, the VBE administrators did set-up their specific VBE pool of trust criteria in the TrustMan system. The trust criteria included in their VBE pool were selected from the general set of trust criteria as presented in Section 3.3 based on the preferences and perceptions of trust for each VBE. Table 6.3 shows the VBE pool of trust criteria preferred by each VBE network.

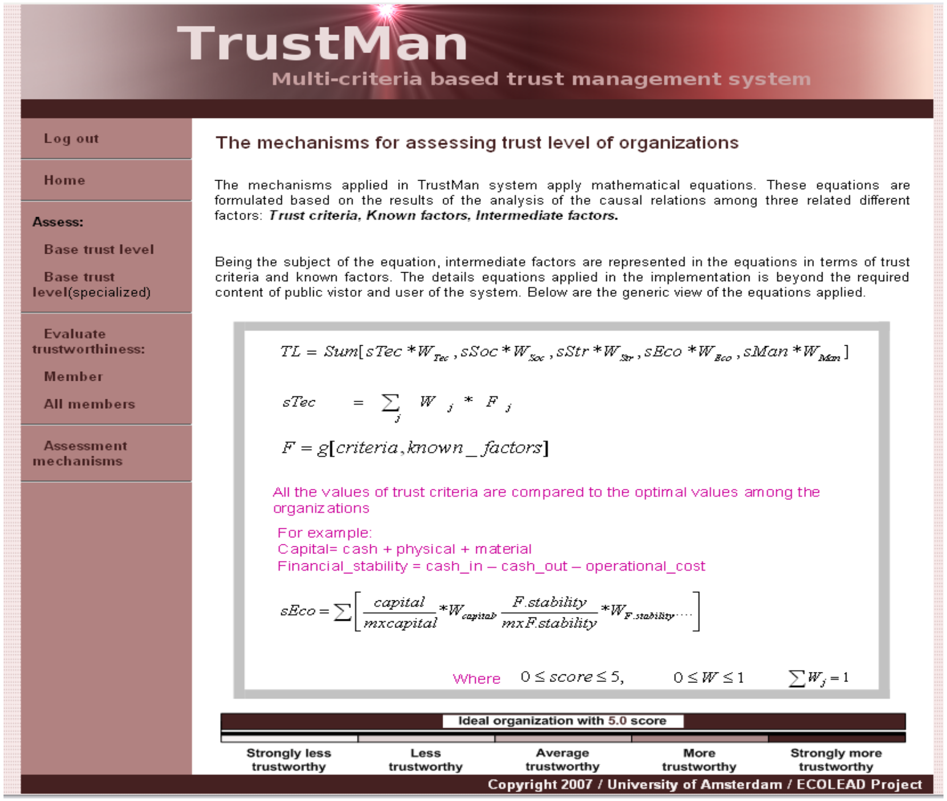
Table 6.3: Different pools of trust criteria preferred by VBE networks
A: IECOS, B: CBN, C: ISOIN, D: SMT and B&C: joint VBE networks of ISOIN and CBN

Trust perspective	**Trust requirements**	**Trust criteria**	**A**	**B**	**C**	**D**	**B& C**
Structural	Structural strength	Size	x	x	x	x	x
		Competences	x	x	x	x	x
		Personnel expertise	x	x	x	x	x
	Business strength	Geographical coverage		x	x	x	x
		Joint ventures		x	x	x	x
		Centres		x	x	x	x
		Workload allocation	x	x			x
Social	Participation	Activities participated			x	x	
		Service contribution			x	x	
	Compliance	Standards complied			x	x	
Economical	Capital	Cash	x		x	x	x
		Physical	x	x	x	x	x
		Material	x	x	x	x	x
	Financial stability	Cash in			x	x	x
		Cash out			x	x	x
		Profit/Loss			x	x	x
		Operational costs			x	x	x
	VO financial stability	Cash in	x		x	x	x
		Cash out	x		x	x	x
		Profit/Loss	x		x	x	x
	Financial standards	Auditing standards		x	x	x	x
		Auditing frequency		x	x	x	x
Technological	ICT-Infrastructure	Network speed – Broadband	x	x	x	x	x
		Interoperability	x	x	x	x	x
		Availability	x	x	x	x	x
	Technology standards	Protocol supported		x	x		x
		Software standards		x	x		x
		Hardware standards	x	x	x		x
		Security standards		x	x		x
	Platforms	Operating systems	x	x	x		x
		Programming languages		x	x		x
	Platform experience	Applied in VOs	x	x	x		x
		External project applied	x	x	x		x
		Duration held	x	x	x		x
Managerial	Stable management	Years in power		x	x	x	x
		Legal status (management)		x	x	x	x
		Frequency of power change		x	x	x	x
	VO-Collaborative behaviour	VO opportunistic behaviour	x	x	x	x	x
		VO collaborations	x	x	x	x	x
		VO leadership history	x	x	x	x	x
	Reliability	Quality	x	x	x	x	x
		Adherence to delivery dates	x	x	x	x	x

B. Managing inter-organizational trust using the TrustMan system

During the experimentation, a number of processes related to the management of trust between organizations were performed by the VBE networks using services provided by the TrustMan system. We have categorized these processes into five groups (P1 to P5), particularly related to the following:

P1: ***Improving the understanding of trust concepts:*** Organizations need to properly understand the concepts of trust as perceived within the VBE in order to accept the results of the assessment of their trust level. To support this process the TrustMan system maintains information related to the following among others: (1) All trust elements applied to the assessment of trust level of organizations, (2) Presentation and interpretation of trust level of organizations, and (3) Mechanisms for assessing trust level. These pieces of information can be accessed by all VBE member organizations. Figure 6.14 represents a screenshot of the TrustMan system showing (at higher-level of aggregation) the description of the mechanisms used to assess the level of trust in organizations. This process is supported by services 3, 4 and 6 as presented in Table 6.2.


TrustMan
Multi-criteria based trust management system
Log out
Home
Assess:
Base trust level
Base trust level(specialized)
Evaluate trustworthiness:
Member
All members
Assessment mechanisms
Ideal organization with 5.0 score
Strongly less trustworthy
Less trustworthy
Average trustworthy
More trustworthy
Strongly more trustworthy

The mechanisms for assessing trust level of organizations

The mechanisms applied in TrustMan system apply mathematical equations. These equations are formulated based on the results of the analysis of the causal relations among three related different factors: ***Trust criteria, Known factors, Intermediate factors.***

Being the subject of the equation, intermediate factors are represented in the equations in terms of trust criteria and known factors. The details equations applied in the implementation is beyond the required content of public vistor and user of the system. Below are the generic view of the equations applied.

$$TL = Sum[sTec * W_{Tec}, sSoc * W_{Soc}, sStr * W_{Str}, sEco * W_{Eco}, sMan * W_{Man}]$$

$$sTec = \sum_j W_j * F_j$$

$$F = g[criteria, known\_factors]$$

All the values of trust criteria are compared to the optimal values among the organizations

For example:
Capital= cash + physical + material
Financial_stability = cash_in – cash_out – operational_cost

$$sEco = \sum \left[\frac{capital}{mxcapital} * W_{capital}, \frac{F.stability}{mxF.stability} * W_{F.stability} \cdots \right]$$

Where $0 \le score \le 5$, $0 \le W \le 1$ $\sum W_j = 1$

Copyright 2007 / University of Amsterdam / ECOLEAD Project

Figure 6.14: Description of mechanisms for assessing trust level of organizations

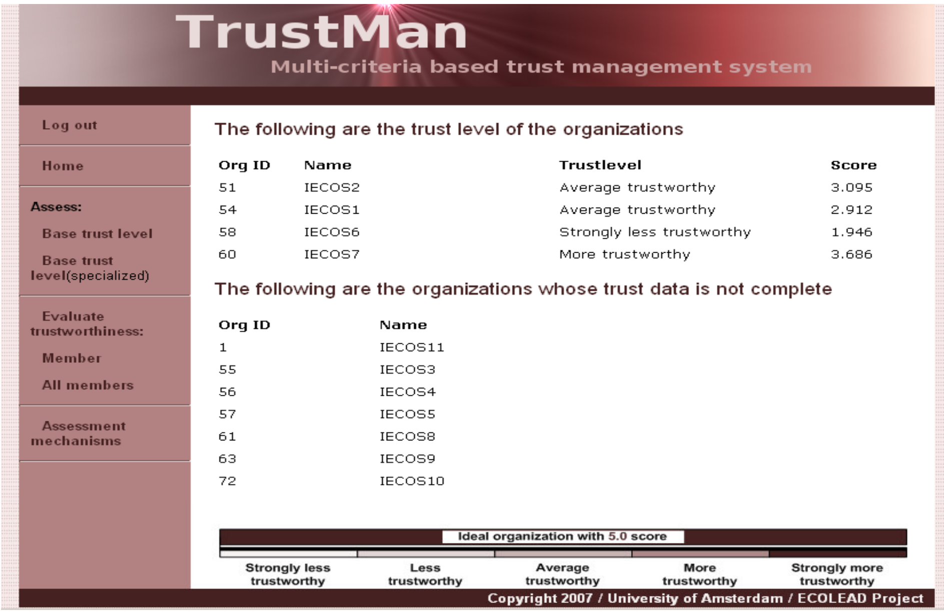
This figure shows a screenshot of the user interface displaying information about the mechanism for assessing the trust level of organizations as presented in Section 6.3.1, indicating how it is formulated in the TrustMan system to enhance the understanding of users.

P2: ***Presenting and interpreting the trust level of organizations:*** Upon assessing the trust level, the trustor organization shall present the results to all trustee organizations and explain the validity and correctness of their levels of trust. Thus, the trustor needs to be prepared to describe the ranges of scores for the trust level and their related interpretation as exemplified in Table 5.1.

P3: ***Selection of trust criteria:*** The services provided by the TrustMan system to support this process are aimed at facilitating a VO broker to select the trust criteria that meet the requirements of the brokered opportunity. This process is supported by service 2 as presented in Table 6.2 and its user interface is shown in Figure 6.10.

P4: ***Assessment of trust level of organizations:*** This process comprises two activities, namely, *assessing the base trust level of organizations* (performed by the VBE administrator) and *evaluating specific trustworthiness* (performed by the VO broker). This process is supported by services 1 and 2 as presented in Table 6.2. The VBE administrator uses the service for assessing trust level of organizations for two purposes: (1) To get a general picture of the balance of levels of trust in organizations in the VBE (see Figure 6.15), and (2) To get detailed results of the analysis of the trust level of one organization (see Figure 6.13).

Figure 6.15 shows results of the process of assessing the base trust level of all member organizations in the VBE. The figure also indicates those organizations whose trust related data is not fully submitted in the system.


TrustMan
Multi-criteria based trust management system
Log out
Home
Assess:
Base trust level
Base trust level(specialized)
Evaluate trustworthiness:
Member
All members
Assessment mechanisms
Ideal organization with 5.0 score
Strongly less trustworthy
Less trustworthy
Average trustworthy
More trustworthy
Strongly more trustworthy
Copyright 2007 / University of Amsterdam / ECOLEAD Project

The following are the trust level of the organizations

Org ID	Name	Trustlevel	Score
51	IECOS2	Average trustworthy	3.095
54	IECOS1	Average trustworthy	2.912
58	IECOS6	Strongly less trustworthy	1.946
60	IECOS7	More trustworthy	3.686

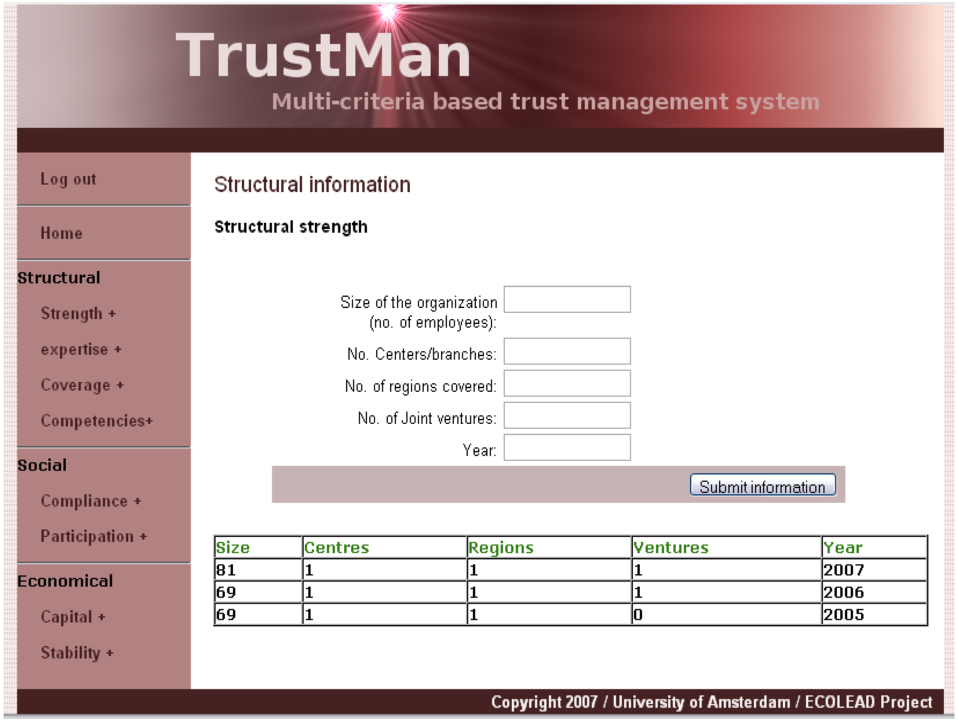
The following are the organizations whose trust data is not complete

Org ID	Name
1	IECOS11
55	IECOS3
56	IECOS4
57	IECOS5
61	IECOS8
63	IECOS9
72	IECOS10

Figure 6.15: Results of assessment of trust level for all organizations in the VBE

This figure shows a screenshot of the user interface displaying the final results of the assessment of trust level for all organizations in the VBE. The interface also indicates those organizations for which some trust related data is not complete in the system.

P5*:* ***Management of trust related data:*** This process is performed by each organization in the VBE to ensure that its trust related data is up-to-date. Every organization can access the TrustMan system to use the service for managing trust related data (service 4 as presented in Table 6.2) to view its own data and submit new data as shown in Figure 6.16.



Structural information

Structural strength

Size of the organization (no. of employees):

No. Centers/branches:

No. of regions covered:

No. of Joint ventures:

Year:

Size	Centres	Regions	Ventures	Year
81	1	1	1	2007
69	1	1	1	2006
69	1	1	0	2005

Copyright 2007 / University of Amsterdam / ECOLEAD Project

Figure 6.16: Viewing and submitting organizational trust related data

This figure shows a screenshot of the screenshot of the user interface displaying a form for submitting trust related data related to the structural perspective. The interface also shows the previous data existing in the TrustMan system related to the logged in organization.

C. Analyzing the improvements on performed processes and gained benefits

Business organizations aim to optimize their profit while operating in a market. An organization's profit can be enhanced by addressing among others, the following issues:

- Raising the *price* of products
- Acquiring more *customers* and increasing *sales*
- Minimizing production/delivery *resources*
- Reducing the *time* of production or delivery of products/services.

Our research provides conceptual results (methodologies, approaches, mechanisms, etc.) as presented in Chapters 2, 3, 4, and 5 and software prototypical result (the TrustMan system) presented in this chapter. The resulting software has the potential of helping organizations enhance their collaborative performance and in doing so raise their profits. When organizations trust each other they can efficiently collaborate and this consequently enhances the performance of both organizations and the network. However, our research results are unlikely to directly influence the price of their products, nor are these results likely to directly enhance the acquisition of more customers.

Our research results may, however, influence the use of resources and the time needed to accomplish certain processes. For example, the services supporting processes related to the assessment of level of trust in VO partners will reduce the number of human resources and the time needed to perform such processes. This will result in less VO setup cost, which will enhance the profit achieved. Thus, while testing the TrustMan system, the VBE administrators evaluated improvements on processes that were performed using the TrustMan system.

To indicate the quality of services provided by the TrustMan system in terms of improvements on performed processes two groups of indicators were used: ***quantitative indicators and qualitative indicators***.

1. **Quantitative indicators:** These are indicators that can be measured in numbers and are applied to quantitatively analyze and evaluate the improvements on the processes supported by the TrustMan system. Table 6.4 describes two quantitative indicators, namely: *resources and time*, applied to evaluate the TrustMan system.

Table 6.4: Quantitative indicators applied to evaluate the TrustMan system

Indicator	Value	Description
C1: Resources	Increase or decrease in percentage	Resources refer to the commodities and personnel that are used in the production of goods and services. Resources may include natural resources (commodities that are valuable in their relatively natural form, such as machines, and so on), human resources, financial resources, etc. Considering our software result the possible improvements in performing the above mentioned processes (P1-P5) can be observed in terms of the reduction of the number of involved human resources. This indicator is measured as a 'percentage' of change of the number of people involved in a certain process.
C2: Time	Increase or decrease in percentage	Time here refers to the days, weeks, months, and so forth that have elapsed between the starting point and the finishing point of a certain process. It is measured as a 'percentage' of change of the time needed to accomplish each process.

The quantitative evaluation of the TrustMan system was done by VBE administrators by estimating the reduction of time and resources for the five processes (P1-P5) as introduced earlier in this section. Table 6.5 shows the estimated reduction of time and resources (in terms of percentages) for the five processes. The results were collected using a questionnaire presented in Annex C. As shown in Table 6.5 there was reduction of time and human resources for all process performed by the VBE networks using the TrustMan system. The graphical representation (Figure 7.2) and the interpretation of these results are presented in Chapter 7.

Table 6.5: Results of evaluation of the TrustMan system using quantitative indicators (The numbers in this table refers to percentage of reduction of time and resources)

		P1	P2	P3	P4	P5	Average
ISOIN	Time	50	20	45	40	40	40
	Resource	20	25	20	20	20	20
IECOS	Time	25	25	25	25	25	25
	Resource	20	20	20	20	20	20
CBN	Time	20	20	20	20	20	20
	Resource	10	10	10	10	10	10
SMT	Time	20	20	20	20	20	20
	Resource	10	10	10	10	10	10
Average	Time	29	21	28	26	26	26
	Resource	15	16	15	18	15	16

2. **Qualitative indicators:** These are indicators that cannot be measured with numbers and are applied to evaluate the TrustMan system using some grading scheme. Table 6.6 shows five qualitative indicators applied to evaluate the TrustMan system. It also provides a brief justification for choosing and applying each indicator in the evaluation.

Table 6.6: Qualitative indicators applied to evaluate the TrustMan system

Indicator	Value	Description
C3: Innovation	SoA, innovative or very innovative	State of the art and practice (SoA) refers to innovation as the development of concepts and tools that do not already exist in the market. Using this indicator, VBE administrators can indicate the quality of services provided by the TrustMan system as compared to those services that they have been applying in their activities.
C4: Reliability	High, normal, or low	Reliability is the ability of a system to perform and maintain its functions in routine circumstances, as well as in hostile or unexpected circumstances. To be reliable, a system must perform its functions and produce results of consistent quality, irrespective of the time or running environment. Using this indicator, VBE administrator can indicate the quality of services provided by the TrustMan system when remotely accessed using computer networks. This aspect is important considering the distributed nature of VBEs.
C5: Usability	Easy, normal, or difficult	Usability refers to the effectiveness, efficiency, and satisfaction that users can achieve when using a particular system. High usability means that a system is: easy to learn and remember, efficient, visually pleasing and fun to use, quick to recover from errors, etc. Users of the TrustMan system are decision makers of organizations who aim at getting information about the trust of other organizations for the purpose of making strategic decisions, such as establishing business collaborations with them. These users might not have strong expertise in computer science and mathematics and thus the TrustMan system must have user friendly interfaces.
C6: Expectation	Highly achieved, achieved, not achieved	We assumed that the demonstrating networks have certain objectives that they were expecting to achieve by adapting the developed solutions. The networks are able to indicate how their expectations were achieved.
NA - Not Applicable	NA (Not Applicable)	The task is completely new and has not previously been performed in the network. Therefore, NA refers to the fact that the comparative and quantitative evaluation is not possible due to lack of this feature in the past.

The evaluation results collected during the take-up were analyzed and summarized on the basis of the four qualitative indicators (C3 – C6) as shown in Table 6.7. The results were collected using a questionnaire presented in Annex C. The graphical representation (Figure 7.1) and the interpretation of these results are presented in Chapter 7.

To quantitatively analyze the collected evaluation results that applied qualitative indicators, these grading schemes were mapped into some range of numbers (scores). The mapping was as follows:

- Highest grade (i.e. very innovative, high, easy, highly achieved) is mapped into a score of 3,
- Medium grade (i.e. innovative, normal, and achieved) is mapped into a score of 2, and
- Lowest grade (i.e. SoA, low, difficult, and not achieved) is mapped into a score of 1.

After conversion, a numerical analysis was performed focusing on the average score for all processes performed by each VBE for every evaluation indicator. For example, the results from ISOIN network are converted as follows:

1. An average score for each indicator was calculated based on all processes: innovation is 2.8, reliability is 3, usability is 2.6, and expectation is 2.6.
2. The average score for all indicators was computed for ISOIN: 2.75.

The average score represents the general acceptance of our results by the specific VBE networks as shown in Table 6.7 and graphically represented in Figure 7.1

Table 6.7: Results of evaluation of the TrustMan system with qualitative indicators

VBEs	**Processes**	**Qualitative evaluation indicators**				**Average score (0-3)**
		Innovation	**Reliability**	**Usability**	**Expectation**	
ISOIN	P1	Very innovative	High	Easy	Highly achieved	2.75
	P2	Innovative	High	Easy	Achieved	
	P3	Very innovative	High	Normal	Highly achieved	
	P4	Very innovative	High	Easy	Highly achieved	
	P5	Very innovative	High	Normal	Achieved	
IECOS	P1	Innovative	High	Normal	Achieved	2.4
	P2	Innovative	High	Normal	Achieved	
	P3	Innovative	High	Easy	Achieved	
	P4	Innovative	High	Easy	Achieved	
	P5	Innovative	High	Easy	Achieved	
CBN	P1	Innovative	High	Easy	Highly achieved	2.45
	P2	Very innovative	Normal	Easy	Achieved	
	P3	Innovative	High	Normal	Achieved	
	P4	Very innovative	Normal	Easy	Highly achieved	
	P5	Innovative	High	Difficult	Not achieved	
SMT	P1	Very innovative	High	Easy	Highly achieved	2.5
	P2	Innovative	High	Normal	Achieved	
	P3	Very innovative	High	Easy	Achieved	
	P4	Very innovative	Normal	Easy	Highly achieved	
	P5	Innovative	High	Normal	Achieved	

6.7 Chapter discussion and conclusion

This Chapter addresses the analysis, design and implementation of functionalities and services to support the management of inter-organizational trust in VBEs. It presents the development of the TrustMan system and services that address the requirements for inter-organizational trust in VBEs. These requirements have been identified through the requirement analysis of the TrustMan system (mainly addressed in Chapters 1 and 6), involving trust experts and VBE experts and through performing some empirical studies at running industrial VBEs.

The chapter first presents the concepts of the VBE management system (VMS), and then the VMS's subsystems and the interactions among those subsystems. The chapter then presents in detail the development of the TrustMan system and focuses specifically on each of the following aspects:

+ ***Specification of the TrustMan system***: As a step towards developing the TrustMan system, we have performed the analysis to identify its users and their user requirements, and based on the user requirements we have specified the needed functionalities and services.
+ ***Architectural design of the TrustMan system*****:** In this thesis we have adopted and applied the service oriented architecture and specifically the web service technology standards to design the architectures of the TrustMan system. Based on these concepts, two kinds of architectures (the interoperability architecture and four-layer componential architecture) are designed for supporting different aspects during the implementation of the TrustMan system. Furthermore, some partial architectures are also designed for the TrustMan system, such as those related to orchestration and choreography of services based on web service standards.
+ ***Implementation aspects applied to the development of the TrustMan system***: The implementation of the TrustMan system is done in the Java language. Since Java is platform independent, the adaptability of the TrustMan system to different technical running environments is assured.
+ ***Replicability, adaptability and customizability of the TrustMan system****:* As addressed in Section 6.6.1, the TrustMan system is replicable because it: (1) uses general set of trust criteria, (2) uses generic mechanisms for assessing trust level of organizations, and (3) provides mechanisms for enabling or disabling its features which assures its adaptability and customizability. It is also adaptable because it supports: (i) setting-up a pool of trust criteria to meet the requirements of every specific VBE, and (ii) tuning a set of trust criteria when the system when some conditions have changed in the VBE such as emergence of new trust objectives. Furthermore, it is also customizable because it supports: (a) tailoring the mechanisms for assessing the level of trust in organizations to meet the requirements of each specific user by changing the weight for each trust criteria in the implemented equations, and (b) configuring user interfaces to meet requirements of a specific user in the VBE.
+ ***Take-ups and experimentation of the TrustMan system***: The TrustMan system has been tested by four running industrial VBE networks, and the evaluation results are collected, in particular those related to indicators presented in Table 6.4 and Table 6.6. The evaluation of the TrustMan system is also discussed in Chapter 7.

In response to the MRQ4 and its related sub-question (SRQ4.1, SRQ4.2, and SRQ4.3), this chapter has addressed the development of services supporting the processes relating to the management of inter-organizational trust in VBEs. In Chapter 7 an integrated view is given on how all the research questions as presented in Section 1.5 are addressed.

Chapter 7

Conclusion, validation, lessons learned and future work

7.1 Introduction

This chapter presents a summary of the achieved results and concludes the thesis. It first briefly presents how and where in the thesis the research questions introduced in Section 1.5 are addressed and reflects on the achievements of our research in relation to the research objectives. The chapter then addresses the evaluation and validation of our proposed solutions and concepts. Finally, the chapter concludes with a discussion of the lessons learned and proposes three directives for the future work in this area.

7.2 Reflection on research findings

Each main research question presented in Section 1.5 corresponds to one or more chapters in the thesis. In this section we briefly summarize answers to each research question and how they contributed to achieving our research objectives.

7.2.1 Reflection on responses to the research questions

MRQ1: How the diversities in the purposes for which trust among organizations need to be established (from trustor to trustee) as well as trustor's concerns and preferences can be handled?

Generally, the set of trust criteria applied to assess the level of trust in an organization may differ among different trust objectives due to dissimilar perceptions and preferences on trust among trustor organizations. As explained in Chapters 5 and 6 the preference of a trustor organization influences its selection of trust criteria to apply in assessing the level of trust in trustee organizations. Thus it is not possible to generalize for all trustors the selection of the set of trust criteria for all cases of trust establishment between organizations.

MRQ2: How can the understanding of many elements and concepts related to rational trust within a VBE be supported for its stakeholders?

In Chapter 4, we have presented models of trust relationships between organizations. These models are developed for the purpose of supporting organizations in achieving a common understanding of concepts related to inter-organizational trust. By assisting organizations in gaining insight into inter-organizational trust, the proposed models will enable these organizations make knowledgeable and informed decisions on trusting others. In Section 4.3, we have proposed the *ontology-based formalism* that supports organizations in achieving and maintaining common understanding about the fundamental concepts of inter-organizational trust.

MRQ3: How can formal mechanisms be developed to rationally assess and formally reason about the level of trust in organizations?

The level of trust in an organization can neither be measured with a single trust criterion nor interpreted with a single metric. A multi-criteria approach is proposed in this thesis for assessing the organization's level of trust in VBEs. The thesis proposes the HICI approach for systematically identifying and characterizing fact-based trust criteria for organizations, as presented in Section 3.2. The HICI approach is applied to identify a large general set of trust criteria for organizations as presented in Section 3.3, validated by experts in the area to be comprehensive.

On the basis of the characterized trust criteria we have proposed mathematical formulas for assessing the level of trust in the organization. The suggested mechanism applies analysis of causal influences among the trust criteria, the known factors and the intermediate factors to generate these formulas, as presented in Chapter 5. As such, we have shown that the level of trust in an organization can be measured in terms of a series of fact-based trust criteria. Furthermore, the perceptions of trust differ between organizations which in turn influence the trustors' preferences regarding which trust criteria to apply in assessing trustees' level of trust. Therefore, as proposed in this thesis the mechanisms for assessing trust level of an organization must be customizable to apply the set of trust criteria preferred by the trustor. Trustor organizations can also use these mathematical equations to rationally reason on the accuracy of the results of the assessment of the level of trust in trustee organizations.

MRQ4: How can the establishment of inter-organizational trust relationships in VBEs be facilitated?

A number of systematic steps must be followed to establish sustainable inter-organizational trust relationships and for this purpose, as presented in Section 2.5, guiding steps are proposed. As proposed in these steps the management of inter-organizational trust as addressed in Chapter 6 is required to controlling the balance of levels of trust among organizations in the VBE. TrustMan system is designed on the basis on of the Service Oriented Architecture (SOA) and in particular web service standards. The applied SOA standards enhance the replicability, adaptability and sustainability of TrustMan system in different application environments.

As addressed in Chapter 2, there are also other fundamental related issues that need to be properly considered and analyzed while establishing trust relationships between organizations, including: the analysis of possible risks associated with trust relationships between organizations (addressed in Section 2.3.5) and the validation of the trust-related data that is used to assess the level of trust in organizations (addressed in Section 2.4).

7.2.2 Reflection on achievement of research objectives

Based on the addressed research questions mentioned in Section 7.2.1, we can state that both research objectives of RO1 and RO2 stated in Section 1.5 of the thesis are achieved as described below.

RO1: To properly support the management of trust aspects in VBE, providing generic and comprehensive "concepts, approaches, mechanisms and models" needed for supporting:

- *Common understanding of the aspects relating to rational trust,*
- *Assessment of organizations' level of trust,*
- *Creation of inter-organizational trust,*
- *Establishment of trust relationships between organizations".*

In this thesis we have characterized the inter-organizational trust addressing among other aspects: the identification of fact-based trust elements for organizations, the modeling of trust relationships between organizations, the assessment of trust level of an organization, and support for the establishment of trust relationships between organizations. The research objective – RO1 – is achieved by answering research questions MRQ1, MRQ2, and MRQ3, as summarized in Section 7.2.1.

RO2: Providing a validated prototype implementation for a trust management system in VBEs in order to assist organizations in achieving various trust-related objectives.

The analysis, design, implementation and operation of the TrustMan system are addressed in detail in Chapter 6. The TrustMan system provides services supporting the tasks related to management of trust between organizations in VBEs. The approach applied to the development of TrustMan system and the set of considered aspects provide the response to the main research question MRQ4 as summarized in Section 7.2.1. We have achieved the RO2, in relation to the development of TrustMan system, by: identifying a number of potential users, analyzing users' requirements, specifying functionalities and services, and designing system architectures and user interfaces, as summarized in Section 7.2.1.

7.3 Evaluation and validation of research results

This section presents the evaluation of our research findings. First, it describes the approaches followed to validate our research findings. Second, it addresses the empirical validation performed by VBE networks. Third, it presents the validation of TrustMan system with standard indicators and against other related systems. Finally, it presents the validation of our research findings within the scientific community.

7.3.1 General evaluation approaches

In science, we are keen to evaluate our achieved results and the steps we followed to produce the results. For a standard software development project the evaluation focuses on measuring key aspects of results such as products, processes, and resources and then use this information to determine whether we have met our goals such as: productivity, performance, quality and other desirable attributes [Pfleeger, 2001]. But there are many possible evaluation techniques to choose from, and it is important to understand which one(s) are most appropriate for an application. For this research, we have chosen the approaches suggested by Pfleeger [Pfleeger, 2001] to evaluate our findings against the following four techniques:

- ***Case study***: This technique is particularly useful in depicting a holistic portrayal of a client's experiences and results regarding a system. Case studies are used to organize a wide range of information about a case and then analyze the contents by seeking patterns and themes in the data and by further analysis through cross comparison with other cases. A case (under study) can be related to individuals, programs, or any unit, depending on what the program evaluators want to examine through in-depth analysis and comparison. Most case studies involve the use of quantitative indicators. We have applied this technique to perform an empirical evaluation of TrustMan system with quantitative indicators as further addressed in Section 7.3.3.

- ***Feature analysis***: This technique is primary used to rate and rank the attribute of a developed software product, in order to evaluate whether it is innovative on basis of specific standards or against other products. As presented in Section 7.3.4, we have applied this technique to evaluate and validate our developed research results on the bases of standard indicators as inspired by ISO 9126. We have also applied this technique to evaluate our results within the scientific community as further addressed in Section 7.3.5.

- ***Survey***: This technique is primarily a retrospective study to try to document expectations and outcomes in given situations. Surveys are often done in social sciences, where attitudes are polled to determine how population feels about a particular set of issues, or a demographer surveys a population to determine trends and relationships. In computer science, surveys are very similar to that, we record information to determine how project participants and other stakeholders reacted to a particular method, tool, or technique. We have also applied this technique to perform an empirical evaluation of our results with qualitative indicators as addressed in Section 7.3.3.

- ***Formal experiment***: This technique is used when values of some independent but representative variables are manipulated, and we observe changes in dependent variables, in order to determine how changes in the input affect changes in the output. This technique is mostly applied to evaluate the effectiveness and accuracy of algorithms. Considering that our research is not focused on testing algorithms, we did not apply this technique to evaluate our achieved results.

7.3.2 Validation of our achieved results

A fundamental step guiding us during our research was related to the validation of our resulted findings. We have successfully validated our research findings, using the three techniques mentioned above, namely: empirical validation, feature analysis (with standard indicators and within research community), survey (empirical validation with qualitative indicators), and case study (empirical validation with quantitative indicators), presented in Section 7.3.1 as follows:

- ***Experimentation in running industrial VBE networks*** *(Empirical validation)*: Our research aimed at providing innovative solutions to support the management of inter-organizational trust in VBE networks. As part of the research requirement specification, a number of VBE's requirements (presented in Chapter 1) related to the management of inter-organizational trust were identified and analyzed. To validate our research findings against these identified VBE's requirements, our proposed solutions were tested by four running VBE networks during the ECOLEAD project. This empirical validation task focused on evaluating the innovativeness of the conceptual results and software prototypical results (in line with "*the case study*" technique). The empirical validation of our research findings is presented in Section 7.3.3.

- ***Validation with standard indicators and against other systems*** *(self validation)*: In parallel to performing the empirical validation, another step was to analyze whether our proposed solutions are developed following scientific approaches and standards. Therefore, we have validated our prototypical result (the TrustMan) applying scientific indicators and against other existing related trust management systems. This validation process (in line with "*the feature analysis*" technique) is presented in Section 7.3.4.

- ***Validation within scientific community*** *(peer reviewed validation)*: Also in parallel, we focused on consultation with other experts in the area of inter-organizational trust management to collect suggestions, comments, etc., for the purpose of validating our achieved results. This validation process (in line with "*the feature analysis*" technique) also heavily focused on presenting and publishing our research findings in scientifically and internationally accepted channels in related areas as presented in Section 7.3.5.

7.3.3 Empirical validation – Achievements in relation to VBE requirements

Our research findings are classified into two main categories, namely: the conceptual results including methodologies, mechanisms, approaches, etc., and the prototypical results including the TrustMan system and its set of developed functionality. These achieved results were tried and experimented within four industrial VBE networks for the purpose of validation against the requirements related to management of inter-organizational trust. The VBE networks that participated in validating the findings include: the Swiss Microtech (SMT), the ISOIN, the Cebenetwork (CBN), and the IECOS (see their descriptions in Annex C). These empirical evaluation and validation of our results was performed applying a set of *qualitative indicators* to evaluate their level of innovation, reliability, usability, and expectation, as well as a set of *quantitative indicators* to evaluate the needed resource and time.

A: With qualitative indicators

To qualitatively validate the research findings some questionnaires (see Annex C) were developed in order to collect empirical evaluation results from the above four industrial VBE networks. Figure 7.1 shows a bar chart representing these results and more specifically the generalized picture regarding the validation and acceptance of the proposed research findings and developments by these VBE networks. The numbers shown in Figure 7.1 represent scores referred to as the level of acceptance of our research findings by the VBE networks. These scores are computed on the basis of quantitative values obtained for each qualitative indicator mentioned in this section. The quantitative values of indicators are obtained by mapping the applied qualitative grading schemes into some range of numbers. This mapping and the analysis of evaluation results of our research findings with qualitative indicators is addressed in Section 6.6.2, and summarized in Table 6.7. The score of: 3 represents strong acceptance, 1.5 represents average acceptance, and 0 represents the poor acceptance.

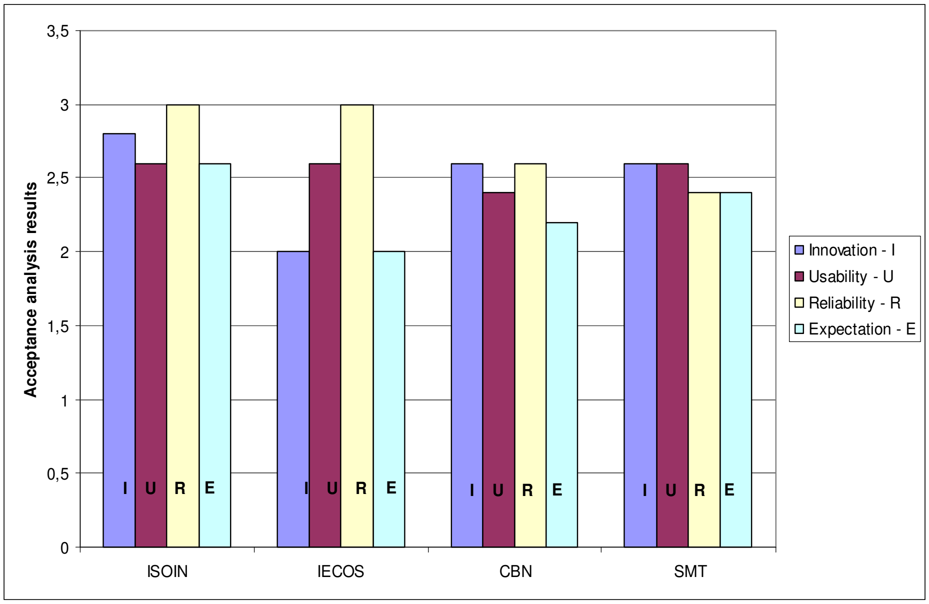


Figure 7.1: Empirical validation of research findings with qualitative indicators by VBE networks

This figure shows the results of evaluation both the conceptual and prototypical results produced by TrustMan system applying several qualitative indicators. The conversion of qualitative indicators to numbers and their computations whose results are indicated in this graph is presented in Section 6.6.2.

B: With quantitative indicators

To quantitatively evaluate our research findings each VBE estimated their reduction of time and resource, in terms of a percentage, after applying our solutions in performing the processes related to management of inter-organizational trust. In Section 6.6.2 we present and analyze the processes that were performed by the VBEs with support of services provided by TrustMan system. The average percentage of reduction on the amount of the resources consumed and the time spent for the tested processes is shown in Figure 7.2. The quantitative analysis related to empirical validation of our developed results is presented in Section 6.6.2.

As shown in Figure 7.1 and Figure 7.2 and also on the basis of the analysis presented in Section 6.6.2, we can conclude that both the conceptual results and the software prototypical result produced by this research are validated, very well accepted and directly applicable to the industrial VBE networks. Furthermore, based on these positive empirical evaluation results we can also conclude that VBE's requirements related to management of inter-organizational trust as stated in Section 1.4 are properly addressed by this thesis.

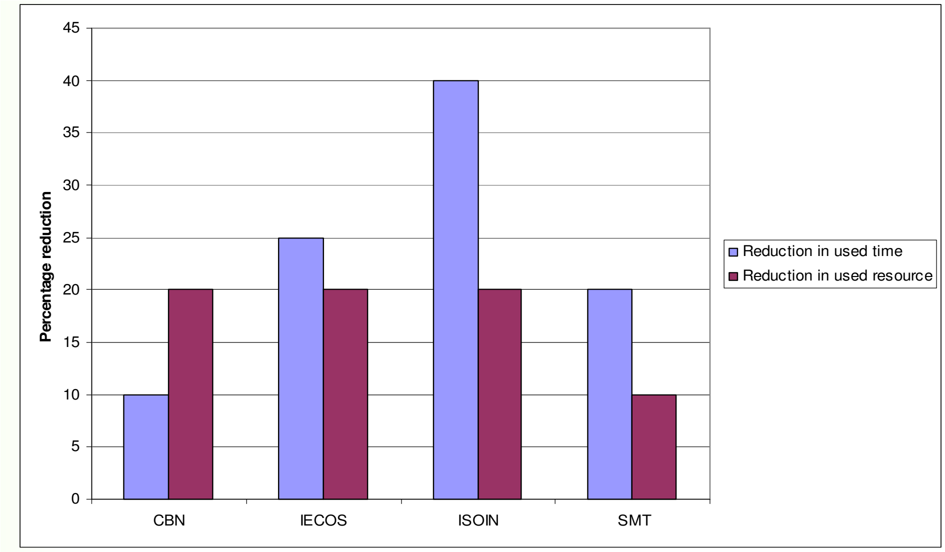


Figure 7.2: Quantitative evaluation of developed results by VBE networks

This figure shows the results of evaluation of the TrustMan system applying quantitative indicators. The detailed analysis is presented in Section 6.6.2.

7.3.4 Self validation – With standard indicators and against other systems

In this thesis, to evaluate the quality and the level of innovation of the proposed conceptual and prototypical solutions we have applied a set of indicators inspired by *ISO 9126 quality factors of software*. For each of the six categories presented in Figure 7.3 a number of more specific indicators are defined. With these indicators we have validated the TrustMan against five other related trust management systems as mentioned below.

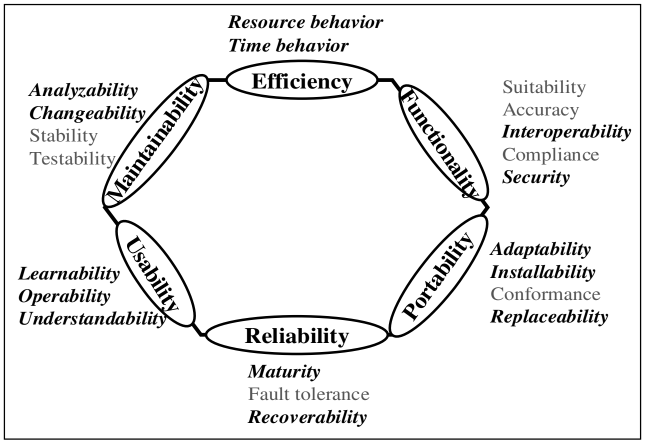


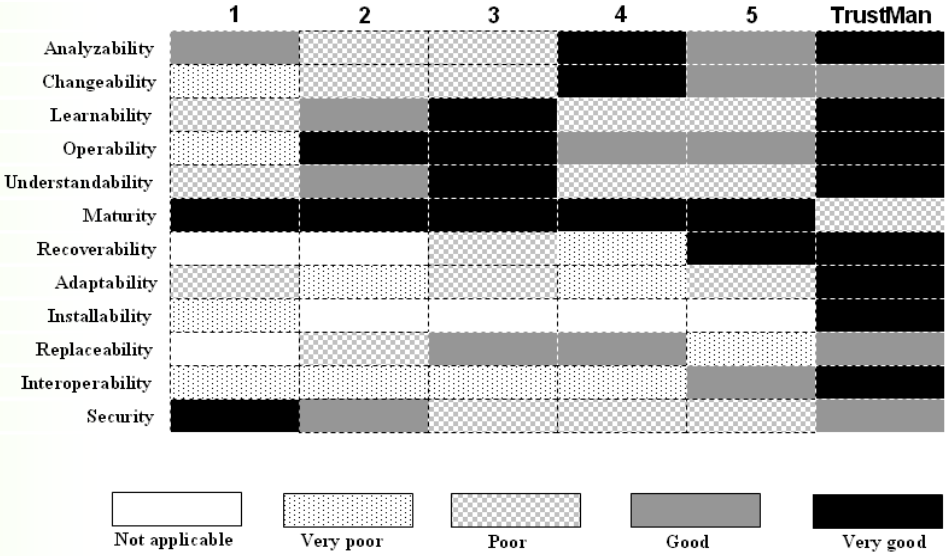
Figure 7.3: Evaluation indicators inspired by ISO 9126 quality factor of software products

This figure shows the standard indicators for evaluating software as inspired by ISO 9126. The bold indicators were applied for evaluating the TrustMan system.

Indicators shown in Figure 7.3 with italic and bold font type are selected by us as most applicable for our validation purpose applied for evaluating the TrustMan system against the following five related systems which are further described in Annex B:

1. *DRACO (COMARCH, Poland):* This is a commercial system supporting the evaluation of trust level of organizations that aim at forming a collaborative consortium. The assessment of trust level of the potential partners is based on the security level of systems owned by trustee organizations which will be applied to facilitate the collaboration.
2. *okCupid (www.okcupid.com):* This is a freeware online system supporting the analysis of trust of individuals for the purpose of creating an online community. The analysis of trust is based on comparisons of individuals' profiles against the profile of the owner of the community.
3. *Trusted Advisors Associates (http://trustedadvisor.com/):* This is a freeware online system supporting individual self assessment of trustworthiness by answering a set of questions.
4. *Trust assessment wheel (http://www.darden.virginia.edu/faculty/james.htm):* This is an online research prototype system supporting analysis of trust among students for the purpose of co-working in group work. It is based on a set of guidance and criteria organized in wheel.
5. *Truster (http://www.truster.org/):* This is a freeware online system, based on online unique identifications (such as email addresses) supporting the analysis of trust of individuals on the basis of their performance data from different online sites.

The detailed definitions of applied indicators, as shown in Figure 7.3 and Figure 7.4, are provided in Annex B.



	1	2	3	4	5	TrustMan
Analyzability	▓	▒	▒	■	▓	■
Changeability	░	▒	▒	■	▓	▓
Learnability	▒	▓	■	▒	▒	■
Operability	░	■	■	▓	▓	■
Understandability	▒	▓	■	▒	▒	■
Maturity	■	■	■	■	■	▒
Recoverability	□	□	▒	░	■	■
Adaptability	▒	░	▒	░	▒	■
Installability	░	□	□	□	□	■
Replaceability	□	▒	▓	▓	░	▓
Interoperability	░	░	░	░	▓	■
Security	■	▓	▒	▒	▒	▓

□ Not applicable ░ Very poor ▒ Poor ▓ Good ■ Very good

Figure 7.4: Evaluation of TrustMan system with scientific indicators

This figure shows the evaluation results for the TrustMan system with standard indicators and against other systems as further addressed in Annex B.

Figure 7.4 shows a summary of evaluation results of TrustMan system with the above mentioned scientific indicators and against the five mentioned systems each shown by their specific number above. We have one by one tested the features of these five systems in comparisons with the TrustMan system. As shown in Figure 7.4, although this is a self-test, our results show that on most tested features the TrustMan system score better than other related systems for the applied validation indicators. The interpretation and comparison of some example rows of Figure 7.4 is presented in Annex B.

7.3.5 Peer reviewed validation – Within scientific community

To validate our research findings within the scientific community we have focused on achieving as many high quality publications as possible, addressing different subjects related to management of inter-organizational trust in VBEs. The Table 1.2 shown in Section 1.7 presents the three fundamental subjects (SB1, SB2 and SB3) related to inter-organizational trust, as classified in this thesis and summarized in Figure 1.3, namely:

SB1: *Requirement analysis and specification of the management of inter-organizational trust*
SB2: *Modeling and designing mechanisms for assessing level of trust in organizations*
SB3: *Developing a system supporting the management of trust between organizations*

Achievements of this research in relation to these three subjects can be illustrated through the acceptance of our results within the scientific community, considering the number of publications appeared in high quality channels, including: *journal articles, book chapters, and peer reviewed international conference proceedings*. Figure 7.5 represents the current status of publications that have contributed to this thesis in relation to each off these three subjects. A complete set of the author's publications is presented in Annex A.

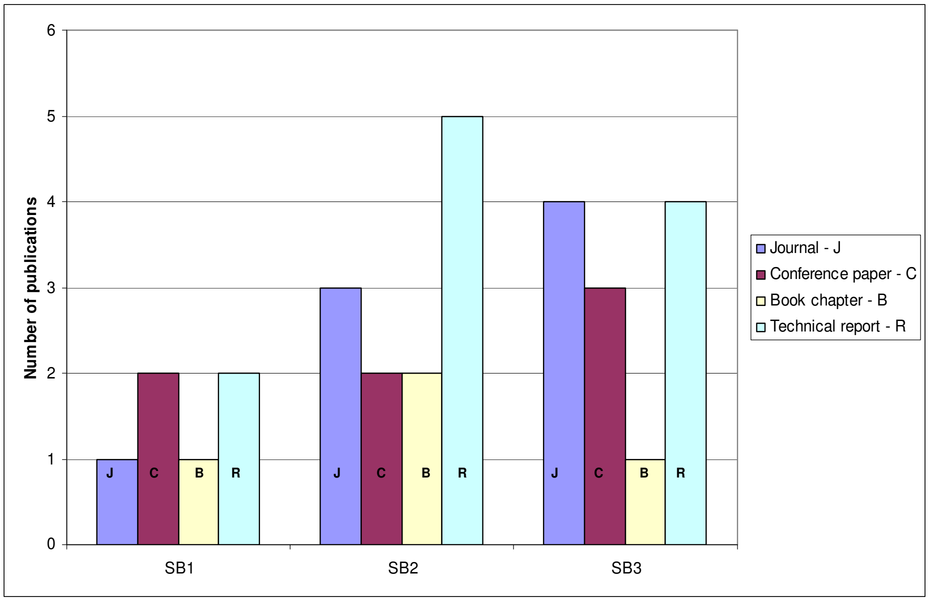


Figure 7.5: Status of publications achieved by the author related to this thesis per subject
See the complete list of publication achieved by the authors in Annex A.

7.4 Lessons learned and future work

Performing research goes hand-in-hand with gaining new insight into the addressed subject. However, while increasing the insight into the subject there are always discovery of some new challenges that may go beyond the conditions set for research, such as the time, resources, availability of data and knowledge, etc. Such challenges, which therefore, cannot be addressed by the research, form the foundation or basis for future work. A few crucial lessons that we have learned during this research are addressed in this section as suggestions for future work in the area of management of inter-organizational trust.

7.4.1 Inter-organizational trust: lessons learned

The fundamental lessons we have learned during this research can be classified into five categories, namely related to: (a) Emerging definition of inter-organizational trust in VBEs, (b) Identification and characterization of fact-based trust elements for organizations participating in VBEs, (c) Measurement of the level of trust in organizations in VBEs, (d) Management of inter-organizational trust in VBEs, and (e) Establishment of inter-organizational trust relationships in VBEs. These lessons that we have learned in relation to each of the above five categories are described below.

a) Related to emerging definition of inter-organizational trust in VBEs

We have learned that there is no consensus yet on the definition of trust both in the research community and in business practice. This means that it is hard to find common understanding among people or organizations about what trust means across different disciplines of research and practice. By means of requirement analysis, literature study, expert consultations, and empirical study of VBE networks, we have realized that it is challenging to formulate a concrete definition for organizational trust that can address its measurement criteria and cover its fundamental aspects while being applicable to all domains of the VBE networks.

We have ascertained that the level of trust in organizations needs to be measured rationally. Thus the definition of trust must also address some fundamental rational concepts that can support reasoning about its measurements. We have provided a definition of inter-organizational trust as presented in Chapter 1 that incorporates fundamental rational aspects of trust in VBEs. The main challenge related to establishing the definition of rational trust is to convince different stakeholders to alter their current definition of this concept, which typically – within their traditional practice and especially among individuals – is considered to be a very subjective aspect. Therefore, it is challenging to convince trust actors to accept the current emerging definition of trust, considering its rational aspects as well as the formal mechanisms for analyzing trust in organizations.

b) Related to identification of fact-based trust elements for organizations participating in VBEs

We have learned that the identification of fact-based trust elements for organizations cannot be efficiently achieved in an ad hoc manner. For trust related studies, the trust elements for organizations in VBEs must be first systematically identified and characterized to ensure that a comprehensive set is achieved that can be then customized and applied to different VBEs. In Chapter 3, we have presented the HICI approach, which provides systematic stages that can be followed to identify, characterize and analyze trust criteria related to organizational performance data. We have also learned that the identified trust criteria might need to be tuned over a certain period of time, depending on some changes in the VBEs' requirements that are related to the management of inter-organizational trust.

c) Related to the measurement of level of trust in organizations in VBEs

We have learned that the level of trust in an organization can neither be measured with a single parameter, such as a trust criterion, nor interpreted with a single metric. As characterized in our research, the level of trust in organizations is measured in terms of a set of trust criteria selected by a trustor organization, depending on that organization's preferences and perception of trust. In order to facilitate the multi-criteria measurement of the level of trust in organizations, certain key aspects need to be addressed, including: the identification of relevant trust elements for organizations, the modeling of trust relationships between organizations, and the formulation of mechanisms for assessing the level of trust in organizations, as addressed in Chapters 3 and 5 of the thesis.

d) Related to the management of inter-organizational trust in VBEs

We have learned that the tasks related to the management of trust between organizations in VBEs need to be developed as a subsystem of the VBE management system. This is due to the fact that the current manual processes for trust assessment practiced in industry are becoming increasingly inefficient, mostly subjective and require analysis of large amount of complex data to accomplish them. In dynamic markets these processes must be performed quickly and thus need to benefit from the support of advanced ICT systems.

We have addressed the design and development of tasks related to the management of inter-organizational trust by proposing the TrustMan system. Among other functionality, the TrustMan system shall support the assessment of the level of trust in organizations. However, the final decision regarding trusting other organizations is always made by the trustor organizations. The TrustMan system also supports handling tasks related to managing inter-organizational trust in VBEs. It shall provide trustor organizations, such as the VBE administrator, with properly analyzed and compiled information related to the trust history of VBE member organizations in order to support the trustor in making informed decision.

e) Related to the need for systematic steps for Establishing Trust Relationships among organizations in VBEs

We have learned that the establishment of trust relationships between organizations must be systematic and well organized, and thus detailing every aspect, including the preceding and proceeding steps. We have learned that there is a need for a framework to guide the establishment of trust relationships between organizations. For this purpose, in Section 2.5 we proposed a set of ordered steps needed to guide the establishment of inter-organizational trust relationships. For each proposed step a supporting service is developed in the TrustMan system as addressed in Chapter 6.

7.4.2 Inter-organizational trust: future work

Sufficient research has supported the current achieved conclusions, but it will never be enough to address future conclusions. Such future conclusions require further research in the future. Nevertheless, same future research topics can be defined in the conclusions of the current work. Despite the extensive findings presented in this thesis, the subject of management of inter-organizational trust still has many open challenges that need to be addressed. We can suggest the following four topics for future work in this area.

a) Analyzing statistical correlation for the use of trust criteria in VBEs

Certain characteristics of the society and market might influence trustor organizations on their selection of trust criteria that are used to assess the level of trust in trustee organizations. For example, if an organization is doing business in a very socially-oriented community then adhering to social values of that society may seem more important than achieving healthy profits. However, in such a community there is an obvious risk of economic failure, such as failing to achieve the needed economic profit to survive. Thus, the trustor may need help to properly identify the needed criteria for trusting others. It is very difficult in general to predict or even analyze which trust criteria to use at the VBE for each trust objective.

Nevertheless, when some trust criteria have been in use in the VBE, in relation to certain objectives, for a relatively long period, this data can be recorded in the VBE. Furthermore, collected empirical data related to trustee’s performance at the VBE and/or VOs can indicate if choosing certain trust criteria by the trustor instead of certain other trust criteria proves to be a good indicator of organizations’ trustworthiness.

Furthermore, certain trust criteria may not often be selected by trustor organizations. If this trend arises, it will discourage trustee organizations to pay attention to those less frequently selected trust criteria and thus they will not enhance their performance related to those trust criteria. However, this does not mean that those trust criteria may never be selected in the future. That means if they are selected, they might lower the trustworthiness of certain organizations, and may thus present an unexpected or uncommon organization’s trust picture. It is in general unclear when and how these patterns relating to the selection of trust criteria by trustors will occur.

Predictive studies or analysis of statistical correlations based on empirical data can support defining some indicators for the above example cases. Further research needs to be carried out addressing the above two aspects.

b) Complementing fact-based trust analysis with opinion-based trust analysis

In Section 2.3.4 we discussed and distinguished the concepts of rational trust and subjective trust. This thesis addresses the research on rational trust for supporting the realization of trust between organizations on the basis of their fact-based data. There are however, a number of key practical challenges related to the application of rational trust analysis approaches in business. The following challenge has been identified to need further research:

Acquiring trust related-data on time: In our approach, the level of trust in an organization is rationally measured on the basis of a set of trust criteria. This means that updated trust related data for all preferred trust criteria must be available in order for the trust level of an organization to be computed. In practice, however, when the amount of required trust related data increases, it may be hard to collect this data from organizations in time. Therefore, other complementary approaches, such as a subjective trust assessment approach can be considered in the event that trust-related data are missing for application of our rational approach.

Opinion-based approaches apply subjective data, such as reputation, to assess the trustworthiness of organizations. Although the base concepts of the two approaches, one rational and one opinion-based for analyzing trust differ the opinion-based approach may complement the rational-based approach when fact–based data are missing. In future research, when a new approach is introduced on how the results from rational trust analysis can be complemented with the results from subjective trust analysis, then the assessment results of the TrustMan system can be augmented with the results from other subjective systems.

Furthermore, in future, other systems may be developed supporting rational analysis of inter-organizational trust that may be used by some VBE organizations. For example, if some trust data of an organization related to one trust perspective of the TrustMan system is missing while another trust assessment system can compute the related scores for that trust perspective, then it may be possible to integrate those scores within the TrustMan system in order to provide a complete assessment of the trust level of the organization. In other cases, both TrustMan system and another trust assessment system might for example both generate some scores for certain trust perspectives, which may be also considered by TrustMan system. In either case, first the scores from another system shall be normalized according to the boundaries of scores generated by the TrustMan system, and second, the trustor organization shall set the weights for how it values the scores from each system.

c) Exploiting VBE-related trust concepts in PVC environments

PVCs (Professional Virtual Communities) are analogous environments to the VBEs, as they both have many similarities being long-term strategic alliances that focus on preparing their members for future involvement in potential short-term collaboration. A fundamental difference between VBE and PVC however is their members; while VBEs comprise of organizations, PVCs consist of individuals.

This thesis addresses inter-organizational trust to support cooperation in VBEs and collaboration in VOs that are configured within VBEs. Although inter-organizational trust and inter-personal trust have been clearly shown to differ, as addressed in Section 2.2.1, the base approach introduced for inter-organizational rational trust establishment as applied in VBEs have the potential to be also applied for PVCs, which opens up a new challenge in need for further research.

To conclude, in this work we have shown that trust is a fundamental aspect in facilitating and smoothing goal-specific collaboration among organizations. As such, trust among organizations needs to be properly created applying rationally assessed trustworthiness. A number of challenges, as addressed in this thesis, need to be properly addressed to support the rational assessment of trust level of organizations, for which this thesis has contributed to solve.

Annex A

List of author’s publications

The following is the list of publications achieved by the author of this book which provided relevant contribution to the content of this dissertation. The publications are classified into three groups SB1, SB2 and SB3 on the basis of the three main subjects addressed in this thesis as presented in Section 7.3.5.

No	Description	Subject
Journal articles		
1.	***S.S. Msanjila,*** & H. Afsarmanesh. On development of TrustMan system assisting configuration of temporary consortiums. *In the International Journal of Production Research; Special issue: Virtual Enterprises – Methods and Approaches for Coalition Formation.* Taylor & Francis, Volume 47, issue 17, pg. 4757-4790 (Online January 2009) September 2009. (2009)	SB3
2.	***Msanjila, S.S.,*** & Afsarmanesh, H. FETR: A Framework to Establish Trust Relationships Among Organizations in VBEs. *In the International Journal of Intelligent Manufacturing; Special issue: Trust, Value Systems and Governance in Collaborative Networks.* 0956-5515 (Print) 1572-8145 (Online), Springer, (November, 2008).	SB3
3.	***Msanjila, S.S***. & Afsarmanesh, H. Trust Analysis and Assessment in Virtual Organizations Breeding Environments. *In the International Journal of Production Research; Special issue: Enhancing performance in collaborative networked industries*. ISSN (Print): 0020-7543, Taylor & Francis. Pg. 1253-1295 (April 2007 – online, March 2008 – printed).	SB2
4.	***Msanjila, S.S***. & Afsarmanesh, H. Modeling Trust Relationships in Collaborative Networked Organizations. *In the International Journal of Technology Transfer and Commercialisation; Special issue: Data protection, Trust and Technology*; Inderscience. ISSN (Print): 1470-6075. Vol. 6, issue 1. pg. 40-55. (July, 2007).	SB2
5.	***Msanjila, S.S***. & Afsarmanesh, H. On Architectural Design of TrustMan System Applying HICI Analysis Results. The case of technological perspective in VBEs. *In the International Journal of Software*. Academy Publisher, ISSN 1796-217X. pg. 17-30 (April 2008).	SB1 SB3
6.	***Msanjila, S.S.*** & Afsarmanesh, H. Specification of the TrustMan System for Assisting Management of VBEs. *In Lecture Notes in Computer Science*	SB3

No	Description	Subject
	[LNCS: 4657], Springer. Pg. 34-43. (September 2007).	
7.	H. Afsarmanesh, L.M. Camarinha-Matos, & ***S.S. Msanjila.*** On Management of 2nd Generation Virtual Organizations Breeding Environments. *In the Journal of Annual Reviews in Control.* Elsevier. (2009).	SB2
Book chapters		
1.	***S.S. Msanjila***, & H. Afsarmanesh, Inter-organizational trust in VBEs. *In Methods and Tools for collaborative networked organizations.* ISBN: 978-0-387-79423-5, Springer, New York, 2008. Pg: 91-118.	SB1 SB2
2.	***S.S. Msanjila,*** & H. Afsarmanesh, A Multi-Model Approach to Analyze Inter-organizational Trust. *In Collaborative Networks reference modeling.* ISBN: 978-0-387-79425-9, Springer, New York, 2008. Pg: 195-216.	SB2
3.	H. Afsarmanesh, ***S.S. Msanjila***, E. Ermilova, S. Wiesner, W. Woelfel, & M. Seifert. VBE management system. *In Methods and Tools for collaborative networked organizations*. ISBN: 978-0-387-79423-5, Springer, New York, 2008. Pg: 119-154	SB3
Peer reviewed international conference papers		
1.	***S.S. Msanjila***, & H. Afsarmanesh. Automating trust assessment for configuration of temporary partnerships. I*n the proceeding of international conference on information technology for balanced automation system (BASYS).* ISBN: 978-0-387-09491-5, Springer, Porto, Portugal. Pg. 95-105, June 2008.	SB3
2.	***Msanjila, S.S.*** & Afsarmanesh, H. Establishing Trust Relationships among Organizations in VBEs. *In Establishing the foundation of collaborative networks. Proceedings of 8th PRO-VE 2007*, Springer, pp. 3-14. Guimarães, Portugal. September 2007.	SB3
3.	***Msanjila, S.S.*** & Afsarmanesh, H. Specification of the TrustMan System for Assisting Management of VBEs. *In the proceedings of 4th International conference on Trust, Privacy and Security in Digital Business (TrustBus'07),* Springer, pp. 34-43. Regensburg, Germany. September 2007.	SB3
4.	***Msanjila, S.S.*** & Afsarmanesh, H. HICI: An approach for identifying trust elements – The case of technological perspective in VBEs. *In proceedings of International conference on availability, reliability and security (ARES-2007),* pp. 757-764, IEEE computer society press. Vienna. April 2007.	SB1
5.	***Msanjila, S.S.*** & Afsarmanesh, H. Assessment and creation of trust in VBEs. In *Network-centric collaboration and Supporting Frameworks. Proceedings of 7th PRO-VE'06, Springer, pp 161-172,* Helsinki, Finland, September 2006.	SB2
6.	***Msanjila, S.S.*** & Afsarmanesh, H. Understanding and Modeling Trust Relationships in Collaborative Networked Organizations. *In Proceedings of international conference on Business, Law & Technology present and Emerging Trends, Volume 2,* International association of IT lawyers (*IAITL), pp 402-416,* Copenhagen, Denmark , December 2006.	SB1 SB2
7.	Afsarmanesh, H. Camarinha-Matos, L. M. & ***Msanjila, S.S***. Virtual Organizations Breeding Environment: Key Results from ECOLEAD. *In the proceedings of International conference on Cost Effective Automation in Networked Product Development and Manufacturing – CEA'2007, pp. 2(1-8).* Monterey, Mexico. October 2007.	SB3
8.	***Msanjila, S.S.,*** Tewoldeberhan, T., Bockstael-Blok, W., Janssen, M., &	SB2

No	Description	Subject
	Verbraeck, A. E-Supply Chain Orchestration Using Web Service Technologies. A case using BPEL4WS. *In proceedings of International Conference on Information and Resources Management Association (IRMA),* San Diego California, May 2005.	SB3
9.	Tewoldeberhan, T.W., Verbraeck, A., & ***Msanjila, S. S***. Simulating Process Orchestrations in Business Networks: A case using BPEL4WS. *In proceedings of 7th International Conference on Electronic Commerce*, ACM publisher, pp. 471-477, China, September, 2005.	SB2 SB3
Technical reports (fundamental for this thesis)		
1.	***Msanjila, S.S.***, Ermilova, E., Afsarmanesh, H. & Bakker, E. Prototype of the advanced support tools, methods and services for VMS: PCMS, ODMS, and TrustMan system. Technical report, ECOLEAD project, 2007.	SB3
2.	Graser, F. ***Msanjila, S.S.***, Ermilova, E., Afsarmanesh, H., Wölfel, W., & Mores, S. Specification and Prioritization of VBE Management Functionality. Technical report, ECOLEAD project, 2006.	SB2
3.	Graser, F., ***Msanjila, S.S.***, Dikici, C., Ermilova, E., Afsarmanesh, H, Woelfel, W., Hassan, A.I. & Decker, P. Prototype of the core functionalities / tools for VMS. Technical report, ECOLEAD project, 2007.	SB3
4.	Camarinha-Matos, L.M., Afsarmanesh, H, ***Msanjila, S.S.,*** Macedo, P., Rosas, J., Abreu, A., Jarimo, T., Graser, F., & Klen, A. Basis for interoperability among models. Technical report, ECOLEAD project, 2007.	SB2
5.	***Msanjila S.S.,*** Afsarmanesh, H, Hodik J., Rehak, M., & Camarinha-Matos L. Creating and supporting trust culture in VBEs. Technical report, ECOLEAD project, 2006.	SB1
6.	***Msanjila, S.S.***, Afsarmanesh, H., Wölfel, W., Mores, S., Dikic, C., & Graser, F. VBE Management System (VMS) Requirements and Architecture Design. Technical report, ECOLEAD project, 2006.	SB3
7.	Romero, D., Galeano, N., Giraldo, J., Molina, A., ***Msanjila, S. S.,*** Afsarmanesh, H., Bollhalter, S., & Oswald, M. Characterization of VBE Value Systems and Metrics. Technical report, ECOLEAD project, 2006.	SB2
8.	Camarinha-Matos, L.M., Pereira Klen, A.P., Ferrada, F., Afsarmanesh, H, Jarimo, T., ***Msanjila, S.S.,*** & Graser, F. Principles for a reference model for Collaborative Networks. Technical report, ECOLEAD project, 2006.	SB2
9.	Eschenbaecher, J., Jansson, K., Karvonen, I., Ollus, M., Mulder, W., Klen, A.P., Riikonen, H., ***Msanjila, S.S.***, Salkari, I., Paganelli, P., Klen, E.R. Loss, L., & Negretto, U. Challenges in Virtual Organisations Management: Report on methods for distributed business process management. Technical report, ECOLEAD project, 2005.	SB1
10.	Grzegorz, S., Tomasz, S., Mulder, W., Wangham, M., Fraga, J., Rodrigo, M., & ***Msanjila, S.S.*** Configurable multi-level security architecture for CNOs. Technical report, ECOLEAD project, 2005.	SB2 SB3

Other publications

Master of Science thesis

Msanjila, S.S. Modeling and simulation of web service based business processes. BPEL based business process specification. *A thesis for fulfillment of masters of Science degree in Systems engineering, policy analysis and management, specializing in Systems engineering.* Section of systems engineering, Delft University of Technology (TUDelft), July 2004.

Bachelor of Science thesis

Msanjila, S.S. Towards developing Swahili Linux operating system. A feasibility study and requirement specification. *A thesis for fulfillment of Bachelor of Science degree with Computer Science.* Department of Computer Science, University of Dar es Salaam (UDSM), June 2001.

Annex B

TrustMan validation with standard indicators and against related systems

A key aspect for the research is related to evaluating the quality and the innovation of the achieved results. This annex provides the descriptions of standard indicators applied to the evaluation of the TrustMan system.

B.1 Applied standard indicators

Although indicators (measurable attributes) frequently used in the field of computer science, it is still possible to systematically evaluate the level of quality and innovation of developed models and systems [Pressman, 2005]. The evaluation is based on a set of clearly defined rules, which characterize the possible qualitative indicators. In this thesis to evaluate the quality and innovation of the TrustMan system we apply standard indicators inspired by the ISO 9126 quality factors of software [Pfleeger, 2001] as addressed below.

1. Functionality

Functionality refers to the state of being functional and especially focusing on a particular set of functions or capabilities associated with computer software, computer hardware or an electronic device. The key aspects related to functionality that are considered for the evaluation of the TrustMan system are ***interoperability and security***.

1.1 **Interoperability:** With respect to software, the term interoperability is used to describe the capability of different programs to exchange data via a common set of exchange formats, to read and write the same file formats, and to use the same protocols. Interoperability is the ability of a provider system to work with recipient systems without special effort on the part of the client system. To realize interoperability among systems a set of standards must be defined and followed during the development of those systems.

Interoperability of the TrustMan system: *The TrustMan system is developed using the java programming language. It provides services that can be accessed through a web interface by human users and through invocation by system users. Web service technology standards are applied to the development of TrustMan system. Thus as described in Section 6.5.2, the remote invocation of services provided by the TrustMan system applies the SOAP protocol. This support the interoperability of the TrustMan system with other systems developed applying these standards.*

1.2 Security*:* Security of a system refers to protecting the information managed by that system and the system itself from unauthorized access, use, disclosure, disruption, modification, or destruction. It is also concerned with the confidentiality, integrity and availability of data stored and managed by the system.

Security of the TrustMan system**:** *The TrustMan system manipulates performance data of organizations, expressed in terms of their trust criteria, to assess their trust level. The performance data can be too strategic for the owner organization to disclose to other organizations. To enhance the security of the trust related data stored in the TrustMan system, we have classified the access to the system depending on roles of users. This security aspect is further addressed in Section 6.4.2.*

2. Efficiency

Efficiency refers to a system's ability to perform (support performing) a process with optimal use of time and resources. As such, it refers to increasing productivity of a system while minimizing the amount of consumed resources and time taken to meet a set of requirements for the output, such as the quality. We address the efficiency of the TrustMan system by considering two quantitative indicators, namely, ***resources and time*** as addressed in detail in Section 6.6.2 and Chapter 7.

3. Maintainability

Maintainability refers to the ease with which a software system or a component of a system can be modified to correct faults. It also refers to the possibility to improve performance or other attributes of the system and to adapt the system to a changed environment. In other words, maintainability measures the ease and speed with which a system can be restored to an operational status after a failure had occurred. We have evaluated the maintainability of the TrustMan system with two indicators, namely: ***analyzability and changeability***.

3.1 Analyzability: Refers to the ease/possibility to in detail examine a system in order to identify causes of problems/faults that are experienced in operations of the system.

Analyzability of the TrustMan system: *As stated earlier, the TrustMan system is developed using the java programming language. Modules developed to support the operations of the TrustMan system are grouped into sets of integrated services. Each module is developed to provide one complete service such as computing a score for a single trust perspective. These modules operate independent of each other while executed to provide the required services. Thus each module can be analyzed and modified independent of others.*

3.2 Changeability: Refers to the quality of a system to allow replacement of some of its modules without major modification of others modules. This quality is related to the independent nature of modules in the system.

Changeability of the TrustMan system: *As explained earlier, the modules of the TrustMan system operate independent of each other. Thus they can be replaced with new modules which meet the format and type of input and out data.*

4. Usability

Usability is a qualitative attribute of a system that assesses how easy user interfaces are to use. It includes aspects such as: (1) Who are the users, what do they know, and what can they learn? (2) What do users want or need to do? (3) What is the general background of the users? (4) What is the context in which users are working? (5) How much training do users need? (6) What documentation or other supporting materials are available to help the users and can those users find the solutions they seek in those materials?

Usability can be indicated by the quality of the system related to ***learnability, operability, and understandability***.

4.1 Learnability: Refers to the easy for which users can accomplish basic tasks the first time they encounter the system. According to ISO 9126, in software testing the learnability of the system is defined as the capability of a software product to enable the user to easily learn how to use it.

Learnability of the TrustMan system: *Human interfaces designed to support each group of users to access the TrustMan system are developed as web based interfaces. The interface is designed to support a particular user to access only specific functionalities which makes it possible to develop simple but efficient interfaces that facilitate users with basic knowledge of accessing website to easily use the TrustMan system.*

4.2 Operability: Operability refers to the ability of a system to let users access its functionality without an appeal of high level of technical knowledge.

Operability of the TrustMan system: *Mechanisms developed to support the computation of the trust level of an organization are based on a set of mathematical equations. Understanding such equations is quite difficult for users who have little knowledge of both mathematics and computer science. As implemented in the TrustMan system, these equations are hidden and their related services are developed to the level at which they can be easily executed by users through the web interface.*

4.3 Understandability: Refers to the degree to which the purpose of the system is clear to evaluators or users. To achieve understandability the system should be comprehensible for users and not only for developers. There are many aspects addressing the understandability of a system including: application structure, navigation, procedures, terminology, etc. Understandability may also be achieved when users are supported to know the state of their task, what to do next, how the application reacts to certain inputs, and so on.

Understandability of the TrustMan system: *As described in Section 6.4.2, user interfaces of the TrustMan system are classified per user category. Furthermore, user interfaces for each user category are classified per main functionality (integrated service). Example interfaces are those supporting the access of functionalities for: managing trust related data, assessing and viewing trust level, tuning and for viewing trust criteria, etc. The classification of interfaces per user group enhances the understandability of the TrustMan system.*

5. Reliability

Reliability refers to the ability of a system or its components to perform the required functions without a failure under stated conditions for a specified period of time. Reliability can be indicated by ***maturity and recoverability*** of the system.

5.1 Maturity: In engineering discipline the maturity of a product is measured in terms of the time which has elapsed since the product was introduced in the market. Considering the fast evolution of software, the time elapsed is not sufficient indicator to measure maturity of software. One methodology applied to analyze the maturity of software is examining aspects related to the development approach, programming language, applied standards, etc.

Maturity of the TrustMan system: *As stated earlier, the TrustMan system is developed using the java programming language. Java is a proven programming language which implies a system developed in java shall have a high reliability in relation to maturity indicator. However, the TrustMan system itself is not mature since it is still new to the market.*

5.2 Recoverability: Refers to the ability to restore a system deployment from a point at which a failure has occurred to a normal operation state without any loss of data. The ability to recover quickly from a system failure or disaster depends not only on having current backups of data, but also on having a predefined plan for recovering that data on new hardware. Recoverability is enhanced when software is developed on the basis of a well defined set of standards and the reconfiguration is well thought during the development stage.

TrustMan system: *TrustMan system is developed on the basis of well established standards as inspired by web service technology. These standards enforce that the components of the system must be developed as simple and independent to each other as possible. Thus the components can be recovered and even replaced without affecting the operability of other components. Furthermore, the developed components of the TrustMan system are logically separated with the storage and management of trust related data. Thus failure of the system can hardly have any effect on the stored data and therefore, its backup can be made independent of the state of the system, such as using the functionalities provided by the database management system.*

6. Portability

Portability refers to the ease with which the software can be transposed from one environment to another, such as from one (e.g. operating system) to another platform. The pre-requirement for portability is the generalized abstraction between the application logic and system interfaces. When developers are targeting several platforms with the same application, portability is the key issue for achieving cost reduction. Among others portability of a system can be evaluated in relation to ***adaptability, installability and replaceability.***

6.1 Adaptability: The construction of software in modern computing contexts is increasingly concerned with volatile and unpredictable nature of both user requirements and business environments. A number of research fields have thus emerged, which seek to increase the adaptability of systems, both before, but even after software has been built and deployed. One key aspect of adaptability is that the software should be capable of running on any platform.

Adaptability of the TrustMan system: *TrustMan system is developed using the java programming language. Java is a platform independent programming language and thus the developed systems can run on any platform. Therefore, the TrustMan system can be stated as an adaptable system. Furthermore, the perceptions of trust differ among users of the TrustMan system. To enhance adaptability of the TrustMan system to different VBE environments, we have developed a supporting module based on logical operations. The logical operations support users to enable or disable some trust criteria to meet their preferences and perceptions on trust. The TrustMan system was successfully tested by different VBE networks as described in Section 6.6.2 which indicate its adaptability.*

6.2 Installability: The installability is a characteristic which allows easy configuration of a system at a designated environment. It correlates with metrics which measure the effort and time needed to install the software in a specified environment.

Installability of the TrustMan system: *Installing the TrustMan system can be done by simply copying the class files into the publishing directory of the web server. Thus the installation does not need any special technical knowledge and therefore, the installability of TrustMan system can be stated as easy.*

6.3 Replaceability: Refers to the characteristics that relate to the ease with which a system can be replaced with another system without using much technical knowledge, resources or time.

Replaceability of the TrustMan system: *The replacement of TrustMan system can be done either for the entire system or some specific modules. If it is needed to replace the entire TrustMan system then the new system must match the schema of the database which is designed to manage the trust related data. If it is needed to replace some modules of the*

TrustMan system then the new modules must at least match the input and output data. There will be no need to reconfigure classes in other modules of the system.

B.2 Related trust management systems

A number of systems supporting some tasks related to the management of trust among actors were analyzed and their functionalities compared to those provided by the TrustMan system. Below we provide a brief description of five example trust management systems.

1. Dynamic Responsibility Authorization for Collaborative Organizations – DRACO *(COMARCH, Poland)*

This is a commercial system developed by COMARCH Company, first as a prototype during the ECOLEAD project period, and then later enhanced for business purposes. The system is applied to analyze trust among collaborating partners based on security of the collaboration infrastructure. The main assumption is that security and trust are fundamentally related. Without properly defining these concepts, the configured collaborations will hardly show their full potential. When the number of participants (members) in a VBE is large, the organizations involved may have no initial trust relationship on forehand. The security of the infrastructure plays an important role in supporting the establishment of trust between participants by dynamically facilitating authorization, sharing, exchanging and assigning roles among partners while working together to achieve a joint goal. To achieve this facilitation, all applied local systems must be configurable to meet the security indicators as defined in the DRACO system, such as reliability, availability, access control, identifications, etc.

2. okCupid.com (www.okcupid.com)

This is a freeware system accessed online and is developed to support individuals to create their communities of friends. Trust among partners in these communities is assessed based on matching profiles of membership applicants to the profiles of the owner of the online community. Profiles are characterized with a number of common elements. Each element is assigned with some optional values that a user can select while creating his/her profile. If a specific user wants to join a certain community then his/her profile is matched with the profile of the owner and the result is provided in terms of percentage. If the matching percentage is equal or greater than the threshold set by the owner of the community then the owner is notified about the potential new member in order to make a decision.

3. Trusted Advisor Associates (http://trustedadvisor.com/)

This is a freeware system accessed online that supports individuals to assess their own trust level by answering dynamic questionnaires. Based on the answer that the actor provides in response to the current question, the system dynamically decides about the next question selecting it from the large pool of questions. Once all required questions are answered the system computes the trust level based on a pre-defined formula. Each answered question is related to one of four trust criteria applied in this system, namely: Credibility I, Reliability I, Intimacy (I) and Self-orientation (S). The trustworthiness (trust quotient TQ) of an actor is calculated using the following equation:

$$TQ = \frac{C + R + I}{S}$$

4. Trust assessment wheel (http://www.darden.virginia.edu/faculty/james.htm)

This is an interactive guidance supporting students to analyze the trust of others for potential collaboration at school. It is designed to support students to trust each other and facilitate co-working in a group work. The guidance provides a number of trust criteria organized in a wheel. Based on the answers that a student provides on some specific questions the guidance suggests some possible trust criteria. The student will then decide about the final preferred set of trust criteria to apply in assessing trustworthiness of others.

5. Truster (http://www.truster.org/)

Truster.org is a free central online reputation system. It utilizes the latest OpenID identification technology (such as yahoo ID, Microsoft messenger ID, etc.) to uniquely identify an online user and allows all users of the system to see his rating and feedbacks. Each user has his/her own-personal profile page. Users can then inform the Truster about what forums and sites they are members in (example: ebay, forums, blogs and so on) and customize their profiles (picture, emails etc). When an online transaction is made, the user authorizes the other site to submit their feedback to Truster.org. Feedback will include the deal URL, overall experience with the person and other trust related information. Finally, the user will get a Truser.org trustworthiness rating (ranging between 0-5) and rating symbol (thumbs up is the best and thumbs down the worse and other symbols denote ratings in between).

B.3 Evaluation of TrustMan system with standard indicators

Figure 7.4 shows the results of the evaluation of TrustMan system with standard indicators and against other related systems. As it can be seen from that figure the TrustMan system performs better than other related trust management systems for supporting the management of inter-organizational trust in VBEs. Based on the evaluation results as shown in Figure 7.4 the following are example fundamental conclusions in relation to evaluation of the TrustMan system against other systems:

- TrustMan system performs better than other systems in relation to the analyzability indicator. The other systems are difficult to analyze due to a number of reasons for example: (1) the mechanisms applied to match the profiles in the okCupid.com system are not clear and missing detailed description, and (2) the relation between the four criteria applied in the "Trusted Advisor Associates" and the large set of questions asked to the user is difficult to analyze and not detailed in the system.
- Considering changeability indicator, the modules of TrustMan system are easier to change than those implemented in other systems except the Trust Assessment Wheel because the later is system providing guidelines on how trust can be analyzed. Thus those guidelines can easily be changed with other guidelines than changing java classes in modules of the TrustMan.
- DRACO system performs better than the TrustMan system in the aspects of security. A number of security services needed to support collaboration among organizations in distributed environments are implemented in DRACO system. However, in the TrustMan system the needed security services are remotely invoked from the ECOLEAD ICT infrastructure as addressed in Chapter 6. The invocation process might have some difficulties, such as network failure, and in such cases the TrustMan system might fail to assure the required security level.
- TrustMan system provides services that can be accessed by other VMS subsystems through invocation methods (see in Chapter 6) which results to a high interoperability with other VMS subsystems. However, the five compared system does not support service invocation and thus they have limited interoperability.
- The maturity of TrustMan system is lower than all other compared system considering the popular indicator used in the market, namely, the time since it was developed and deployed at different environments.

Annex C

Empirical evaluation – questionnaire

C.1 VBE networks involved in evaluation

Experimentation of the TrustMan system and its related conceptual results (methodologies, approaches, mechanisms, etc.) was performed by four VBE networks, namely: IECOS (Mexico), Swiss Microtech (Switzerland) ISOIN (Spain), and Cebenetwork (German). The description of these VBE networks is provided below.

Integration Engineering and Construction Systems – IECOS: IECOS S.A de C.V is a Brokerage network created by the Centre of Innovation in Design and Technology of the Tecnologico de Monterrey, Mexico. IECOS is divided into three business units: (1) *IECOS Technology:* This business unit offers the development of new products, processes and manufacturing systems; (2) *IECOS Supply Services:* This business unit offers the integration of associated enterprises capable to deliver manufactured products (mainly metal-mechanic and plastic parts) according to the quality, cost and delivery time expected by the customer; and (3) *IECOS Engineering:* The business unit develops customized solutions in the electronic and mechanical engineering processes. In 2000 IECOS adapted the Virtual Organisation (VO) model in its collaborative businesses and activities. The result of this strategic decision is that brokers in IECOS network select and integrate competencies of different Mexican small and medium enterprises (SMEs) from a pool of companies – VBE – as their main manufacturing partners. This is done in order to be able to capitalize on new business opportunities and introduce new product in specific market sectors [Source: Galeano, et al., 2008].

Swiss Microtech – SMT: Swiss Microtech is a network (founded in 2001) of seven independent SMEs active in the screw manufacturing industry. The main focus of SMT is on producing parts for the automotive, medical, space and telecommunication sectors and it exports 90% of the production amount. Among the seven SMT members, four of them are competitors and the three others bring complementary competences. Each company keeps its full independence to serve its own customers, and alliances (virtual organizations) are created to address new markets or orders that are out of reach for single companies. Swiss Microtech started collaborating with a Chinese partner network located in the Guangdong Province to cover the Chinese market and find suppliers for simple and cost effective parts. [Source: Galeano, et al., 2008].

Ingenieria y Soluciones Informaticas – ISOIN: ISOIN is the core technological partner of the Aeronautic Cluster of Andalusia. It coordinates innovation activities for the adoption of the advanced CNO (collaborative networked organization) paradigm. The Aeronautic Cluster of Andalusia brings together three prime contractors (EADS-CASA, AIRBUS and GAMESA), 93 subcontractors and a number of supporting entities (Universities, Research Centres and Regional Governments) in order to increase process efficiency and collaboration while fostering innovation. Most companies are located in the provinces of Seville and Cadiz in the South of Spain. ISOIN coordinates its activities under stable collaboration agreements, mainly under a subcontracting form, constituting organizations which are operating with a common ICT infrastructure. As the core technological partner of the Cluster, ISOIN acts as a leader to promote research initiatives and best practices for the adoption of technological pillars towards the collaborative enterprise paradigm within the aeronautical value network [Source: Galeano, et al., 2008].

CeBeNetwork group – CBN: CBN carries out worldwide complex development projects for the European air transport industry and other innovation driven branches. CeBeNetwork GmbH Engineering & IT is the core company of the CeBeNetwork Group. The company offers its customers comprehensive services and products in the fields of cabin, flight physics, systems and structures. As a strategic supplier of the Airbus

Group, CeBeNetwork Engineering & IT has the responsibility to organize specialized collaborative activities and the delivery of entire project solutions. CeBeNetwork is the leader of an engineering supplier network of 39 companies, mostly active in the aeronautical industry. It is also a strategic supplier of services to the main customer – the airbus group – in the civil aerospace industry [Source: Galeano, et al., 2008].

C.2 Description of the questionnaire

In the table below, we present the questionnaire applied to collect evaluation results for the TrustMan system from the four VBE networks described earlier in this annex. The evaluation of the TrustMan system focuses on the five processes (P1-P5) as presented in Section 6.6.2. The description of evaluation indicators considered in this questionnaire is presented in Section 6.6.2.

P1	Improving the understanding of trust concepts through provision and access of relevant information			
	Type of indicator		Value	Comment/reason
	Quantitative criteria	Resources		
		Time		
	Qualitative criteria	Innovation		
		Reliability		
		Usability		
		Expectation		
P2	Presenting and interpreting the trust level of organizations in the VBE			
			Value	Comment/reason
	Quantitative criteria	Resources		
		Time		
	Qualitative criteria	Innovation		
		Reliability		
		Usability		
		Expectation		
P3	Selection of trust criteria for assessing the trustworthiness of organizations			
			Value	Comment/reason
	Quantitative criteria	Resources		
		Time		
	Qualitative criteria	Innovation		
		Reliability		
		Usability		
		Expectation		
P4	Assessment and measurement of the trust level of organizations in VBEs			
			Value	Comment/reason
	Quantitative criteria	Resources		
		Time		
	Qualitative criteria	Innovation		
		Reliability		
		Usability		
		Expectation		
P5	Management of trust related data (Submission, access, …)			
			Value	Comment/reason
	Quantitative criteria	Resources		
		Time		
	Qualitative criteria	Innovation		
		Reliability		
		Usability		
		Expectation		

Bibliography

Citation	Reference
Adan & Resing, 2001	Adan, I. & Resing, J. Queueing Theory. *Department of Mathematics and Computing Science, Eindhoven University of Technology*. The Netherlands, (2001).
Ahuja, 2000	Ahuja, G. Collaboration networks, structural holes, and innovation: A longitudinal study. *In Administrative Science Quarterly*, Vol. 45, pg. 425–55, (2000).
Afsarmanesh et al., 2008	Afsarmanesh, H., Msanjila, S.S., Ermilova, E., Wiesner, S. & Woelfel, W. VBE management system. *In methods and tools for collaborative networked organizations.* ISBN: 978-0-387-79423-5, pg. 119-154. Springer, New York, (2008).
Afsarmanesh & Ermilova, 2007	Afsarmanesh, H. & Ermilova, E. Ontology Management for VO Breeding Environments. *In the proceedings of 9th International conference on the Modern Information Technology in the Innovation Processes of the Industrial Enterprises.* Pg. 124-137, Italy, (2007).
Afsarmanesh, et al., 2007	Afsarmanesh, H., Camarinha-Matos, L. & Msanjila, S.S. Virtual organizations breeding environments: key results from ECOLEAD. *In the proceedings of International conference on Cost Effective Automation in Networked Product Development and Manufacturing – IFAC-CEA'2007.* Monterey, Mexico, (2007).
Afsarmanesh & Camarinha-Matos, 2005	Afsarmanesh, H. & Camarinha-Matos, L.M., A framework for management of virtual organization breeding environments, *In the proceedings of the Collaborative Networks and their Breeding Environments*, PRO–VE'05, Spain, pp. 35–49, (2005).
Akkok, 1998	Akkok, N. The causal modeling technique. PhD thesis for the degree of candidate of Scientist in informatics, *Computer Science, Institute of informatics, university of Oslo*, Norway, (1998).
Assinakopoulos & Macdonald, 2002	Assinakopoulos, D. & Macdonald, S. A dual approach to understanding information networks. *In the international journal of networking and virtual organizations*, vol. 1, no. 1, pg 1-16, (2002).
Avila-Rosas & Luck, 2005	Avila-Rosas, A. & Luck, M. A direct reputation model for VOs formation. *In Multi-Agent Systems and Applications*, Springer, Heidelberg, (2005).
Barenblatt, 1987	Barenblatt, G. I. Dimensional analysis. *Gordon and Breach Science publishers*. ISBN: 3718604388, (1987).
Blaze, et al., 2009	Blaze, M., Kannan, S., Lee, I., Sokolsky, O., & Smith, J. M. Dynamic trust management. *In IEEE Computer, Special. Issue on Trust Mangement, pg.44-52, 2009.*
Blomqvist, 2005	Blomqvist, K. Trust in a Dynamic Environment – Fast Trust as a Threshold

	Conditions for Asymmetric Technology Partnership Formation in the ICT sector. In Trust in Pressure, Investigation of Trust and Trust Building in Uncertain Circumstances. Edward Elgar Publishing Inc. 2005.
Boslego, 2005	Boslego, J. 'Engineering Social Trust' *International Health, Harvard International Review,* Vol. 27, no. 1, Spring (2005).
Bourdieu, 1983	Bourdieu, P. 'Forms of capital' in J. C. Richards (ed.) *Handbook of Theory and Research for the Sociology of Education*, New York: Greenwood Press, (1983).
Byne, 2006	Byne, B. M. Structural equation modeling with EQS: Basic concepts, Applications, and Programming. Second edition, ISBN: 978-0-8058-4125-1, *Routlege Academic*, 2006.
Camarinha-Matos & Afsarmanesh, 2008	Camarinha-Matos, L. M. & Afsarmanesh, H. Collaborative Networks Reference Modeling. ISBN 978-0-387-79425-9, Springer, New York, 2008.
Camarinha-Matos & Afsarmanesh, 2006	Camarinha-Matos, L. M. & Afsarmanesh, H. Collaborative Networks: Value creation in a knowledge society. *In knowledge enterprise: Intelligent strategies in product design, manufacturing and management*, pg. 26-40, Springer, (2006).
Camarinha-Matos & Afsarmanesh, 2005	Camarinha-Matos, L.M. & Afsarmanesh, H., Collaborative networks: a new scientific discipline. *In the International Journal Intelligent Manufacturing*, Vol. 16, pg. 439–452, (2005).
Castelfranchi & Falcone, 2000	Castelfranchi, C. & Falcone, R. Trust Is Much More than Subjective Probability: Mental Components and Sources of Trust. In proceedings of the 33rd Hawaii International Conference on System Sciences (2000).
Center, 2008	Center, J. Organizational Management. In non-profit good practice guide – Promoting the power of shared knowledge. web: www.npgoodpractice.org/topics/organizational/default.aspx. Accessed on April 2008.
Clay & Strauss, 2000	Clay, K. & Strauss, R. Trust, risk and electronic commerce. The 19th century lessons for the 21st century. *In the proceedings of the 93rd annual conference on Taxation,* National tax association and ecommerce, Mexico, (2000).
Cosimano, 2004	Cosimano, T. F., Financial institutions and trustworthy behavior in business transactions. *In the Journal of Business Ethics*, Vol. 52, pg. 179–188, (2004).
Crave et al., 2006	Crave, S. Bouron, T & Ladame, S. Using social capital as a conceptual framework for professional virtual communities formalization. *In proceedings of PRO-VE 2006 conference, IFIP, Vol. 224, Network-Centric Collaboration and Supporting Frameworks* (Camarinha-Matos, L., Afsarmanesh, H. & Ollus, M.-editors), pg. 371-378, Springer, (2006).
Currall & Judge, 1995	Currall, S. C. & Judge, T. A. Measuring trust between organizational boundary role persons. *In Organizational Behavior and Human Decision Processes,* Vol. 64**,** No**.** 2, (1995).
Dasgupta, 1988	Dasgupta, P., Trust as a commodity. *In Trust: Making and Breaking Cooperative Relations*. Basil Blackwell: New York. Pg. 49–72, (1988).
Field & Hoffner, 2003	Field, S. & Hoffner, Y. Web services and matchmaking. *In the international journal of networking and virtual organizations*, Inderscience, Vol. 2, No. 1, page 16-32, (2003).
Galeano, et al., 2008	Galeano, N., Molina, N., Beeler, J., Monnier, F., Pouly, M., Aguilera, C., Olmo, A., Laessig, D., Tiefensee, B. VBE pilot demonstrators. *In methods and tools for collaborative networked organizations*. ISBN 978-0-387-79423-5, pg. 405-430. Springer (2008).

Gambetta, 1988	Gambetta, D. Trust: Making and Breaking Cooperative Relations. *Basil Blackwell*. 1988.
Ge et al., 2004	Ge, Y., Yang, J.B., Proudlove, N. & Spring, M. System dynamics modeling for supply-chain management: A case study on a supermarket chain in the UK. *In the International Transactions in Operational Research*, Vol. 11, pg. 495-509, (2004).
Geerlings, 2001	Geerlings, W.S.J., Verbraeck, A Groot, R.P.T. & Damen, G., Manpower forecasting; a discrete-event object-oriented simulation approach. *In the Proceedings of the 34th Hawaii International Conference on System Sciences*, pg. 3005–3015, (2001).
Gloor, et al., 2008	Gloor, P.A., Paasivaara, M., Schoder, D., Willems, P. Finding collaborative innovation networks through correlating performance with social network structure. *In the International Journal of Production Research*, Vol 46, page: 1357-1371, Taylor & Francis, 2008.
Good, 1988	Good, D., Individuals, interpersonal relations, and trust. *In Trust: Making and Breaking Cooperative Relations*. Edited by D.G. Gambetta, Basil Blackwell: New York. Pg. 31–48, (1988).
Grandison, 2000	Grandison, T. & Sloman, M., A survey of trust in Internet applications. *In the IEEE Communication Survey Tutorial*, Vol. 3, pg. 2–16, (2000).
Greenland & Brumback, 2002	Greenland S., & Brumback, B. An overview of relations among causal modeling methods. *In the international journal of epidemiology*. Vol. 31, pg. 1030–1037, (2002).
Hovmand, 2003	Hovmand, P.S. Analyzing dynamic systems: A comparison of structural equation modeling and system dynamic modeling. *In Stractural equation modeling: Applications in ecology and evolutionally biology. ISBN*: 9780521781338, Cambridge University Press, (2003).
Howe, 2004	Howe, W.J. Organizational management in workflow applications – Issues and perspectives. *In the international journal of information technology and management*. Kluwer academic publisher. Vo. 5, No. 3, pg. 271-291, 2004.
Human & Provan, 1997	Human, S.E. & Provan, K.G. An emergent theory of structure and outcomes in small-firm strategic manufacturing networks. *In Academy of Management Journal*, Vol. 40, No. 2, pg. 368–403, (1997).
Hurmelinna-Laukkanen & Blomqvisit, 2007	Hurmelinna-Laukkanen, P & Blomqvisit, K. Fostering R&D collaboration – The inter-play of trust, appropriability and absorptive capacity. In Establishing the foundation of collaborative networks [eds. Camarinha-Matos, L.M., Afsarmanesh, H., Novis, P. & Analide, C.] Boston, Springer, pg. 15-22, 2007
Huynh et al., 2004	Huynh, T.D., Jennings, N.R. & Shadbolt, N.R. ‘FIRE: an integrated trust and reputation model for open multi-agent systems’. *In the* pr*oceedings of the 16th European Conference on Artificial Intelligence (ECAI)*, Kluwer Academic Publishers, Valencia, Spain, pp.18–22. (2004).
Iriondo et al., 2003	Iriondo, J. M., Albert, M.J. & Escudero, A. Structural equation Modeling: An alternaltive for assessing causal relationships in threatened plant populations. *In the International Journal of Biological Conservation.* Elservier. Vol. 113, pg. 367-377, (2003).
Ishaya & Mundy, 2004	Ishaya, T. & Mundy, D.P., Trust development and management in virtual communities. *In Trust Management.* Springer: Berlin, pg. 266–276, (2004).
Jones, et al., 2000	Jones, S., Wilikens, M., Morris, P. & Masera, M. ‘Trust requirements in e-business. A conceptual framework for understanding the needs and concerns of different stakeholders’. *In the Journal of Communication of the ACM*, Vol. 43, No. 12, December, pp.80–87, (2000).

Jøsang, & Lo Presti, 2004	Jøsang, A. & Lo Presti, S., Analysing the relationship between risk and trust. *In proceedings of Trust Management Second International Conference,* Oxford, UK, pp. 135–145, (2004).
Keen, 1999	Keen, P. G. W. Competing in the chapter 2 of the internet business: Navigating in a new world. (www.peterkeen.com/delft2.htm), 1999.
Kini & Choobineh, 1998	Kini, A. & Choobineh, J. Trust in electronic commerce: definition and theoretical considerations. *In the proceedings of the 31st Annual Hawaii International Conference on System Sciences*, Kohala Coast, Hawaii, pp.51–61. (1998).
Kirkwood, 1998	Kirkwood, C. W. System Dynamics Method. *Ventana System Inc*. (1998).
Korba & Song	Korba, L. & Song, R. A Reputation Evaluation System for Mobile Agents. *In the published in Proceedings of the 5th International Workshop on Mobile Agents for Telecommunications Applications*. Marrakech, Morocco. October 8-10, 2003.
Kreger, 2003	Kreger, H. Fulfilling the web services promise. Communication of ACM, Vol. 46, No. 6, 2003.
Lahno, 2001	Lahno, B. On the emotional character of trust. *In the Journal of Ethics Theory Moral Practice*, Vol. 4, pg. 171–189, (2001).
Lee & Turban, 2001	Lee, M.K.O. & Turban, E. A trust model for consumer Internet shopping. *In the Journal of Electronic Commerce,* Vol. 6, No. 1, pg. 75-91, (2001).
Lichiello & Turnock, 2002	Lichiello, P. & Turnock B.J. "Guidebook for Performance measurement". Turning point – Collaboration for a new century in public health. (2002).
Lucas, 2005	Lucas, L.M. The impact of trust and reputation on the transfer of best practices. *In the Journal of Knowledge Management*, Vol. 9, Issue 4, pg. 87-101, Emerald Group Publishing Limited, 2005
Maciaszek, 2007	Maciaszek, L.A. Requirements analysis and system design. *ISBN: 978-0-321-44036-5. Third edition. Pearson Education Limited* (2007).
Mayer, et al., 1995	Mayer, R. C. Davis, J. H., Schoorman, F. D. An integrated model of organizational trust. *In Academic of Management review.* Vol 20 No. 3, pg 709-734, (1995).
Mezgar, 2006	Mezgar, I. Trust building for enhancing collaboration in VOs. *In proceedings of PROVE 2006 conference IFIP, Vol. 224, Network-Centric Collaboration and Supporting Frameworks*, [L.M. Camarinha-Matos, H. Afsarmanesh and M. Ollus – editors], pg. 173–180, (2006).
Morgan & Hunt, 1994	Morgan, R.M. & Hunt, A. D. The commitment-trust theory of relationship marketing. *In the Journal of Marketing*, Vol. 58, pp.20–38. (1994).
Msanjila & Afsarmanesh 2008a	Msanjila, S.S., Afsarmanesh, H. FETR: A Framework to Establish Trust Relationships Among Organizations in VBEs. *In the International Journal of Intelligent Manufacturing; Special issue: Trust, Value Systems and Governance in Collaborative Networks*. ISSN 0956-5515, Springer, (2008a).
Msanjila & Afsarmanesh 2008b	Msanjila, S.S & Afsarmanesh, H. Inter-organizational trust in VBEs. *In methods and tools for collaborative networked organizations.* ISBN 978-0-387-79423-5, pg. 91-118. Springer (2008b).
Msanjila & Afsarmanesh 2008c	Msanjila, S.S & Afsarmanesh, H. A multi-model approach to analyze inter-organizational trust in VBEs. *In Collaborative Networks Reference Modeling*. ISBN 978-0-387-79425-9, pg. 195-216. Springer, New York, (2008c).
Msanjila & Afsarmanesh, 2008d	Msanjila, S.S. & Afsarmanesh, H. On architectural design of TrustMan system applying HICI analysis results. In the I*nternational Journal of Software.* Academy Publisher, ISSN 1796-217X. pg. 17-30 (2008d).
	Msanjila, S. S. & Afsarmanesh, H. Trust Analysis and Assessment in Virtual

Msanjila & Afsarmanesh, 2007a	Organizations Breeding Environments. *In the International Journal of Production Research, ISSN (print) 0020-7543*, pg. 1253-1295, Taylor & Francis. (2007a).
Msanjila & Afsarmanesh, 2007b	Msanjila, S.S. & Afsarmanesh, H. Modeling trust relationships in Collaborative Networked Organizations. *In international Journal of Technology Transfer and Commercialization,* ISSN (print): 1470-6075, Vol. 6, No. 1, pg. 40-55, Inderscience, (2007b).
Msanjila & Afsarmanesh, 2007c	Msanjila, S. S. & Afsarmanesh, H. HICI: An approach for identifying trust elements – The case of technological perspective in VBEs. *In proceeding of International conference on availability, reliability and security (ARES-2007),* pg. 757-764, Vienna, (April 2007c).
Msanjila & Afsarmanesh, 2007d	Msanjila, S.S. & Afsarmanesh, H. Towards establishing trust relationships among organizations in VBEs. In establishing foundation of collaborative networks – Proceedings of PRO-VE 2007, Springer, pg. 3-14, (2007d).
Msanjila & Afsarmanesh, 2007e	Msanjila, S.S. & Afsarmanesh, H. Specification of the TrustMan system for assisting management of VBEs. *In the lecture notes of computer science series*, LNCS 4657, pg 34-43, Springer, (2007e).
Msanjila & Afsarmanesh, 2006a	Msanjila, S. S. & Afsarmanesh, H. Assessment and creation of trust in VBEs. *In proceedings of PRO-VE 2006 conference, IFIP, Vol. 224, Network-Centric Collaboration and Supporting Frameworks* (Camarinha-Matos, L., Afsarmanesh, H. & Ollus, M.-editors), pg. 161-172, Springer, (2006a).
Msanjila & Afsarmanesh, 2006b	Msanjila, S. S. & Afsarmanesh, H. Understanding and modeling trust relationships in collaborative networked organizations. *In Business, Law and Technology: Present and Emerging Trends,* (Kierkegaard, S.M. –editor), Vol. 2, ISBN87-991385-1-4, pg 402-416, IAITL, (2006b).
Msanjila et al., 2005	Msanjila, S.S., Tewoldeberhan, T.W., Janssen, M., Block-Bockstel, W. & Verbraeck, A. E-supply chain orchestration using web service technologies: a case using BPEL4WS. *In the Proceedings of Information Resource Management Association Conference*, San Diego, pp. 282–285, (2005).
Mukherjee, 2003	Mukherjee, A. A model of trust in online relationship banking. *In the Journal of Bank Marketing*, Vol. 2, pp.5–15, (2003).
Ozcan, et al., 2006	Ozcan, A. E., Jean, S., & Stefani, J. Bringing Ease and Adaptability to MPSoC Software Design: A Component-Based Approach. *In Lecture Notes in Computer Science, LNCS 3956,* pp. 118–137, Springer-Verlag Berlin (2006).
Papazoglou & Georgakopoulus, 2003	Papazoglou, M.P. & Georgakopoulus, D., "Service-Oriented Computing". *In the Communications of the ACM*, Vol 46, No. 10, (2003).
Parnell, et al., 2008	Parnell, G. S., Driscoll, P.J., & Henderson, D. L. Decision making in systems engineering and management. ISBN, 978-0-16570-8. *Wiley – Interscience*, (2008).
Pearl, 1998	Pearl, J. Graphs, causality, and structural equation models. In the journal of sociological methods and research. Vol. 27, No. 2, pg. 226-264, (1998).
Peltz, 2003	Peltz, C. Web services orchestration and choreography. *In the IEEE computer*, Vol. 36, No. 10, (2003).
Pfleeger, 2001	Pfleeger, S. L. Software engineering – Theory and practice, second edition, ISBN 0-13-029049-1. Prentice Hall, USA, 2001
Pinyol, et al., 2007	Pinyol, I., Sabater-Mir, J. & Cuni, G. How to talk about reputation using a common ontology: from definition to implementation. *In the proceedings of 6th International joint conference on Autonomous Agents and Multi-agent Systems – W20: Trust in Agent Societies,* pg 90-101. Hawaii, (2007).

Povey, 1999	Povey, D. "Trust Management," http://security.dstc.edu.au/presen tations/ trust/, (1999).
Preece, 2004	Preece, J. Etiquette, empathy and trust in communities of practice: Stepping-stones to social capital. *Journal of Universal Computer Science, vol. 10, No. 3, pg. 294-302 (2004).*
Pressman, 2005	Pressman, R. S. Software Engineering: A Practitioner's Approach. Sixth edition, ISBN: 0072853182, *Published by McGraw-Hill*, (2005).
Putnam, 1995	Putnam, R. D. Bowling Alone: America's Declining Social Capital. *In the Journal of Democracy*, vol. 6, no. 1, pg. 65-78 , (1995).
Rabelo, et al., 2006	Rabelo, R.J., Gusmeroli, S., Arana, C., Nagellen, T.: The ECOLEAD ICT infrastructure for collaborative networked organizations. *In: Camarinha-Matos, L., Afsarmanesh, H., Ollus, M. (eds.) IFIP International Federation for Information Processing. Network-Centric Collaboration and Supporting Frameworks*, vol. 224, pg. 161–172, 2006.
Ratnasingam, 2003	Ratnasingam, P. Inter-organizational trust in business-to-business e-commerce: a case study in customs clearance. *In the journal of Global Information Management*, 2003.
Resnick, et al., 2000	Resnick , P., Kuwabara, K., Zeckhauser , R., &. Friedman, E. "Reputation Systems." *Communications of the ACM, Vol. 43 No.* 12, pg. 45-48, 2000.
Resnick & Zeckhauser, 2000	Resnick, P. & Zeckhauser, R "Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputatoin System." In proceedings of *NBER Workshop on Empirical Studies of Electronic Commerce*. (2000)
Rhody, 2002	Rhody, S. Why web services. *In the web services journal*, vol. 2, issue 2, 2002.
Rolfe, 2006	Rolfe, G. Validity, trustworthiness and rigour: Quality and the idea of qualitative research. *Journal of Advanced Nursing, Vol. 53, No. 3,* Blackwell publishing Ltd. (2006).
Rousseau, et al., 1998	Rousseau, D.M., Sitkin, S.B., Burt, R.S. & Camerer, C. Not so different after all: a cross-discipline view of trust. *In Academic Management Review*, Vol. 23, pg. 393–404. (1998).
Seigneur & Jensen, 2004	Seigneur, J.M. & Jensen, C.D. Trading privacy for trust. *In Proceedings of Second Trust Management International Conference*, pp. 93–107, UK, (2004).
Settle, 1998	Settle, J. The element of 'trust' in mediation: practice pointers drawn from theory. *In the ADR Report*, Vol. 2, pg. 5–7, (1998).
Sharratt & Usoro, 2003	*Sharratt, M. & Usoro, A.* Understanding Knowledge-Sharing in Online Communities of Practice. In the electronic journal of management, vol.8, no 2. pg. 187-196, (2003).
Smith & Barclay, 1997	Smith, J. M. & Barclay, D. W. The effects of organizational differences and trust on the effectiveness of selling partner relationships. *In the Journal of Marketing, Vol.* 61, (1997).
Sztompka, 1999	Sztompka, P. Trust: A Sociological Theory. *Cambridge University Press*: Cambridge, UK. (1999).
Szulanski, 1995	Szulanski, G. Unpacking stickiness: An empirical investigation of the barriers to transfer best practice inside the firm. *In Academy of Management Best Papers Proceedings*, pg. 437–41, (1995).
Vreede, 1995	Vreede, G.J. de. Facilitating Organizational change – The participative application of dynamic modeling. *PhD thesis. TUDelft*, (1995).
Weth & Bohm, 2006	Weth, C. V. D. & Bohm, K. A unifying Framework for Behavior-Based Trust Models. *OTM 2006, LNCS 4275, pg. 444-461,* (2006).

Summary

On Inter-Organizational Trust Engineering in Networked Collaborations

Industrial organizations increasingly face more challenges in the market and society, among which the scarcity of resources, short delivery time requirement, frequent emergence of new technologies, demand for wide variety of competencies, and limited availability of up-to-date experts, can be mentioned. Coping with these conditions require continuous restructuring and changes in organizations, which is only achievable by large organizations. Due to their small size, lack of competitive capital and inability to acquire complex opportunities, *Small and Medium Enterprises* (SMEs) cannot cope with this needed speed of change. Instead SMEs seek other new approaches to remain competitive, such as collaboration within the networks of organizations, namely the virtual organizations (VOs). However, both research and practice has shown that dynamic time/cost-effective and fluid creation of VOs requires the pre-existence of the so called Virtual organizations Breeding Environments (VBEs). The main aim of VBEs is to create the needed commonality and preparedness in SMEs, prior to the moment of VO creation. One crucial preparedness aspect within the VBEs, addressed by this thesis, involves establishment of rational inter-organizational trust among the VBE members, which both enhances their chances of being selected for VO participation, and motivates their effective collaboration within the VOs.

The primary focus of the thesis is on: (1) *Identification of trust elements* considering variations of actors' preferences and requirements for trust establishment, (2) *Formulation of approaches and mechanisms* to support the analysis of inter-organizational trust and establishment of trust relationships, (3) *Development of trust management system* to support the management of inter-organizational trust within VBEs. The main innovative solutions introduced in the thesis, in relation to management / creation of rational trust among organizations, include:

- *An approach to identify trust elements for organizations (Chapter 3)*: This is a three-stage approach applied to identify trust elements for organizations. The approach is also applied to analyze hierarchical relations among trust elements, impact relations between trust criteria and trust level, and causal influences among trust criteria.
- *A customizable set of trust elements for organizations (Chapter 3)*: In collaboration with industrial VBE networks we have identified three large customizable sets of trust elements. Each set supports the realization of one of the three main trust objectives, namely creation of trust of: (1) One VBE member organization to another (2) One VBE member organization to the VBE administration, and (3) An external stakeholder (e.g. a customer) to the VBE.

- *Conceptual modeling of trust elements (Chapter 4)*: We have applied three modeling formalisms, namely, object-based formalism, record-based formalism and ontology-based formalism to develop models supporting different actors' purposes, such as development of modules for trust management systems, designing relational database schema, and analyzing taxonomy relations among trust elements to enhance understanding of trust concepts by actors.
- *Mechanisms for assessing trust level of organizations (Chapter 5)*: We have developed a modeling approach based on mathematical equations for formulating mechanisms that support the rational assessment of organization's level of trust.
- *Development of trust management system (Chapter 6)*: We have proposed a model for supporting the development of services that are supporting the processes related to the management of inter-organizational trust. The model addresses users, requirements, functionalities, and architectures of the system.

The achieved results are evaluated and validated using three approaches, namely: (1) *Empirical validation – achievements in relation to VBE requirements:* focused on experimenting within running VBE networks. (2) *Self validation - with standard indicators & against other systems)*: focused on application of some standard (ISO) indicators to compare our approach against others. (3) *Peer reviewed validation - within scientific community:* focused on presenting our approach in scientific events and publishing our research results in cited Journals and peer-reviewed conference proceedings as well as book chapters.

Samenvatting

Over Interorganisatorisch (Technisch) Construeren van Vertrouwen in Netwerk Gekoppelde Samenwerkingsverbanden

Industriële organisaties komen steeds meer uitdagingen tegen in de markt en de samenleving, waaronder schaarsheid van bronnen, eisen voor korte levertijden, nieuwe ontwikkelingen op technologisch gebied, de vraag naar een verscheidenheid aan competenties en de beperkte beschikbaarheid van experts. Om met deze omstandigheden om te kunnen gaan is continue verandering en herstructurering van organisaties noodzakelijk, hetgeen alleen haalbaar is voor grote organisaties. Vanwege hun kleine omvang, onvoldoende kapitaal en hun onvermogen om complexe expertise te verkrijgen, zijn *Kleine en Middelgrote Ondernemingen* (KMOs) niet in staat om zich snel genoeg aan te passen. In plaats daarvan zoeken KMOs andere en nieuwe manieren om competitief te blijven. Een voorbeeld is de samenwerking binnen netwerken van organisaties, namelijk Virtuele Organisaties (VOs). Zowel onderzoek als praktijk heeft uitgewezen dat de dynamische, tijd/kosteneffectieve en vloeiende creatie van deze VOs een zogenaamde Virtuele organisatie BroedPlaats (VBP) vereist. Het voornaamste doel van een VBP is, voorafgaande aan de totstandkoming van een VO, het creëren van de benodigde gemeenschappelijke bereidheid in KMOs. Dit proefschrift behandelt één cruciaal voorbereidingsaspect binnen KMOs, namelijk het opbouwen van rationeel interorganisatorisch vertrouwen tussen de KMO leden. Dit vergroot hun kansen om geselecteerd te worden voor deelname in een VO en stimuleert een meer effectieve samenwerking binnen de VOs.

De primaire focus van dit proefschrift ligt op: (1) het *Identificeren van vertrouwenselementen*, rekening houdend met diversiteit aan voorkeuren en eisen voor vaststellen van vertrouwen, (2) het *Formuleren van benaderingen en mechanismen* om het analyseren van interorganisatorisch vertrouwen en het vaststellen van vertrouwensrelaties te ondersteunen, en (3) het *Ontwikkelen van een vertrouwensbeheersysteem* om het beheer van interorganisatorisch vertrouwen binnen KMOs te ondersteunen. De belangrijkste innovatieve oplossingen, in relatie tot het beheer en het creëren van rationeel vertrouwen tussen organisaties, die in dit proefschrift worden geïntroduceerd, omvatten:

- *Een aanpak voor het identificeren van vertrouwenselementen voor organisaties (Hoofdstuk 3)*: Deze aanpak bestaat uit drie stappen om vertrouwenselementen voor organisaties te identificeren. De aanpak wordt ook toegepast om hiërarchische relaties tussen vertrouwenselementen, invloed relaties tussen vertrouwenscriteria en vertrouwensniveau, en causale invloeden tussen vertrouwenscriteria te analyseren.
- *Een aanpasbare set van vertrouwenselementen voor organisaties (Hoofdstuk 3)*: In samenwerking met industriële VBP netwerken hebben we drie grote aanpasbare verzamelingen van *vertrouwenselementen* geïdentificeerd. Elke verzameling ondersteunt de totstandkoming van één van de drie hoofd vertrouwensdoelstellingen,

te weten het creëren van vertrouwen tussen: (1) twee deelnemende VBP organisaties, (2) één aan een VBP deelnemende organisatie en de administratie van de VBP, en (3) een externe belanghebbende (bijv. een klant) en de VBP als geheel.

- *Het conceptueel modelleren van vertrouwenselementen (Hoofdstuk 4)*: We hebben drie modelleer formalismes, te weten, een object, gegevensbestand en ontologie gebaseerd formalisme, toegepast om modellen te ontwikkelen. Deze modellen ondersteunen verschillende actor doelen zoals het ontwikkelen van modules voor vertrouwensbeheerssystemen, het ontwerpen van relationele database schema's en het analyseren van taxonomische relaties tussen vertrouwenselementen. De analyse van deze taxonomische relaties dient het begrip van vertrouwensconcepten door actoren te verbeteren.
- *Mechanismen om het vertrouwensniveau van organisaties in te schatten (Hoofdstuk 5)*: Door middel van een wiskundige modelleeraanpak hebben we mechanismen beschreven die een rationele inschatting van het vertrouwensniveau van een organisatie ondersteunen.
- *De ontwikkeling van een vertrouwensbeheerssysteem (Hoofdstuk 6)*: We hebben een model voorgesteld ter ondersteuning van de ontwikkeling van diensten. Deze diensten ondersteunen het beheer van de processen gerelateerd aan interorganisatorisch vertrouwen. Het voorgestelde model omvat de gebruikers van het systeem, de gestelde eisen en functionaliteit aan het systeem, en architecturen voor de verschillende onderdelen van het systeem.

De behaalde resultaten worden op drie verschillende manieren geëvalueerd en gevalideerd, namelijk: (1) *Empirische validatie – resultaten in relatie tot VBP eisen:* gericht op het experimenteren met bestaande VBP netwerken. (2) *Zelf validatie – met standaard indicatoren en vergelijking met andere systemen:* gericht op de toepassing van een aantal standaard (ISO) indicatoren om onze aanpak met anderen te vergelijken. (3) *Collegiale Toetsing – binnen de wetenschappelijke gemeenschap:* gericht op het presenteren van onze aanpak op wetenschappelijke bijeenkomsten en het publiceren van onze onderzoeksresultaten in geciteerde tijdschriften en collegiaal getoetste conferentie publicaties evenals hoofdstukken in een boek.

Acknowledgements

My PhD work has finally come to an end. The findings presented in this thesis are achieved during a research work of several years. Now, I look back with delight reflecting many nice moments, difficult times, and promising work that I experienced during the entire research period. During this period, I collaborated with colleagues, friends and relatives, and thus in this section, I would like to use this opportunity to express my appreciation to everybody that I met and worked with in this research.

First of all I would like to thank my promoter Prof. Peter M. A. Sloot and my co-promoter Dr. Hamideh Afsarmanesh. On one hand, it was Prof. Peter M. A. Sloot who guided me in the last part of my research, while giving me his support on my work. On the other hand, I would like to thank my co-promoter Dr. Hamideh Afsarmanesh for giving me the opportunity to become a member of her group (the COLNET group), and for all the confidence and support that I have received from her. While doing research with Hamideh during the last years, I have learned about many issues associated with academic life, in particular those related to: writing publications in good English, carrying out and reporting high-level scientific research, collaborating with people of different culture and with different level of knowledge and so on. Without her dedication and tirelessness supervision this thesis would not have reached this final shape that it presently has. I am very grateful to both of you for all the work that we have done together during the last years.

In the same way, I want to thank all the members of the COLNET group with whom I shared many professional and recreational activities. In particular, I would like to give my appreciation to Ekaterina Ermilova for her commitment in our collaboration during the entire period of my research work. Katja, we will always remember the busy times we had together and the late-night working while we were trying to meet the deadlines for submitting papers and deliverables of ECOLEAD project. To other members of the COLNET group namely, Ozugl, Victor, and Ammar, thank you for your senior advices on working style and doing research in projects as it is cultured in the group. It was a pleasure for me to work with such a nice multi-cultural and multi-national group of people.

To my officemate in Matrix I, Henriette thank you for the timely responses on jokes, they kept me smiling and got me out of work related stress; Mattijs thank you for your competitive participation in making joyful jokes in the room, it always made me think of more new jokes. But surely, Katja, Henriette and Mattijs thank you for the four committed years in helping me in a number of aspects related to my thesis. It is hard to mention all these aspects in this paragraph which is dedicated to you. I'm grateful for your support.

I also want to express my appreciation to the members of the evaluation committee for the time that they dedicated to the promotion activities. I'm also thankful to the partners of the ECOLEAD project since without their collaboration, provision of the real-case application

scenarios related to industrial VBE networks, and performance of validation, this research would have been so hard to empirically develop.

Furthermore, during the elaboration of this thesis I received the assistance of many colleagues and friends within the Human Computer Studies Lab (HCS). I would like to thank Saskia van Loo for her tirelessness working on reminding and helping me with all administrative tasks and deadlines. I would also like to thank the following for their advices on different aspects of my research: Vera Hollink, Victor de Boer, Jochem Liem, Sennay Ghebreab, Gerben de Vries, Sophia Katrenko, Niels Netten, Frank Nack, Vanessa Evers, Wouter Jansweijer, Floris Linnebank, Wico Mulder, Jacobijn Sandberg, Maarten van Someren, Jan Wielemaker, Andi Winterboer, Bert Bredeweg, Paul Sales, Jafar Tanha and all those whose names are not in this list. I would also like to thank Heather Lane, Samir Saberi, Austin Ajah and Mwateni for helping me with different aspects of writing my thesis. Finally, I would like to thank the members of my family, Adela (the mother of the family), Masaka (the son) and Judith (the daughter), for their patience and tolerance during the last years of missing their family's dad.

Simon Samwel Msanjila

ISBN: 10: 9057761963

ISBN: 13: 9789057761966