Using Information Security as a Facet of Trustworthiness for Self-Organizing Agents in Energy Coalition Formation Processes

Christine Rosinger[1], Mathias Uslar[1], Jürgen Sauer[2]

Abstract

Trustworthiness - besides other decision making factors like technical or regulatory requirements - can be one key aspect for the decision making in coalition formation processes with agents in the energy domain. In this paper the trustworthiness facet information security is used to describe the realized security measures and standards of the systems for coalising energy agents as one trust building factor. These realized security measures are assessed and used for the decision making in the coalition formation process. This contribution shows also some of the results for developing a trust model for a multi-agent-based energy management system in the "*Smart Nord"* project.

1. Introduction and motivation

There are different issues for the motivation of using a trust model/system as one security measure for an agent-based energy management system.

The reorganization from a monopolistic electricity market to a distributed smart grid and also the liberalization of this market with its unbundling induces the need of more information and communication technologies (ICT). The increasing ICT leads to a higher threat potential, as a result of new and more intelligent actors and additional interfaces and data exchange that are introduced in the energy domain. Thus, the energy domain requires more revised and in some cases even new security measures because of the special requirements of the energy domain [1].

The increased usage of decentralized power plants results in a distributed structure of the power grid. To control, organize, and act at markets in an economic way and even to reach a higher automation level, one possible solution is to use multi-agent-systems, as it is actually realized in the project "*Smart Nord*"[3] [2]. In this project, producers, consumers, and storages of energy are represented as agents who form coalitions to act at an energy marketplace.

The main motivation using a trust model is the occurrence of malicious agents. Different attack motivations [3] like e.g. achieve economic advantages can mislead malicious agents to misuse the system for their own advantage. In a worst case scenario, malicious agents can create a system blackout if they cooperate as a botnet. To thwart such attacks, the application of a reputation or a trust system [4] shall prevent this. Additionally, such a trust model should restrict the actions of the malicious agents and acts as one security measure, respectively, increases information security.

1.1. Outline

This paper provides an overview of first results of a distributed trust model which is developed in the project *"Smart Nord"*. This contribution focusses at the trustworthiness facet information security which will be used as a trust building factor for the coalition formation process of self-

[1] OFFIS – Institute of Information Technology, 26121 Oldenburg, Germany, christine.rosinger@offis.de, mathias.uslar@offis.de

[2] University of Oldenburg, 26111 Oldenburg, Germany, sauer@uni-oldenburg.de, Department of Computing Science

[3] The homepage of the "*Smart Nord*" project can be found at www.smartnord.de/.

organizing energy agents. After this introduction, Section 2 gives a short definition of the terms reputation, trust and trustworthiness, and their use in the project *"Smart Nord"* where this trust model is applied. In Section 3, related work of this security assessment approach is described and Section 4 shows an overview of the trust model. Section 5 illustrates the ontology-based concept of assessing security measures of a computational system of an energy agent. Afterwards in Section 6, a preliminary use case is applied to show this approach exemplarily. Finally, the paper ends with conclusions and an outlook in Section 7.

2. Terms: Reputation, trust and trustworthiness

To get a consolidated understanding of the terms reputation, trust and trustworthiness; first, the difference between the terms reputation and trust and the relationship of trust and trustworthiness needs to be explained. After that, the terms are classified in the project "*Smart Nord".*

2.1. Difference of reputation and trust

In common understanding, the terms reputation and trust are frequently applied with the same meaning. The difference of the terms is defined as follows [5]:

The term *reputation* means that a group or a community of entities (agents) has a common opinion or understanding about another entity. This reputation or reputation value was built up by the community and they, altogether, have only one common value about this other entity (as shown in Figure 1, left side): The group of the entities *A, B, C, and D* as community has one reputation value about entity *E*. Within a reputation system every entity uses the same reputation value about one entity, which means that a reputation system is a kind of a centralized approach.

In difference to reputation, the concept of *trust* describes a local meaning or understanding and represents the subjective opinion or feeling from one entity towards another entity. Additionally, trust can be distinguished into direct and indirect trust like in the trust model "Web-of-Trust" [6]. This is further described in Figure 1 on the right side: *Entity A* wants to get into a trust relationship with *entity B*. *A* has no former direct experience with *B* but *A* has a direct trust relationship with entity *C*, which furthermore has a direct trust relationship with *entity B*. In this way, *A* can get some indirect information or referral trust about *B* over its direct relationship with *C*. Within a trust system, every entity has its own trust value to another entity. Thus, each entity can have a different trust value towards another entity which represents a kind of decentralized approach.

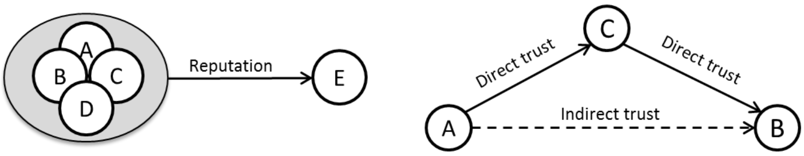

Figure 1: Difference of reputation and trust

2.2. Relationship of trust and trustworthiness

Trust and trustworthiness will be considered and used if one entity has to rely on another entity. The difference of trust and trustworthiness depends on the viewpoint. Trust is a property of entity A in relation to Entity B; Entity A has trust in entity B. In distinction to trust, trustworthiness is a property of entity B but has also a relation to entity A; Entity B represents its trustworthiness (in front of other entities), e.g. from the view of entity A [7]. In this paper, both terms are used for the trust model depending on the viewpoint.

2.3. The context of the project *"Smart Nord"*

Within the project *"Smart Nord"*, a trust system for a decentralized and self-organizing multi agent system will be designed. The decentralized approach of trust in comparison of the centralized approach of reputation is applied because it is similar to the decentralized energy supply design which is realized in the project and this decentralized approach is more adaptive. Additionally, the distributed storage of the trust values should prevent a single-point-of-failure of the trust system.

3. Related work

This contribution should show an approach to assess security measures of a computational system and – especially in the context of the *"Smart Nord"* project – of a computational system of an energy agent. Generally, for the assessment of security realizations, security metrics are used to improve the security in a system or architecture [8]. But this is not really an assessment of security measures; it is rather assessing the impact or barely counting the attacks. To realize an improvement over existing systems or even in the development of architectures, risk analyses [9], [10] and principles like security by design [1] or security standards [11] are applied. These described techniques are a kind of top-down approach.

The assessment of the security measures in the approach of this paper is rather a bottom-up approach. The energy agents negotiate and use the assessment of the security measures to decide to go into cooperation with the potential partners. But this assessment approach, described in Section 5, bases on how risk analyses are executed for security improvement.

4. Trust model for self-organizing MAS in the energy domain

The trust model which is developed in the *"Smart Nord"* project supports the trustworthy coalition formation of time-table-based active power provision. It consists of two parts: the structure and the application of the trust model.

4.1. Structure of the trust model

The structure of the trust model is shown in Figure 2. One main component of this structure is the integration of different facets of trustworthiness [12] and combining these facets to one trust value [3], [4]. Trustworthiness facets defined in the project *"Smart Nord"* are for example:

- *Credibility* represents the former behavior of an agent.
- *Reliability* forms a prediction value of technical data from the plant for the product delivery performance.
- *Information security* assesses realized security measures of the agent/plant system.

Figure 2 shows an illustration of the trust model. Besides the described facets, there are different ones that will not be considered in the project *"Smart Nord"* but can still affect trustworthiness. Generally, the facets are distinguished into trust building a priori and at runtime. Additionally, the trust value of an agent A_j from the viewpoint of A_i always refers to a context and is also time-dependent. Hence, the trust value tv can be expressed as quintuple:

$$Trust\ value\ tv = \left[Trustor\ A_i, Trustee\ A_j, Context\ c, trustworthiness\ tw, timeframe\ t\right].$$

Furthermore the trustworthiness tw can be expressed as the following hextuple:

$$trustworthiness\ tw = [Functional\ correctness\ fc, safety\ saf, informations\ security\ sec,\\ usability\ u, credibility\ cre, reliability\ r].$$

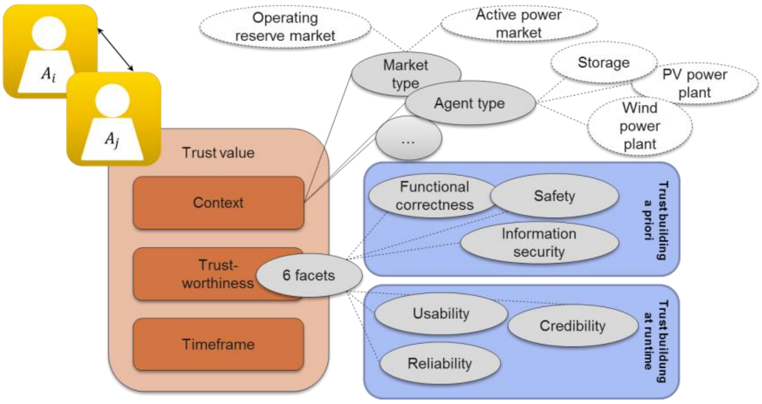

Figure 2: Illustration of Trust Model

4.2. Application of the trust model

The second main part of the trust model is the consideration of different phases a trust value has to go through during its lifecycle which is shown in Figure 3. The first appearance of a trust value is in the *initial trust* phase. This occurs when an agent is generated or joins the community. In this phase it has to be decided and determined which value the trustworthiness will be. Facets that have a trust building a priori can be applied in this *initial trust* phase. After this, the *calculation* or *update* phase takes place where e.g. the former behavior of an agent is regarded. This behavior is then included into the value or the value is updated. The *storage* phase considers where and how the different facets are stored and how tampering can be prevented. After a value was stored, there is a relationship back to the *calculation* and *update* phase because this is the main life circle of the value. After *storage* there are different other possibilities what happens next with the value. The *exchange/distribution* phase is concerned with the method how the values are exchanged and distributed between the agents and also a secure transfer of the values is considered. In the *utilization* phase, the different facets of the trust value are combined, goal functions are applied and guidance recommendations are given. If a value is compromised by malicious agents, revocation of the value has to be initiated.

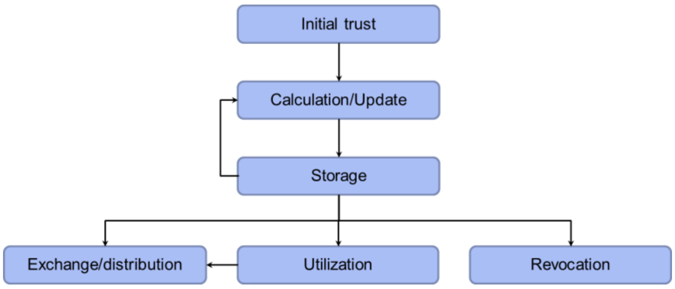

Figure 3: Phase model of the trust model

One of the main purposes of this paper is the presentation of how the trustworthiness facet information security for the agent-based energy management can be realized. This will be shown in the following Section 5.

5. Information security as a trustworthiness facet

Trustworthiness, as used here for the trust model in the intelligent energy management with self-organizing agents, is a value of one agent which represents its actual trustworthiness in a specific context. Trustworthiness in common consists of multi facets [12] – as shortly described in the previous section. One of these trustworthiness facets is information security, which takes into account that the more security measures a system of an agent applies, the higher is the assumed trustworthiness of the agent. Additionally, for this information security facet it is expected that if an agent realizes its security measures in a standard-based way, the agent is considered more trustworthy. In the following, the *basic security assessment model* and the *security value assessment method* are described which are necessary for the information security facet.

5.1. Basic security assessment model

In Figure 4, an overview of the basic security assessment model as ontology is depicted. The solid lines represent hierarchical relationships between the concepts shown in blue and red-striped boxes and the dashed lines are object-property relationships, which can be reasoned. The green oval shows the security value which is calculated by the security assessment model and which represents the result of the assessment phase.

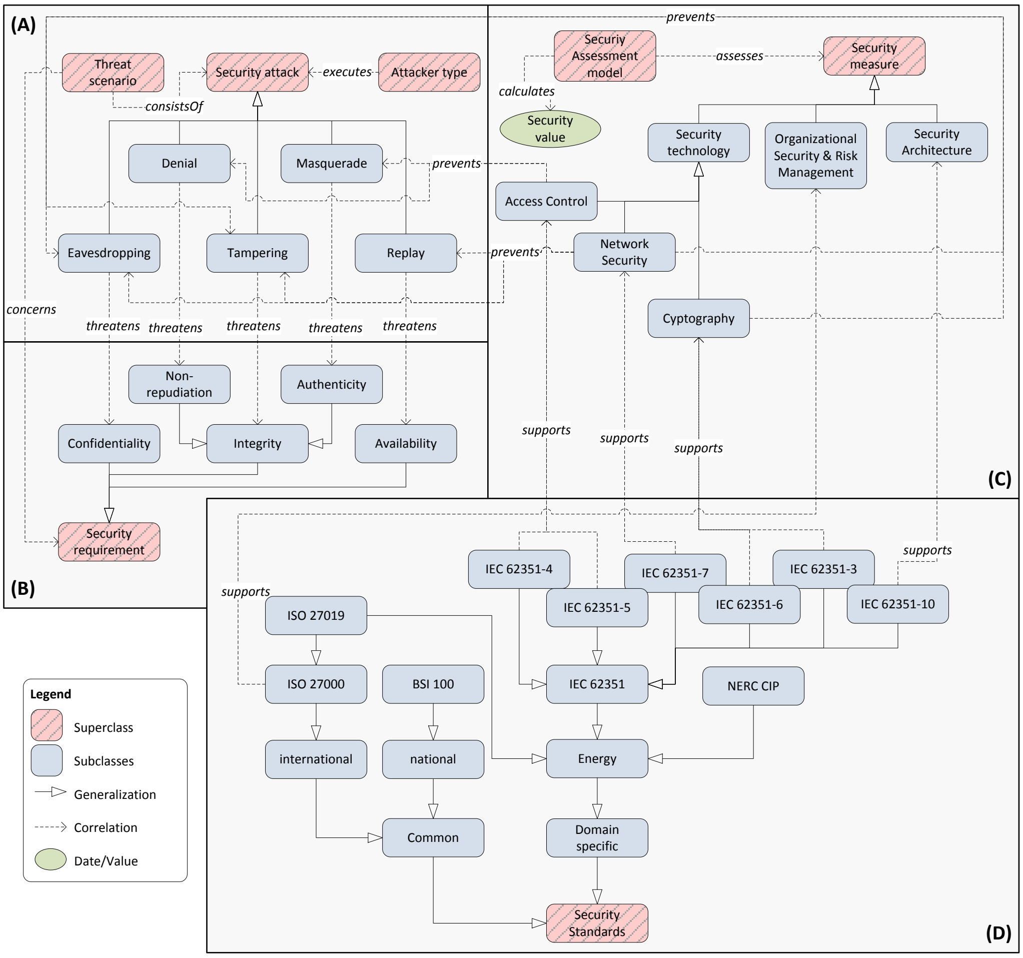

Figure 4: Assessment of implemented information security measures

The basic security assessment model in Figure 4 is segmented into four parts. Part (A) on the left upper side shows the concept *security attack* which consists of *threat scenarios* and is executed by an *attacker type*. Additionally, the corresponding concepts *eavesdropping*, *denial*, *masquerade*, *tampering* and *replay* are depicted. In part (B), on the left lower side in Figure 4, *security requirements* are illustrated which have to be guarded. Furthermore, the derived concepts *confidentiality*, *non-repudiation*, *integrity*, *authenticity*, and *availability* are shown. These concepts are pairwise threatened by *security attacks*. Part (C) shows the *security measures* with its sub-concepts *security technology* (*access control*, *network security*, *and cryptography*), *organizational security & risk management*, and *security architecture*. These *security measure* concepts are also pairwise associated over object-properties with their corresponding *security attack* concepts.

Copyright 2014 BIS-Verlag, Oldenburg, ISBN: 978-3-8142-2317-9

Additionally, they are related with the appropriate *security standard*s which support the security measures. The security standards are depicted in part (D). Even in part (C) – the most relevant concept for this assessment – the *security assessment model* concept is associated with the *security measure* concept over the object property *assesses*. Finally, this *security assessment model* concept with its assessment functions realizes the overall *security value*.

Figure 5 gives a deeper insight into the *security measure* and *security assessment model* concepts of the ontology from part (C). On the right side, the concept *security measure* is separated in the three concepts *security techniques* – which shows different exemplarily realizations of the concepts *access control*, *network security* and *cryptography – organizational security & risk management* and *security architecture*. On the left side, the *security assessment model* concept is depicted which calculates the *security value*. For this calculation the *assessment model* has different *consideration* concepts with various *functions*, which are formed on the basis of assumptions. Additionally, for the *assessment* the *consideration* concepts support each other.

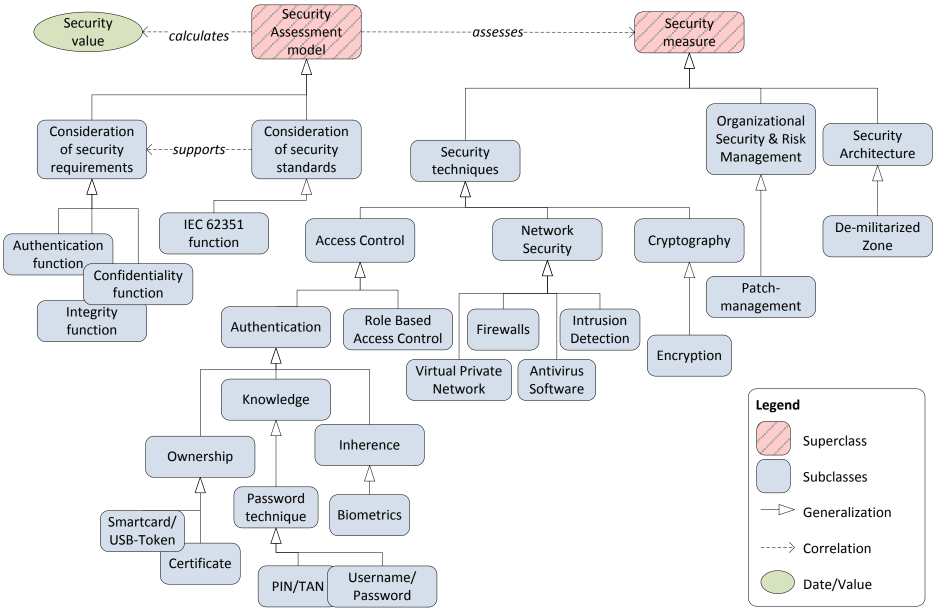

Figure 5: Assessment of information security measures

The approach of the assessment is based on the described ontology. Every agent of the energy management system realizes its security in a different way. Thus, for every agent instances from the ontology of its security realization are created. After the instantiation, over the *security measures* concept can be reasoned which *security requirements* have been protected for securing the system and whether useful and appropriate combinations of security measure are implemented. With that process, the *security assessment model* concept supported by reasoning and the *consider functions* calculates the *security value*.

5.2. Security value assessment method

Security assessment consists of assumptions because there are always different requirements and every user has to decide on his own which security requirements are the most important for his particular use case.

The presented security assessment method is based on a regular risk analysis [9],[10] with the assumption that the more security requirements are covered the more trustworthiness can be expected. Thus, the security assessment per agent consists of three parts. First, the *consideration of security requirements* concept of the ontology recognizes which security measures are realized and infers which security requirements are protected with these measures. This results in an assessment value A per security requirement $secreq$. Second, the *consideration of security standards* infers which standards are used for the realization and which security requirements are covered with them. This results in a 20 percent improvement of the assessment per security requirement $secreq$ if this security requirement is realized with a security standard (St); if there is no standard-based realization no improvement is obtained. Thirdly, there is a priority between 1 (low) and 4 (high) – which is based on the protection demand categories of the German “Federal Office on Information Security (BSI)[4]” – to get a weighted factor $Prio$ for the security requirements $secreq$. This priority has to be determined by the operator of this assessment on behalf of the appropriate use case.

For the final security assessment per agent $Sec(Agent)$ a weighted average with the single assessment per security requirement $A(i)$, the assessment of standard-based realization per security requirement $St(i)$, and the priority per security requirement $Prio(i)$ can be built which can be seen in formula (1). $\#secreq$ implies in this case the number of security requirements.

$$Sec(Agent) = \frac{\sum_{i=1}^{\#secreq} A(i)*St(i)*Prio(i)}{\sum_{j=1}^{\#secreq} Prio(j)} \tag{1}$$

6. Preliminary use case example

In this section a use case example of a coalition formation process with the trustworthiness facet information security between three energy agents will be described. This facet and also all the other trustworthiness facets (see Section 3) should function as trust building factor and support the decision making process of finding the right coalition partners.

Agent A_1 which initiates the coalition is called *initiator*; all other agents are the *responders*, in this use case these are the agents A_2 and A_3. Before starting the process with the call for proposal the initiator A_1 requests the trust values of the responder agents A_2 and A_3. This trust value consists normally, as described before, of different facets but this use case example is limited to the facet information security which calculation is described in the following paragraph.

	Security requirements: Agent A_2					Security requirements: Agent A_3				
	Authenticity	Integrity	Confidentiality	Availability	Non-repudiation	Authenticity	Integrity	Confidentiality	Availability	Non-repudiation
Single assessment	0.8	0.6	0.5	0	0	0.5	0.4	0.8	0	0
Standard-based (y/n)	n	y	y	-	-	n	n	y	-	-
Priority	4	3	3	1	2	4	3	3	1	2
Product	3.2	2.16	1.8	0	0	2.0	1.2	2.88	0	0
Total assessment	$\frac{3.2+2.16+1.8+0+0}{4+3+3+1+2} = 0.55$					$\frac{2.0+1.2+2.88+0+0}{4+3+3+1+2} = 0.47$				

Table 1: Example of security assessment calculation

Agent A_2 gets for its authentication a value of 0.8 in contrast to Agent A_3 who has a value of 0.5. For example, Agent A_2 realizes its authentication via 2-factor authentication (password and USB-token), and agent A_3 realizes its authentication only with a simple authentication (only with a password). Both agents have no standard-based realization of the measure. If they would have a standard-based realization in any of the measures, we assume an improvement of 20% for the

[4] The homepage of the BSI can be found at: https://www.bsi.bund.de/EN/Home/home_node.html.

trustworthiness, limited to an upper bound of 1. Furthermore, Agent A_2 and A_3 have the following values that can be seen in Table 1 in row *"single assessment"* for the other security requirements. In row *"standard-based (y/n)"* it can be seen, if these measures are realized in a standard-based way or not. Row *Priority* shows the assumed priorities for the different security requirements in this agent-based use case example. After that, in row *product* the three factors are multiplied – remember: standard-based realization gives 20% improvement limited to an upper bound of 1. Finally, the last row shows the calculation of the total assessment derived from formula (1).
For this use case this means that the initiator agent A_1 has the choice between agent A_2 who has a security value of 0.55 and agent A_3 who has a value of 0.47. Hence, A_1 takes A_2 for the coalition because of its better security realization. In a real scenario, the initiator agent has to include into this decision at first of course the contribution of energy the agent wants to provide and – as described before – the different facets of trustworthiness.

7. Conclusion and outlook

This contribution provides an overview of a trust model that is applied in the context of negotiating energy agents. The focus of this paper is the trustworthiness facet information security. Thus, an ontology-based approach of assessing security measures is described and examined, on the basis of a use case example.

For future work, the different factors of the information security facet in the context of the *"Smart Nord"* project needs to be estimated and evaluated. After the finalization of the different facets, the combination of the different facets has to be considered and examined.

Acknowledgement

The Lower Saxony research network 'Smart Nord' acknowledges the support of the Lower Saxony Ministry of Science and Culture through the 'Niedersächsisches Vorab' grant programme (grant ZN 2764/ZN 2896).

References

[1] Suhr, A., Rosinger, C., and Honecker, H., "System Design and Architecture – Essential Functional Requirements vs. ICT Security in the energy domain", Int. ETG-Congress 2013 (ETG-FB 139), 2013.

[2] Nieße, A., Lehnhoff, S., Tröschel, M., Uslar, M., Wissing, C., Appelrath, H.-J., and Sonnenschein, M., "Market-Based Self-Organized Provision of Active Power and Ancillary Services: An Agent-Based Approach for Smart Distribution Grids", COMPENG 2012, 2012.

[3] Rosinger, C., Uslar, M., and Sauer, J., "Threat Scenarios to evaluate Trustworthiness of Multi-agents in the Energy Data Management",EnviroInfo 2013, 2013.

[4] Rosinger, C., Uslar, M., and Hockmann, F., „Reputationssysteme für selbstorganisierte Multi-Agenten-Systeme in Energiemanagementsystemen", VDE-Kongress 2012, 2012.

[5] Jøsang, A., Ismail, R., and Boyd, C., "A Survey of Trust and Reputation Systems for Online Service Provision", Journal Decision Support Systems, 2007.

[6] Schmeh, K., „Kryptografie – Verfahren, Protokolle, Infrastrukturen", dpunkt Verlag, 2009.

[7] Castelfranchi, C., and Falcone, R., "Trust theory: A socio-cognitive and computational model", Wiley, 2010.

[8] Jaquith, A., "Security Metrics: Replacing Fear, Uncertainty, and Doubt", Addison-Wesley, 2007.

[9] International Organization for Standardization (ISO), "ISO 27005: Information technology — Security techniques — Information security risk management".

[10] CEN-CENELEC-ETSI Smart Grid Coordination Group, final document in mandate M/490 group SGIS "Smart Grid Information Security", 2012.

[11] International Electrotechnical Commission (IEC), "IEC 62351 part 1 - 11, Power systems management and associated information exchange - Data and communications security", 2007 – 2013.

[12] Steghöfer, J.-P., and Kiefhaber, R., "Trustworthy organic computing systems: Challenges and perspectives", in Autonomic and Trusted Computing and Trusted Computing, Springer Berlin Heidelberg, 2010.