SUSTAINABLE VIRTUAL UTILITIES BASED ON MICROGRIDS

Rune GUSTAVSSON
School of Engineering, Blekinge Institute of Technology
Ronneby, SE-372 25, Sweden

ABSTRACT

Next generation of energy systems, being dependant on Renewable Energy Resources (RES) and Distributed Generation (DG), will typically be based on flexible virtual cells of cells of balanced power consumption – generation, that is microgrids, rather than present day vertical hierarchical grid systems. Furthermore, the supporting information infrastructure and non-linear dependencies will pose new dependability challenges to the systems involved. As a consequence, we have to decouple present day proprietary hierarchical SCADA systems into sets of services that allow for horizontal as well as vertical integration supporting operations and business models of future virtual utilities. The virtual utilities are integrating two critical infrastructures; power grids and cyber networks. To allow for this flexibility and assuring dependability we argue that the underlying infrastructures should be modelled as Service Oriented Architectures (SOA). We propose in this paper a methodology towards ensuring quality of service in virtual utilities based on microgrids.

Keywords: Microgrids**,** SCADA, Critical Infrastructures, Critical Information Systems, Service oriented systems, Quality of Service, Autonomic computing.

1. INTRODUCTION

To meet increased demands of energy as well as requirements of preservation of our environment and natural resources future utilities have to incorporate Renewable Energy Resources (RES) and Distributed Generation (DG) to a much greater degree than today. Furthermore, due to deregulations and increased dependability, the energy systems of today show an increased brittleness. To cope with the combinations of needed flexibility and increasing brittleness new kinds of supporting information infrastructures and intelligent components of future energy systems are presently investigated. The presentation in this paper is partly based on results from the EC project CRISP[1] on 'Distributed Intelligence in Critical Infrastructures for Sustainable Power'.

In the next section, 'Assessments of present day grid based systems', some shortcomings and vulnerabilities of present day energy systems are presented. We focus on the increasing dependability of software in critical infrastructures. In Section 3 'Microgrid based virtual utilities', we argue for a decoupling of present day SCADA systems into a set of services. This decoupling is supported by *Emerging standards from International Electro technical Commission (IEC)*[2] (Section 3.2) and enabled by the emergence of *Service Oriented Architectures*[3] supporting future information and communication systems (Section 3.3). In Section 4 we assess 'Sustainable clusters of microgrids'. The paper ends with some pointers towards future R&D in the section 'Conclusions and future work'.

The focus of the paper is to introduce a novel 'Information and Communication Technology (ICT)' perspective on SCADA systems to harness some of their inherent vulnerabilities as described in Section 2 and to enable design and maintenance of future microgrid based virtual sustainable utilities.

2. ASSESSMENTS OF PRESENT GRID SYSTEMS

During 2003 at least three major power-system blackouts happened in August-September, that is, the blackouts in US – Canada, Italy, and Sweden – Denmark. The causes of these catastrophic events (not the least in economic terms) have been reported in several reports elsewhere.

From the US-Canada report of the 2003-08-14 blackout we find the following listing of causes to the disaster. The listing is coupled to recommendations by the investigators of actions to remedy some of the shortcomings found. The listing includes the following headings:

Institutional issues related to the disaster
Insufficient investments
Lack of training of personnel
Insufficient maintenance
Non-functioning procedures of operation

Need of standardizations
Establishment of *enforceable* standards

Need of technological improvements
Specifically the role of ICT and Power Grid Management and Dependable software.

The issue of non-dependable software and lack of operators understanding of the system behaviour was the root cause of the US-Canada blackout. In fact, a vulnerability in the General Electric Management System XA/21 (a SCADA system) at FirstEnergy Corporation, Ohio triggered the event. The primary cause was a software bug (software vulnerability) creating a "race condition" in the interactions between

[1] EC project CRISP Distributed Intelligence in Critical Infrastructures for Sustainable Power, ENK5-CT-2002-00673: www.crisp.ecn.nl.

[2] IEC standards, e.g., IEC 61850, IEC 61970, IEC 61968: http://www.wg14.com

[3] The NESSI Technoligical Platform promoted by thirteen major European ICT corporations on Services Architectures and Software Infrastructures Driving the Knowledge Economy: www.nessi-europe.com/

modules of a subsystem. This kind of software vulnerabilities are well-known problems in distributed computing. However, the affected software contained more than 3 million lines of code and had run without problems in more than 1 million operation hours before the critical event happened. The triggering of the critical event had a “window” of a few seconds and the event become disastrous when the operator did not understand the ramifications of the software failure (updating of system states) but closed down the system and went to lunch.

As a matter of fact, the *Blaster IT – worm* have impacted operations of nuclear power plants at FirstEnergy before 2003-08-14. The possible causalities between that event and the later “software –bug” event are not fully understood at this point in time. Anyhow, the Blackout itself clearly shows the critical interdependencies between power grids and information systems (SCADA).

The US-Canada blackout in 2003 is the worst case of that kind so far with over *50 million people* affected (estimated societal cost over 50B US$) and the power breakdown also affected other critical infrastructures of the society. Among those was *the grounding of over 5000 information networks* due to lack of electric power. The event clearly illustrated the increasing vulnerability to our society due to critical inter-dependencies of critical infrastructures. Of particular interest are efforts on Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP). A good overview of the related efforts in the US is the recent book *Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation*, by Ted Lewis (2006).

In this paper we focus in particular on challenges related to dependable software and protection of information in Critical Infrastructures (CI). Regarding issues of Critical Information Infrastructure Protection (CIIP) we argue that the protection mechanisms depend on the *type* of information at hand. To that end we have identified the following three types of information (Mellstrand and Gustavsson, 2006c):

- Information of type I_1. That is, information supporting execution of software.
- Information of type I_2. That is, information supporting the middleware and related services of the information system.
- Information of type I_3. That is, the information supporting the users (operators) of the systems.

In the paper we focus less on protection of information of type I_1 and type I_2, *the computational part*, of service oriented information systems. This focus is described in several papers by the authors (Gustavsson, 2006a, 2006b; Gustavsson and Mellstrand, 2007; Mellstrand, 2005, 2007; Mellstrand and Gustavsson, 2006a, 2006b, 2006c). We focus in this paper on issues related to protection of information of type I_3 (the actual load of the information system) related to information management of virtual utilities based on mocrogrids (Section 4). However, we argue that if we fail to protect information of type I_1 then we eventually fail to protect information of type I_2 and I_3. Furthermore, the introduction of a service-oriented architecture of information systems allows us to have a structured approach towards CIIP as outlined above. Not the least issues related to operator support of software intensive systems, e.g., SCADA systems.

Present day SCADA systems mainly focus on modeling and protection of information of type I_3 and not explicitly on the information types I_1 and I_2 supporting the computations of information system (Sections 3.1 and 3.2). However, information system failures are mainly caused by software bugs and vulnerabilities that causes natural failures as well as failures due to exploits by adversaries. Manipulation or misuse of user-centric information (I_3), e.g., by ´spy-ware´ or ´mal-ware’, are often enabled by exploits of software system vulnerabilities (Mellstrand, 2005).

Critical networked infrastructures such as present and future energy systems are examples of *software intensive* distributed systems. The introduction of software and interface standards between software components and supporting communication increases flexibility but also vulnerability of the systems. Furthermore, software also introduces feedback loops that cause non-linear system phenomena obscuring analysis of causality and forensics at breakdowns (De Marco and Braden, 2006, Mellstrand 2007). A recent study of sources of failures in critical infrastructures during 12 years has identified that more than 65% of failures were caused by vulnerabilities in software (exploits of vulnerabilities by malicious intruders or software failures (bugs)) (Rahman *et al*, 2006).

3. MICROGRID BASED VIRTUAL UTILITIES

In this section we focus on the needed transformation of supporting information SCADA systems to enable new energy based business processes and grid protections in future microgrid based virtual utilities. The transformation of SCADA systems is needed for two reasons:

- Inherent vulnerabilities in present systems
- Need for new architectures supporting future sustainable energy systems

In short; we have to replace present day vertical, closed and hierarchical SCADA systems with flexible service-oriented systems for information management in cell-based virtual utilities (microgrids) in order to incorporate *Renewable Energy Sources* (RES) and *Distributed Generation* (DG) as well as new added-value *energy-based services*.

Each (virtual) cell is characterized by the *energy balance production = consumption*. The idea is to have a more robust and flexible system of cells of cells than present day hierarchical energy systems (Gustavsson *et al* 2005b). We give below (Section 3.1) a short overview of current SCADA systems with some well-known limitations and shortcomings.

The needed transformation of supporting infor-mation SCADA systems is to enable new energy based business processes and grid protections in future cell-based virtual utilities. The transformation of SCADA systems is thus needed for two reasons:

- Inherent vulnerabilities in present systems
- Need for new architectures supporting future sustainable energy systems

In short; we have to replace present day vertical, closed and hierarchical SCADA systems with flexible service-oriented systems for information management in cell-based virtual utilities (microgrids) in order to incorporate *Renewable Energy Sources* (RES) and *Distributed Generation* (DG) as well as new added-value *energy-based services*. Each (virtual) cell is characterized by the *energy balance production = consumption*. The idea is to have a more robust and flexible system of cells of cells than present day hierarchical energy systems.

Decupling of SCADA system functions into the required open information system requires a set of standards and data models as well as new architectures. Those issues are addressed in Sections 3.2 and 3.3. Security and dependability issues related to the new systems are addressed in Section 4.

3.1 CLASSICAL SCADA SYSTEMS

A typical control system architecture of power systems is given in Figure 1. The vertical hierarchical architecture of the information system closely mirrors the hierarchical structure of the classical power grid. If present day SCADA systems were as simple as Figure 1 suggests, the vulnerabilities would be limited. But in reality, SCADA networks are intertwined with cooperate networks, vendor connections, business partner connections, related websites, accounting and business process applications, and corporate databases. In practice, most SCADA systems live in a messy world of interdependent information systems. Access to SCADA networks has steadily grown as productivity needs have increased, the number of business partners has grown, and the ease of networking has prompted public utilities, energy companies, and power operators to connect everything to else. Communication has improved efficiency and lowered costs, but it has also opened SCADA to network intrusion. It has added more vulnerability to the infrastructures it was designed to enhance.

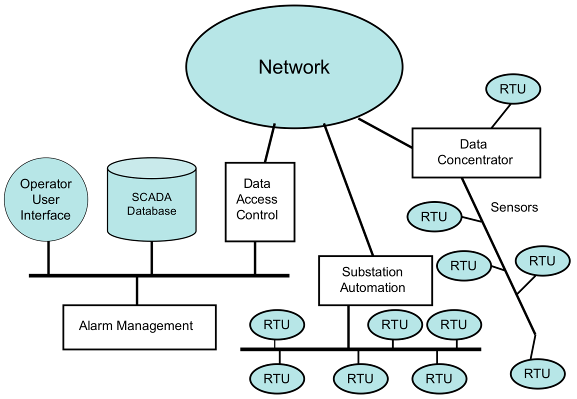

Figure 1 Standard control system architecture (SCADA) of power systems and its components consisting of computers, networks, databases, Remote Terminal Units (RTUs), and software.

To make matters worse, most devices in SCADA networks are low-cost and low-powered – optimized to be deployed by the tens of thousands. The RTUs are often inexpensive microcomputers with limited memory. They are not designed to support impenetrable security. For example, they usually do not support difficult to crack cryptography or employ expensive firewall equipment that can block unauthorized access. Many RTUs are accessible over a simple dial-up telephone – an access method that can be used by anyone from anywhere in the world (Lewis, 2006).

Assessments of vulnerabilities of Critical Infrastructures typically depict the energy system, specifically power systems, as the most critical infrastructure for our societies. As a matter of fact the greatest vulnerabilities of power systems exists “in the middle”, that is, in the transmission and distribution layer of the power grid. Faults occur and propagate through major portions of the connected grid, because of critical links, insufficient distribution capability, and cascade failures.

To quote from (Lewis, 2006): “This leaves SCADA/EMS as the vulnerability of greatest concern. Unfortunately, SCADA/EMS components – computers, networks, and software – will remain complex and unreliable for a long time because securing an infor-mation system is well known to be problematic. Thus far, it has been impossible to build software that is guaranteed to be bug-free. These software flaws leads to networks becoming disconnected, data being lost, and computers being disabled. As long as software is flawed, there will be faults in industrial control systems such as SCADA and EMS”. In fact we believe that designing and implementing “secure” software for SCADA systems is in practice impossible. That is why we advocate approaches towards securing execution environments as a more pragmatic approach towards assured dependable SCADA systems (Gustavsson and Mellstrand, 2007; Mellstrand, 2005, 2007; Mellstrand and Gustavsson, 2006a, 2006b, 2006c).

3.2 EMERGING STANDARDS BY IEC

The ongoing development of IEC standards supports the decoupling of SCADA systems and fit very well into a service-oriented ICT support for future energy-based business systems (Handschin *et al*, 2006). Furthermore, those standards could support development of more dependable and secure ICT systems than those that build on Internet standards alone. We will investigate those issues in subsequent experiments on our experimental test bed developed for those purposes (Gustavsson and Fredriksson, 2005; Gustavsson, 2006a, 2006b; Gustavsson *et al*, , 2005a, 2005b; Mellstrand and Gustavsson, 2006a, 2006b, 2006c).

3.3 SERVICE ORIENTED ARCHITECTURES

It should be noted that decoupling of SCADA functions enables flexibility if we recombine the functions in a structured and flexible way. The following Figure 2 captures the main components of Service Oriented Architectures (SOA). Service Oriented Architectures allows for design and maintenance of flexible and scalable distributed information systems. An application is configured from a set of services. The services are typically of two kinds. That is, basic support services (Middle-ware) or user-centric support services. The services are typically reusable and configurable. The application or service-bundle is maintained according to a set of *Service Level Agreements* (SLAs) that facilitate and monitor the proper coordination of the service bundle during operation (Gustavsson, 2006a, 2006b; Gustavsson and Fredriksson, 2005).

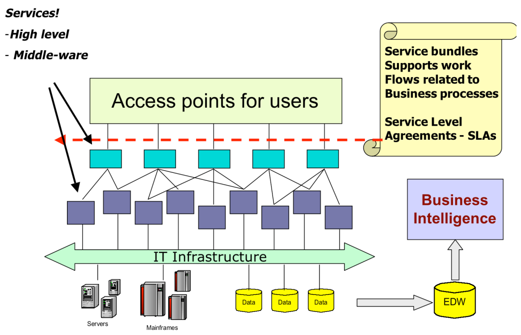

Figure 2 Basic components of Service Oriented Architectures (SOA)

The SOA architecture of future virtual utilities (or clusters of microgrids) supports the information structures of the individual cells as well as the global cluster. Each cell has a configuration as illustrated in Figure 3 below.

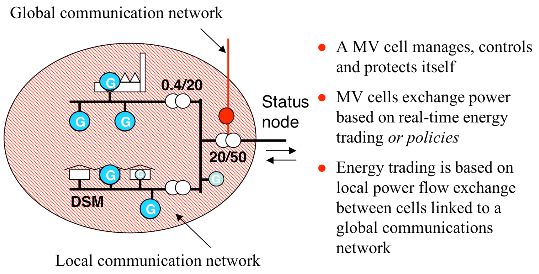
Global communication network
0.4/20
Status node
20/50
DSM
G
Local communication network
A MV cell manages, controls and protects itself
MV cells exchange power based on real-time energy trading *or policies*
Energy trading is based on local power flow exchange between cells linked to a global communications network

Figure 3 Main components of a microgrid cell structure

The load balance of production and consumption within a cell is supported by different mechanisms. In the CRISP project we investigated mechanisms based on computational prize markets based on bidding in auctions and high-level energy based business processes (Schaeffer *et al*, 2006).

4. SUSTAINABLE CLUSTERS OF MICROGRIDS

Future cell-based utilities consist of the energy system and an embedded information system (ICT). In fact we have interdependencies between *two* critical infrastructures. Protection of critical infrastructures (CIP) and of critical information infrastructures (CIIP) is of major international concern, as we noted earlier, not the least in the upcoming EU FP7 programme.

We have in CRISP outlined a framework addressing to some extent CIP as well as CIIP. Since software is the glue within and between infrastructures we have on one side focused on trustworthy and dependable software. On the other side we addressed performance of ICT networks in monitoring, maintaining and protecting the grid. We begin with the first concern and address later the ICT and microgrid issues.

In fact in a running system there will be software of different quality and of different origin (own developed software, COTS, proprietary software, and legacy systems). Furthermore, the software modules might be involved in interactions not intended, or thought of, at design and implementation time (as we have witnessed for SCADA systems). Still we expect and depend upon a trustworthy behaviour of our systems!

The following equation captures our approach towards trustworthy computations:

Computation = Code + Execution (1)

Most of contemporary models aiming at assuring correct computations have been focusing on assessing and testing the code itself (black box and white box testing, etc.). Our approach is towards assuring correct *execution*. We have to that end identified and tested different mechanisms supporting assessments of the *running state* of execution. Our results towards securing execution and protecting systems at runtime are very promising and will be pursued towards protecting execution of services in a service oriented architecture.

Our configurable experimental test bed used in validating our mechanisms for protecting execution has also been used in experiments related to ICT performance (delay and throughput) related to CRISP experiments. By tailoring routing algorithms we have validated that we can protect (detect, localize, and restore) the power grid even in time-critical situations (Mellstrand and Gustavsson, 2006a, 2006b, 2006c).

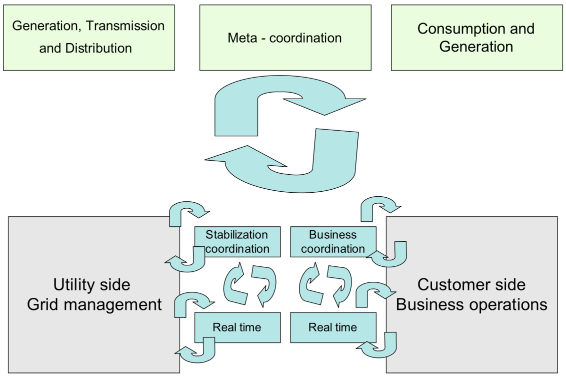
Generation, Transmission and Distribution
Meta - coordination
Consumption and Generation
Utility side Grid management
Stabilization coordination
Business coordination
Real time
Real time
Customer side Business operations

Figure 4 Coordination patterns in future virtual utilities

The CRISP experiments involve (technical) power grid protection and high-level business processes based on demand-supply matching. In effect those two applications can be modelled on the same service oriented platform. That approach allows us to integrate RES and DES in a principled way in clusters of microgrids. We have outlined a common business model coordinating the grid protection and the business model that allows us to buy or sell energy from a cell (in a "yellow" state) in order to avoid a critical situation (load shedding or black-out) and to bring the grid back to a "green" state (Figure 4) (Gustavsson *et al*, 2005a, 2005b).

Equation (1) above indicated that we modelled protection of computation as protection of execution. We take a similar route towards *information protection* (applies to all three types of information identified in Section 2). To that end we introduce the following equation:

Information = Representation + Interpretation (2)

Classical information protection (the Confidentiality, Integrity, Availability (CIA-model)) mainly focus on protecting the *representation* of information, of type I_3, by means of cryptography, PKI, and access control. Those methods have many known weaknesses and limitations including scalability and maintenance. To counter that we address the *Interpretation capabilities*, i.e., the tools that are available for a user in a given context for access and management (including visualization) of representations. The backbone of this approach is high-level dialogue models related to workflows of tasks (an extended CommonKADS framework (Schreiber *et al*, 1999; Gustavsson *et al*, 2005b)). We have in this framework indicated how we could secure for instance business processes related to demand-supply matching. This line of work is promising but still in an early phase.

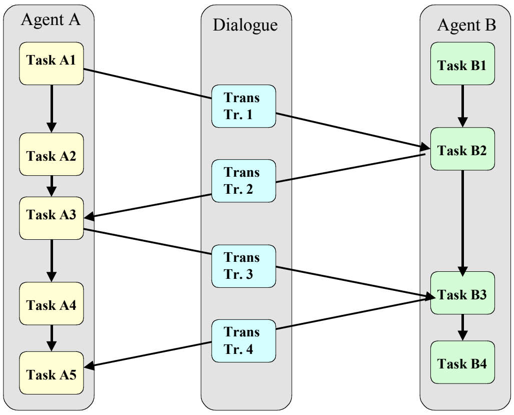

Figure 5 The general structure of a dialogue diagram

From Figure 5 and equation (2) we can in a structured way analyze and implement appropriate information protection mechanisms (e.g., related to business processes based on demand-supply matching) at appropriate levels, e.g., dialogues, tasks, workflows, information items, and supporting agent capabilities and access rights.

The bottom line is that we have within the CRISP identified and partly validated important mechanisms towards dependable and assured business services based on microgrid clusters (virtual utilities).

Vulnerabilities in distributed systems (and hence SOA systems) are mainly due to complexities related to *information exchange* between components across boundaries. Monitoring this information exchange is supported by means of models for controlling information flow across interfaces. Protocols, data models and tools for information control (e.g., parsers and interpreters checking syntax and sometimes semantics) are indispensable in this context. The set of protocols and data models provided by IEC (Section 3.2) is a valuable support in designing and maintaining future resilient SCADA systems. As the IEC data models mainly focus of information of type I_3 we also have addressed protection of information types of the underlying computational system, that is I_1 and I_2 (Gustavsson, 2006a, 2006b; Gustavsson and Mellstrand, 2007; Mellstrand and Gustavsson, 2006c). In fact, we have designed mechanisms supporting *resilience of missions* (selfhealing) in service oriented computing (Gustavsson and Fredriksson, 2005). That is, characteristics of *autonomic computing*[4] of the supporting computational infrastructure maintained by the information flows if type I_1 and I_2.

5. CONCLUSIONS AND FUTURE WORK

We have outlined in this paper a principled methodology that supports assured service-based computations. We also argue that future virtual utilities will be cell-based to cope with societal demands on sustainable energy supply. Finally, we argue that a suitable ICT infrastructure to support those virtual utilities will be based on service-oriented architectures and emerging standards from IEC. In short, future SCADA-systems will be based on flexible sets of services, where SLAs (Service Level Agreements) will *ensure appropriate Quality of Service* (Gustavsson, 2006a, 2006b). The paper reports work in progress. Future work will be in international and national collaborations with academia and industry in EC and nationally funded projects, for instance the EC funded project INTEGRAL[5], on the topics put forward in the paper. Specifically, experimental based R&D related to CIIP and CIP with focus on clusters of microgrids.

6. REFERENCES

[1] De Marco, C. and Braden, Y. (2006) Threats to Electric Power Grid Security through Hacking of Networked Generation Control. In *Proceedings of CRIS Third International Conference on Critical Infrastructures*, Alexandria, VA

[2] Gustavsson, R. and Fredriksson M (2005). Process algebras as support for sustainable systems of services. Invited paper to a special issue on *Applicable Algebra in Engineering, Communication and Computing* named *Algebraic Approaches for Multi-Agent Systems*.

[3] Gustavsson, R., Mellstrand, P., and Törnqvist, B. (2005a) *Information Security Models and Their Economics*. CRISP Deliverable D1.6, BTH.

[4] Gustavsson, R., Mellstrand P., Törnqvist B., and Akkermans, H. (2005b). *Dependable ICT Support of Power Grid Operations*. CRISP Deliverable D2.4, BTH.

[5] Gustavsson, R. (2006a). Ensuring dependability in service oriented computing. In *Proceedings of The 2006 International Conference on Security & Management (SAM'06)* at The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing, Las Vegas, 2006.

[4] www.research.ibm.com/autonomic/

[5] EC funded project INTEGRAL - *Integrated ICT-platform based Distributed Control (IIDC) in electricity grids with a large share of Distributed Energy Resources and Renewable Energy Sources,* 2007 – 2010.

[6] Gustavsson, R. (2006b) Proper use of Agent Technologies in Design and Implementation of Software Intensive Systems. In *Proceedings of the 2nd International Workshop on Integration of Software Engineering and Agent Technology (ISEAT 2006)* at the Sixth International Conference of Quality Software (QSIC 2006), Beijing.

[7] Gustavsson, R. and Mellstrand, P. (2007) Ensuring Quality of Service in Service Oriented Critical Infrastructures. In special issue of the *International Journal of Critical Infrastructures (IJCIS)*, Indersciemce, 2007.

[8] Handschin, E., Krause, O., Wedde, H. F., and Lehnhoff S. (2006) The Emerging Communication Architecture in Electrical Energy Supply and its Implications. In *Proceedings of the CRIS Workshop 2006. Influence of Distributed and Renewable Generation on Power System Security*. Res Electricae Magdeburgenses, MAFO Band 13, 2006.

[9] Lewis, T. (2006) *Critical Infrastructures Protection in Homeland Security. Defending a Networked Nation*. Wiley-Interscience, ISBN-13: 978-0-471-78628-3.

[10] Mellstrand, P. (2005) *Protecting Software Execution by Dynamic Environment Hardening*. BTH licentiate dissertation series no. 2005:12.

[11] Mellstrand, P. (2007) *Informed System Protection*, BTH Doctoral Dissertation Series No. 2007:10. School of Engineering. Blekinge Institute of Technology (BTH).

[12] Mellstrand, P. and Gustavsson, R. (2006a) An Experiment Driven Approach Towards Dependable and Sustainable Future Energy Systems. In *Proceedings of CRIS Third International Conference on Critical Infrastructures*, Alexandria, VA, September 2006.

[13] Mellstrand, P. and Gustavsson, R. (2006b) Preventing Buffer Overflows by Dynamic Environment Hardening. In *Proceedings of CRIS Third International Conference on Critical Infrastructures*, Alexandria, VA, September 2006.

[14] Mellstrand, P., and Gustavsson, R. (2006c). Experiment Based Validation of CIIP. In *Proceedings of 1st International Workshop on Information Infrastructure Security (CRITIS´06)*, special track at 9th Information Security Conference (ISC 2006).

[15] Rahman, H.A., Beznosov, K., and Marti, J.R. (2006) Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports. In *Proceedings of CRIS Third International Conference on Critical Infrastructures*, Alexandria, VA.

[16] Schreiber, G, et. Al. (1999) Knowledge Engineering and Management. The CommonKADS Methodology. MIT Press, ISBN 0-262-19300-0.

[17] Schaeffer, G. J., Warmer, C., Kamphuis, R., Hammelberg, M., and Kok, K. (2006) Field Tests Applying Multi-Agent Technology for Distributed Control: Virtual Power Plants and Wind Energy. In *Proceedings of the CRIS Workshop 2006. Influence of Distributed and Renewable Generation on Power System Security*. Res Electricae Magdeburgenses, MAFO Band 13,2006.