VIKING

(Vital Infrastructure, NetworKs, INformation and Control System ManaGement)

Summary of VIKING results

Project co-funded by the European Community within the 7th Framework Programme.

Table of Contents

Figures

1 Project Data

Grant Agreement number: 225643

Project acronym: VIKING

Project title: Vital Infrastructure, networKs, InformatioN and control system manaGement

Project Period:	**from**	**to**
	01/11/2008	**30/11/2011**

Project Coordinator:

E-Mail: Gunnar Bjoerkman <gunnar.bjoerkman@de.abb.com>

Scientific Coordinator:

E-mail: Mathias Ekstedt <mathias.ekstedt@ics.kth.se>

Project website address: www.vikingproject.eu

2 Executive Summary

Society is increasingly dependent on the proper functioning of the electric power system. Power outages might potentially lead to situations of non-functioning societies with devastating economical and humanitarian consequences. Power systems have for a long time been electrically designed to provide a high level of availability of the power delivery. However, in order to operate effectively the power systems today are highly dependent on an ICT infrastructure with control and SCADA (supervisory, control, and data acquisition) systems. Also these control systems have ever since their birth been designed for high reliability and availability. However, security was never an issue when these systems were designed. During the last decade these system have been interconnected to many other types of IT systems like enterprise resource planning systems, geographical information systems, customer management systems, maintenance management systems and, in many installations, with direct or indirect connections to Intranet/Internet. In the last years, because of this interconnection, much attention has been directed to the threat from directed and undirected cyber attacks towards control systems. With the spread of the Stuxnet malware specifically targeting control systems for critical infrastructure, the cyber threat has gone from theoretical speculations to a present risk for critical infrastructure operators.

The purpose of the VIKING project has been investigate and to better understand vulnerabilities in SCADA and control system and their underlying ICT infrastructure and to combine this knowledge with the consequences in the power system and the society at large if theses vulnerabilities indeed are exploited. With this knowledge the project has also been suggesting a number of countermeasures for identified weaknesses. Three types of weaknesses have been studied in the project: Firstly, functions of SCADA/EMS (Energy Management System) in terms of Automatic Generation Control (AGC) and State Estimation (SE); Secondly, SCADA and control system architecture as a whole with its data flows and connectivities, its software components, and its user/access right structure; and Thirdly, communication infrastructure has been scrutinized in greater detail. In order to connect vulnerabilities to risk in terms of power blackouts and costs for the society a demonstration test bed has also been developed in the project.

In order to demonstrate possible cyber attacks and their consequences on the SCADA system, in the power grid and in the society a Testbed has been implemented. The Testbed mainly consist of four parts: a simulated transmission network, integrated with a simulated distribution network, both operated by a (real) SCADA system, and finally connected to an underlying society simulator that defines load profiles as well as the economic production profiles based on gross domestic product (GDP) in a virtual society called the VIKING country. Finally, societal costs of cyber attack incidents have been calculated using the simulator for a number of scenarios, illustrating how cyber security risk assessments could be made all the way from ICT vulnerabilities to economic consequences.

Throughout the project, results have been disseminated in terms of scientific articles publically available and project reports available on request (due to the sometimes sensitive results). Altogether, results from the project have been presented in 48 scientific papers and journal articles and at 39 industrial and scientific conferences.

3 Summary description of project context and objectives

3.1 Main objectives

The main objectives of VIKING have been:

- To investigate the vulnerability of SCADA (Supervisory Control And Data Acquisition) systems operating electric power systems and to connect this to the cost of cyber attacks on society
- To propose and test strategies and technologies to mitigate these weaknesses
- To increase the awareness for the importance of critical infrastructures and the need to protect them

With these objectives the project are targeting several groups as the beneficiaries of the project results. Firstly, operators of critical infrastructure can be helped to make better decisions when planning security enhancement projects. More specifically IT and information security responsibles at the organizations are a prime target group for the project. Also risk analysers and responsibles, e.g. on government level, could be helped by the results since they can be helped with understanding how big the risks originating from cyber security breaches and their societal consequences are in comparison to other types of risks the organization faces. A third group of beneficiaries are SCADA system vendors which can use the results from the project to improve their product offerings with more secure solutions.

3.2 Background and context

Society is increasingly dependent on the proper functioning of the electric power system, which in turn supports most other critical infrastructures: water and sewage systems; telecommunications, internet and computing services; air traffic, railroads and other transportation. Many of these other infrastructures are able to operate without power for shorter periods of time, but larger power outages may be difficult and time consuming to restore. Such outages might thus lead to situations of non-functioning societies with devastating economical and humanitarian consequences. For this reason, this consortium has decided to concentrate its research on the systems for transmission and distribution of electric power. We anticipate that many of the results will be applicable to the protection of other critical infrastructures.

The operation and management of the electric power system depend on computerized SCADA and control systems. Keeping these systems secure and resilient to external attacks as well as to internal operational errors is thus vital for uninterrupted service. However, this is challenging since the control systems are extremely complex. Yet, the systems are operating under stringent requirements on availability and performance: If control and supervision are not done in real-time, the power network may come to a collapse.

SCADA systems include functions for remote collection of vast amounts of data from measurements placed in strategic points, e.g. power stations, in the geographically widely spread processes and for the remote control of process devices. Many SCADA systems include computerized models of the process, which enables simulation of alternatives process states and of optimization. Due to legal and environmental constraints, e.g. for building of new high voltage power lines or power stations, the primary process itself is difficult to expand which in its turn leads to higher and higher utilization of the existing transmission and generation resources. The process is, in other words, operated closer to its physical limits. Thus, the SCADA systems are becoming increasingly critical for achieving availability and security of the supervised infrastructure.

During the last decade risks associated with malicious attacks hitting SCADA and control systems have gained much attention both in practice and academia. After the targeted attack by the Stuxnet malware became known to the general public this threat is not longer only theoretical. The profile of the threat is however changing from organization to organization. Threat may come from highly advanced and dedicated attackers, so called advanced persistent threat (APT), or from so called script kiddies mainly using existing known exploits, or just it might be undirected malware that spreads to anyone being unprotected for them. The VIKING project has not studied threat agents per se, but many of the vulnerabilities studied are more likely to be exploited by skilled attackers.

Altogether the threats present to the SCADA and control systems can be counteracted in a vast number of different ways. Solutions include better staff training at utilities that increases awareness and enhances behavior, better management setting up policies and processes for increasing security, better management of the SCADA and control systems as such, deployment of better technical security solutions that prevents, detects or reacts on attacks at the utilities, the development of new technical security solutions at security and SCADA system vendors, enhancement of secure software development methodologies at vendors, as well as enhanced regulations on governmental level. The VIKING project has been focusing on technical issues at the both the utility, i.e. the user-side, and the vendor. More concretely, the project has developed methods for decision support for security planning of SCADA and control system architectures and communication as well as technical solutions to weaknesses in standard SCADA system functionality in terms of Automatic Generation Control and State Estimation. The project thus combines a holistic system management perspective—in order to counteract sub-optimization in the design—with in-depth analysis and development of security solutions adapted to the specific requirements of power system operations.

Looking at cyber security vulnerabilities and countermeasures is however only half of the scope of VIKING. A main objective with the project has been to also look at the consequences of potential cyber attacks. Depending on which part of the SCADA and control system architecture that is attacked and how the external consequences might vary tremendously. Cyber attacks could potentially lead to major national blackouts lasting for long periods to no visible effect at all. Therefore, in order to understand risks related to cyber security, attacks must always be understood in its context in term of the affected power system and society. In order to build up this understanding the project has built a test bed consisting of a virtual (simulated) society with a virtual (again simulated) power system including transmission and distribution grids with a number of voltage levels from 400kV to 0,4 kV. The whole scope of the VIKING project is illustrated in Figure 1.

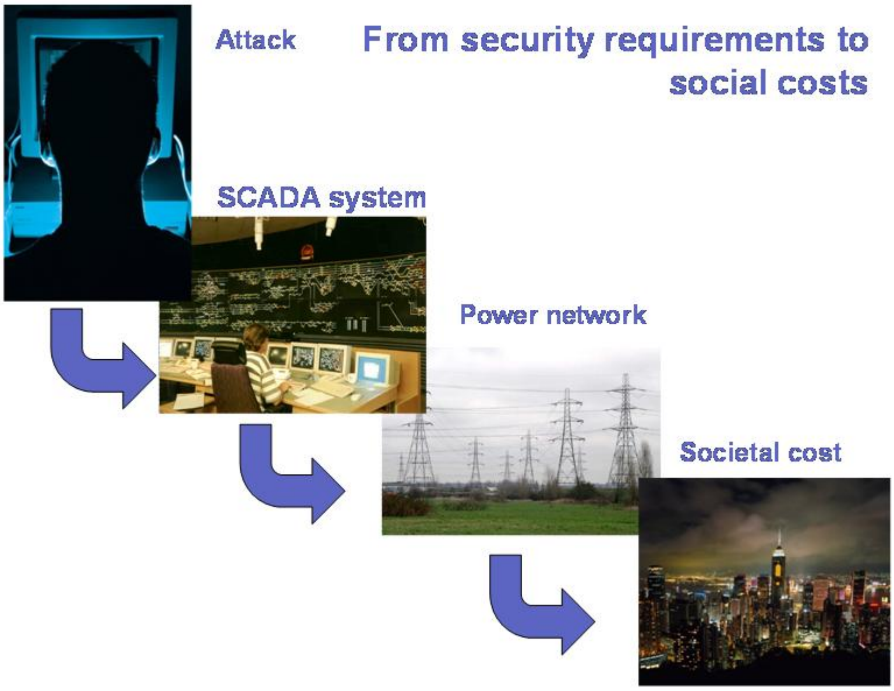

Figure 1 - Overall scope and structure of VIKING.

4 Main S&T results/foregrounds

This chapter briefly describes the main results of the VIKING project. In general the project takes a model-based approach to the problem domain. Models have been developed for SCADA system architectures, SCADA system functionality, power networks, and a society. Just as all models, the purpose the models developed in the VIKING project has been to simplify reality to be able to study some specific aspect of it in a more practical manner. Essentially the models' fills four purposes: to enhance SCADA and control system configurations with respect to cyber security at utilities; to estimate cyber security risks in terms consequences of cyber attacks at utilities; to suggest improvements to vendors for future security solutions in SCADA systems; and to provide a general increase of awareness about cyber security weaknesses and risks among all stakeholders in the area of critical infrastructure operation.

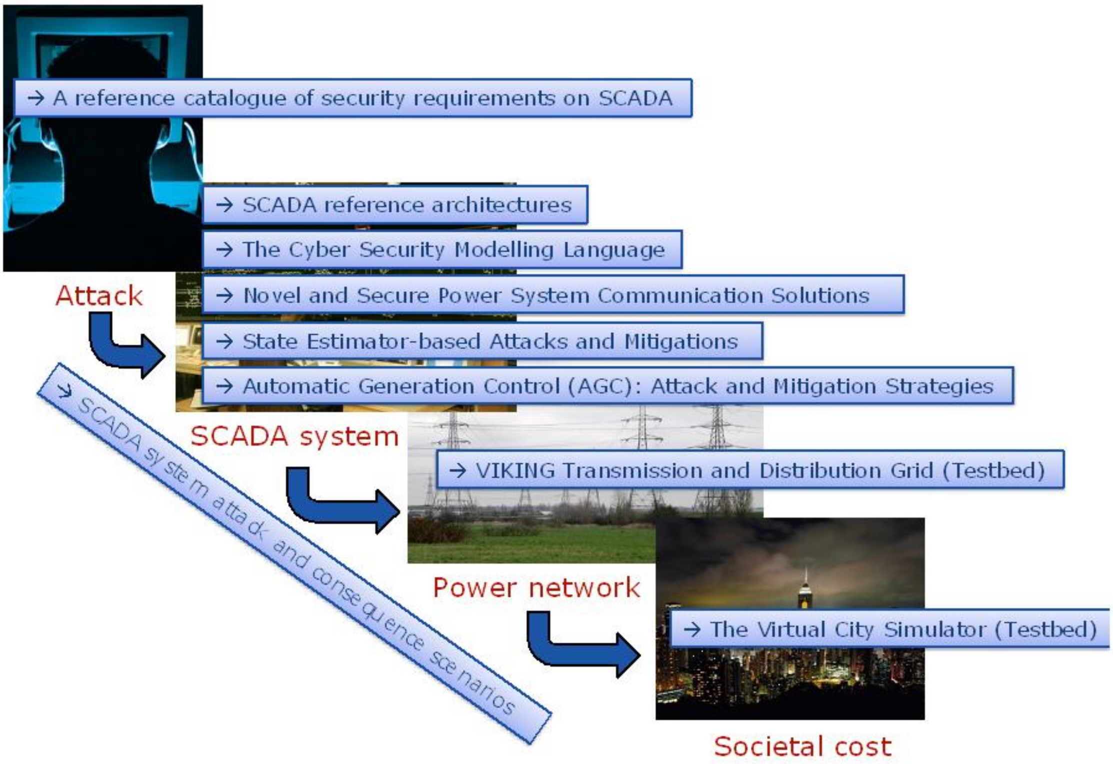
→ A reference catalogue of security requirements on SCADA
→ SCADA reference architectures
→ The Cyber Security Modelling Language
→ Novel and Secure Power System Communication Solutions
→ State Estimator-based Attacks and Mitigations
→ Automatic Generation Control (AGC): Attack and Mitigation Strategies
Attack
SCADA system
→ VIKING Transmission and Distribution Grid (Testbed)
Power network
→ The Virtual City Simulator (Testbed)
Societal cost
→ SCADA system attack and consequence scenarios

Figure 2 - Main deliveries mapped to the VIKING project scope.

In Figure 2, the main results are mapped to the overall scope of VIKING presented in Figure 1. The results will be further described in chapters 4.1 through 4.9. In

Table 1, the components and results of VIKING are described in a bit more details. In the table the work is described in two dimensions: industrial domain and kind of model (or non-modeled equipment). The industrial domain dimension simply describes what the subject area that is targeted by the model. ICT infrastructure refers to all the technology that is part of the platform or underpinning infrastructure that is needed to operate a SCADA system including operating systems, communication equipment, network services, etc. The SCADA and control system functionality refers to a rather wide range of functions such as alarm management, state estimators, historian database services, data engineering, and much more. Power system refers to grids from high to low voltage levels. Finally, society refers to the inhabitants and the organizations of nations. In the other dimension the "VIKING models" on the top row refer to results that have been developed as part of the project. The majority of those results are models whose purpose is to analyze or depict some specific aspect of the addressed domains, like maps representing the real world. From a scientific point of view these models should be proved correct or true in order to be useful. (This validation has of course also been addressed in the project). When building these "VIKING models" occasionally other models have been used as input or validation, these modeled on the next row in the table. In the project a test bed has also been developed, mainly for the purpose of demonstrating and "packaging" the results. The test-bed is built up from a number of models simulating various parts of the reality, described on the third row. These models are just accepted as being true or correct. No validation has been undertaken with respect to these models in the project. In the Testbed also "non-simulated" equipment is present, described on the last row. This equipment is simply equipment that is used exactly as in the Testbed also in real world settings.

Table 1 - Overview of VIKING components.

Domain	ICT-Infrastructure	SCADA/control system functionality	Power system	Society
Developed models/results; ”VIKING models”	• Cyber Security Modeling Language (D2.2, D3.1) • Novel and Secure Power System Communication Solutions (D4.2)	• SCADA reference architectures (D2.3) • State estimator/bad data detection attack security index (D3.2, D4.1, D4.2) • AGC attack model (D3.2) • AGC attack mitigation filter (D4.3)	• Hybrid system representaion of power networks (D2.4,D2.5). *For AGC modelling.* • Two-Area, two machine power system (D2.5) *For AGC modelling.* • Two-Area, multi machine power system (D4.3). *For AGC modelling.* • Distribution net: *Virtual City Simulator* (D3.3) • Power Load and Restoration profile: *Virtual City Simulator* (D3.3)	• Attack Magnitude Index, *Virtual City Simulator* (D3.3) • Business (GDP) profiles: *Virtual City Simulator* (D3.3) • Optimal Power Flow Based Economic Index (D4.3). *For State Estimator Attack modeling*
Other models used for validation of ”VIKING models”	• IEEE 118 bus and IEEE 300 bus (used as blueprints for communication networks)	• ABB Network Manager State Estimator and Bad Data Detection. *In test bed.*	• IEEE 118 bus*. In AGC modeling used for detailed study of dynamics and area behavior.* • ABB/VIKING 40 bus. *In test bed.*	• None
Simulated reality in test bed (These models are accepted/unquestioned for their respective context)	• WAN emulator: *ModelNet*	• Substation Automation functionality: *Astron NTS*	• Transmission net: *ABB OTS* (VIKING/ABB 40 bus) • Distribution net: *Astron NTS* • Distribution net: *Virtual City Simulator* (D3.3) • Power Load and Restoration profile: *Virtual City Simulator* (D3.3)	• Business (GDP) profiles: *Virtual City Simulator* (D3.3)
Real equipment in test bed (i.e. equipment that is not used for simulating something else, but are components that are the ”real thing”)	• Computers, network equipment, operating systems, infrastructure services (VPN, RDP, Wireshark, etc.), vulnerability exploit tools (Back track/ Metasploit)	• SCADA, EMS, Historian, Data Engineering, PCU, HMI : *ABB Network Manager*	• None	• None

The reminder of this chapter briefly describes the results of the VIKING project. The following sub chapters are organized according to the results as such not according to the individual models depicted in

Table 1. Some results are also individual models in the table but other results are a combination of several models.

4.1 SCADA system attack and consequence scenarios

In an attempt to bridge descriptions of human behavior, seen from a hacker perspective, and SCADA system behavior and properties, the project has developed a number of Story Board descriptions over how attacks could happen and what the consequences would be. These Story Boards also serve to tie together the different other results of the project. As described above, most of the results from the projects are different kinds of models that can be used to analyze different aspects of cyber security incidents. The Story Boards make use of the different models and put them into context by describing a fictitious, yet realistic, story in an easy to comprehend way for non-technical readers. The Story Boards describe a story, in prose, on why this specific attack scenario could happen in real life. We have imaginary characters and organizations, mostly taken from Nordic mythology, to make the stories more "real-life like" and we have tried to describe the motivation why and on which targets these people would seek to attack a process control system used for supervision and control of electrical networks.

Each Story Board starts with the story. Based on the story we have defined the assumptions for the story and we have used the assumption and the story to calculate an index on how high the probability will be that this specific attack would compromise the control system. For these calculations we have used the scientific work done mainly in Work Package 2 and 3 that we call CySeMoL (Cyber Security Modeling Language). For an overview of CySeMoL see section 4.4 below.

In order to calculate the economical consequences in terms of lost Gross Domestic Product from a blackout caused by a successful attack, we have used the work done in Work Package 3.3. In this work package we have defined and developed a virtual society simulator that we call ViCiSi (Virtual City Simulator) that is able to model both the static and dynamic society behavior. See section 4.8 for an overview of ViCiSi. For each relevant Story Board we define the cost caused by the blackout based on ViCiSi calculations for four virtual countries in Europe. Observe that we are not modeling, for example Germany, but a virtual country with the same power consumption pattern and economical structure as Germany. In addition, we are aware that economical loss is not the only consequence from blackouts and we, therefore, also report a blackout magnitude value that provides a more qualitative picture of potential consequences in the society.

For each Story Board we have added a list of mitigation examples that will decrease the probability of success for the Story Board attack. Based on these proposed mitigations we have used CySeMoL to calculate a new, lower probability that the attack will compromise the control system. The mitigation examples do not claim to be the most efficient mitigation and we have neither considered how difficult, feasible or costly the countermeasures are to implement. The purpose of these examples is mainly to illustrate CySeMoL from a user's point of view; what kinds of models are to be modeled by the user as well as what kind of analysis results that can be delivered in return by CySeMoL.

One of the important parts of the VIKING project has been to analyze attacks on power system applications. These are domain specific, mathematical based computer applications used for studies on alternative operational situations, power grid security analysis and grid optimization. We have found that intelligent attacks on Automatic Generation Control and State Estimator can succeed and could lead to network instabilities or wrong optimization solutions and we are proposing domain specific mitigation for these attacks. The work in these areas has been done within Work Packages 2 and 4. Two of the Story Boards (number 2 and 3) are dedicated for these attacks and for their mitigation solutions.

The communication networks between substation and control center and between control centers could be a very sensitive target for attacks. In Work Package 4.2 we propose some innovative mitigation also for these types of attacks. Several of the Story Boards describes attacks on communication networks and in the mitigation part of these Story Boards is taken from the results of Work Package 4.2.

Work Package 5 in VIKING is concerned with the build up of a VIKING Test Bed including a real SCADA system and an emulated network plus models of the high voltage network, substations, the distribution network and the society. Several of the Story Boards, but not all, have a corresponding Test Case description, which is a kind of User Manual with step-for-step descriptions for Test Bed users how to demonstrate the corresponding Story Board. We have for each Story Board defined if this Story Board is possible to execute on the Test Bed or not. The Test Case descriptions are found in VIKING deliverable D5.3b.

In total, we have defined and described the following Story Boards:

- Using automatic control sequences to open HV breakers
- Manipulating of AGC setpoints to destabilize network
- Manipulation of SCADA measurement to fool State Estimator
- Using the inter-center communication to open HV breakers
- Using remote workstation to open MV breakers
- Using unencrypted RTU communication to interrupt power supply
- Denial of Service attack on RTU communication to blind SCADA
- Exploiting Internet browser environment to open HV breakers
- Using Data Engineering to manipulate picture linking
- Using SA engineering tools to manipulate protection settings
- Using SA tools to remotely trip transmission line
- Manipulating transformer protection setting to overload transformer
- Open a "backdoor" in SCADA for later attack on HV breakers

The Story Board descriptions give, as can be seen above, only a limited number of examples of cyber attacks on SCADA systems and their consequences. Time and budget have limited the number of attacks we could describe as Story Boards. We have tried to select attacks that are as diverse as possible but it is obvious that there are many more known and easily imaginable attacks that could be described in this way. Furthermore, a whole category of attacks that it is not treated in the VIKING project is the realm of unknown attacks, which might well be the most dangerous of all. However, we are convinced that mitigating those attacks described in these Story Boards will increase the resiliency of the SCADA against cyber attack substantially.

Physical attacks on primary equipment are not in the scope of the VIKING project neither is a more general analyses of social engineering aspects nor have we made any deeper analysis of which skills are required by the attacker. However, some of the Story Board descriptions have to include social engineering aspects to make them probable and complete, e.g. how to get access to user credentials. Other attacks are combined with damages on physical equipment due to natural forces but not coming from intentional physical attacks.

One area of attacks that we have not described as Story Boards are attacks on ancillary equipment in the control and computer rooms like uninterruptible power supplies (UPSes), air conditions, phone system, physical access system, etc. Many of these ancillary systems have an access to the Internet for maintenance or remote diagnostics mostly over an enterprise environment. An attack on the ancillary systems could easily make the control system or the control room unusable.

The Story Boards are presented in D5.3a.

4.2 A reference catalogue of security requirements ranging from SCADA system threats

As the first step in the project a reference catalogue of security requirements related to SCADA systems were developed. Figure 3 describes the method we have chosen for defining the security requirements that are the main output of this work package. A database of unsorted threats was compiled from three different sources: cyber security experts, literature and the (few) publically known cases of cyber attacks. The resulting raw threat database contains threats on very different levels of granularity and of different kinds. It is unavoidable that there are many threats that are similar to each other. However, due to its sources, it is believed that on a reasonable level of abstraction the database covers the known cyber threats. In order to abstract from the untidiness of the raw database, a set of refined threats were identified. The comprehensiveness of the refined threats is strengthened by ensuring that they cover all of the individual threats in the raw database. As a final stage, the refined threats were converted into requirements by a straight-forward syntactical operation.

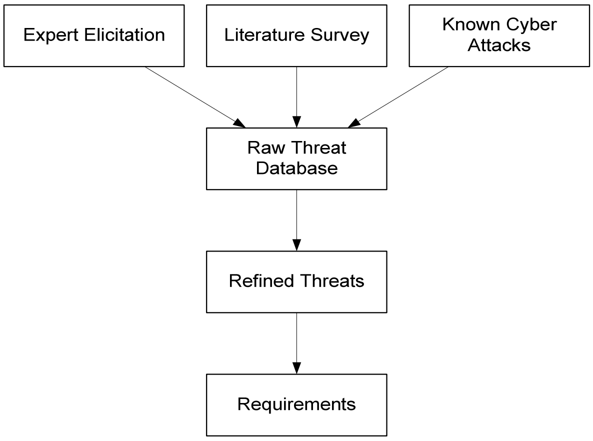

Figure 3 – The work package methodology.

For the refinement of the raw threats, the following criteria were employed:

- Conformance: It is beneficial if the refined threats comply with categorizations employed elsewhere. To ensure conformance, a set of candidate threat categorizations were identified from literature. These were then evaluated against the criteria below.

- Completeness: It is important that the refined threats cover all possible specific threats. The refined threats must cover all threats in the raw threat database. In order to ensure completeness, each raw threat is mapped to a refined threat

- Specificity: Too abstract refined threats are uninformative (the extreme would be one single refined threat to which all raw threats were mapped; it would be comprehensive but uninformative). In order to ensure the specificity and meaningfulness of the refined threats, several iterations between raw threats, categories and refined threats in both directions was necessary.

In the final step, the refined threats were transformed into requirements. This step is a purely syntactic step so that the threat "An attacker may gain unauthorized access to the SCADA network through the office network" is transformed into the requirement "The system shall not allow unauthorized access to the SCADA network through the office network".

The SCADA security requirements are reported in D1.1.

4.3 SCADA Reference Architectures

In order to have a good baseline for the analysis of SCADA systems the project has developed a number of reference architectures, i.e. commonly deployed solutions, for SCADA systems. These patterns are represented as a set of descriptions that capture the vast majority of SCADA systems' architecture on a high level. The patterns developed in the project focus on:

- Software services in SCADA systems and software services that SCADA systems exchange data with.

- Data flows among these services

- How services are placed in different network zones.

In comparison to the Cyber Security Modeling Language (CySeMoL) described in section 4.4 below, these reference architectures are describing the application level workings of a SCADA system whereas CySeMoL is devoted to the infrastructure part of the system architecture. The purpose of the SCADA reference architectures is to clarify how SCADA systems are commonly designed and deployed in practice today by employing a stringent model framework. It is thus focusing on the state-of-practice rather than state-of-art. The reason for this is that the purpose of the VIKING project starts off with the motivation to effectively enhance security in an operating legacy system environment. A state of the art solution can thus only be achieved over a very long period of time by changing different parts of the existing solution, not through a green field approach. Furthermore, emphasis is placed on control centers and data exchange with other systems and zones. The reference architectures have been identified and developed through a literature study and number of interviews with SCADA system vendors.

The reference architecture firstly contains a set of reference services of SCADA systems. These are thus services or functions that common in SCADA systems. Secondly, it contains a set of reference dataflows between the different services. These dataflows have also been described with respect to how common they are in the existing base of installed SCADA systems, according to the different vendors interviewed. Finally, a three main reference zone architectures were identified: isolated systems, single firewall architecture, and de-militarized zone architecture. For each main reference zone architecture, also a number of variants and deviations are reported with respect to what services that are located in what zone for the different vendor solutions.

Substation communication, the internal workings of SCADA systems/EMS (Energy Management Systems)/DMS (Distribution Management Systems) and the internal workings of substations have not been the focus of the reference models and only tentative models over substation architectures and wide area communication architectures have been developed.

SCADA reference architectures are further described in D2.3.

4.4 The Cyber Security Modeling Language

In summary, CySeMoL is a language (or Meta model) in which system architectures are described. The language contains general-purpose entities such as *services*, *data flows*, *operating systems*, as well as security specific entities such as *intrusion detection systems*, *firewalls* and *patch management processes*. The language also defines how these concepts can be related to each other as well as some important properties (from a security perspective) of the entities, such as for instance if an operating system is using non-executable memory or if services have known vulnerabilities. With the language, users of CySeMoL are able to describe their system architectures. In addition to this purely descriptive part of CySeMoL, a mechanism for calculating a value that could be considered a security index is also included in the language. In essence, this mechanism is an attack/defense graph, which describes how different attacks and attack steps could be performed in the system architecture and its different components. So, depending on the exact configuration of the architecture, different attack paths will be possible for an attacker to accomplish. For all those attack paths, CySeMoL provides numerical estimates for how likely it is that all the different attack steps are possible to accomplish. These estimates are given as conditional probabilities (specified in Bayesian networks). As an example, Table 2 illustrates numerical figures of conditional probabilities of how likely it is to succeed with a semantic (rather than brute force) denial of service attack on a computer given the following two parameters of the system architecture; if the targeted host has a known vulnerability and if the attacker has access credentials to the targeted host.

Software Vulnerability Present	Attacker has Access Credentials	Expected Likelihood of Attack Success
Yes	Yes	0.72
Yes	No	0.53
No	Yes	0.60
No	No	0.38

Table 2 - Conditional probabilities for expected likelihood of a semantic DoS attack success.

CySeMoL then combines a great number of such conditional probabilities of attack steps and associated countermeasures into an aggregated expected likelihood of success for the whole attack path. This aggregated value is then finally what was labeled as the security index above. A more detailed discussion about these values is provided in the next section.

Data for the CySeMoL calculation mechanism

Of course, at the core of the CySeMoL lie the conditional probabilities used for the calculations. These figures have to a large extent been collected by asking security experts in surveys on their opinions of the impact of different countermeasures on different attacks, such as the DoS example above. For all questions the explicitly stated assumption to the respondent has been that the attacker is a professional penetration tester with one week of preparation. Some of the figures are also deterministically derived, and some have been derived from previously published studies. In total four surveys has been conducted on various parts of the CySeMoL with answers from 165 respondents as maximum and a handful of respondents as minimum. In order to identify qualified respondents (identifying which experts that really are experts) Cooke's classical method has been used. This method essentially weight different respondents depending on how good they are at answering some test questions relevant to the area of the survey questions (that the CySeMoL developers have known the answers to). This means that only a few of the for instance 165 respondents mentioned above performed good enough to be called experts. A philosophical note worth mentioning is that Cooke's method tries to identify the true answer to questions rather than to have a large amount of answers to generalize from. If the truth is found it does not matter how many respondents that have stated it. All answers, i.e. conditional probabilities, have been collected also including the respondents' opinion on the uncertainty of the answer (expressed as a three point estimation). For instance, for the first estimate in Table 2 above the average answer (of the respondents selected as the "true experts") is 72%. However, there is a 5% chance that the value is below 32% (again, on average) and a 95% chance that the value is below 95% (on average). Another way of expressing it would be that there is a 90% chance that the attack success value is between 32% and 95%. As we can see from this example the figure 72% here is acquainted with a large share of uncertainty. However, in the calculations made in the present version of CySeMoL only the expected mean value is used, i.e. 72% in the example above.

Intended usage of CySeMoL

The intended usage of the CySeMoL is to support security analyses of SCADA and control system architectures. It should support users that are not necessarily security experts themselves. If the user provides a system architecture, the CySeMoL can provide a security estimate in terms of attack probabilities. So, by analysing different architectures and different attack processes the user can get a better understanding of available weak spots in the architecture. In addition, it also provides a clue on how effective different mitigation strategies (probably) are. As described above, the figures provided are often acquainted with quite big uncertainty. This imposes that the calculated percentage value figure should be treated with care. The results should be seen as a support for reasoning about different alternative scenarios or mitigations. On average a scenario with attack success probability of 10% is more resilient towards the analysed attack process than one with 30%, even included the uncertainties (that in general are the same magnitude for scenarios). Essentially the user needs to define two things: 1) the system architecture (including a number of properties), and 2) which targets they would like to analyse as well as starting points for the attacks. I.e., CySeMoL delivers results for (the most probable attack path between) pairs of a single starting point and a single target. But, in order to get a more complete and holistic understanding of the whole architecture several such pairs needs to be considered. Again, comparing scenarios without analysing the complete set of potential pairs will provide an indication of their relative security.

Since the CySeMoL is quite large and complex, it is extremely time consuming to do the calculations by hand. Thus, all examples in the project have used the Enterprise Architecture Analysis Tool (EAAT)[1] to calculate the results and visualize the models. The EAAT as such is however not developed within the VIKING project.

Notes on the objectivity of the CySeMoL.

The correctness of results of the CySeMoL is to a large extent determined by the empirically collected conditional probabilities. A wide range of experts, both academic and practitioners, have been involved in the validation process. In the survey, Cooke's classical method has been used which is the state of the art method for expert knowledge elicitation. The method does not accept anyone as an "expert" but test all respondents with a test questions. Before, the surveys were sent out the parameters that were included in the survey was also validated with respect to their importance in a qualitative way by cyber security professionals. Both of these actions ensure the correctness in the details of the CySeMoL. Furthermore, the aggregated results (the attack path estimations) of the CySeMoL have also been validated through a Turing test. In the Turing test, both cyber security professionals and the CySeMoL were asked to assess a number of scenarios. All these assessments were then given to another group of cyber security professionals to judge if they believed that the results seemed reasonable (without knowing who produced the assessment). CySeMoL performed equally well in comparison to the cyber security professionals (it was neither best nor worst and everyone was performing in the same "magnitude").

Nevertheless, it is important to realize that the figures are "soft facts" rather than "hard" statistical data. This is due to the fact that no statistical data is available for the scope of CySeMoL and it is not feasible, given the limited time of the VIKING project, to produce a sufficient amount of new data with better quality than the surveys. This means that we have ended up with much uncertainty in the results. This uncertainty is likely to reflect both that more detailed information about the system architecture is needed in order to make better predictions, but also that the answers to the questions that CySeMoL addresses are simply not known. (It could of course also be that the wrong people were asked. But this has at least carefully been tried to avoid by using a well-known scientific methods.)

[1] KTH - Royal Institute of Technology, Enterprise Architecture Analysis Tool homepage, www.ics.kth.se/eat

In many aspects CySeMoL can be enhanced and complemented in future works. By removing the following currently used assumptions CySeMoL could be improved:

- The attacker has been simplified to one type of attacker with a lot of variance related to it. So how well these figures represent advance persistent threats or script kiddies needs to be further studied.
- The focus of CySeMoL is on addressing the availability and integrity objectives of the system rather than protecting the confidentiality (due to the SCADA and control system focus of the VIKING project). Thus, in the current version, countermeasures related to deterrence and recovery is not yet considered.
- The focus of CySeMoL is mainly on technical parts of security. Thus, other type of cyber security attacks that involves non-technical aspect, e.g. social engineering, information security governance and physical attacks are treated in a very rudimentary in this version.
- The conditional probabilities that produce the CySeMoL results needs to be updated from time to time as knowledge of both attackers and defenders change over time. CySeMoL reflects a snapshot of knowledge dated approximately to 2010.

Despite the abovementioned limitations, we believe that CySeMoL provides significant contribution in providing a systematic approach for analyzing the cyber security of SCADA and control systems. From an academic point of view this delivery should not be considered the end of CySeMoL but rather the beginning.

The CySeMoL is further described in D2.2, and report on its application is found in D3.1.

4.5 Automatic Generation Control (AGC): Attack and Mitigation Strategies

Power systems are divided into control areas, each of them supervised and controlled by a SCADA system. These areas could be either entire countries or, as in Germany, parts of the same country.

Within the SCADA environment, measurements of frequency, voltage and current at different points of the network are taken and are sent through communication channels to the control centre. The SCADA system processes the collected information and alerts the operator if needed. The Transmission System Operator (TSO) has then the ability to control one or more of the system variables like the status of the switches, the generator voltage and power set points, the tap changer ratio of LTC transformers or other configuration settings. This interaction raises security issues, since attack scenarios can be based on the manipulation of the above mentioned variables and can potentially cause catastrophic economic and social effects.

The Automatic Generation Control (AGC) is one of the few control loops that are closed over the SCADA system without human operator intervention. The primary objective of the AGC is to regulate frequency to the specified nominal value and maintain the power exchanged between the controlled areas to the scheduled values by adjusting the generated power of specific generators in the area. AGC actions are usually determined for each control area at a central dispatch centre. Measured system frequency and tie line flows are sent to this centre; a feedback signal that regulates the generated power is computed and sent to the generators participating in the AGC through the SCADA system. The absence of the human in this control loop increases the vulnerabilities of the power system due to a potential cyber-attack that can manipulate this control signal.

To reveal these vulnerabilities, we conducted research to analyse the safety of the system in the case that an attacker has gained access to the AGC signal of one control area and is able to inject an undesirable input to it. The first aim was to verify whether it is possible for the attacker to use the AGC signal to lead the system states out of their safe operating limits: cause generator tripping by making the frequency in one are unacceptably high, or load shedding by making the frequency too low, or tie line tripping by disturbing the regulated power flow or causing power oscillations between the areas. Afterwards, we attempted to construct the attack signal that could indeed destabilize the system. To help the SCADA system to react rapidly after such an attack, mitigation strategies were designed, in the form of fault detection and isolation filters that raise an alarm if an attack is detected and/or automatically disconnect the AGC returning the system to stable (albeit suboptimal) operation. To achieve these objectives, appropriate power system modelling methodologies had to be developed, including large scale modelling and proper reduced models. In the sequel, a short description, towards our research on the above mentioned topics, is provided.

Verification analysis

We first determined whether there exists a signal for the attacker that could irreversibly disturb the system. Toward this objective, we developed a new framework and defined a systematic methodology, based on reachability analysis, for identifying the impact that an intrusion in the AGC might cause to the power system. For this analysis we considered a two-area power network. A dynamic nonlinear two-machine frequency model, which is suitable for load-frequency studies for the two interconnected areas, was developed to represent the two-area power system. The results of this study showed that there exist suitable control signals that the attacker can feed to the system instead of the AGC commands and cause the system trajectories to violate the safe operational envelope. In the deliverables D2.5 and D3.2 we described the basic steps of the developed methodologies and provided numerical results to support our findings.

Robust attack policy design

Having verified the existence of an attack policy which can destabilize the system, we tried to synthesize such an attack signal. Simulation results quickly revealed that the attack signal cannot be random, but has to be optimized if it is to cause significant disruption. To this end an open loop procedure, based on Markov Chain Monte Carlo optimization, was considered to identify an optimal attack signal. Motivated by the fact that the results are very sensitive to parameter uncertainty, a systematic algorithm, based on feedback linearization, and was then proposed to construct a feedback policy that an intruder may use to disrupt the network. Since in practice an attacker would only have partial information about the parameters of the power system and the values of its states, a nonlinear observer was designed and a sensitivity analysis was carried out to quantify the effect of the parameter uncertainty and model mismatch.

The feedback policy was successfully applied to a two-machine power network. We then introduced the attack signal to a four generator power system which exhibits inter-area and intra-area modes. For a more realistic implementation we then applied the same policy on the large scale IEEE 118-bus network which was divided arbitrarily into two control areas. For the latter, since the policy for the construction of the attack signal could be only applied to a low order system, a methodology to appropriately reduce the large scale network to a simplified one that maintains the most valuable information that an attacker would need, was developed.

Figure 4 shows the overall structure of the attack approach. The attack signal was generated following our proposed method using the appropriately reduced model of the large scale network, and served then as feedback to the IEEE 118-bus network through the manipulated AGC signal of one of the two areas.

The proposed methodology and the basic results are documented in D3.2.

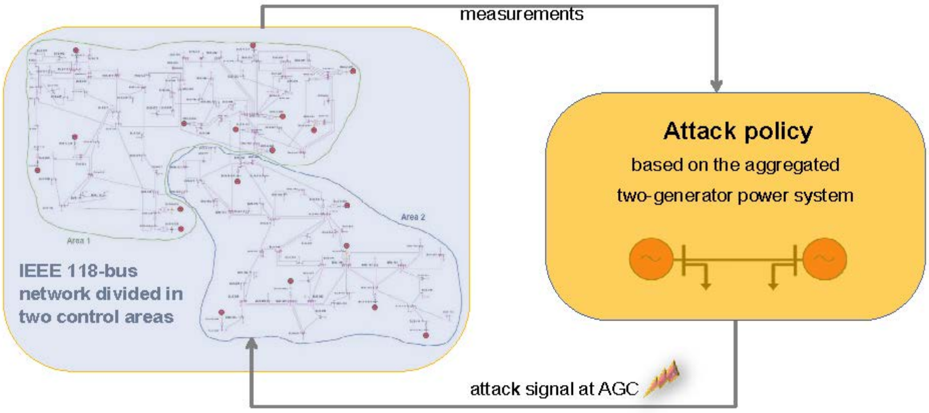
measurements
Area 1
Area 2
IEEE 118-bus network divided in two control areas
Attack policy
based on the aggregated two-generator power system
attack signal at AGC

Figure 4 - Attack signal loop. The attack signal generated by the two-machine power system is applied to the IEEE 118 bus network.

Mitigation strategies

On an attempt to identify possible counter-measures against an intrusion in the AGC, ETH proposed a novel methodology to enhance the cyber security of the AGC during normal operation. Although both the AGC signal and frequency measurements can be continuously monitored in the control room, it is not obvious how to assess whether an abnormal behaviour has occurred due to a normal load deviation, or as a consequence of an abnormal AGC intrusion. Since an AGC attack may lead to load shedding or generation tripping in less than a minute, it is crucial to diagnose the AGC intrusion sufficiently fast before any disruption in the system. If the intrusion is detected on time, one may limit the damage by disconnecting the AGC.

A protection framework was developed by designing a Fault Detection and Isolation (FDI) filter to evaluate the AGC consistency in order to diagnose an intrusion action. This FDI filter is constructed based on a model of the power network utilizing available measurements from different parts of the system. The diagnosis filter is insensitive to normal perturbations, such as load changes of the network, and highly responsive to any exogenous intrusion in the AGC signal.

For the needs of the FDI analysis, both the non-linear and the linear multi-machine frequency model of a large scale Two-Area power system were developed.

Figure 5 illustrates the performance of the FDI filter applied to the nonlinear frequency multi-machine model of the IEEE 118-bus power network (including 59 dynamic states).

The filter is fed by measurements of the generator frequencies and the mechanical power of the turbines.

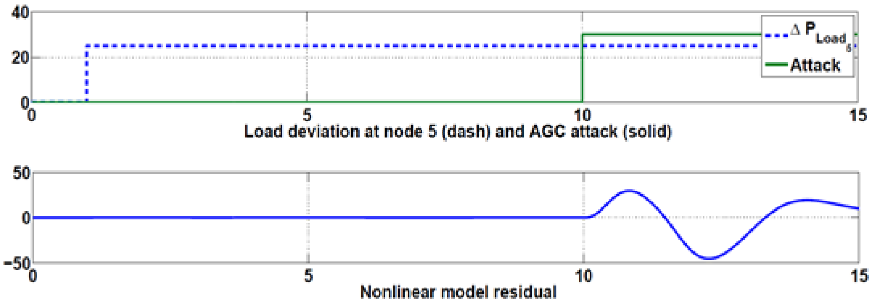

Figure 5 - FDI filter response

The figure in the top panel depicts a scenario with two signals: a load change at node 5 of the network at 1 sec, and an intrusion signal additive to the normal AGC signal starting at 10 sec. The second figure demonstrates the filter reaction in this scenario. Even though the load change at node 5 leads to deviations in some generators frequency, the FDI filter recognizes that this corresponds to normal behaviour and does not react to it. However, the filter successfully differentiates the frequency deviations cause by the abnormal AGC signal after time 10 sec, and immediately reacts.

The proposed methodology and the corresponding results are documented in D4.2.

4.6 State Estimator-based Attacks and Mitigations

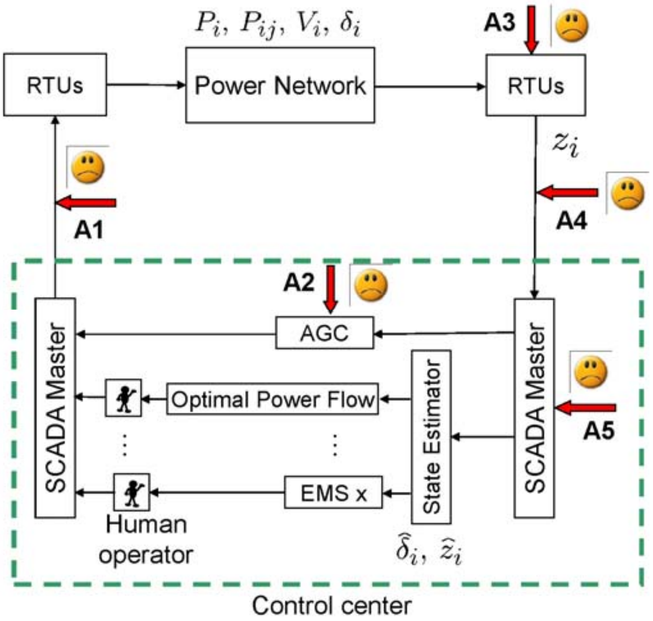

Figure 6 - A schematic block diagram of a power network, a SCADA system, and a control center.

In Figure 6, a schematic block diagram of a modern power network control system is shown. Note that the figure presents a very simplified picture of these complex systems, and only components explicitly treated in this part of VIKING are included. The power network models we consider are on the transmission level. They should be thought of as large and consisting of up to hundreds of buses that are spread out over a large geographic area (a region in a country, for example). We have here mainly considered the VIKING country network, which consists of 40 buses.

To monitor and control the behavior of such large-scale systems, SCADA systems are used to transmit measurements, status information, and circuit-breaker signals to and from Remote Terminal Units (RTUs) that are connected to substations. The technology and the use of the SCADA systems have evolved quite a lot since the 1970s when they were introduced. The early systems were mainly used for logging data from the power network. Today a modern system is supported by Energy Management Systems (EMSes) such as automatic generation control (AGC), optimal power flow analysis, and contingency analysis (CA), as is indicated in Figure 2. For such large-scale systems, lost data, failing sensors, or lack of sensors in certain areas, are common. The incoming data is therefore often fed to a so-called *state estimator* (SE) which provides EMS and the human operator in the control center with hopefully accurate information at all times. For example, the SE will provide estimates of power flows and injections that are not even measured. To remove faulty data possibly due to noise, the state estimator is supplemented by its Bad Data Detection (BDD) system. The BDD system works by checking that the received measurement data reasonably well matches a physical model of the power network. However, as SCADA/EMS systems are increasingly more connected to office LANs in the control center, these critical infrastructure systems are potentially accessible from the internet. The SCADA communication network is also heterogeneous and consists of fiber optics, satellite, and microwave connections. Data is often sent without encryption. Therefore many potential security threats exist for SCADA/EMS systems. In particular, we have here studied how an attacker can inject false data at points A3-A5 in Figure 6, while avoiding triggering the BDD system. This means the state estimator will provide false state information to the human operator, while he/she does no warnings. Hence, the human operator could be fooled to for instance destabilize the system or to run it in a non-optimal operating point. The data attack A3 could be conducted by an attacker that hijacks an RTU in the field to transmit false data. The data attack A4 could be conducted by an attacker that intercepts the communication going to the control center. Finally, the attack A5 could be conducted by an attacker that accesses the database in the SCADA master system.

Our first contribution in this area we presented in Deliverable 4.1. There we introduced security indices that measure how hard it is to perform undetectable false-data attacks against the SE, as described above. One index measures ”attack hardness” by counting the minimum number of sensors that needs to be corrupted together with the target sensor to avoid detection by the BDD system. An important conclusion is that redundancy measures based on the commonly used “hat matrix” can be misleading. Hence, the introduced index gives a more reliable picture of a system’s security against false-data attacks. The second contribution in Deliverable 4.1 is that we study the problem of how to allocate a limited number of protected measurement devices. To measure the effect of the allocation, we used the introduced security index. We suggested three different greedy-type algorithms for allocation. By means of example, we showed that even with a rather small number of protected measurement devices, it is possible to obtain so-called perfect protection. Perfect protection here means that there is no longer a feasible undetectable false-data attack on the system.

In Deliverable 3.2, we then verified the feasibility of the data attacks against the SE in the VIKING country 40-bus system by conducting experiments in the VIKING test bed. We provided a comprehensive framework to analyze and study the impact of a class of stealthy deception attacks targeting the SE component through measurement data corruption. The results obtained by these experiments showed that computations based on linear models of the system provide valid attacks that successfully corrupt the target measurements without triggering any BDD alarms. The results also indicated that linear models can be used for large attacks as well, although otherwise expected. This study showed that improved BDD schemes and methods to ensure measurement and data protection are desirable, and this was further studied in Deliverable 4.3. It should be emphasized that the attacks considered in Deliverable 3.2 exploited an inherent weakness in BDD system algorithms, and does not indicate weaknesses in the specific test bed used.

In Deliverable 4.3, we showed how normal BDD schemes can be complemented with a simple test which checks a special model mismatch on the measured reactive power flows. The test can be used to alert the operator of the “undetectable” false-data attacks, and warn him/her that an attack is in progress. In addition to this, we provided some analysis tools that can be used to estimate the magnitude of possible undetectable false-data attacks based on the model knowledge of the attacker. This can be useful for tuning thresholds in BDD schemes. We also showed how one can estimate the economic impact of SE attacks by using the Optimal Power Flow (OPF) algorithm. The idea was demonstrated on the VIKING 40-bus network, which was also used in Deliverable 3.2. We showed that many of the possible undetectable false-data SE attacks do not seem to have severe economic consequences, but some of them indeed can increase operational costs, especially if they affect measurement data close to generators.

4.7 Novel and Secure Power System Communication Solutions

There is a wide variety of communication infrastructures and a protocol used in power system communications, both between the substations to the control centres and between the control centres themselves. As an example, substation to control centre communications, which is essential for power system state monitoring and control, is often performed over low bitrate point-to-point connections (e.g., using modems) but it is also performed over high speed optical communication networks. There is also a variety of application layer protocols, from proprietary protocols to recently standardized ones (e.g., DNP3 or IEC 60870-5). Some of the application layer protocols have been extended to support authentication and confidentiality, but deployments are slow. Nevertheless, the actual communication network topology and the application layer protocols used have an impact on the vulnerability of the power system, as explained on the example of power system state estimation in the following.

The attack model used in the previous subsection assumed that each individual measurement can be subject to attack at a unit attack cost. While this is theoretically interesting to consider, such a model is not very realistic. In reality, each measurement datum is obtained by a transducer, which converts voltage or current measurements into optical or low-voltage signals, which are then sampled. The sampled data are transmitted through the process bus (often some kind of Ethernet network) of the substation automation network to the RTU located at the substation. The RTU then transmits the data to the control centre over the SCADA communication network. Depending on the system configuration, the transmission can be triggered by the control centre (if it polls the RTU) or can be initiated by the RTU when certain conditions are met. To manipulate the measurement data, an attacker could get access to the process bus or to the SCADA communication network, and in either case he or she would be able to modify several measurement data at unit cost. Thus, the topology of the communication infrastructure influences the cost of performing an attack and the cost of mitigation. We use two example communication network topologies to illustrate how.

The first example network topology is a star topology, in which every RTU communicates to the control centre via a point-to-point link. This model can be suitable for legacy SCADA systems that rely on leased lines and the Plain Switched Telephone Network (PSTN) for communications. In this model, an attacker can modify all data sent by an RTU at unit cost by attacking the corresponding communication link. Similarly, the operator can protect all data sent by an RTU at unit cost by authenticating the data (e.g., by installing an RTU that supports authentication). If this cost model is used, the cost of performing a targeted attack against a measurement becomes significantly lower, but so does the cost of mitigating targeted attacks. Furthermore, it is possible to identify a set of communication links or RTUs, such that if they are protected, the system cannot be attacked. This set can be found efficiently by starting from a dominating set of the substation-level power system network topology (that is, a set of substations such that every substation is either a member of the set or adjacent to a member of the set). The cardinality of this set of substations is significantly lower than the cardinality of the set of measurements that have to be protected if one assumes that each measurement can be attacked at unit cost.

The second example network topology is a mesh topology, in which communication links run along transmission lines between the substations and the measurement data from a substation are potentially routed via other substations to the control centre. This model can be suitable for more recent SCADA systems that rely on optical ground wire

(OPGW) cables running between the tops of high-voltage towers, and on Synchronous Optical Networking (SONET) or Synchronous Digital Hierarchy (SDH), to establish logical circuits between the substations and the control centre. Since data are routed via substations, an attacker who gets access to the switches at a substation can potentially manipulate the data carried over all circuits traversing that substation. Thus, by successfully attacking the communication equipment at a single substation, an attacker might be able to perform successful attacks against several other substations. In addition to adapting the attack cost metric to this topology model in order to capture the number of substations that need to be attacked, one can also define a metric that captures the number of attacks that could become possible through an attack on a single substation. Results show that the cost of attacks is significantly lower under this network topology, and many attacks become possible through getting access to a single substation. However, the complexity of the network topology not only makes attacks easier, but it also opens up new opportunities for mitigation. For example, an operator can change the routing of the data through the network, or can introduce multi-path routing to increase the attack cost.

The security of the state estimator can not only be violated through the injection of false data. An attacker could block the communication between substations or between control centres that perform, e.g., distributed state estimation over large geographical areas. One way to mitigate such attacks is to relay data between the control centres. If relaying is done in a sufficiently randomized manner then it would be difficult for an attacker to identify the sender and the receiver of a message. The protocol standardized for information exchange between control centres, the Inter Control centre communication protocol (ICCP), allows associations to be relayed over control centres, so that a mixing network could potentially be used to hide the identity of the sender and the receiver of an ICCP association from an outside attacker.

Nevertheless, a mixing network introduces the possibility of inside attacks: due to the long lifecycles of SCADA systems software corruption is a threat, and the complexity of the code-base makes corruption hard to detect. A compromised control centre can reveal the routing information of the mixing network and thereby it can enable attacks despite using a mixing network. One possible solution to mitigate the attacks even in the presence of compromised control centres is to use anonymity networks to establish overlay routing paths among the control centres. An anonymity network hides the sender and/or the receiver of the messages routed through the overlay from the relaying nodes, and thereby it makes it difficult for an inside attacker to identify the associations between the nodes. Depending on whether it is the sender, the receiver or the association between a pair of nodes that is to be hidden, an anonymity network can be designed to provide sender, receiver or relationship anonymity, respectively.

Mixing networks and anonymity networks help mitigating attacks, but they come at the price of increased data rates and end-to-end delay. Increased data rates lead to increased communication costs, while long delays are undesirable for time-sensitive data; hence the mixing and anonymity networks have to be configured appropriately. Ideally, one would like to maximize the anonymity provided by the system, but at the same time have low overhead. While these two requirements might be contradictory, interestingly we found that it is not always the highest overhead that leads to the best relationship anonymity. Another important aspect of anonymity networks is that the optimal overhead is a function of the number of compromised nodes. This is, however, unknown. Hence, the optimal system parameters are hard to find in practice. Our results showed, however, that if the number of compromised nodes is unknown then it is best to optimize the system for a high number of compromised nodes, as doing so will results in a system that is less sensitive to the actual number of compromised nodes.

More detailed information can be found in Deliverable D4.2.

4.8 The Virtual City Simulator – A model for calculating societal costs of incidents

In this summary a comprehensive method for the assessment of costs and consequences caused by disturbances in the critical and vital infrastructure of a society is presented. The assessment is based on a virtual society. This society is a simplified but still functioning virtual society. It has static as well as dynamic properties. It has the vital features of a society. The virtual country is created by a software product – ViCiSi, the Virtual City Simulator. ViCiSi has been applied in the Viking-project and the created virtual country is named Viking Country.

The scope of ViCiSi can be summarized in this fictitious telegram:

Telegram from VBC (Viking Country Broad Casting): *"A local outage, with the Impact Magnitude 6.8, has occurred in part of the Viking Capital. About 380.000 inhabitants had an outage this afternoon. The societal cost to the Viking Country is estimated to 8.2 million Euros. VPT, The Viking Power Transmission company, reported that power was restored to everyone at eight o'clock."*

The content of ViCiSi is how the figures in the telegram are assessed.

The ViCiSi is capable of modeling a simplified society, with only the vital features of a society. It has static as well as dynamic properties reflecting societal and business activities and critical infrastructure on an individual object level:

- Necessary infrastructure like blocks, apartments, streets, electricity grids etc.
- Companies, public and private service operations producing welfare.
- People living in the city, having a comfortable life and consuming welfare.

The ViCiSi further relates power demand to an economic life; business activities to consumption of welfare, and all activities are specified in terms of production or consumption of Gross Domestic Product (GDP). Each individual object in a ViCiSi virtual society has individual power demand profiles and business activity profiles specified for a time period specified in the system. With this capability a ViCiSi virtual society can:

- Measure the lost power production and lost consumption of welfare
- Measure the economic activity in the society by measuring the production and consumption of welfare

Thus, the assessment of societal costs calculated by the ViCiSi is comprised of an extensive impact cost calculation, based on GDP and business activity profiles. The calculations are summarized in D3.3.

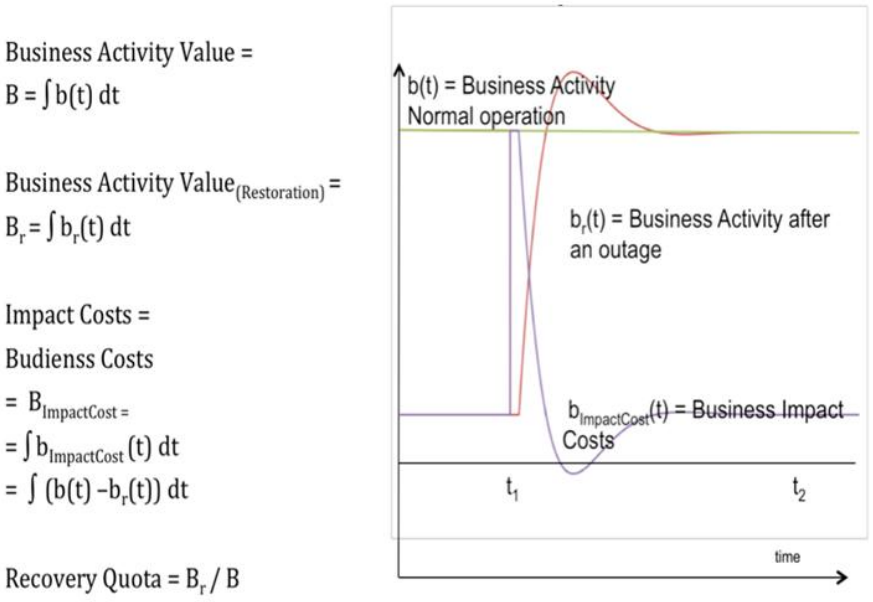
Business Activity Value =
$B = \int b(t)\,dt$
Business Activity Value$_{(Restoration)}$ =
$B_r = \int b_r(t)\,dt$
Impact Costs =
Budienss Costs
= $B_{ImpactCost =}$
$= \int b_{ImpactCost}(t)\,dt$
$= \int (b(t) - b_r(t))\,dt$
Recovery Quota = B_r / B
b(t) = Business Activity
Normal operation
$b_r(t)$ = Business Activity after an outage
$b_{ImpactCost}(t)$ = Business Impact Costs
t_1
t_2
time

Figure 7 - Summary of the ViCiSi impact cost calculations.

In addition to the economic calculations of the ViCiSi, a qualitative non-monetary societal impact magnitude index has been developed in the project. In this index the society is viewed and assessed from a micro perspective and a macro perspective. From the micro perspective, i.e. from the individual standpoint, the length of an outage is the most interesting dimension. In the micro perspective an outage means the loss of welfare, inconvenience, problems with transportation, no fuel at the gas station, problems with emergency calls etc. The number of affected people is not assessed in the micro perspective. From a societal standpoint - or the macro perspective - the consequences are dependent of the number of affected people. The magnitude of those risks is related to both the number of affected persons and the length of the outage. The micro dimension is covered by the so called Disturbance Length Order. The number of influenced people is covered by the Impact Incidence. Finally, these two dimensions are combined into the Impact Magnitude dimension.

The Impact Magnitude is defined in such a way that

Impact Magnitude = Disturbance Length Order + Impact Incidence

The range of Impact Magnitude is [0, ≈10+]

The range of Disturbance Length Order is [0, ≈5+]

The range of Impact Incidence is [0, ≈5+]

The definition of Impact Magnitude has similarities with the Richter Magnitude Scale, used for assessing earthquakes and is illustrated in Figure 8.

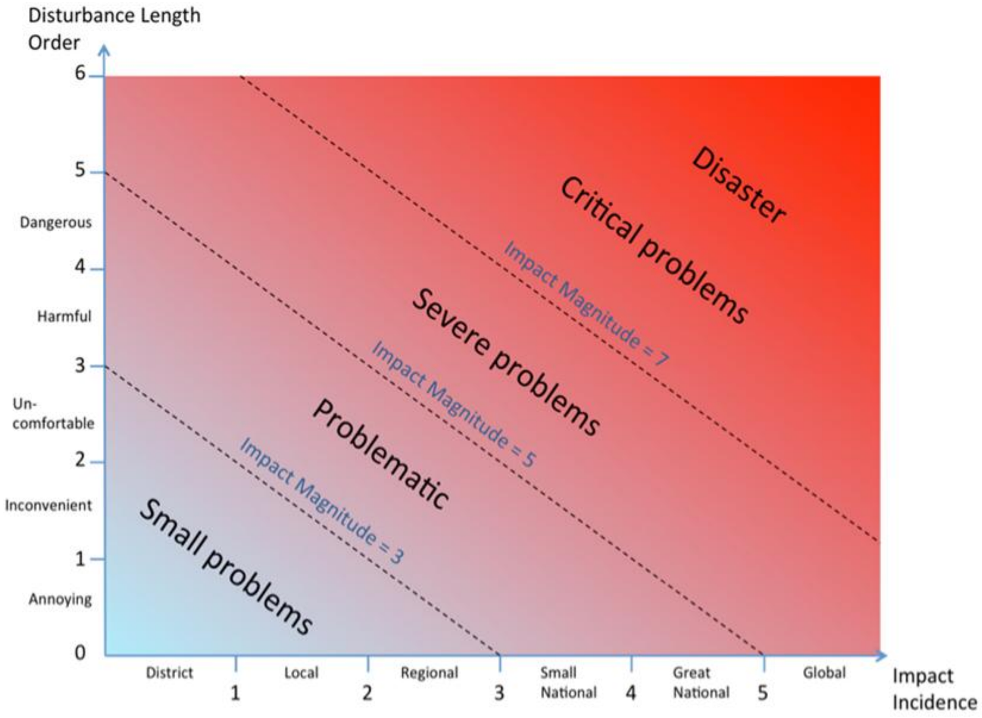

Figure 8 - Illustration of the Impact Magnitude

ViCiSi and the assessment of Impact Cost and Impact Magnitude have in the VIKING project been used for modeling the impacts of electric power outages. In the next step – outside the VIKING project – the aim is to implement also other critical infrastructures, such as water and wastewater distribution, telecommunications and transportation. The final goal is to use ViCiSi as a test bed for the dependencies of vital infrastructure.

The ViCiSi and the Impact Magnitude index have been reported in D3.3.

4.9 The VIKING Testbed

The main objective of the developed test bed is to demonstrate cyber attacks on a SCADA system and the corresponding consequences in the power grid and on the society in a virtual environment.

The VIKING Test bed has the following objectives:

- Demonstrate to project stakeholders cyber attacks on SCADA systems and their consequences in the power network and in the society.
- Internal use for the VIKING security research and to investigate mitigation alternatives.

- Verification of models, tools and methodologies developed for VIKING purposes.

VIKING test bed functional overview

The VIKING test bed consists of components from a real-life SCADA system and simulated components that use models to represent reality.

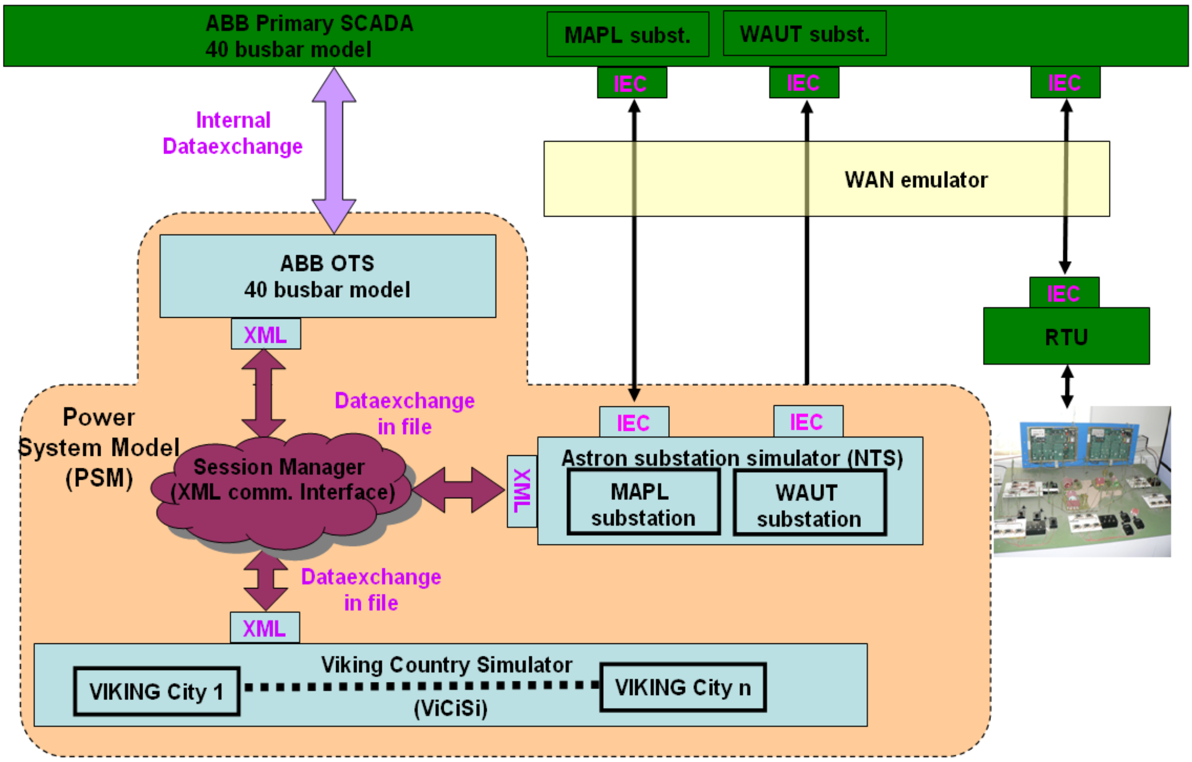

Figure 9 - Testbed functional design.

The real-life components of the Testbed are the following (which marked with green color in Figure 9):

- The ABB SCADA system is located in the top of the VIKING test bed hierarchy. This system could be the main target of the possible attacks. With this SCADA system the test bed user is able to monitor and control the transmission network part (400 and 220kV) and also the distribution network part (120, 40 and 10kV) of the VIKING power network. This SCADA/EMS system consisting of redundant SCADA servers, Front Ends, Operator Workstations and a redundant Local Area Network. The SCADA/EMS system software includes SCADA application with data warehousing plus advanced power system applications for a high voltage Transmission System. The SCADA system also has IEC 870-5-104 communication interfaces for the internal communication (for example to communicate with the NTS and remote terminal unit (RTU).

- Remote Terminal Unit (RTU), for collection of process data and communication to the SCADA system.

The Power System Model (PSM) contains the modeled components of the Testbed. The PSM model part of the Testbed is simulating the transmission and distribution electrical network (including substations, generations, transmission lines, transformers, switching devices, loads, etc.) and the detailed society model which is fed with electrical power by the transmission and distribution network. The components are the following:

- ABB Operator Training Simulator (OTS), which contains a high voltage transmission power system model. This is a semi-dynamic model that models quasi-stationary characteristics of primary electrical components, e.g. rotating masses in generators. It includes generation control to balance generation to loads. This model based on the ABB 40 bus bar power system model.

- Substation (Network) Simulator (NTS), which models the internal configurations, the switching equipment of two high / middle voltage electrical substation including operation of protections, automations and interlocks. The Substation Simulator also models 40KV/10KV feeders and the corresponding field devices.

- Society simulator (ViCiSi). ViCiSi calculates the electrical loads in the society on different load points for different times and voltage levels. As described in the previous chapter, the main objective of ViCiSi is to calculate the consequences of outages in the society in the form of cost for missed BNP production. ViCiSi can be parameterized to model different countries inside the European Union using load and society statistics.

In order to control the flow of data between the PSM components of the Testbed (OTS, NTS, ViCiSi) and the execution of the corresponding programs, a control program was required, which called Session Manager (SM). The session manager on one hand provides an XML interface between the collaborative Power System Model (PSM) parts and on the other hand controls and schedules the simulation processes.

Wide Area Network emulator (WAN emulator) It emulates the communication traffic between NTS / RTU and ABB SCADA system. The reason to use an emulator in the Testbed is to enable the possibility to disturb the communication with the Denial of Service (DoS) attacks in order to blind the SCADA system and to introduce false telegrams in the traffic to and from the SCADA.

The Testbed is physically located at KTH in Stockholm.

VIKING Testbed in use

Inside the VIKING project itself the VIKING Testbed provided a virtual environment, where different type of potential cyber attack was possible to execute. In other hand the consequences of these attacks and possible mitigations on the SCADA and the power system, turned into analyzable using the ViCiSi and the test bed features. The "Report on case studies" document (D5.3 delivery) described the results of these examinations.

Beyond the VIKING project the VIKING Testbed gives platform:

- For educational purposes (for university students as well as industry)

- To validate SCADA product enhancements (for example Bad Data Detection)

- To organize awareness trainings for system operators.

- For demonstration purposes

In the deliverable D5.3c a functional and design description of the VIKING Testbed is found.