The VIKING Project: An Initiative on Resilient Control of Power Networks

Annarita Giani, Shankar Sastry
Department of Electrical Engineering and Computer Sciences
University of California at Berkeley
Berkeley, CA USA
{agiani, sastry}@eecs.berkeley.edu

Karl H. Johansson, Henrik Sandberg
School of Electrical Engineering
Royal Institute of Technology (KTH)
Stockholm, Sweden
{kallej, hsan}@ee.kth.se

***Abstract*—This paper presents the work on resilient and secure power transmission and distribution developed within the VIKING (Vital Infrastructure, networKs, INformation and control system ManaGement) project. VIKING receives funding from the European Community's Seventh Framework Program. We will present the consortium, the motivation behind this research, the main objective of the project together with the current status.**

I. Introduction and Motivation

Supervisory control and data acquisition (SCADA) networks contain computers and applications that perform key functions in providing essential services. In this project we concentrate on SCADA networks for power systems. SCADA systems are continuously becoming more advanced and complex. Simply put, more effective infrastructure operation requires more accurate process models, which in turn require more advanced functionality and elaborate data collection and processing in the control systems. The result is increased internal technical complexity of the control systems. In addition to the external infrastructure operational requirements, the technical evolution of the systems is also driven by the technical evolution in IT in general; new services and solutions are constantly developed and existing ones are enhanced. This further increases the complexity of the overall systems. However, the increasing internal complexity of the systems is not the most challenging trend today. Instead, it is the fact that SCADA systems are no longer isolated but that they are extensively networked with other information systems of the company that forms the greatest challenge. These networks and corporate IT networks are often connected to enable engineers to monitor and control the system from points on the corporate network. Also corporate decision makers can obtain instant access to critical data about the system status.

Examples of important security areas in modern integrated SCADA systems are for instance: communication networks to the process; control centers and their computers; connections for software maintenance and remote diagnostic from system vendors; communication to other control centers; the office LANs and their systems; firewalls separating different networks, including the Internet, see Figure 1.

In VIKING we propose to address this challenge by developing cyber-physical models that specifically address the interaction between the (cyber-) IT systems and the (physical) power transmission and distribution systems, see Figure 1. We propose to use methods from the area of hybrid systems for this task. Hybrid systems [1] have been a topic of intense research for the past decade, in the boundary between computer science and control engineering. They provide a unified framework for jointly modeling continuous systems (like the power transmission and distribution processes) and discrete systems (like the SCADA systems). Our team is in a unique position to apply this methodology to the power transmission and distribution systems, since it brings together teams that have pioneered developments in the area of hybrid systems with teams that have extensive experience on the modeling of the physical and the IT systems themselves. The approach of VIKING is to enhance data integrity, reliability and robustness of SCADA systems through the development and application of such a rigorous modeling and analysis framework. This type of holistic approach with hybrid models has up to now not been used for modeling these types of system with the goal of examining security aspects of the complete and integrated system. The aim of VIKING is to advance the state of art from examining and testing existing systems for security problems to model-based analysis and prediction of the security state of SCADA systems.

We are aware of other efforts in the same field. CRUTIAL (CRitical UTility InfrastracturAL resilience) [2] is a FP6-IST project funded by the European Commission that focus on the interaction between SCADA and power systems. However, their approaches are significantly different from ours. VIKING considers not only vulnerabilities in SCADA and power systems, but also the effects of the exploitation of these vulnerabilities in terms of the effects on electricity users, in terms of extent of potential outages, etc. as well as the costs of these effects. Also we will be employing modelling approaches that differ from CRUTIAL. Although CRUTIAL featured architectural modelling of SCADA systems, VIKING will combine these with probability-based security assessment approaches. VIKING will also explore the potential of cyber-physical modelling frameworks within the frame of SCADA system security. These hybrid system models integrate the

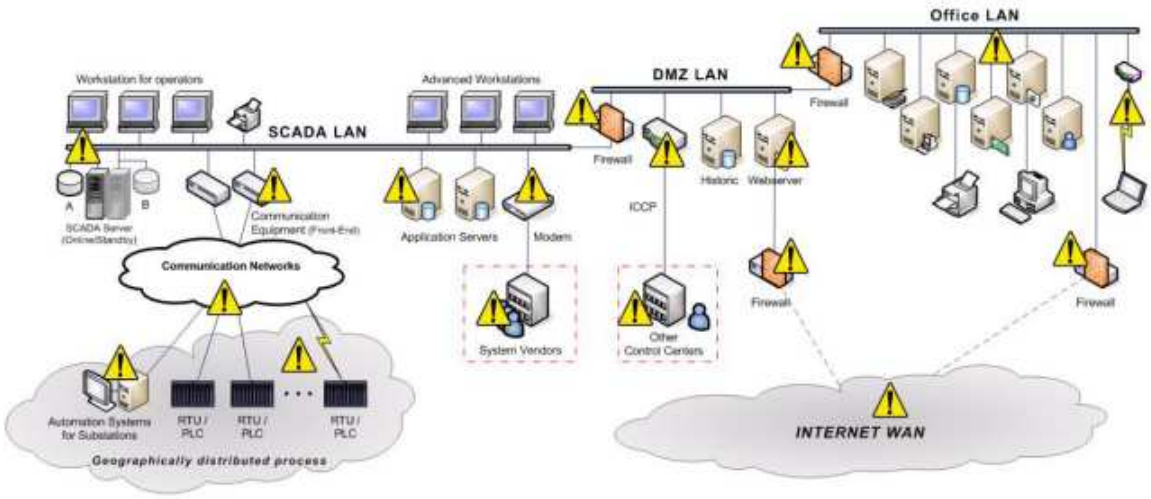

Fig. 1. Complex interconnected networks.

logics and discrete events of the SCADA system with the continuous dynamics of the physical power transmission and distribution networks in a way that has not been done with previous models. A comprehensive detailed list of the European Electricity Projects can be found in [3].

Also the United States focuses in developing an effective critical infrastructure protection and resiliency plan. Academic organization work with the private sector to ensure that targets are protected against all hazards. TRUST [4] is a NSF project focused on the development of cyber security science and technology that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for the nation's critical infrastructure. It addresses next generation SCADA and other networked embedded systems that control critical physical infrastructures and futuristic infrastructures such as "smart" buildings and structures" (e.g., active-bridges whose structural integrity depends on dynamic control or actuators). At the University of Illinois at Urbana Champaign within the Information Trust Institute there is the TCIP (Trustworthy Cyber Infrastructure for the Power Grid) project [6]. TCIP's research plan is focused on securing the low-level devices, communications, and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyber-attacks, and/or power emergencies. National labs concentrate on maintaining and upgrading the security and reliability of the energy infrastructure. Their efforts goes from building testbed used by vendors to test their products [5] to more theoretical challenges such as the analysis of wide-area, large-scale using hybrid systems [7].

II. The Consortium

Diverse backgrounds are needed to address the various challenges of the project. Industry brings the experience with real working systems while academia contribute with the theoretical work. For this reason the research team consists of representatives from the industry such as vendors, service providers and utilities as well as from academical institutions. The industrial partners are

- ABB [8], one of the worlds leading engineering companies.
- E.ON [9], one of the major public utility companies in Europe and the worlds largest investor-owned energy service provider with a target market in Central Europe, the United Kingdom, Northern Europe, and the Midwestern United States.
- MML Analys and Strategi AB [10], a small consulting firm focusing on management support through process development, decision-making support through mathematical analysis and simulation.
- Astron Informatics Ltd. [11], a Hungary based company with expertise in the area of power systems, engineering activities related to EMS/SCADA systems (data modeling, database population).

The academic partners are KTH, ETH and University System of Maryland Foundation. An important member of the Quality Evaluation Group is the University of California at Berkeley.

III. Objective

The vision of this project is to increase the understanding of vulnerabilities of integrated control systems and their impact on the electric power transmission and distribution system, as well as to devise solutions to eliminate or to mitigate these vulnerabilities. The overall goal of the VIKING project is to make the information and control systems robust against attacks and operational errors. The four strategic objectives are described below.

1) Provide a holistic framework for identification and assessment of vulnerabilities for SCADA systems. The framework should provide computational support for the prediction of system failure impacts and security risks.

2) Provide a reference model of potential consequences of misbehaving control systems in the power transmission and distribution network that can be used as a base for evaluating control system design solutions.
3) Develop and demonstrate new technical security and robustness solutions able to meet the specific operational requirements that are posed on control systems for our target area.
4) Increase the awareness of the dependencies and vulnerabilities of cyber-physical systems in the power industry.

The security research and development process is cyclic and does not terminate, as new threats and system functions are continuously appearing. So the first step of security requirement analysis should be performed recurrently. The cyber-physical system, composed of the physical power transmission and distribution system and the associated SCADA system, gives rise to a large-scale hybrid model. Based on the requirements and the cyber-physical model, vulnerabilities can be identified. Their security and fault impacts are analyzed and assessed. The vulnerabilities can now be ranked in order to design appropriate protection mechanisms, considering cost and complexity on the one hand and the system performance and robustness on the other. These mechanisms are then evaluated with respect to the security requirements. The security risks and requirements of the improved system might now be reassessed and a new cycle can be started. This cycle is reported in Figure 2.

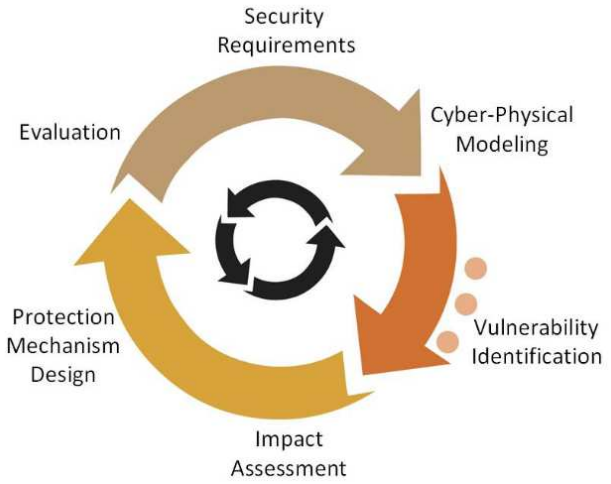

Fig. 2. Cyclic approach to build resilient systems

IV. Security Issues in Power Network Control

In Figure 3, a schematic block diagram of a modern power network control system is shown. Remote Terminal Units (RTUs) connected to the substations transmit and receive data from the control center using the SCADA system. The technology and the use of the SCADA systems have evolved quite a lot since the 1970's when they were introduced. The early systems were mainly used for logging data from the power network. Today a modern system is supported by many Energy Management Systems (EMS) such as automatic generation control (AGC), optimal power flow analysis, and contingency analysis, as is indicated in the figure. With the advent of new sensors such as PMUs (Phasor Measurement Units), so-called Wide-Area Monitoring and Control Systems (WAMS/WAMC) have also been introduced [12]. This introduces yet another layer of control in the modern power network control systems. Even more important for the VIKING project is that the SCADA/EMS systems now are interconnected to office LANs, and through them they are connected to the internet. Hence, today there are more access points to the SCADA/EMS systems, and also more functionality to tamper with.

Six possible types of attacks **A0**-**A5** on the power network control system are indicated in Figure 3. The attack **A0** is a physical attack on the power network or the SCADA system infrastructure. Such attacks are *not* considered in the VIKING project. Instead the focus is on cyber attacks. Somewhat arbitrary, we have split the cyber attacks into the categories **A1**-**A5**.

By **A1, A2, A3** we mean cyber attacks on the SCADA system itself. The SCADA system consists of front end computers at the substations and RTUs, a heterogenous communication network consisting of fibre optics, satellite, microwave connections etc., and finally a host computer at the control center ("SCADA master"). Possible attacks here could be Denial of Service (DoS) attacks on the RTUs or manipulation with sensors (**A1**), deception attacks on the communicated data (**A2**), or attacks directed to the SCADA master (**A3**). A deception attack on sent measurements will mainly affect the performance of the state observer, whereas a deception attack on sent commands could open circuit breakers in the power network. These type of attacks are of major interest in the VIKING project.

By **A4** we mean cyber attacks on the EMS and the state observer at the control center. The state observer estimates the state of the power network using communicated measurements and tries to locate faulty equipment, for example. The EMS systems use the state estimate to either automatically compute control actions or to suggest actions to a human operator. The latter is much more common than the former. In fact, the AGC is the only truly automatic control loop that is regularly being closed using the SCADA system. Its purpose is to regulate the grid frequency of the power network [13]. An attack on the AGC could destabilize the generation control in the power system. Another EMS application is optimal power flow that tells the operator how power flows should be directed to minimize losses. Possible attacks here could be manipulation of the state observer so that it gives a faulty estimate of the system state. The consequences of this could be that power flows are directed in a bad manner, which could have significant financial effects. Naturally, attacks **A1**-**A3** on the SCADA system will also affect the EMS systems, since theses systems are then fed with bad data (deception attacks), or with no data at all (DoS attacks).

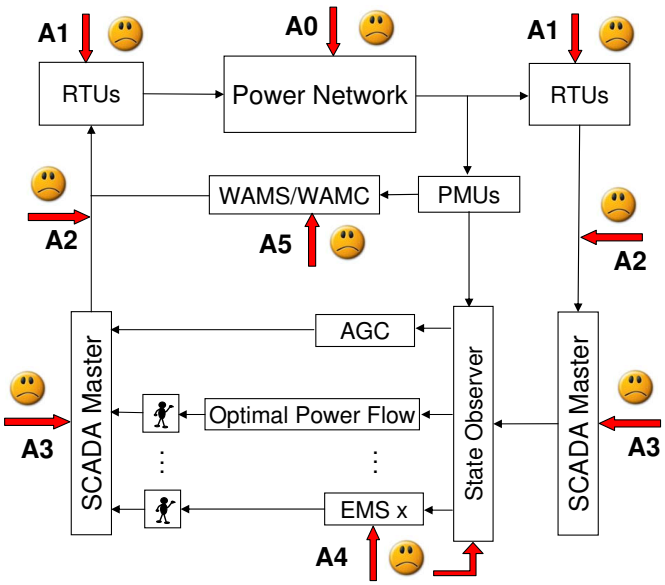

Fig. 3. Block diagram of power network, SCADA, EMS, and WAMS/WAMC systems. Remote Terminal Units (RTUs) connected to the substations transmit and receive data from the control center using the SCADA system. At the control center, a state estimate is computed and is used by Energy Management Systems (EMS) to send out commands to the power network. The human figures indicate where a human is needed in the control loop. **A0**-**A5** indicate some of the possible attacks on the system.

By **A5** we mean cyber attacks on WAMS/WAMC systems. WAMS/WAMC systems can be used to detect and to attenuate inter-area oscillations in the power network, for example, since PMU measurements are taken at a high frequency [12]. Not many WAMS/WAMC systems are in operation today, but they are likely to become more common in the future. Since these systems have a large degree of autonomy and process large amounts of data, they are potential targets of future cyber attacks. It is also possible that they will be integrated with the SCADA/EMS systems, and PMUs are sometimes already today used to improve the state observer, as is shown in Figure 3.

V. VIKING Approach to Security

The project is divided into seven work packages. Each of them comprises all activities related to a particular task to be addressed.

- Work package 0 (**Management**) acts as coordination of the technical work of VIKING and it is lead by ABB Germany.
- Work package 1 (**Requirement Study**) deals with understanding security requirements on SCADA systems for transmission and distribution networks. The requirements are classified in terms of their origin. In each of the categories requirements are further classified in terms of their criticality. It is proposed a rough classification of requirements into: *must* (critical requirements that must be absolutely fulfilled), *should* (important requirements that need to be fulfilled if at all possible) and *could* (secondary requirements to be fulfilled whenever higher priority requirements permit). The main work in this package will be done by ABB Sweden. KTH, Astron and E.ON will support, especially on the requirement specification from the physical process.
- Work package 2 (**Modeling**) provides the necessary modelling foundations on which threat assessment and mitigation methodologies can be based. The main objectives identifying threats and vulnerabilities of the power transmission and distribution systems, developing architectural models over SCADA system designs, and developing mathematical and computational models for the interaction between the physical transmission and distribution processes and the IT infrastructure. ETH is work package leader, in the modelling work. This is mainly an academic group.
- Work package 3 (**Risk assessment and evaluation methodologies**) develops methods to identify and predict the impact of system failures and security risks. The group is lead by KTH with support from ETH.
- Work package 4 (**Mitigation and protection**) develops methodologies and protocols for the mitigation and protection of critical infrastructures. The focus will be on systemic and architectural aspects, with development of new methods and protocols for anomaly and threat detection and countermeasures through secure resource management and communication protocols. KTH will lead in cooperation with ETH. The universities of Maryland and Berkley have an important role to play here with expertise and these specific areas.
- Work package 5 (**Case studies and test-bed**) evaluates some of the methodologies on a VIKING test-bed that can be configured to simulate the critical infrastructure of a power network and a wide range of attacks. To demonstrate the impact of the proposed solutions in different parts of a SCADA system for a power network, a test-bed for the simulation of systems at local (substation) level, network level and central level including wide and local area communication will be integrated with a commercial SCADA system. The test bed will be located at KTH. ABB Sweden, as development centre for ABB's SCADA system, will be supporting Astron.
- Work package 6 (**Public awareness, exploitation and dissemination**) brings together all the activities related to the interaction of VIKING with the outside world. The project involves two different types of outreach activities: Plans for follow-on exploitation of the project results by the industrial partners and public dissemination of the results by the academic partners. The leader is E.On Sverige.

The diagram in Figure 4 summarizes the interdependencies between the various work packages. Yellow arrows indicate logical relationships between work packages. The black arrows refer to activities which will lead to dissemination and exploitation.

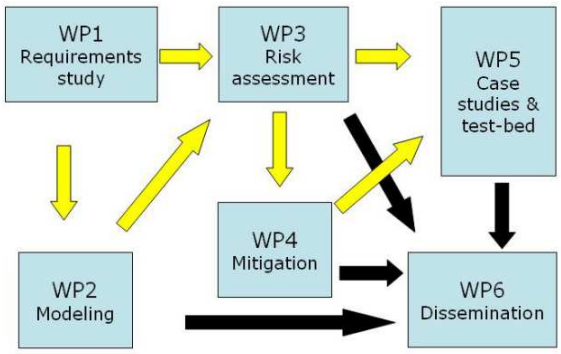

Fig. 4. Interdependency between work packages

The project focuses on the following areas.

- **Modelling and assessment of vulnerabilities of SCADA systems and their effects.** Attacks and failure in SCADA systems may result in complex processes of interconnected events. Our goal is to detect these processes and track their evolution. An effective approach involves accurate process modelling. A model is an abstract description of how the system evolves in time. In particular, the situation in complex environments is even more complex, since all the information to infer the actual state of the system is not available at any single node. There are in fact cases in which the observable data from SCADA system does not represent the state of the physical system.
- **Methods for anomaly and threat detection.** New standards and recommendations are further away from being implemented in operational systems. Furthermore, cryptographic schemes work under the assumption that an attacker is not able to physically access hardware. This assumption may fail in the case of SCADA systems, since the network and the connected hardware systems are generally left unattended after deployment. In addition, currently used sensory hardware is not resistant to physical tampering. If an adversary captures a sensor, he can easily extract the cryptographic primitives and keys, as well as exploit the shortcomings of the software implementation [14]. Even if the hardware that emits sensor data is kept secure, a skilful attacker can intercept this stream and perform decryption. Once the adversary has obtained the cryptographic keys, he is able to access the sensory data in order to modify or exploit it. Therefore, we cannot exclusively rely on traditional cryptographic protocols to protect the security of SCADA systems. This motivates the need for an Intrusion Detection System (IDS), i.e., an application-level module able to detect and to take the right countermeasures against an attacker who is trying to forge the cryptographic scheme. We will investigate and develop techniques for the detection of data anomalies and suspicious traffic due to malicious tampering, or sensing node malfunction and provide models for expected system behaviours under such conditions.

VIKING will develop methodologies applicable to a variety of critical infrastructures, but the evaluation and testing will be focused on power distribution and transmission networks.

VI. Current Status

We are now six months into the project and we just delivered a document representing the requirements study made for the first work package. The document contains known and expected threats to the Cyber Security of Control Systems. Threats were collected through a web application that was developed and published to the members of VIKING. Among the submitted threats there were a significant number of similar threats with only slight differences in for example location of the attack. The raw data has been refined such that revised threat descriptions are provided to cover multiple of those collected. Each new description have a reference to the original threats for cross-reference purposes. Examples of threats are:

1) RT-0001: Mistakes/vulnerabilities due to lack of training or experience.
2) RT-0002: Access to process communication channels.
3) RT-0003: Access to control system LAN.
4) RT-0004: Manipulation of master process engineering data.

The collected threats will be assessed in subsequent work packages.

Acknowledgment

This work has been supported by the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 225643. The authors would like to thank the other members of the projects, Gunnar Björkman, Erik Johansson from ABB, John Lygeros, Manfred Morari, Göran Andersson from ETH, Mats BO Larsson from MML, Rita Lenander, Gitte Bergknut from E.ON, Attila Kovács, Attila K. Mergl from Astron, Pontus Johnson, Torsten Cegrell, Lars Nordström, Gunnar Karlsson, André Teixeira from KTH, John Baras, Tao Jiang from Maryland for their team work.

References

[1] J. Lygeros, K. H. Johansson, S. Simic, J. Zhang, and S. Sastry, *Dynamical properties of hybrid automata* IEEE Transactions on Automatic Control, 48:1, 2-17, 2003.
[2] http://crutial.cesiricerca.it/
[3] http://ec.europa.eu/research/energy/pdf/synopses_electricity_en.pdf
[4] http://www.truststc.org/
[5] http://www.inl.gov/scada/
[6] http://www.iti.uiuc.edu/content/tcip-trustworthy−cyber−infrastructure−power−grid
[7] http://www.ornl.org/sci/electricdelivery/security_widearea.html
[8] http://www.abb.com
[9] http://www.eon.com
[10] http://www.mml.se
[11] http://www.astron.hu
[12] M. Zima, M. Larsson, P. Korba, C. Rehtanz, and G. Andersson, *Design Aspects for Wide-Area Monitoring and Control Systems*, Proceedings of the IEEE, pp. 980–996, vol. 93, no. 5, May 2005.
[13] P. Kundur, *Power System Stability and Control*, McGraw-Hill, 1994.
[14] C. Hartung, J. Balasalle, and R. Han, *Node Compromise in Sensor Networks: The Need for Secure Systems*, Department of Computer Science University of Colorado at Boulder, 2005.