Abstract — The purpose of this paper is to give an overview of the VIKING project including its motivation and background. The VIKING project has been started to investigate the increased cyber security risks for deliberate attacks on critical infrastructures coming from SCADA systems and to propose mitigation.

The second part of this paper describes the principle design of modern SCADA systems in order to give a better understanding of this technology.

The VIKING project is an EU financed Framework 7 Collaborative STREP Project and is part of themes 4, ICT, and 10, Security. VIKING stands for Vital Infrastructure, NetworKs, INformation and Control Systems Management and aims on making SCADA system more resilient against cyber attacks.

I. INTRODUCTION

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 fully non-functioning societies with devastating economical and humanitarian consequences.

The operation and management of the electric power system depend on computerized industrial control systems, so called SCADA systems standing for System for Control And Data Acquisition. 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.

The VIKING project will take a holistic approach and investigates the risks for cyber attacks on all parts of the SCADA system including substation control systems, communication networks and central control systems. The project aims to model the whole chain from cyber attacks, modeled via attack trees, over architectural SCADA system models, power system models down to societal models in order to evaluate the cost and consequences for the society from cyber attacks on SCADA systems. One important part of the project is to verify models and proposed mitigation methods on a test bench.

A second part of this paper will discuss the principle design of modern computerized control systems including data acquisition, event and alarm handling, user interface, process models, optimization and simulation in order to increase the understanding how these systems are designed.

The VIKING project results could potentially have substantial, practical importance for the implementation and usage of SCADA systems. Therefore, the VIKING consortium includes the industrial partners ABB, E.ON and Astron. ABB is one of the world leading SCADA vendors and E.ON is one of the major energy utilities in Europe. Astron is a system integrator working in Hungary. Possible benefits resulting from the new approaches in VIKING will be described from an industrial view point in the last section of the paper.

II. THE VIKING PROJECT

The VIKING project will concentrate its research on computerized system for the supervision and control of electrical transmission and distribution networks. One of the reasons to limit the project to the electrical process is that the results of VIKING is believed to be applicable to other SCADA systems used for other critical infrastructures like gas, water, telecommunication, etc. and, as described in the Introduction, the vital importance of the electricity supply.

These computerized control systems include functions for remote collection of vast amounts of real-time data coming from measurement devices placed at strategic points, e.g. in transformer substations, in the geographically widely spread process and for the remote control of process devices. Many SCADA systems include computerized models of the supervised process which enables simulation of alternatives process states and 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, distribution and generation resources. The process is, in
other words, operated closer to its physical limits. Thus the SCADA systems are becoming increasingly critical for the operation of the process and therefore are becoming a critical component for the availability, safety and security of the supervised infrastructure.

The objective of the VIKING project is to develop, test and evaluate methodologies for the analysis, design and operation of resilient and secure industrial control systems for critical infrastructures. Methodologies will be developed with a particular focus on increased robustness of the control system. As mentioned, the focus is on power transmission and distribution networks. The project combines a holistic 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 networked control systems.

The traditional approach to verify the security of SCADA systems has been ad-hoc testing of existing commercial SCADA system in laboratory environments. The systems to be examined have been installed in different labs and tested by skillful people searching for cyber attacks vulnerabilities. The focus in these tests has been on the protection of the central computer system of the SCADA system, since the central computer system has most connections to the outside world through office networks, vendor links and Internet.

In the VIKING project we will take an alternative and complementary approach to SCADA system security. Firstly we will study the whole control system from the measurement points in the process itself over the communication network to the central computer system as illustrated in the following picture with the yellow exclamation marks indicating potential targets for cyber attacks.

Figure 1 – SCADA System vulnerabilities

Secondly, and more importantly, we take a model-based approach to investigating SCADA system vulnerability. Models are defined for the SCADA system, for the electrical process as well as for the society that is dependent on the electricity supply. The society models are used to evaluate the economic consequences coming from disturbances in the electricity supply and to give load scenarios for the simulations. The power system models are in turn used to evaluate the effects on the electricity supply caused by SCADA system misbehavior. Finally, SCADA system architectural and cyber-physical models are employed to assess the effect on SCADA system behavior caused by cyber attacks. Based on analysis performed on these models, VIKING will propose mitigation actions to be taken to decrease or to eliminate these risks. The results of the project will be evaluated on a test-bed that can be configured to simulate cyber attacks on the power network coming from SCADA and the corresponding consequences in the virtual society.

The modeling approach is indicated in the following picture.

Figure 2 – Modeling approach

With this approach the project hopes to achieve the following research results.

- Estimates of the security risk and consequences (in terms of monetary loss for the society) based on threat trees, graphical system architecture and society models
- Comparable, quantitative results for IT security for different control system solutions and implementations
- Use of existing model based application as application level Intrusion Detection Systems to detect manipulation of data
- Use of innovative and existing communication solutions to secure power system communication
- Help with identifying "weak spots" and how to mitigate them
- An environment for performing what-if analyses of the security risk impact of different architecture solutions.

III. SECURITY INCIDENTS

The number of security incidents reported in the area of critical infrastructures has increased significantly over the last few years. Even attacks on control systems are becoming more frequent and sophisticated. The diagrams shown below were published in the Pipeline and Gas Journal [3]
The incidents in the diagrams above include directed and malicious intrusion attempts as well as unintentional security breaches done by mistake. In addition to the threats from viruses and hackers breaking into computer systems, there is a growing concern over the possibility of network based terrorist attacks against infrastructure and critical process industries.

Many of the reported incidents were initiated by people with legitimate access to the network. In general, these attacks are the most difficult ones from which to protect a system, because insiders (or former insiders) are the most likely persons to have access to passwords, codes, and systems, and to have knowledge about the nature of the system and its potential vulnerabilities. Recently, however, the share of externally sourced incidents has increased drastically, particularly in the form of virus and worm infections. In many cases, virus and worm infections are caused by connecting a portable computer or storage device that has previously been connected to an infected environment [4].

There is no single solution or technology for network security that fits the needs of all organizations and applications. While basically all computer systems are exposed to intrusion attempts, the potential consequences of such attempts are vastly different for different types of applications.

Cyber security measures aim at protecting the confidentiality, integrity, and availability of a computer system from being compromised through deliberate or accidental attacks. This is accomplished by implementing and maintaining a suitable set of controls to ensure that the security objectives of the organization are met. These controls should include policies, practices, procedures, and organizational structures, as well as software and hardware implemented security functions.

The security measures that are applied to a specific installation should be proportional to the assessed risk in terms of probability of a successful attack and the potential consequences. For a small system with a few users controlling a non-critical process this risk is obviously smaller than for a large system spanning multiple sites with safety critical processes in several countries and continents and thousands or even tens of thousands of users.

It is not possible to achieve 100% security in an interconnected environment. A network that is arranged with state-of-the-art security measures may still be vulnerable through connections to the networks of suppliers, contractors or partners. Even a network that is perceived as being totally isolated from the outer world is vulnerable to security intrusions from different sources, such as the occasional connection of portable computers, modems that are not properly disconnected or unauthorized installation of software.

### IV. RESTRUCTURING OF THE POWER INDUSTRY AND ITS IMPACT ON SCADA SYSTEM

The security of computer systems in general and of SCADA systems in particular, has become increasingly critical. Changes resulting from electric power industry restructuring have increased the need for heightened information security efforts in this industry. In many countries, unbundling of the power generation function from the power delivery and retail functions, as well as deregulation of the power generation market, have motivated power plant and network owners/operators to reduce costs and improve plant and network operating efficiency. To do this, these owner/operators have implemented several changes and new practices that can potentially affect the cyber security of their power plants.

The most significant impacts of these changes relate to the SCADA systems that are used to operate many transmission and distribution networks and power plants worldwide. For example, many transmission network owner/operators have added connections between their corporate office networks and their SCADA systems. This interconnectivity allows corporate decision makers to obtain instant access, for example, to critical data about the status of their operating assets. However, this interconnection also opens new vulnerabilities to the SCADA system, as the corporate network then becomes a potential additional access point to the control system.

Other practices to improve network efficiency include enabling remote access to SCADA systems by company engineers, contractors, vendors, and others via dial-in...
modems and other means. But, like the interconnection with the corporate network, this practice introduces new access points to the SCADA system. Visiting employees from other locations, hired contractors, and other authorized parties also need to access the corporate network from their laptop computers to gather information to aid decision making and maintenance activities. Such access may, in turn, unleash viruses or malicious code on the SCADA systems.

The drive to improve network operation is also leading to increasing standardization of SCADA technologies. SCADA systems are increasingly implemented on Microsoft Windows and UNIX/Linux operating system-based platforms, enabling a broad range of third parties to offer software that can help optimize plant operation and maintenance techniques. Similarly, most SCADA systems comply with OPC (a Microsoft-based standard for open connectivity) and with the standardized protocols of major manufacturers of Remote Terminal Units (RTUs).

Providing and managing enterprise-wide Information System (IS) security is a moving and dynamic target, complicated by continuous technical, organizational, and political changes, global interconnections, and new business models such as Internet-based e-commerce. IT security is a complex challenge requiring procedural as well as technical measures.

V. PRINCIPLE DESIGN OF SCADA SYSTEMS

To improve the understanding of what a SCADA system really is, and how it is designed, a short introduction on SCADA systems architecture is included in this report.

Modern SCADA systems designed for geographically widespread processes have a principle design as shown already in Figure 1 above. We will in the following discuss the major components one by one.

A. Process connection

Measurement devices like voltage and current transformers are placed in the supervised process and will measure analogue process values like active/reactive power, and voltages and also digital values like open/close state of breakers, isolators and transformer tap changers positions. The signals from the measurement devices are connected to electronic units, so called Remote Terminal Units (RTUs), which are placed in transformer substations or in power stations. These RTUs have the primary task of transforming the measured signals into digital format and transmit them to the central control system and to receive command and setpoints signals from the control centre and to execute these control orders to the primary equipment.

The number of signals in one RTU can vary from several dozen to a few thousand. These signals are traditionally connected via separate signal cables from each sensor to the RTU input board via marshalling cabinets.

In recent years it has become increasingly more common for RTUs to be equipped with interfaces to a serial bus on which various types of secondary station equipment, e.g. protective relays, are connected. These Intelligent Electronic Devices (IEDs) contain information about the process values which is transmitted directly from these devices over the station bus and a gateway to central control system without the need to use dual sensors and extra wiring. An international standardization work has been ongoing for a number of years and has resulted in a number of standards for station bus communication. IEC 870-5-103 is now an established standard in station control systems and IEC 61850 is a coming standard with higher ambition and scope. The intent of this standardization is, of course, to enable mixing of equipment from different manufacturers that can communicate with each other and with the central control system.

Modern generation and transformer stations frequently have their own local SCADA system including operator consoles with advanced man-machine communication to allow local control of the station. These local SCADA systems have access to all local information via the station bus and process buses. The connection to the central control system is handled by a communication node (gateway) on the station bus, which converts the local information to a communication protocol to the central operations center. Many transformer stations are unmanned, which means that those local SCADA systems are only used occasionally.

B. Communications

RTUs and station control systems communicate with the central control system over different type’s communication networks and are using many types of media. Traditionally, the utilities are the owner of the communication networks since the process owners want to have full control of the networks to ensure that communication, especially during major process disturbances, is always available. However, this practice, especially in distribution networks, is becoming increasingly difficult to motivate when public communication services are becoming cheaper.

The networks used for SCADA communication are characterized by relatively low transmission speeds, typically 1200 to 9600 bits per second. Because of the low communication speed and the high requirements for data security, all SCADA vendors did traditionally use their own, proprietary communication protocol between the control center and the RTUs. Since no telegrams should be wrong, especially when commanding the process, protocols have been highly secure with many parity bits. The design rule has been that all single bit errors can be corrected and all dual bit errors are detected. Since these protocols used to be proprietary it was difficult to mix RTUs from different manufacturers in the same system.

This fact has driven a standardization process for RTU protocol and today most of the newly installed SCADA systems and modern RTUs support the international
standard IEC 60870-5-101 and IEC 60870-5-104 (TCP/IP based) and the de-facto standards DNP3.0 and MODBUS. Because of the long life of RTU installations (up to 30 years) there are still lots of older types of vendor specific protocols in operation.

A clear trend today is toward more fiber-based networks with higher communication speeds and TCP/IP based protocols. This will in the long term lead to changes in SCADA system structure and in the distribution of functionality between central control centers and substation systems, but this trend is slow.

C. Central Control Centre

The Central Control Center systems in all modern implementations are built around a Local Area Network (LAN) based on Ethernet to which all servers, workstations and other equipments are connected. This LAN can be single or redundant, but is most commonly doubled for availability reasons. For the same reason are all application servers redundant and operator workstations so designed that they can take over process operation from each other if anyone should fail. One of the main design criteria for control center configurations is to avoid that a single device failure could bring down the entire control center. Figure 4 below shows a typical, bigger control centre configuration with redundant LAN and servers.

Redundant Front-End servers are responsible for the communication with RTUs and Station Control System. The Front-Ends poll the RTUs for new information which is sent to the SCADA servers. The Front-Ends are also responsible for monitoring and managing data acquisition network.

The process information from the Front-End servers are sent to the SCADA servers and stored in a real-time database. The real-time database maintains an image of the current process state as accurate as possible. The time difference between the real process state and the information in the real-time database is normally in the range of a few seconds.

SCADA servers are today implemented on commercially available computers based on UNIX/Linux or Windows with vendor specific SCADA software and comprehensive applications. The reason that virtually all major SCADA vendors use proprietary real-time databases is that the performance at process disturbances and for operator picture call-up can not be solved with the technology available today in commercial relational databases.

The main task of SCADA is to monitor the process data for significant changes and to alert operators about these changes. Such a significant change can be a breaker opening initiated by line protection or a voltage measurement over an alarm limit. On the other hand, a small change of active power within the permissible limits is just stored in the database for presentation in process displays but do not call for special attention. Significant changes are collected chronologically in Event and Alarm lists including local time stamps. Event lists record all what happens in the process, all operator actions and all events in the control system, while Alarm lists requires an active acknowledgment from the operators to confirm their attention.

The operators use process displays on the workstations to supervise the status of the real-time process and to command breakers and isolators or to send new setpoints to local processing units. Automatic commands for "close-loop" regulations exist but are rare, mostly the operators close the loop of active regulation.

Man-machine workstations are the tools for the operator to monitor and control the process. They are usually based on PC computers equipped with multiple VDUs and are using modern, full graphic technologies to present process information in different views. The information on operator workstations is automatically updated by the SCADA servers as soon as any significant change is detected in the process. Modern presentation techniques, e.g. multiple windows, information zoom (declutter) and layers, is employed to give the best possible view of the process to the operators under all circumstances. Figure 5 illustrates one example of dynamically updated station display.
An important task for SCADA systems is to record and archive all incoming data from the process and all operator actions. For this purpose the SCADA systems use special archive servers (Data Warehouses) usually based on a commercial relational database such as Oracle. Based on the relational database, there is a variety of data mining, reporting and programming tools available for different types of users ranging from the normal control room operators to system users and application experts.

Archiving functions must have the capacity to record all information coming from the process through RTUs, station computers, and other control centers, plus archiving of event and alarm and calculation results. This means that many thousand of data points have to be stored every second. The archive function uses many types of media such as DVD or tape robots for automatic long-term storage when disk space is no longer enough. In this way virtually unlimited storage can be achieved.

It is common for a control center to be a part of a control hierarchy within the company or a country. For example, a regional control center will be connected to a national control center. The data exchange between centers will in this case take place using standardized protocols for inter-center communication where the most common today is ICCP (or TASE.2). This protocol includes functions for data acquisition and command and is, like RTU protocols, normally not encrypted.

D. Office Connection

Today it is common for office network to be connected to the SCADA systems to enable normal PC users in the office network to be connected to the SCADA real-time database and archives. This allows the office users to build specific reports and applications working directly with real-time and historical data. This, of course, means that a strict authority scheme must be applied combined with firewalls. SCADA systems are nowadays, to further increase security, configured with so-called 'Demilitarized Zones' (DMZs), an isolated network part between the office network and the SCADA. The DMZ prohibits data access directly from the office network to the real-time LAN. This means that replicas of the real-time database and the historical archive have to be placed in the DMZ and protected by firewalls on both sides.

E. Process Models

So far we have only discussed SCADA systems as pure data acquisition and control systems. All measurements are acquired independently of each other and the process knowledge, i.e. how various objects of the process are interconnected are only shown in pictures. The same SCADA system can be used independent of the monitored process since the basic SCADA functions, i.e. data acquisition and control and event and alarm reporting, are used in all types of process monitoring.

If the SCADA system should include a more intelligent understanding of the monitored process, models of the various process objects must be introduced. These models are, of course, different depending on the type of process that is targeted. There is a difference in behavior between a compressor in a gas pipeline and a transformer in an electrical network although they perform similar functions in the networks. It is also important to define the connectivity, i.e. how the various process objects are connected to each other, for example, on which bus a certain circuit breakers is connected. This connectivity is combined with real time measurements of breaker and isolator states to create a dynamically updated “bus-branch” model.

Defining these models for a certain utility is a substantial work because of the vast number of monitored objects. Special tools have been developed by the SCADA suppliers to support the users in defining and maintaining these models efficiently. Support for imports from other computer systems, for example, a GIS system (Geographical Information System) where the data is maintained are often included.

F. Advanced Applications

Using the dynamic topological models discussed in the previous section, it is possible to implement advanced applications. These applications will be unique for each process type based on the different physical characteristics of the process. Perhaps the most clear examples of such applications exists for electrical SCADA systems, where for a long time such applications have been used based on relatively simple mathematical models of the electricity grid, i.e. Ohms and Kirchhoff’s laws. It is not the purpose of this report to discuss the different types of applications in detail but a brief description how these applications work can provide a better understanding of their use and importance.

By using a non-complete real-time measurement vector (not all points in the network have measurements) the complete power flow state of the network can be calculated (State Estimation) provided that the network is observable, i.e. enough measurements are available. This calculated state defines all voltages and phase angels in all nodes and can be used to calculate the active and reactive power flows for the whole network. The resulting network state can also be used to simulate new situations in the network, for example, after disconnecting a transformer for maintenance or for other operational changes in the grid. These studies are normally done in a parallel database, a so-called study database, in order not to disturb real-time operation. Load flow calculations can automatically be done for all possible errors in the network (N-1 analysis) and warnings or recommendations for grid changes to avoid dangerous situations can be issued before the contingencies actually occur.

These electrical applications make it possible to calculate
the optimal flows in the network in order to minimize, for example, the active losses which could mean substantial economical savings. Similarly, the optimal production schedules with regard to the best use of resources (nuclear power, oil, gas, water) can be calculated and applications for automatic control of generating units according to the approved schedules are available.

Process models and applications can also be used to achieve realistic operator training environments with instructor consoles and operators to be trained in normal and disturbed process situations.

VI. PRACTICAL IMPLICATION OF VIKING

Already now, in the middle of the VIKING project, it is possible to see potential, practical implementations as a result of the research work. Some of these implications will be direct results of VIKING project as deliverables and others could be spinoffs that could explored by the academic or industrial partners. In the context of this paper we will only indicate some rough ideas which have been discussed within the project. We are convinced that many more possible results of VIKING will emerge during the continued project work.

The generic SCADA architecture that will be developed in the VIKING project could be applied to individual commercial SCADA system. Such an analysis could be performed in a specialized tool which would lead analyzers of a certain SCADA system by asking specific questions, e.g. have you applied a DeMilitarized Zone in your configuration or do you use encryption in your Inter-Center Communication and many more. The tool would, as an end results, give a quantitative value of the cyber security of the analyzed system. It would be possible to use such a tool for testing specific actions to improve security, e.g. how much would the IT security improve by adding encryption for parts of the RTU traffic or introducing an Intrusion Detection System.

Another possible application of the VIKING research work would be to use the existing advanced application for an application level Intrusion Detection System. The SCADA systems are in the somewhat unique position to have model based applications that know how the process should behave. This knowledge can be used to detect manipulated process data or make the effort to fool the system with false data much higher.

We have also looked into the possibility to use multiple communication paths to the RTUs and Substation Automation Systems. Such additional paths exist in almost all real installations because the communication network structure follows the meshed structure of the electrical network. Traffic could be divided in such way that it would be impossible to reconstruct a telegram or to enter false telegrams by accessing the traffic on a single communication line. Such a solution could make the management of encryption keys unnecessary which is, in itself, a risk in geographically wide spread processes.

The industrial partners ABB, E.ON and Astron have joined the VIKING project with the intention of improving and extending their product and service offerings or, as in the case of E.ON, to make their existing and future installations of SCADA systems more secure. E.ON is already today very active in the area of SCADA system security and hopes to further improve their knowledge base by an active participation in the VIKING project.

ACKNOWLEDGMENT

This VIKING project has been partly funded by the European Community’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 225643. The author would simply like to thank all the other members of the projects and other associated persons that have actively contributed to the ongoing work of VIKING.

REFERENCES

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

Power System Control Centers: Past, Present and Future Proceedings of the IEEE, Vol. 93, No 11, November 2005


