Challenges in Power System Information Security

György Dán, Henrik Sandberg, Gunnar Björkman, Mathias Ekstedt

Abstract

The transition from today's power systems to the smart grid will be a long evolutionary process. While it might introduce new vulnerabilities, it will also open up for opportunities for improving system security. In this article we consider various facets of power system security. We discuss the difficulty of achieving all-encompassing component level security in power system IT infrastructures due to its cost and potential performance implications. We outline a framework for modeling system-wide security, which facilitates the assessment of the system's security despite its complexity by capturing the interaction between system components. We use the example of power system state estimation to illustrate how the security of the system can potentially be improved by leveraging the knowledge of the physical processes and the significant amount of redundant information. Finally, we touch upon the problem of information availability, a key security requirement in power system control and operation systems.

Index Terms

System-wide security, SCADA communications, State estimation, Information availability

I. Introduction

The vision of the smart grid brings along challenges for both the power engineering and the IT community. From a power engineering perspective the challenges are mainly in how to integrate distributed generation and renewable energy sources with large-scale central power generation and demand side management, without loosing on operational efficiency and on power system reliability. The solution to this challenge seems to be in a tighter integration of the power system with information technology (IT). Tighter integration leads unavoidably to that the proper operation of the future power grid will rely increasingly on the reliable and secure operation of the communication and IT infrastructure.

Reliability and performance have traditionally been key design goals for the IT infrastructure used in power systems, and only in recent years has also security received attention. One main reason for why security only recently has become a concern is that the power system IT infrastructure used to be an isolated, stand alone system. Power system IT infrastructures are, however, increasingly integrated with other IT infrastructures at the power utilities, including public infrastructures. The primary reasons for IT integration are increased business efficiency and effectiveness, as well as reduced operational costs by for instance allowing corporate decision makers to obtain instant access to critical data about the status of their operating assets. Information flow across system boundaries is expected to increase in the future, among others, in order to enable the vision of the smart grid.

G. Björkman is with ABB AG, Mannheim, Germany. E-mail:gunnar.bjoerkman@de.abb.com

G. Dán, H. Sandberg and M. Ekstedt are with the School of Electrical Engineering, KTH, Royal Institute of Technology, Stockholm, Sweden. E-mail: {gyuri,hsan,mathias.ekstedt}@ee.kth.se

Corresponding author: György Dán, Osquldas väg 10, 10044 Stockholm, Sweden.

The integration of the power system IT infrastructure with other IT infrastructures and the need to access information across system boundaries increases the exposure of the power system IT infrastructure to attacks, and hence security will be of increasing importance in the future. When designing the security solutions for future power systems, we should, however, make use of the lessons learnt from securing the existing infrastructure for a number of reasons.

First, the way to the smart grid of the future will be a long evolutionary process starting from today's power grid, both in terms of technology and in terms of organizational structures. The new deployments will have to coexist and interoperate with old, legacy equipment and will have to fit into the current organizational structures and security practices.

Second, the communication and IT infrastructure of today's power systems have to satisfy very diverse application requirements. At one extreme, in the case of management information exchanged between utilities, data is transferred in batches with very loose delay constraints, and standard cryptographic protocols like TLS can be used to provide authentication and confidentiality. At the other extreme, in the case of substation automation and inter-substation protection, the communication delays must be kept in the order of a few milliseconds, so that the delay introduced by encryption algorithms can already be critical for proper system operation. Thus, security solutions might have to be tailor-made for the specific application scenarios.

Third, the power system's communication and IT infrastructure already consist of a vast number of components. The cost of securing the millions of components of a continent-wide infrastructure can be prohibitive, and therefore it is important to understand how the security of individual system components contributes to and affects the secure operation of the power grid. Also, in addition to the traditional IT and communication infrastructure security solutions and practices, in a cyber-physical system models of the physical process can often be leveraged to improve system security.

In this article we survey some recent results related to power system information security. To illustrate the main ideas, we give examples from three areas with a focus on system level security, i.e., proper system operation despite attacks. In Section II, we outline the current role of SCADA systems in power system operation, we discuss important aspects of their operational security and outline a framework for modeling and analyzing the system-wide security with a focus on network induced security threats. In Section III, we summarize some recent results from power system state monitoring. This example illustrates how knowledge of the physical process can be used to improve system security in spite of unsecure communication networks and protocols. In Section IV, we discuss the communication and security aspects of interconnecting the control systems operated by different actors of the power market. Section V concludes the paper.

II. Component-level vs. system-level SCADA security

At the heart of the IT infrastructure for power system control and operation there are one or several so called Supervisory Control And Data Acquisition (SCADA) systems. Apart from the remote collection of vast amounts of real-time process measurements taken from the grid, e.g., in transformer stations, SCADA systems include functions for the remote control of process devices like breakers and tap changers. The acquired data are presented to the operators in the central control room via an advanced graphical user interface, among others equipped with alarming features to alert the operators to changing operating conditions. Many SCADA systems include computerized models of the supervised process (i.e., the power system). The models enable simulation of alternative process states parallel to the physical process, which can be used for optimization and contingency analysis, as further discussed in Section III.

In addition to the centralized control managed by the SCADA systems, there are also a large number of local control systems in the transformer substations. The intelligence in those distributed

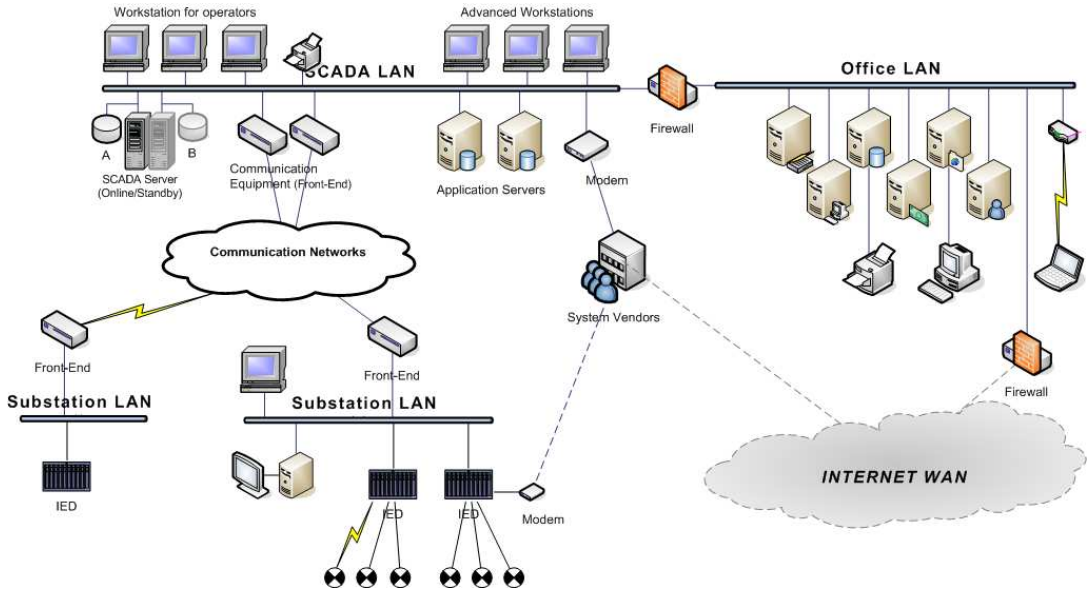

Fig. 1. Simplified architecture of a power system control and operation system. The central SCADA systems, the distributed substation automation systems, and the communication between them constitute a very complex ”system of systems”.

local systems varies from data acquisition units with simple logic to advanced control systems. The functions in the local control systems, such as protection and interlocks, have very stringent performance requirements on the underlying communication infrastructure. Altogether, the central SCADA systems, the distributed substation automation systems, and the communication between them constitute a very complex ”system of systems”, which we refer to as the *power system control and operation system*. A schematic figure of a power system control and operation system is shown in Fig. 1.

A. Performance, reliability and security in a slowly evolving complex system

A particular challenge when studying the security of power system control and operation systems is the mix of modern and legacy system components that are in operation. The typical life time of a power system control and operation system component is often very long. Especially equipment located in the primary substations tend to have a considerable age due to the cost and the difficulty of replacement: it is not uncommon to have 30 years old equipment, e.g., Remote Terminal Units (RTUs), with similarly old proprietary communication protocols. At the same time, the central system at the control room can be relatively modern and can consist of a variety of third party products, like relational databases and power applications from a specific vendor.

With a history of proprietary system components from specialized vendors, the trend today is to rely increasingly on off-the-shelf products, both for hardware and for software, when developing and upgrading power system control and operation systems. This trend makes the development and maintenance cheaper but it also increases the systems’ vulnerability, since the vendors no longer have full control of all system components. Another trend is the use of standard communication interfaces to ensure interoperability between components from different vendors. Standardized protocols for RTU communication like IEC60870-5-101 and -104 have been in use for a long time and, in the same way, control center to control center communication nowadays uses the

Application			Performance - Typical values			Security - Importance		
			Distance [km]	Latency [s]	Throughput [1/sec]	Confidentiality	Integrity Authenticity	Availability
S2CC	SCADA	Data acquisition	1000	$1-10$	5000 meas	Medium	High	High
		Commands		1	0.1 command	High	High	High
		Alarms and events		1	500 events	Medium	High	High
	PMU data for WAMS			2×10^{-2}	18 meas/PMU	Medium	High	High
Substation automation (Intra-substation)			0.5	1	200 meas	Medium	High	High
Line protection (Inter-substation)			50	10^{-3}	2 meas	Low	High	High

TABLE I

APPROXIMATE PERFORMANCE AND SECURITY REQUIREMENTS OF SUBSTATION TO CONTROL-CENTER (S2CC), INTRA-SUBSTATION AND INTER-SUBSTATION COMMUNICATION FOR VARIOUS APPLICATIONS. HIGH LEVEL OF INTEGRITY AND AVAILABILITY HAS TO BE PROVIDED WHILE SATISFYING VERY DIVERSE PERFORMANCE REQUIREMENTS.

standard protocol ICCP or IEC 60870-6/TASE.2. The standardization efforts today focus mainly on power system models like the Common Information Model (CIM) with the goal to ease the exchange of engineering data between and within utilities.

Achieving security in slowly evolving power system control and operation systems is a complex problem. Simply adding state-of-the-art security solutions and mechanisms to existing systems is often not feasible: security solutions can violate requirements on performance and reliability, which continue to have highest priority. Some security solutions would probably meet the requirements if completely new systems and architectures were deployed, but today as well as in the future we have to live with a large share of legacy equipment. Thus, in practice the challenge of security design in power system control and operation systems implies finding a proper level of trade-off between security, system properties like performance and reliability, and cost. Table I illustrates the heterogeneity of the performance and the security requirements of some power system applications.

The next challenge of securing evolving power system control and operation systems is that security itself is an area with many facets. The list of security mechanisms or practices can be made long; firewalls, access control, authentication mechanisms, hardened operating systems, secure communication, intrusion detection systems, just to mention a few. All of these are good practices for improving system security. On top of these the overall security is, of course, also dependent on organizational issues, such as security awareness among staff so that passwords are not revealed or that USB sticks are not introduced without proper precautions, etc.

There exist a number of standards and reference reports that cover several aspects of system security, some with a focus on industrial control systems. One of the more extensive works for power systems is found in NIST's reports on smart grid security [1]. Nevertheless, a great challenge when designing system security solutions is to comprehend how all the implementable security measures affect and depend on each other: while some measures might complement each other, others might be counterproductive. It is often said that the security of a system is not better than its weakest link. A few advanced security solutions will not increase the system's security if there are poor security solutions elsewhere in the system architecture or its surrounding organization. As a simple example in Fig. 1, securing the substation to control center communication is of little benefit if access to the SCADA LAN is possible from the office LAN, which in turn can be accessed from the Internet if the firewalls are not properly configured. To complicate matters even more, security

is a moving target. What was considered secure yesterday can become an open hole overnight if a severe vulnerability is discovered in a software component, like an operating system.

B. System-wide security analysis

The complexity of the problem calls for a system-wide conceptual framework. In the VIKING project we have developed a system architecture modeling language for modeling and analyzing security in power system control and operation systems. An important requirement for this modeling language is that the assessment delivered by it should take a holistic approach to cyber security. However, when looking at security from a system-wide perspective the amount of detailed parameters influencing system security is enormous. All parameters are simply impossible to survey in a consistent manner in practice. One way to manage the overwhelming complexity is to use a 'top-down' approach. This raises the level of abstraction, so that a deductive and deterministic approach must be abandoned in favor of an indicative and probabilistic one. The developed analysis mechanism is based on attack graphs, but due to the system-level of abstraction the graphs are not deterministic as originally suggested by [2], but instead they are implemented in Bayesian networks. Bayesian networks quantify conditional dependencies between random variables, which represents security states of the system. By combining the Bayesian attack graphs with a system architecture modeling language one can achieve an integrated security analysis mechanism for system architecture models. The resulting security estimates are thus probabilities that attacks will be successful, rather than formally proven statements that the systems are in a secure or insecure state. The first version of the modeling language following these ideas was presented in [3]. More detailed attack graphs require quantified conditional probabilities, which is an important area of ongoing work with some initial results in, e.g., [4].

Fig. 2 illustrates the concept of attack graphs. In this simple example the goal is to gain access to the SCADA server, which can be achieved for example through a man-in-the-middle attack. The success of the attack depends on how well the communication links are protected and on the strength of the authentication protocol used to communicate with the SCADA system. By comparing the likelihood of different attack paths it is possible for industrial decision makers to prioritize among the possible countermeasures and choose what equipment to upgrade or install first. This model based and top-down approach thus support rational decision making for improving cyber security in large and complex legacy system architectures.

III. Model Based Secure State Estimation

The modeling language outlined above provides a high-level estimate of the security of the ICT infrastructure, but disregards the inherent resilience of certain SCADA system functionalities. One

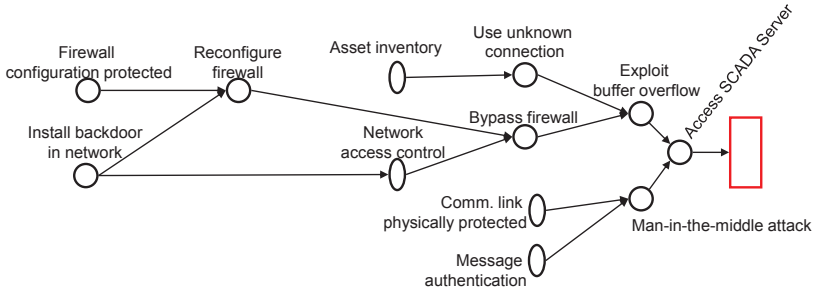

Fig. 2. A simple attack tree illustrating some possibilities for getting access to the SCADA server.

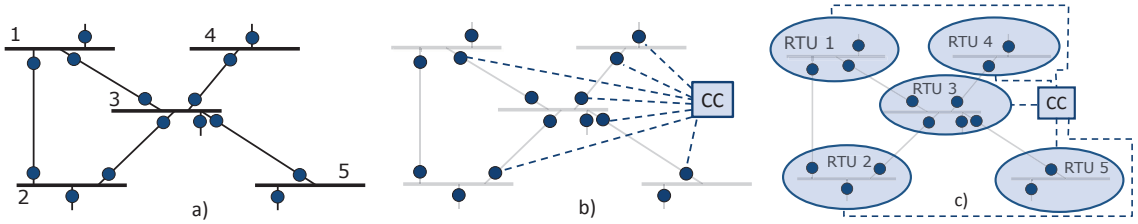

Fig. 3. In figure a), a simple 5 bus power grid is shown. Each bar represents a substation (connected to a city distribution grid or a power plant, for instance) and lines represent transmission lines. The circles indicate measurements of power flows, power injections, and voltages. In figure b), some of the communication links (dashed lines) between measurement devices and the control center (CC) are indicated. This communication topology is an over simplification, and for security purposes a more realistic SCADA communication network topology, such as the one in figure c), is more appropriate. In this case, there is an RTU at each substation, which collects the measurements taken at the substation and sends them over the communication network (dashed lines) to the CC.

of the primary functions of SCADA communications is to enable remote monitoring of the physical process, usually referred to as power system state estimation. Power system state estimation is a key component of SCADA systems. The state of the power system is used by a number of energy management applications, and timely estimates are crucial to ensure proper system operation.

In order to ensure high system availability, measurement data for state estimation are collected such that estimation is possible even if a fraction of the measurement equipment fail. It might thus not be necessary to secure all communications in order to protect the state estimation functionality against attacks. In this section we first describe the communication protocols involved in power system state monitoring and estimation, and then illustrate how a model of the physical system can be used to improve the security of power system state estimation.

A. Substation to Control Center Communications

In general the SCADA communications related to power system state monitoring and estimation are referred to as substation to control center communication (S2CC). Nevertheless, the purpose of S2CC is not only to enable the monitoring of the state of the power system, but also to control the actuators located in the substations. Traditionally, S2CC was performed over low bitrate point-to-point transmission links, e.g., using power line communications, microwave, and leased lines. Modern S2CC increasingly make use of cellular, satellite, and optical communications. Data rates can be in the order of a few Mbit/s for phasor measurement unit (PMU) data transmission. Fig. 3 shows a simple example of a power system and illustrates the corresponding S2CC communication infrastructure.

There is a large variety of application layer protocols for S2CC, and different protocols often coexist within a SCADA system. Legacy protocols, such as Modbus and the proprietary protocols of equipment vendors, are slowly replaced by protocols standardized in the last decade, such as DNP3 and IEC 60870-5 for data acquisition and control, or IEEE C37.118-2005 for PMU data. Neither the legacy nor the standardized protocols were developed with information security in mind, as communication channels were thought to be well protected and substations used to be manned, which made physical access to measurement and communication equipment difficult.

Motivated by the increased use of shared communication channels and the spread of unmanned substations, security extensions that provide confidentiality, integrity and authentication were standardized for these protocols recently, such as the IEC62351-5 for IEC60870-5. Communications

with legacy equipment that does not support the security extensions can be secured using bump in the wire (BITW) solutions, like AGA-12 and YASIR [5]. A BITW solution consists of two devices that are inserted in the communication link near to the sender and the receiver, respectively. The sender side device encrypts the output of the sender, which is then decrypted by the receiver side device. The sender and the receiver are not aware of the existence of the BITW devices.

Although security solutions are available for most communication protocols, deployment has been slow, not only because of the associated equipment costs, but also due to the overhead of managing encryption keys, and because of the potential impact of encryption on data availability in case of a lock out.

B. Communication vs. Application Layer Security

It is important to note that while data integrity and authentication are necessary to secure control communications from the control center to the substations, secure power system state estimation can be achieved at a much lower cost. The reason for the lower cost is the inherent redundancy in the measurements sent from substations. Typical measurements sent over the SCADA network include steady-state active and reactive power flows, power injections, and voltages. Using basic power systems modeling, see for example [6], it is relatively straightforward to write down a system of equations relating the expected measurements to the physical state of the power system (voltage levels and phase angles at busbars). Since the number of measurements typically far exceeds the number of state variables, for a fixed physical state the expected measurements are highly correlated. That is, the measurements received from one substation contain information about the measurements from neighboring substations.

The steady-state power system models capture the *spatial correlation* among the measurements. Since all the measurements are collected at the control center, one can verify whether the received measurements satisfy the power system model reasonably well using statistical tests. If the measurements do not pass the tests, then either the measurements were corrupted or some sensors are faulty (assuming the model is correct). Such tests are routinely performed in the so-called bad data detector (BDD), see for example [6]. The role of the BDD is to identify faulty equipment and remove erroneous data in the state estimation in order to provide the human operator in the control center with the best possible state estimate. The state estimate is used to improve system efficiency and for contingency analysis.

The BDD discussed above was not introduced to provide system security, but it still contributes to such security at a low cost even without encryption. It has been emphasized lately [7] that an intelligent adversary can fool the BDD. The reason is quite simple: as long as the received measurements correspond to a possible physical state, the BDD system will not alarm. An adversary with knowledge of the power system can add a correlated corruption to several measurements and the BDD will not trigger an alarm. Such an attack involves tampering with several sensor measurements simultaneously. Because of the spatial correlation discussed before, these sensors are often geographically dispersed. The adversary will need to intercept measurement data from different sensors (and usually different RTUs), which are typically delivered through different communication channels to the control center. This observation is used in [8] to define a *security index* α_k, which tries to quantify the cost of attacking a particular measurement k. The integer value $\alpha_k \geq 1$ simply denotes the minimum number of measurement values or the number of S2CC communication channels that need to be corrupted to alter measurement k without triggering alarms in the BDD. The cost of performing an attack actually depends on the communication network used for S2CC illustrated in Fig. 3; by attacking the communication between an RTU and the CC an attacker can potentially tamper with all measurements from a substation.

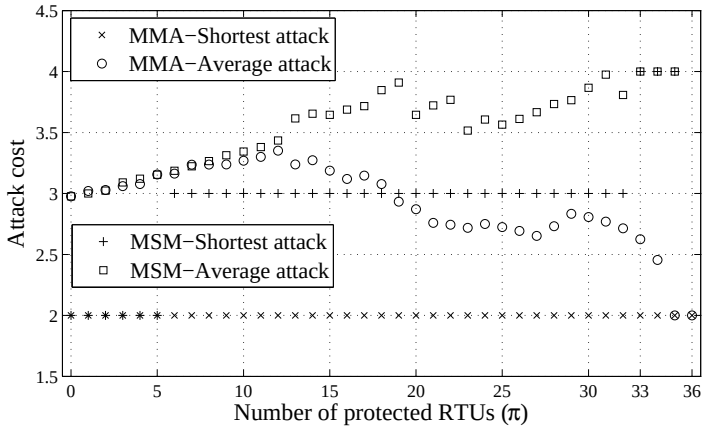

Fig. 4. Attack cost (average or minimum α_k) vs. number of secure RTU to CC communication channels for the IEEE 118 bus power system, reproduced from [8]. Results are shown for two greedy algorithms. MMA aims to maximize the average attack cost. MSM aims to maximize the shortest attack cost. MSM turns out to perform better with respect to both aims. In particular, when securing 36 out of the 118 RTUs using MSM, it is no longer possible to make undetectable attacks against any RTU (the minimum attack cost is infinite).

Securing all substation to control center communications is of course the best way to avoid such attacks, but in a medium scale to large scale power system there are thousands of measurements and potentially hundreds of substations, and the upgrade of all equipment to support security would be very costly. An important question is then if and how the system security can be increased by incrementally upgrading equipment, that is, incrementally installing secure communication channels. This question was addressed in [8], [9] where a limited number of encrypted communication channels were introduced to improve the system security level, as measured by α_k. Ultimately, by combining traditional BDD and by securing a carefully selected subset of measurements (or communication channels) one can achieve that an adversary cannot make an attack against any measurement without triggering a BDD alarm. Fig. 4 shows how the attack cost increases with the number of secure communication channels for a particular example.

There are also other types of equipment that can incrementally improve the security of state estimation. Let us take PMUs as an example, which are expected to be widely used in the smart grid. PMUs provide measurement data at a significantly higher rate (≥ 18 Hz) than used in today's state estimators, and are able to capture fast transients in the power grid. The measurement data from the PMUs, just like today's power flow and injection measurement data, are correlated samples from a physical process. To model the expected measurements from a PMU, a dynamical model of the power system is needed. Such models can capture the *spatio-temporal correlation* among the measurements. An adversary who is basing his presumed undetectable attacks on simple steady-state models will no longer be undetectable, even if the communication channels are not secure.

State estimation, which is at the core of power system operation, is a good example of how system security can be improved at a relatively low cost through combining analytical models, secure communications, and advanced metering technology (PMUs).

IV. Inter Control Center Communication

Conceptually, the purpose of inter-control center communication (ICCC) is very similar to that of substation to control center communications: to enable monitoring of the state of the power system

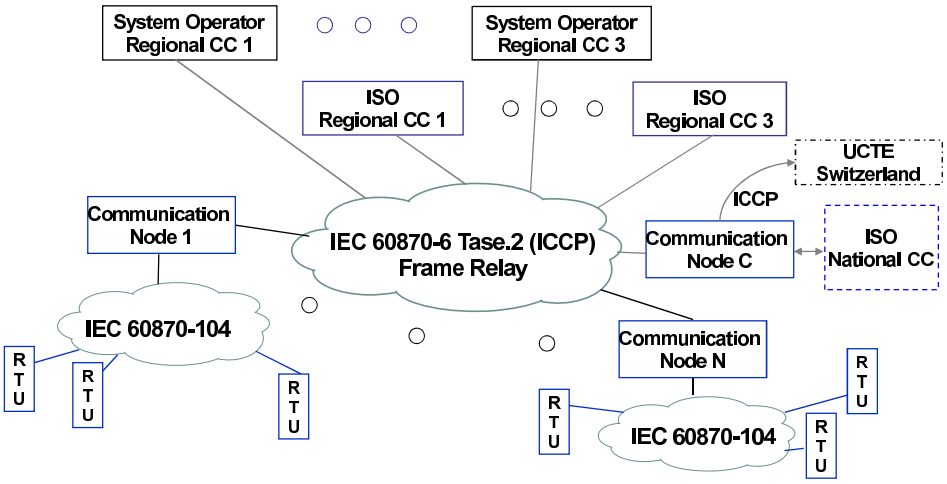

Fig. 5. Schematic view of the SCADA communication infrastructure of the Italian transmission system, which used to be the largest ICCP deployment world-wide [10]. In the actual system measurement data from around 250 RTUs are delivered to one of 22 communication nodes using IEC 60870-5-104 over TCP/IP. ICCP is used to deliver data from the communication nodes to the 3 regional control centers of the transmission system operator (TSO), and to the 3 regional control centers and to the national control center of the independent system operator (ISO). ICCP is used also to communicate to the control center of the Union for the Co-ordination of Transmission of Electricity (UCTE). For simplicity, the figure does not show ICCP connections to power generation control centers.

and to control actuators located in substations. Nevertheless, in the case of ICCC the exchange of information and control messages happens between different organizations, such as distribution service providers, transmission service providers, neighboring utilities, regional and national control centers, electricity producers and other electricity market participants. An example ICCC scenario is shown in Fig. 5 based on the communication infrastructure of the Italian transmission system [10].

The information obtained using ICCC is often used in the state estimation process, hence the security of ICCC affects the security of state estimation. In a smart grid environment, the importance of and the reliance on ICCC is expected to increase for a number of reasons. First, the number of independently managed electricity market participants is expected to increase, and their secure operation requires information about the state of other market participants. Second, due to its distributed nature the stability of the smart grid will rely increasingly on wide area measurement and control systems, which will span several, geographically distant market participants and might require real-time data delivery with stringent delay and throughput requirements.

A. Cryptographic Communication Security

While there have been a number of proprietary protocols in use for inter-control center communications, the predominant protocol in use today is the Inter-Control Center Communication Protocol (ICCP, IEC 60870-6/TASE.2). ICCP provides a point-to-point connection, called an association, between a pair of nodes, that is, two control centers. Two nodes can maintain several ICCP associations with each other simultaneously, and can use different associations to exchange data with different priorities. The rationale for maintaining several associations is that the service level requirements of the information exchanged between two nodes spans a wide range, from real-time data exchange with stringent delay requirements to the bulk exchange of planning data and schedules. ICCP can operate on top of a variety of transport layer protocols, both connectionless and connection oriented, but most often it is used on top of TCP/IP.

Although ICCP was standardized only a few years ago, it does not include either confidentiality, or integrity, or authentication. It only provides access control via so called bilateral tables. Bilateral tables specify the access rights between two control centers that have an ICCP association. Confidentiality, integrity, and authentication can be provided by lower layer protocols, for example, TLS when ICCP is used over the TCP/IP protocol stack. The number of nodes connected by ICCP associations in today's power systems is relatively low, in the order of tens, like in the case of the system shown in Fig. 5. As the number of nodes is low and control centers are relatively well protected key management is not an issue in practice today.

B. Beyond Cryptographic Security: Information Availability

With the problems of integrity, authentication, confidentiality and access control solved to a large extent, the most important issue in ICCC is information availability. Unlike in the past, when ICCC was performed mainly over dedicated point-to-point connections, such as leased lines, communication is shifting to public wide area networks, such as the Internet. The use of public network infrastructures might be cheaper, but it poses stringent requirements on network availability and it exposes ICCC to denial of service attacks. The resilience to network failures can be improved by maintaining multiple independent communication paths between the nodes, at the price of increased costs. If the ICCP connection is established over a TCP/IP network, multi-homing and redundant routers can be used to provide fast failover. The ICCP standard enables such solutions to be implemented over TCP, but there is no standardized solution, and hence the interoperability between the products of different vendors can be an issue in practice. Alternatively, ICCP can be used over the Stream Control Transmission Protocol (SCTP) and can rely on the multipath and failover capabilities of the transport layer protocol. In general there is, however, a trade-off between the frequency of path bouncing and the speed of path failover in the case of a network failure [11].

Denial of service attacks are even more difficult to mitigate. An attacker that monitors the data traffic of encrypted ICCP associations can use traffic analysis to extract information from the traffic patterns, e.g., it can detect the increase of data rates, which is typically a sign of abnormal system state, and can disable communications when it is most needed. Traffic analysis attacks can either be mitigated through masking (i.e., continuously transmitting at the peak rate) or through relaying over mixing networks, which delay every message at random upon relaying. In principle ICCP allows associations to be relayed over control centers, so that a mixing network can be used to hide the identity of the sender and the receiver of an ICCP association from an outside attacker [12].

Nevertheless, a mixing network introduces the possibility of inside attacks: due to the long life-cycles of SCADA systems software corruption is a threat, and the complexity of the code-base makes corruption hard to detect. A compromised control center 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 centers is to use anonymity networks to establish overlay routing paths among the control centers. 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 [12]. 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. The optimal system parameters might be hard to find in practice as they depend on the actual number of attackers, the number of communicating nodes and the traffic matrix [13].

V. Conclusion

The proper operation of today's power system relies heavily on IT, and in particular data communication. With performance and reliability as priority, IT and communication security have only been considered in recent years. Retrofitting a system as complex as today's power system communication and IT infrastructure and preparing it for the requirements of the smart grid is, however, a complex and challenging task. In this paper we discussed the major problems faced when improving power system security, with a special focus on communication security. We briefly described an attack tree-based framework for modeling system-security. Through the example of power system state estimation we showed how the deployment of new equipment can be leveraged to improve system security. Finally, we used the example of inter-control center communication to illustrate the importance of communication availability, which can be facilitated by but is not a direct consequence of cryptographic communication security. In general we believe that IT and communication security solutions for today's and tomorrow's power systems have to be designed with system-level security in mind, not only because doing so allows to maximize the benefit of security investments but also to ensure that the solutions satisfy the requirements in terms of performance, availability and cost.

VI. Acknowledgement

This work was funded by the EU FP7 VIKING project and by the ACCESS Linnaeus Centre at KTH.

References

[1] "NIST, NISTR 7628, Guidelines for Smart Grid Cyber Security, vol. 1-3," http://www.nist.gov, Aug. 2010.
[2] B. Schneier, "Attack trees: Modeling security threats," *Dr. Dobb's Journal*, December 1999.
[3] T. Sommestad, M. Ekstedt, and P. Johnson, "A probabilistic relational model for security risk analysis," *Computers & Security*, vol. 29, no. 6, pp. 659–679, 2010.
[4] T. Sommestad, H. Holm, and M. Ekstedt, "Effort estimates for vulnerability discovery projects," in *Proc. of 45th Hawaii International Conference on System Sciences*, Jan. 2012.
[5] P. Tsang and S. Smith, "YASIR: A low-latency, high-integrity security retrofit for legacy scada systems," in *Proc. of IFIP/TC11 International Information Security Conference*, 2008.
[6] A. Abur and A. Exposito, *Power System State Estimation: Theory and Implementation*. Marcel Dekker, Inc., 2004.
[7] Y. Liu, P. Ning, , and M. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. of ACM Conference on Computer and Communications Security (CCS)*, 2009.
[8] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. of IEEE SmartGridComm*, Oct. 2010.
[9] O. Vuković, K. Sou, G. Dán, and H. Sandberg, "Network-layer protection schemes against stealth attacks on state estimators in power systems," in *Proc. of IEEE SmartGridComm*, Oct. 2011.
[10] H. Mueller, "Outage analysis: Italy," *Network Manager News, News and Information for Users of Network Manager Worldwide*, vol. 2, no. 1, pp. 1–3, 2004.
[11] P. Natarajan, N. Ekiz, P. Amer, and R. Stewart, "Concurrent multipath transfer during path failure," *Computer Communications*, vol. 32, no. 15, 2009.
[12] K. Sampigethaya and R. Poovendran, "A survey on mix networks and their secure applications," *Proc. of the IEEE*, vol. 94, no. 12, pp. 2142–2181, 2006.
[13] O. Vuković, G. Dán, and G. Karlsson, "On the trade-off between relationship anonymity and communication overhead in anonymity networks," in *Proc. of IEEE International Conference on Communications (ICC)*, Jun. 2011.

György Dán received the M.Sc. degree in computer engineering from the Budapest University of Technology and Economics, Hungary in 1999, the M.Sc. degree in business administration from the Corvinus University of Budapest, Hungary in 2003. He received the Ph.D. in Telecommunications in 2006 from KTH Royal Institute of Technology, Stockholm, Sweden, where he currently works as an assistant professor. He was a visiting researcher at the Swedish Institute of Computer Science in 2008. His research interests include the design and analysis of distributed and peer-to-peer systems, and networking aspects of cyber-physical systems. He is a member of IEEE.
Email: gyuri@ee.kth.se
Phone: +46 8 790 4253
Fax: +46 8 790 8400
Mailing address: School of Electrical Engineering, KTH
Osquldas väg 10
10044 Stockholm, Sweden

Henrik Sandberg is an assistant professor at KTH Royal Institute of Technology in Stockholm, Sweden. His research interests include secure networked control systems, model reduction, and fundamental limitations of control systems. He has a M.Sc. degree in engineering physics and a Ph.D. degree in automatic control, both from Lund University, and was a postdoctoral scholar at the California Institute of Technology. He is an associate editor for the IFAC journal Automatica, and is a member of IEEE.
Email: hsan@ee.kth.se
Phone: +46 8 790 72 94
Fax: +46 8 790 73 29
Mailing address: Automatic Control, School of Electrical Engineering, KTH
Osquldas väg 10
10044 Stockholm, Sweden

Gunnar Björkman is employed at ABB Germany in the area of Network Management. He has held several management positions within R&D and Product Management among them acting as global R&D Manager for ABB's range of Network Control products between the years of 1995 to 1999. Björkman has been the Project Coordinator for the recently finished EU FP7 financed security project VIKING. He is also pursuing a PhD study on SCADA security at KTH Royal Institute of Technology in Stockholm, Sweden.
Email: gunnar.bjoerkman@de.abb.com
Phone: +49 621 3817364
Fax: +49 621 3817101
Mailing address:ABB AG, PSNMVM
Kallstadter Strasse 1
68309 Mannheim, Germany

Mathias Ekstedt is an associate professor at KTH Royal Institute of Technology in Stockholm, Sweden. His research interests include systems and enterprise architecture modeling and analyses with respect to information and cyber security, in particular for the domain of power systems. He is the manger of the program IT Applications in Power System Operation and Control within the Swedish Centre of Excellence in Electric Power Engineering and technical coordinator of the EU FP7 project VIKING. He received his PhD from KTH Royal Institute of Technology. He is a member of IEEE.

Email: mathias.ekstedt@ics.kth.se
Phone: +46 8 790 6867
Fax: +46 8 790 6839
Mailing address: School of Electrical Engineering, KTH
Osquldas väg 10
10044 Stockholm, Sweden