Cyber Security for Substation Automation, Protection and Control Systems

Steven Kunsman, Markus Braendle

ABB Inc.

steven.a.kunsman@us.abb.com

USA

1. Introduction

Substation automation, protection and control systems have changed significantly in the past decade and will continue to change with technology advancements. Systems have become more interconnected and provide end users with much more information to allow for higher reliability and greater levels of control. Interoperability between different vendor products and systems has been achieved by developing products and solutions based on open standards and by leveraging commercial technology like standard Ethernet technology. This change in technology has not only brought huge benefits from an operational point of view, it also permits substation automation, protection and control systems to address cyber security issues similar to other traditional, enterprise systems which have been facing the same industry challenges for years. Tightly integrating the control system components and allowing inter-connecting control systems with the external systems not only allows for more and faster information exchange, but, it also provides entry points for hackers and increases the need to protect against cyber-attacks. Using Ethernet and TCP/IP based communications not only make systems more interoperable, but also opened the door for trojans, worms, viruses and Internet based attacks, etc. The need for secure substation automation protection and control systems as well as the entire utility Information Technology infrastructure is being pushed in many markets by regulations to ensure national security due to the potential impact that a coordinated cyber-attack on the electric utility control system could have on wide scale outages. However, the answer is clearly not to block all advancements in new technology which from a reliability side can greatly improve the overall power system performance.

2. Drivers and Trends

Cyber security for automation and control systems in the electric sector has constantly gained attention and importance over the last couple of years. While in the past, cyber security was not considered an issue or a nice-to-have it as become more and more a must-have and continues to do so. There are different drivers and trends that affect the industry as a whole, e.g. how vendors must continue to address cyber security in their products, systems, processes, procedures, and services, or how end users must address security in procurement, installation and operation through both technical and non-technical means.

The level of attention and the drivers for cyber security differs around the world. Currently North America has the strongest focus on cyber security, with Europe being a fast-follower. South America, Middle East, and Asia are steadily increasing their focus. One can expect that in the near future the global interest will reach a similar level.

One of the two main drivers in North America is the NERC CIP (Critical Infrastructure Protection) regulation, for which compliance is mandatory for all utilities part of the bulk electric systems since 2010. The second main driver are the security requirements associated with SmartGrid stimulus funding and the clear statement by US government that no funding would be allocated to projects unless cyber security was properly addressed. Outside North America other countries will likely also increase the focus of government organizations on securing critical infrastructure resulting in local regulations and guidelines.

Overall the demand for cyber security, both from a technical as well as from a process perspective, will increase in the near future. Cyber security will become mandatory requirements in products, systems, solutions, and processes as industry standards are developed and regulations are adopted as law.

3. Reference Architecture

The reference architecture in this section is important to define key functions and their critical interfaces from the overall system perspective. The architecture is the fundamental blueprint for the system architect where key requirements are mapped onto system functions and interfaces as well where the cyber security requirements must be identified. The NIST Cyber Security Working Group is presently developing NISTIR 7628, "Smart Grid Cyber Security Strategy and Requirements." Common terms and language are important when reviewing the various work by industry experts and standardization bodies. Below is an extract from the Second Draft of NISTIR 7628 defining the domain and actors and their relationship in Figure 1 of the SmartGrid system architecture. One important aspect is to clearly define the role and function of an actor to be able to map the cyber security requirements to this role as well as the interface between two actors.

"A **Smart Grid domain** is a high-level grouping of organizations, buildings, individuals, systems, devices or other actors with similar objectives and relying on – or participating in – similar types of applications. Communications among actors in the same domain may have similar characteristics and requirements. Domains may contain sub-domains. Moreover, domains have much overlapping functionality, as in the case of the transmission and distribution domains. An actor is a device, computer system, software program, or the individual or organization that participates in the Smart Grid. Actors have the capability to make decisions and to exchange information with other actors. Organizations may have actors in more than one domain. The actors illustrated here are representative examples, and are not all the actors in the Smart Grid. Each of the actors may exist in several different varieties, and may contain many other actors within them."

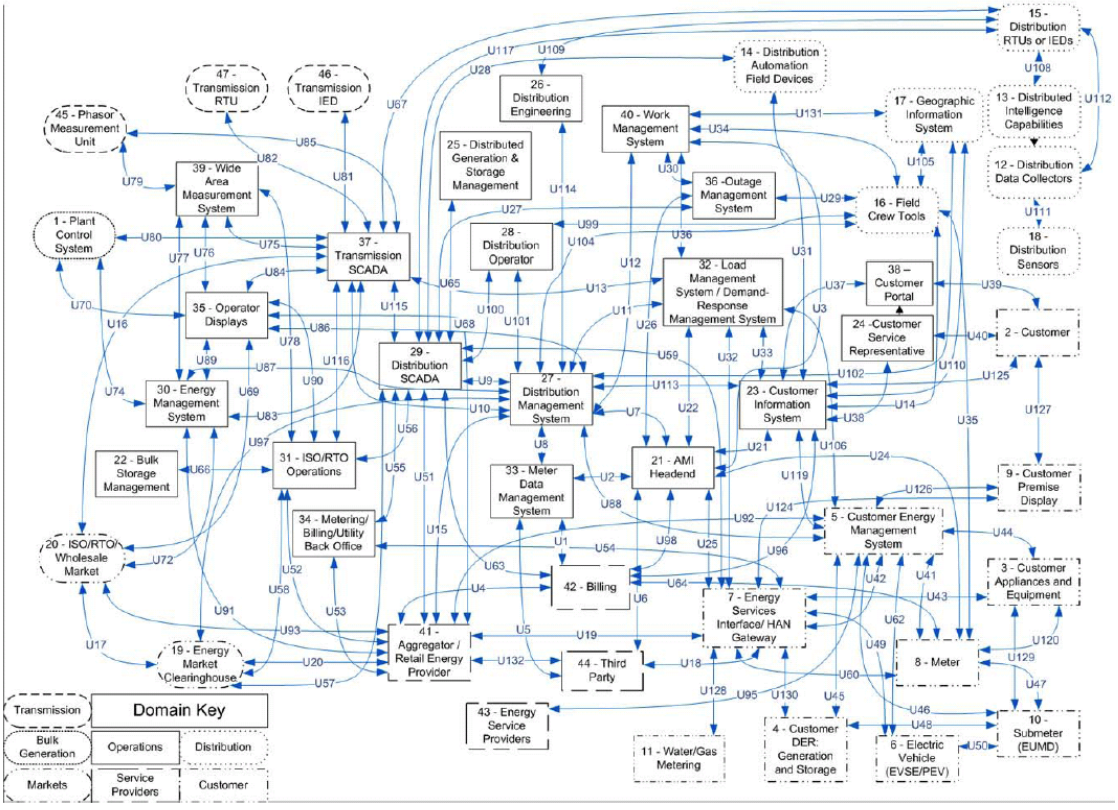


Figure 1 SmartGrid Architecture Source: Second Draft NISTIR 7628, "Smart Grid Cyber Security Strategy and Requirements – Feb 2010

As the NIST work focuses on the overall SmarGrid architecture, work has started in the IEEE Power and Energy Society, Power System Relaying and Substations Committees to define the cyber security requirements for substation automation, protection and control system. Reference architectures for substation automation systems are being defined such that all functions and interfaces related to the applications within the protection and control system are identified and cyber security requirements

mapped onto these components and interfaces. The following is an overview of the key actors from a functional and feature perspective for a substation automation protection and control system components:

- System / Protection Engineering & Maintenance (local and external)
- Station Human Machine Interface / Engineering Workstation
- Substation Control System (SCS)
- Intelligent Electronic Device (IED) / Protection and Control Relay
- Breaker IED
- Remote Terminal Unit (RTU) / Gateway
- Distribution Management System (DMS) / Gateway
- Asset Monitoring System
- Merging Unit / Sensor
- Intelligent Current / Potential Transformer / Non Conventional Instrument Transformer (NCIT)
- Phasor Measurement Unit (PMU) / Phasor Data Concentrator
- Security Management System (external and internal)
- Tele-protection / Inter station control (external)
- Supervisor Control and Data Acquisition (SCADA) (external)
- System Integrity Protection System (SIPS) (external)
- Wide Area Protection System (WAPS) / Wide Area Measurement System (WAMS) (external)
- GPS and Time Server (external)
- Distribution Sensor (external)

The reference architecture in Figure 2 is a Single Boundary Protection Architecture where perimeter protection is deployed and cyber security requirements can be defined on the actors inside the substation as well the interfaces that extend outside of the security perimeter. In this example, the key actors are the RTU/gateway, station computer/HMI and engineering workplace, protection and control IEDs, remote maintenance modem where cyber security solutions include adherence to device level standards, firewall and VPN protection, anti-virus protection, user access and device management.

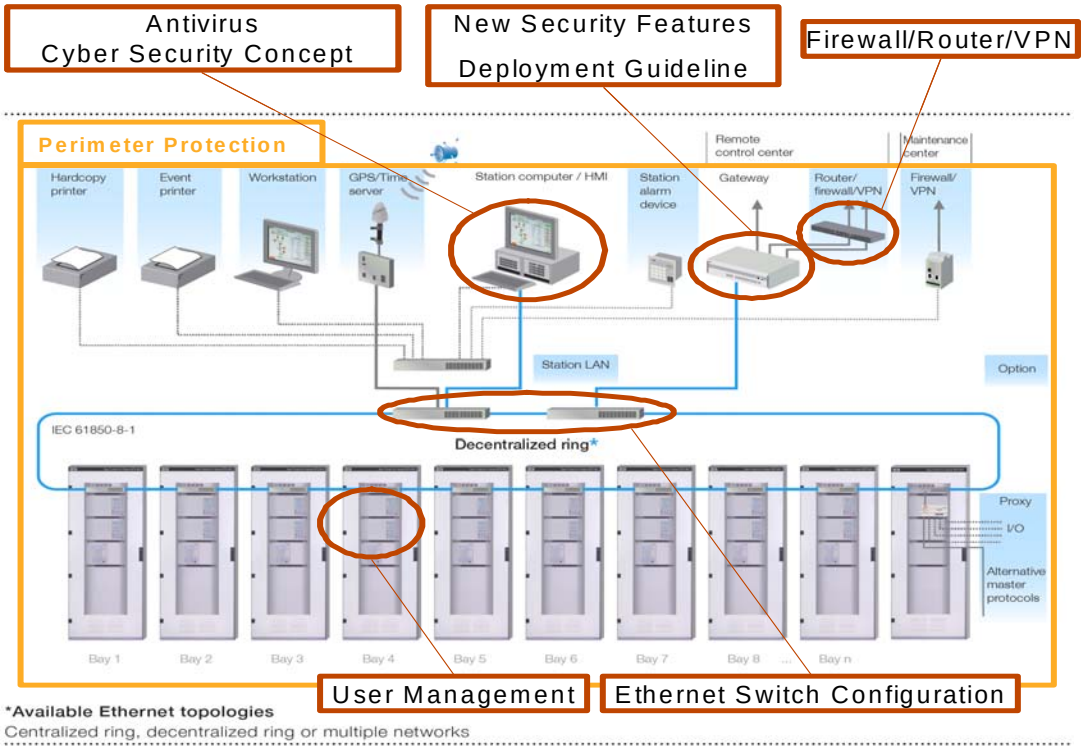


Figure 2: Example Substation Automation System Reference Architecture

In addition to the cyber security requirements on the actor and interfaces, the system architects needs to also consider other characteristics in the system design such as system performance, availability

and reliability. Overall system design and the security solutions can have an impact on system performance if the architecture has constraints like limited bandwidth, small CPUs or restrictive computational capability in some system components, highly distributed systems, slow response times, high sampling rates, etc. It is very important for these characteristics and constraints to be identified as part of the system architecture design and while implementing the security solutions.

Additional architectures are also possible for advanced applications like Process Bus architectures extending protection and control outside the single perimeter for IEC 61850-9-2 process bus interface to non-conventional instrument transformers. For this application, special consideration is required and the use of Multiple Boundary Protection where two or more separate perimeters are established and cyber security requirements are defined for each boundary interface and the functional components or actors with in the boundary. In addition to the process bus, other extension inside the substation can consider wireless interfaces for asset monitoring sensors and other types of monitoring equipment that can provide key information in the operation of the power system apparatus, planning or control system. Likewise, Substation to Substation architectures including tele-protection, SIPS and WAPS and downstream connections for distribution automation equipment pose additional considerations related to cyber security requirements. Each of these applications should have an associated reference architecture such that all actors and interfaces are defined, roles identified and cyber security requirements mapped to ensure safe and reliable operation of the power system.

From a North American perspective, the focus of cyber security requirements has been around NERC Critical Infrastructure Protection (CIP) which provides a foundation to make the power system more secure. NERC CIP today has governance over the bulk power system in the USA and does not apply to non-critical assets outside of the bulk power system. Cyber security architectures should be developed not only the bulk power system but as a utility generic policy and guide for achieving higher levels of security in protection and control systems. The architecture should be deployed independent of voltage level or criticality of cyber assets. It is expected that the US government will put additional regulations in place to help securing the SmartGrid expanding mandatory security requirements to all voltage levels in the power system.

4. Understanding the risk

Cyber security for automation and control systems has become a huge topic and everyone seems to have an opinion about it. The one thing that seems to be missing though is a true understanding of the actual risks. Detailed information on real incidents are still are rarity and solutions are usually based on technology decisions rather than a risk based approach. Many standards, regulations and guidelines exists today (see section 7) but few of them contain a rationale based on risk assessment or threat modeling. The driver and deciding factor for developing, purchasing and deploying security mechanisms is too often based on compliance - compliance to regulations, compliance to standards or compliance to industry “best practices”.

The situation today exists not because of a lack of risk assessment methodologies or because it is not regarded as important. The problem is that risk assessment methodologies use the probability of a threat and its potential impact as a means to calculate overall risk. While there are enough statistical data in enterprise IT environments for both, this statistical information is lacking for automation and control systems.

First, potential threat agents span from script kiddies to organized crime to nations states with threats ranging from malware, targeted attacks, to cyber terrorism. Opinions on how real all of these are and how likely an attack really is seem to be as different as the persons talking about it. Some say it is all just myth and nothing bad is going to happen while others predict doomsday tomorrow. Cyber terrorisms might be a real threat it might also not be, there is just not enough data to confirm or deny it. The truth lies somewhere in the middle; cyber security is a real issue, threat agents do exists and threats are a reality.

Secondly, potential impact of cyber-attacks on automation and control systems is quickly HUGE. Loss of electricity even only to a small residential area can have huge potential impact. Loss of heating in a cold winter or loss of air conditioning in a hot summer brings physical discomfort in the best case but can result in loss of life in the worst case. In traditional enterprise environments potential impact of cyber security incidents is typically measured in financial damage caused by loss of productivity, by downtime, by costs to replace and restore systems or by disclosing proprietary information. Potential damage for enterprise environments does typically not include loss of life.

So how does one then come up with a risk assessment of what to do if the attacker is not known, the likelihood is uncertain and the potential impact is extremely high in most cases? The answer is simple, by protecting what is most important - by answering the “what if” question. What if I cannot control this device anymore? What if somebody else can control this device? These questions have to be answered without considering any external influence at first, i.e. without looking at potential attackers and threats. If a certain device, certain system or certain piece of data is essential to the reliable operation of the primary equipment then it must be protected appropriately. It is important to point out another difference to enterprise IT security here. In a traditional enterprise the main target of protection is usually data, either from being disclosed or from being manipulated. For automation and control systems the main target of protection is the physical process and the primary equipment. The “what if” question must therefore not only be asked for the cyber assets but also, and maybe more importantly, for the primary equipment, e.g. “what if someone opens this breaker?” or “what if this breaker does not open in an emergency?”

Two common misconceptions that still wrongly influence decisions with respect to cyber security solutions are underrating the risk of non TCP/IP based protocols and overrating the risk of physical attacks. Use of serial protocols is often thought of as being a “secure” solution that does not require protection. This belief is sometimes so strong that existing TCP/IP based solutions are replaced with serial protocols for security reasons. Unfortunately this misconception is strengthened by the current NERC CIP regulation which excludes serial protocols as a potential threat vector. However, any communication link can be used for a cyber-attack. Serial protocols might be less prone to attacks but the risk of attacks using serial communication links should by no means be neglected. This fact will likely be reflected by the changes in the upcoming 4th revision of the NERC CIP regulation and is also reflected by ongoing standardization efforts (e.g. IEEE 1711).

Another argument that is often made when discussing the risk of cyber-attacks is the comparison to physical attacks: “if an attacker is physically present in the control environment, e.g. in the substation, it would be much easier to physically damage the equipment than to launch a cyber-attack”. While this statement in not false, it presents a too simplistic view. Yes, physically damaging the equipment is much easier and does not require much know-how, but physically damaging the equipment is also discovered very quickly and the impact is limited locally. A cyber-attack on the other hand could be much more sophisticated, e.g. forcing the system to run inefficiently for a long time without notice or changing protection settings to force unexpected behavior in an emergency. In addition a cyber-attack the local substation might only be used as an entry point to get access to other systems.

5. Back to the basics

Before any specific solutions should be discussed there are a couple of “ground rules” that must be understood. They are the basics for any successful security program and should be committed to first.

Accept responsibility

Anyone involved with critical infrastructure and automation and control systems has to accept responsibility for improving and maintaining security:

- *Owner / operator*: In the end the owner / operator is responsible for security, cyber and physical, of any running control system. Of course the various functions, processes, technologies etc. that are needed to fulfill this responsibility depend to some extend on the work and support of others. But to make sure that the overall system security level is adequate at any point in time is the responsibility of the owner / operator. This responsibility also includes putting pressure on vendors and system integrators and making sure that they have clear requirements.
- *System integrator*: The system integrator is responsible for ensuring that the security capabilities of all system components are used and configured properly. This includes but is not limited to properly setting up network architectures, properly configuring firewall rule sets, or following hardening guidelines provided by the vendors.
- *Vendor*: The main responsibilities of a vendor are threefold: quality, functionality and processes. First, the vendors must take every step possible to increase the security quality, i.e. reduce the attack surface and remove as many vulnerabilities and weaknesses as

possible. This is mainly done by having a well-defined development process that embeds security artifacts such as threat modeling, security reviews orsecurity testing. Secondly, the vendors must develop security functionality to support customer and system integrator requirements. Security functionality includes things like proper access control, security logging, or support for protected communications. The biggest challenge here might just be the different and sometimes contradictory requirements of the many utility users, regulators and various industry working groups and standards. Last but not least vendors must put processes in place to support customers throughout the system lifecycle, e.g. for patch management or vulnerability handling.

Security is about processes

Technology alone can't address security, or, as Bruce Schneier put it, "security is a process, not a product" (www.schneier.com/crypto-gram-0005.html). Some of the biggest challenges in making substation automation, protection and control systems more secure thus relate to human behavior and organizational processes. The first step in any security program should be the development of a security policy – a document identifying the overall security goals and objectives and defining what the valuable assets are that need to be protected. The security policy is the basis for any technical, procedural, or organizational security mechanism, yet clearly defined security policies don't exist for many control systems today. Creating, communicating, and enforcing a security policy are management's responsibility and should no longer be neglected. After developing a security policy, the next step is to build in processes to help establish and enforce it. These processes, for example, would include employee hiring and leaving, but should also describe incident handling and disaster recovery. Additionally, the security policy should offer a well-documented plan about how to deal with possible security incidents or breaches and address questions such as what should be done, who must be involved, and how to restore the system. Just as important as having these processes documented is exercising them regularly to ensure they work.

From this it should also be clear that security is not a one-time investment or purchasing task where buying a "secure control system" or buying security add-ons will solve anything. Of course the technology foundation must be there, but security must be continuously addressed throughout the whole system lifecycle. Technology solutions must be maintained, updated and controlled regularly.

Ignore compliance - at least at first

Anyone that has compliance has their main security goal might as well just stop. Compliance or certification should never, NEVER be the main goal of ANY security activity. Any security expert will agree that there is no single solution that fits all, so why would compliance to a single requirement set be any different? The only exception to this might be a regulation or standard that has three simple requirements:

1. Perform a risk assessment according to a well-defined and vetted process
2. Eliminate all risks that exceed an acceptable risk level
3. Redo everything at least yearly

For anything else compliance or certification should be a side effect. If the regulation or standard is reasonable then compliance should be a natural step of any sound security program. As a vendor we have chosen to follow this principle. We do look at and contribute to all major standards and regulations but we defined our own security strategy and goals several years back under the assumption that if we do a good job any reasonable security standard or regulation will not be a big issue.

Standards or regulations and compliance to them can be a good thing though. Standards and regulations can provide guidelines when setting up a security program and allow external entities to get an impression of a company's security activities. Certification can provide assurance both within a company but also for external customers. But as stated, compliance and certification should be a natural side effect of any reasonable, serious security program.

There is no such thing as 100% security

Security is not perfect and it will never be - vulnerabilities are part of any computer system that was not developed without economic reasoning, i.e. unlimited funds for security. Stakeholders need to accept that automation and control systems are complex IT solutions that will have vulnerabilities and that 100% security is not possible. So instead of blaming a vendor that openly accepts a vulnerability they should see it as a sign of accepting responsibility. Instead of hiding instances of vulnerabilities vendors should accept them, and do anything to mitigate the associated risk – even if that means publicly admitting that there is a problem. Owner and operators on the other hand should not try to hide actual incidents but share them with others - not only so that everyone can learn and improve their security approach but also so that a discussion based on facts, i.e. real incidents can start.

The fact that there is no such thing as 100% security also means that there will always be security breaches and incidents. It is therefore extremely important to not only put protection mechanisms in place but also mechanisms to quickly detect incidents and to be able to effectively react to and isolate security breaches.

Security does not come for free

Another area where a reality check needs to happen is when looking at the cost of security. Achieving and maintaining an adequate level of security does not come for free. This is again true for all stakeholders involved in critical infrastructure and automation and control systems. So everyone must be willing to make security investments for the long run and include the costs in their business models. It would be naïve to think that anyone can increase or provide security without costs and that cyber security does not follow normal economic principles.

6. High Level Security Approaches

Security for substation automation, protection and control systems must cover both physical and cyber aspects. Physical protection includes e.g. setting up physical boundaries, e.g. a fence, a closed control house or locked cabinets or installing video cameras for monitoring purposes. Both physical and cyber protection are necessary, but we will in the following focus on cyber aspects.

Any security architecture must be tailored to the specific installation and should be based on a risk and security assessment. Any system is only as secure as its weakest element. An attacker will actively try to find the weakest element, therefore for a given budget one should strive to achieve a balanced defensive strength across all system components and attack vectors. One of the first steps should always be to do an assessment of the system architecture, which includes identifying the critical assets and all external connections. A typical, modern substation automation, protection and control system will have at least bay level devices that use real-time communication protocols and are responsible for providing protection and station level computers that are used as HMI or gateways to external entities or remote terminal units that connect to network control centers.

Defense in depth

The most important principle for any security architecture is defense-in-depth. Having a single layer of defense is rarely enough as any security mechanism may be overcome by an attacker, It is therefore recommended to architect the system in a way that the most sensitive parts of the system are protected by multiple rings of defense that all have to be breached by the attacker to get to those “crown jewels”.

In addition not only protection mechanisms should be deployed but also means of detecting attacks. This includes both technical measures, such as intrusion detection systems, as well as procedural measures, such as review of log files or access rights.

Least-privileges

A second very important principle to follow in any security program is the principle of “least privileges”. No user or process should be able to do more in the system than what is needed for the job. This principle is not only key to prevent malicious attacks but also very important in preventing “accidents”.

Spreading of a virus for instance that sits on the laptop of an authorized user, can be limited if the user only has minimal access to the system and network.

Network separation

Any computer network should be divided into different zones depending on the criticality of the nodes within each zone. In a typical substation automation environment separate zones could be envisioned for bay level devices and for the station level devices and computers. Depending on the size of the substation having separate zones for bay level devices for each bay might make sense. Zones should be separated by a firewall, application gateway or similar.

In addition the substation automation, protection and control network should be clearly separated from any external network. This can be achieved by e.g. using firewalls to control data access to the control network. In order to authenticate accessing entities, the combination of a firewall with a VPN gateway is a good solution. A more secure architecture is to work with a so-called DMZ (demilitarized zone); a zone that serves as a proxy between external networks and the control system.

The single electronic security perimeter required by NERC CIP will often not be enough and is a good example of why doing security for compliance reasons is not good enough.

Protected communications

Communication both within a substation automation system and with external networks should be protected using encryption and / or message integrity protection if possible. However before doing so, one must look at the performance requirements of the communication links to be protected and take the impact of cryptographic algorithms into account.

For external connections the use of VPN (virtual private networks) is recommended for both operational as well as maintenance and engineering connections. This especially until electric industry specific protocols and the communication gateways supporting those have security built-in. There are currently several industry initiatives on-going to secure e.g. DNPv3 or IEC 60870-5-104, but until products are available supporting these new protocols use of VPN technology can bridge the gap.

Within a substation the situation is similar. For engineering and maintenance access secures protocols such as HTTPS or SSH should be used if available (even if the accessing engineer is physically within the substation).

System Hardening

Relying on network separation and protected communication is not enough. The defense-in-depth principle also demands protecting each individual system component, which includes system hardening. Every single device or computer within the substation automation, protection and control system must be hardened to minimize its attack surface. Hardening includes restricting applications and open ports and services to an absolute minimum. System hardening must also look at user accounts and ensure that only needed accounts are installed, e.g. no guest accounts, and that strong authentication is enforced. This step is best done by asking vendors to provide information on e.g. ports or applications that are needed for normal operations and security hardening guidelines for their products and systems.

Dealing with portable media

Besides static, direct connections between the control network and external networks there also exists temporary, indirect connections that are often not considered when securing substation automation, protection and control systems. Examples for such temporary, indirect connections are mobile devices such as service laptops or portable media such as USB sticks or CDs that are connected to computers within the control network. Because these mobiles devices and portable media are rarely used only within the substation (even though they should in an optimal case) they must be considered a security risk and the control network must be protected accordingly.

Protecting from risks associated with mobile devices, e.g. an infected engineering laptop, can be done by only allowing connecting such mobile devices at dedicated points within a dedicated zone. These zones should be separated from the control network with at least a firewall and should additionally contain intrusion detection systems or malware scanners. The dedicated zone should also create detailed audit logs of all activities.

Protecting from risk associated with portable media, e.g. an infected USB stick, is best done by disabling such media on all hosts. If the use of such portable media is really needed then this should only be possible on hosts that have malware protection running. A more secure solution would be to first scan the portable media on a dedicated "malware scanning station" that is not directly connected to the control network and has up-to-date malware detection software running.

7. Overview of security standards, regulations, and working groups

With the increased importance for cyber security of automation and control systems various working groups have taken on the topic in an attempt to provide standards, regulations, guidelines, or best practice documents. The focus, level of detail and maturity of these documents is quite broad and not all of them are equally applicable for substation automation, protection and control systems. At the moment five initiatives seem to be most advanced, which we will discuss in the following paragraphs.

NERC CIP

The NERC CIP regulations have had the biggest impact on electric utilities so far and been the focal point of most security programs. NERC CIP makes it very clear that the main responsibility for securing the electric grid lies with the utilities and that it is not just about technology. There are some shortcomings of the current version, i.e. the exclusion of serial protocols or the focus on a single electronic security perimeter, but these will likely be addressed in the currently ongoing 4th revision. The NERC CIP regulation is a good example of why compliance should not be the main goal of any security program. Because the regulation is changing and extending its scope utilities that focused their security program on complying to the versions currently in effect will run into problems with future releases.

NIST Smart Grid

Cyber security has been identified as a key enabler for the NIST Smart Grid activities and has gotten a lot of attention within the NIST driven Smart Grid activities. In February 2010 the second draft of the "Smart Grid Cyber Security Strategy and Requirements" document has been released for public comments. The document tries to take a holistic view of cyber security for Smart Grid, i.e. by looking at all applications of Smart Grid. The 2nd draft contains high level security requirements that will have an influence on substation automation, protection and control systems. However, at the time of writing it is not clear yet to what level of detail the requirements will be and how much tailoring needs to be done.

IEEE PES Substation C10 /PSRC H13

Within IEEE PES Substations and PSRC, a joint working group has been formed to look at the applicability and the technical implementation of the NERC CIP and NIST Smart Grid security efforts for substation automation, protection and control systems. The goal of the joint WG is to prepare a standard on "**Cyber Security Requirements for Substation Automation, Protection and Control Systems"** which provides technical requirements for substation cyber security. It presents sound engineering practices that can be applied to achieve high levels of cyber security of automation, protection and control systems independent of voltage level or criticality of cyber assets. Cyber security includes trust and assurance of data in motion, data at rest and incident response.

IEC 62351

IEC 62351 is a technical security standard that aims to secure power system specific communication protocols such as IEC 61850 or IEC 60870-5-104. While most parts of the standard have been

released in 2009 more work is needed before systems compliant to IEC 62351 can be put on the market. First of all the affected communication standards must be changed to support IEC 62351. In addition there are some technical challenges with securing real time traffic that must be addressed by the working group of IEC 62351. [1] gives a more detailed introduction of the IEC 62351 standard series and provides insights on technical limitations as they relate to substation automation, protection and control systems.

IEEE 1686

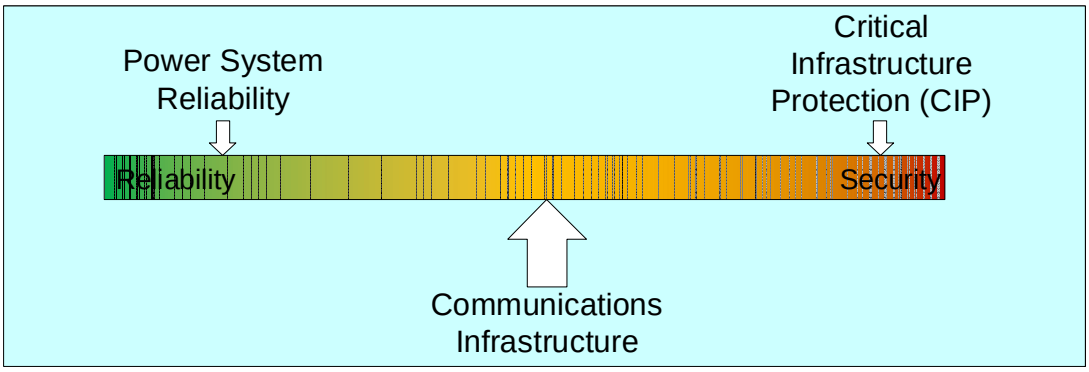
Security of intelligent electronic devices is the scope of IEEE 1686. The document defines in technical detail security requirements for IED's, e.g. for user authentication or security event logging. The standard very nicely points out that a) adherence to the standard does not ensure adequate cyber security, i.e. that adherence to the standard is only one piece in the overall puzzle, and that b) adherence to every clause in the standard may not be required for every cyber security program. With this the standard gives vendors clear technical requirements for product features but at the same time leaves room for specific, tailored system solutions at the customer site.

8. Security impact on system reliability

Evolving technologies like Ethernet and SA standards IEC 61850 are enablers for information exchange to provide the higher reliable system. These commercial and open technologies are much different than the traditional vendor/utility proprietary systems. The key is to take advantage of the open technology at the same time creating a security architecture and philosophy improving the overall security of the Substation Automation System as well as the entire utility IT infrastructure.

As discussed earlier, advanced power system applications are being developed like SIPS and WAMS where their benefit can greatly improve overall system performance and reliability. The challenge between system cyber security and system reliability can be extreme. From a system cyber security perspective, the utility IT infrastructure being restrictive and limiting access will certainly make it more difficult and combat against the external threats. The present NERC/CIP standard is applicable to communications infrastructures using routable protocols (e.g Ethernet TCP/IP). Adherence to the CIP standards can be achieved by deploying serial "non-routable" protocols. The consequence of this is readily observed on the system reliability because the advanced power system application. These applications requiring substation-to-substation exchange of real-time phasor information is not possible via a DNP 3,0 serial interface due to bandwidth limitations.

To return to the discussion in the architecture section, understanding the system performance requirements is critical in being able to deploy a cyber security solution that will meet the utility's security policies. The overall architecture must support the intended application goals and in the example of SIPS, it is improving the overall system reliability which is the ultimate goal of both security and power system performance.



Therefore, the optimal system architecture has the communications infrastructure as a balance to provide the necessary protection to mission critical assets while permitting the information flow that

enables the advanced applications that provide improved system reliability. It is a balance between reliability vs. cyber security.

9. Summary

When we look at the organizations involved in maintaining utility system security—vendors, integrators, end users—it's fair to say that security is "everybody's business." To the extent these groups cooperate with one another throughout the system lifecycle, security will be enhanced. At the same time, perhaps the most important aspect of security for the various players to keep in mind is that it is a journey and not a destination. There will always be new threats. Likewise, there will be new methods and technologies for meeting those threats. Vigilance, cooperation and technical expertise, when applied in unison, offer the best defense.

Literature

[1] F. Hohlbaum, M. Braendle, F. Alvarez, „Cyber Security - Practical considerations for implementing IEC 62351", PAC Conference 2010

Authors Information

Markus Braendle

Division Cyber Security Manager, ABB Power Systems Division

Markus is globally responsible for all aspects of cyber security within ABB's Power Systems division. He heads the Power Systems Security Council which defines, develops, and implements the security strategy for all products and systems within the Power Systems division. Markus is an active member of several security standardization efforts and working groups, e.g., IEEE PSRC H13, Cigre B5.38, ICSJWG or NIST SmartGrid CSCTG, and a recognized member in the industrial control system security community. Markus holds a doctoral degree in Computer Science from the Federal Institute for Technology in Zurich, Switzerland.

Steven A. Kunsman

Group Assistant Vice-President and Head of Global Product Management, ABB Power Systems Substation Automation Products

Steve joined ABB Inc. in 1984 and has 26 years of experience in Substation Automation, Protection and Control. He graduated from Lafayette College with a BS in Electrical Engineering and Lehigh University with an MBA concentrated in Management of Technology. Today, Steve is responsible for ABB Power Systems Substations/Substation Automation Products portfolio worldwide. He is an active member of the IEEE Power Engineering Society PSRC including working group chairperson for H13, an IEC TC57 US delegate in the development of the IEC61850 communication standard and UCA International Users Group Executive Committee co-chairperson.