

# Balancing the Demands of Reliability and Security

## Cyber Security for Substation Automation, Protection and Control Systems



### 1. Introduction

In the past decade, substation automation, protection and control systems have changed significantly, and this transformation promises to continue as increasing demands on the utility infrastructure mandate continued technology advancements. Systems have become more interconnected, providing end users with much more information and enabling higher reliability and greater levels of control. Interoperability between different vendor products and systems has been achieved through product and solution development based on open standards, and by leveraging commercial technologies like standard Ethernet. These technological advances have not only delivered significant operational benefits, but have also increased the exposure of substation

automation, protection and control systems to cyber security issues similar to those faced for years by other traditional enterprise systems.

Tightly integrating the control system components and inter-connecting control systems with external systems not only allows for more and faster information exchange, it also provides entry points for hackers, thereby increasing the need to protect against cyber-attacks. The use of Ethernet and TCP/IP based communications not only makes systems more interoperable, but also opens the door for trojans, worms, viruses and Internet based attacks. The mandate for secure substation automation protection and control systems, as well as security of the entire utility Information Technology infrastructure, is being pushed in many

markets with regulations intended to preserve national security by protecting an electric utility control system from a coordinated cyber-attack with the potential to cause wide scale outages. However, security challenges notwithstanding, the answer is clearly not to block advancements in technology which, from a reliability perspective, will continue to greatly improve the overall power system performance.

## 2. Drivers and Trends

Cyber security for automation and control systems in the electric sector has consistently gained attention and importance over the last couple of years. While in the past, cyber security was not considered an issue, or even a nice-to-have, it has more and more become a must-have, and its importance continues to grow. 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 differ around the world. Currently North America has the strongest focus on cyber security, with Europe being a fast-follower. South America, the 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 that are part of the bulk electric systems. The second main driver is the security requirement associated with Smart Grid stimulus funding and the clear statement by the US government that no funding would be allocated to projects unless cyber security was properly addressed. Outside North America other countries will likely 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 a mandatory requirement 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 in order 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 as where cyber security requirements are identified.

A **Smart Grid domain** is a high-level grouping of organizations, buildings, individuals, systems, devices or other actors with similar objectives that rely on, or participate in, similar types of applications. Actors have the capability to make decisions and to exchange information with other actors. Communication among actors in the same domain may have similar characteristics and requirements. Domains may contain sub-domains. Moreover, domains may have much overlapping functionality, as is the case of the transmission and distribution domains. Organizations may have actors in more than one domain. Each of the actors may exist in several different varieties, and may contain many other actors within them.

Common terms and language are important when reviewing the various works of industry experts and standardization bodies. The NIST Cyber Security Working Group is presently developing NISTIR 7628, "Smart Grid Cyber Security Strategy and

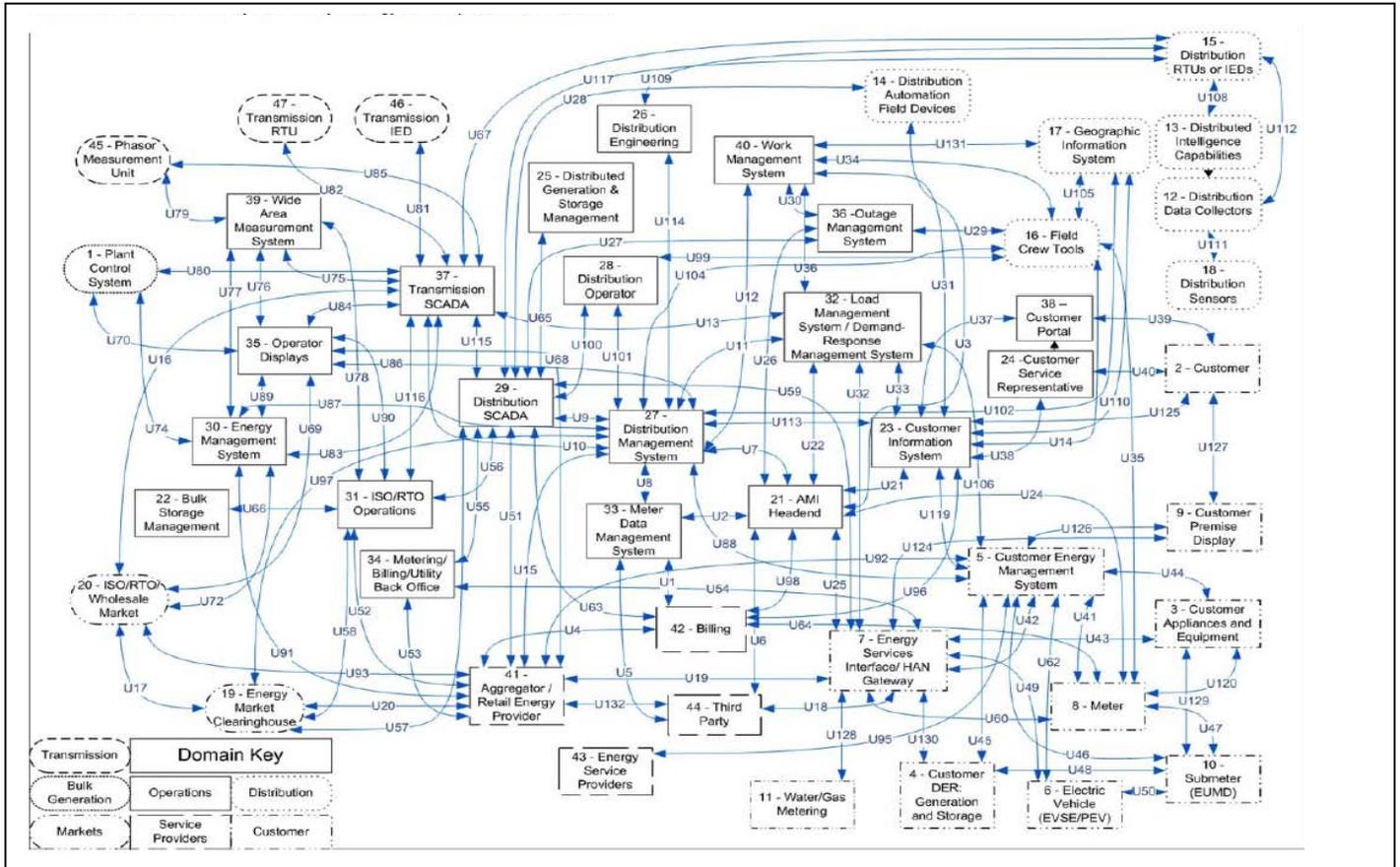


Figure 1 Smart Grid Architecture Source: Second Draft NISTIR 7628, “Smart Grid Cyber Security Strategy and Requirements” – Feb.

Requirements”. Figure 1 is an extract from the Second Draft of NISTIR 7628 defining the domain and actors and their relationship in the Smart Grid system architecture. An important aspect of the strategy is to clearly define the role and function of an actor and the interface between actors in order to map the cyber security requirements for each actor. The actors illustrated here are representative examples, and are not all the actors in the Smart Grid.

Just as the NIST work focuses on the overall Smart Grid 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 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.

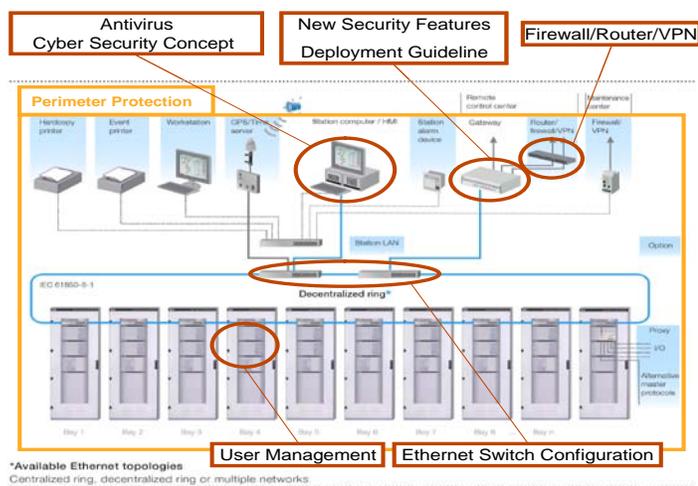


Figure 2: Example Substation Automation System Reference Architecture

In addition to the cyber security requirements on the actor and interfaces, the system architects need 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, such as Process Bus, are also possible for advanced applications such as extending protection and control outside the single perimeter for IEC 61850-9-2 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 as well as the functional components, or actors, within the boundary, is recommended. 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.

Cyber security architectures should be developed not only for the bulk power system, but also 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 secure the Smart Grid, 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. However, the one thing that seems to be missing is a true understanding of the actual risks. Detailed information on real incidents is still a rarity and solutions are usually based on technology decisions rather than a risk based approach. Many standards, regulations and guidelines exist 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 is not due to a lack of risk assessment methodologies, or because cyber security 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 nation states posing threats ranging from malware, to targeted attacks, to cyber terrorism. Opinions on how real all these threats are, and how likely an attack really is, seem to be as different as the people talking about them. Some say it is all just myth and nothing bad is going to

happen while others predict doomsday tomorrow. Cyber terrorism might be a real threat -- it might also not be, there just is not enough data to confirm or deny it. The truth lies somewhere in the middle; cyber security is a real issue, threat agents do exist and threats are a reality.

Second, the potential impact of cyber-attacks on automation and control systems is fast and HUGE. Loss of electricity, even only to a small residential area, can have significant detrimental 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, downtime, costs to replace and restore systems, or disclosure of proprietary information. Potential damage for enterprise environments does not typically include loss of life.

So how does one then come up with a risk assessment of what to do if, in most cases, the attacker is not known, the likelihood is uncertain, and the potential impact is extremely high? The answer is simple, protect what is most important. Identify 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 must 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 disclosure or from manipulation. 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 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 is not false, it presents too simplistic a 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 on the local substation might only be used as an entry point to gain 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 extent on the work and support of others. But, making 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 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, and/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, and/or security 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, and/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](http://www.schneier.com/crypto-gram-0005.html)). Thus, some of the biggest challenges in making substation automation, protection and control systems more secure 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 valuable assets 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 is 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 separation, 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 who has compliance as their main security goal might just as well 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 annually

For anything else, compliance or certification should be an ancillary effort. 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 analyze, and contribute to, all major standards and regulations. However, we defined our own security strategy and goals several years ago under the assumption that, if we do a good job, any reasonable security standard or regulation will be accommodated.

Standards, or regulations, and compliance to them can be a good thing. They 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 never will 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 condemning a vendor that openly acknowledges a vulnerability, users should recognize this 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 there is a problem. Likewise, owners and operators should not try to hide actual incidents but should 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 begin.

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 is not free

Another area where a reality check needs to occur is when looking at the cost of security. Achieving and maintaining an adequate level of security is not free. This is again true for all stakeholders involved in critical infrastructure and automation and control systems. 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 setting up physical boundaries, e.g. a fence, a closed control house, locked cabinets, or installing video cameras for monitoring purposes. Both physical and cyber protection are necessary, but, for the purpose of this discussion, we will focus on cyber aspects.

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. As well, station level computers 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 must be breached by an attacker in order to get to the “crown jewels”.

In addition, not only should protection mechanisms be deployed, but also the 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 preventing malicious attacks but also very important in preventing “accidents”. For instance, spreading of a virus 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 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 security for compliance sake is not sufficient.

### 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 into account the impact of cryptographic algorithms.

For external connections, the use of VPN (virtual private networks) is recommended for both operational as well as maintenance and engineering connections. This is especially recommended until electric industry specific protocols, and the communication gateways supporting them, have

security built-in. There are currently several ongoing industry security initiatives, e.g. DNPv2 or IEC 60870-5-104, but until products are available to support these new protocols the use of VPN technology can bridge the gap.

Within a substation the situation is similar. For engineering and maintenance access, security 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, this 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 ports or applications that are needed for normal operations, as well as 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 of 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 mobile 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 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 permitted at dedicated points within a dedicated zone that is separated from the control network by at least a firewall and has 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, in addition to government driven efforts 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, the following five initiatives discussed below seem to be the most advanced.

### NERC CIP

To date, the NERC CIP regulations have had the biggest impact on electric utilities and have been the focal point of most security programs. The regulation makes a clear statement that the main responsibility for securing the electric grid lies with the utilities and that it is not just about technology but also about processes. There are some shortcomings of the current version, i.e. the exclusion of serial protocols or the focus on a single electronic security perimeter. An additional area for improvement is the definition of critical assets and critical cyber assets. While the definition of what is deemed critical and what is not has been made a bit clearer with version 4, protection of critical (cyber) assets is still done in

an all or nothing fashion. If a cyber-asset is classified as critical all NERC CIP requirements apply. If it is not classified as critical then it need not be protected at all (unless it is within the electronic security perimeter). This all or nothing approach does not take into account different levels of criticality and does not allow for different levels of security, which is a common best practice for security of computer based systems. However, the current ongoing revision is looking at different levels of criticality, which will hopefully lead to a more realistic and more granular approach to cyber security.

### NIST Smart Grid

Cyber security has been identified as a key enabler for the NIST Smart Grid activities and has therefore received much attention within NIST. NIST has released their “Guidelines for Smart Grid Cyber Security” a three volume, 577 page document. The document attempts to take a holistic view of cyber security for Smart Grid, i.e. looking at all applications of Smart Grid. The document acknowledges the reality that not all systems can be equally secured and defines different levels of security (low, moderate, and high) and the different requirements for each.

### IEEE PES Substation C10 /PSRC H13 (IEEE C37.240)

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 were released in 2009, more work is needed before systems compliant with IEC 62351 can be released to the market. First, all the affected communication standards must be changed to support IEC 62351. Additionally, some technical challenges with securing real time traffic must be addressed by the working group of IEC 62351. [1] provides 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.

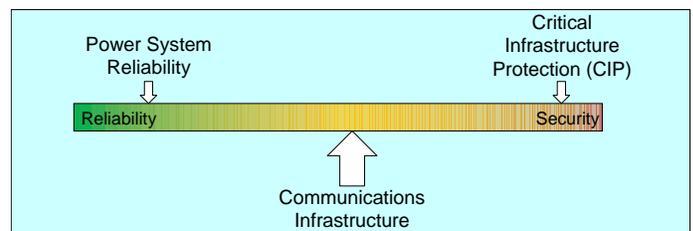
## 8. Security Impact on System Reliability

Evolving technologies like Ethernet and SA standards like IEC 61850 are enablers for information exchange necessary to provide higher system reliability. 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 like SIPS and WAMS are in development. While their benefit can greatly improve overall system performance and reliability, the reconciliation between system cyber security and system reliability can be extreme. From a system cyber security perspective, a restrictive utility IT infrastructure with limited access will certainly make a breach more difficult and combat against 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. However, the system reliability consequence of this is readily observed due to the inability to support advanced power system applications requiring substation-to-substation exchange of real-time phasor information, as this is not possible via a DNP 3.0 serial interface due to bandwidth limitations.

To return to the discussion from the architecture section above, 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 necessary to protect

mission critical assets while permitting the information flow that enables the advanced applications required to improve 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**

Head of Cyber Security, ABB Group

Markus is globally responsible for all aspects of cyber security for the ABB Group. He heads the ABB Group Cyber Security Council a cross-divisional and cross-functional effort to ensure that ABB offerings fully support customers' cyber security requirements. Prior he was the Head of Cyber Security for the Power Systems division and held a number of specialist and management roles within Corporate Research. Markus is a member of several international cyber security standardization efforts and working groups and a recognized member in



the industrial control system security community. Markus holds a doctoral and a masters degree in Computer Science from the Federal Institute of Technology in Zurich, Switzerland.

#### **Steven A. Kunsman**

Vice-President and General Manager, ABB Power Systems - Substation Automation Products North America



Steve joined ABB Inc. in 1984 and has 27 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 North American Power Systems Substation Automation Products business. 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.

## Contact us

ABB Inc.  
North America Corporate Headquarters  
12040 Regency Parkway  
Suite 200  
Cary, NC 27518  
[www.abb.com/substationautomation](http://www.abb.com/substationautomation)