“Developing a Framework to Improve Critical Infrastructure Cybersecurity”

ABB Response to NIST RFI

DISCLAIMER

THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE. NOTHING HEREIN SHALL BE CONSTRUED AS A COMMITMENT OR REPRESENTATION BY ABB. ABB PROVIDES NO WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT TO THE INFORMATION OR PROCESSES CONTAINED IN THIS DOCUMENT, AND ASSUMES NO RESPONSIBILITY FOR SUCH INFORMATION OR PROCESSES OR FOR ANY ERRORS OR OMISSIONS.

IN NO EVENT SHALL ABB BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR FINANCIAL OR ECONOMIC LOSS OF ANY NATURE OR KIND ARISING FROM THE USE OF, OR RELIANCE ON, THIS DOCUMENT, OR ARISING FROM USE OF ANY SOFTWARE OR HARDWARE COVERED BY THIS DOCUMENT.

About ABB

ABB is a global leader in power and automation technologies. Based in Zurich, Switzerland, the company employs 145,000 people and operates in approximately 100 countries, including the United States of America. The company in its current form was created in 1988, but its history spans over 120 years. ABB's success has been driven particularly by a strong focus on research and development. The company maintains seven corporate research centers around the world and has continued to invest in R&D through all market conditions.

The result has been a long track record of innovation. Many of the technologies that underlie our modern society, from high-voltage DC power transmission to a revolutionary approach to ship propulsion, were developed or commercialized by ABB. Today, ABB stands as the largest supplier of industrial motors and drives, the largest provider of generators to the wind industry, and the largest supplier of power grids worldwide.

ABB supplies technology, products and services to a number of the sectors defined as critical infrastructure according to the definition in 42 U.S.C. 5195 - for example electrical power systems, gas and oil production, refining as well as pipelines, water supply and sewage systems or manufacturing. Besides supplying to these critical infrastructures, ABB itself operates a number of manufacturing sites in the U.S., e.g. manufacturing of power transmission equipment and electrical equipment. As such, the responses below focus on the sectors in which industrial control systems (ICS, e.g. DCS, SCADA) and similar systems are used. We acknowledge that our statements may not be applicable to sectors that we are not involved in.

Cyber Security at ABB

ABB fully recognizes and understands the importance of cyber security for its customers and has thus created an organization with top management support at the Group level responsible for all aspects of cyber security. Safety and reliability are given the highest priority in all of our products, systems and services. Cyber security, which is a key aspect of these efforts, is not viewed as a one-time activity, but as an integral and continuous part of the product lifecycle, from early design and development, through testing and commissioning, to life time support service and future adaptations. Similarly, cyber security is viewed as an integral and continuous part of our project lifecycle ensuring both the delivery of a critical infrastructure solution with the appropriate security properties as well as secure execution of the project work itself. Furthermore we strive to support our customers in their efforts to operate and maintain their solutions' security properties throughout their entire operations period.

We continue to build expertise in this area and partner with industry collaborators and specialists as well as academia. By understanding market conditions, customer needs and the cyber environment, ABB works closely with customers to achieve the necessary levels of cyber security without compromising operational performance. These solutions are aimed at reducing business risk, providing comfort and confidence, as well as enabling compliance with standards and legal requirements.

Cyber security issues have been the subject of standardization initiatives by IEEE, IEC and ISA for some time and ABB plays an active role in all these organizations, helping to define and implement cyber security standards for power and industrial control systems. The objective is to establish the necessary levels of cyber security, and maintain that level, even in the face of challenges, while preserving the availability and functional interoperability of systems. As an extension of these efforts in standardization we greatly appreciate the opportunity to provide input to the NIST response to the President's Executive Order 13636.

ABB Response to RFI

1.1 Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cyber security factors into that risk assessment; the current usage of existing cyber security frameworks, standards, and guidelines; and other management practices related to cyber security. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements.

1.1.1 What do organizations see as the greatest challenges in improving cyber security practices across critical infrastructure?

The biggest challenges in improving cyber security for critical infrastructures can be categorized largely in two major groups – organizational challenges which are dominantly concerning people, policies and procedures (e.g. awareness, training, organizational structure, rules and operational maturity) and technical challenges which are dominantly concerning technological issues (e.g. domain specific protocols, adapting enterprise IT security solutions for the control system domain).

Among the organizational challenges, the biggest ones include

- Risk management models for cyber security which deal appropriately with the specific challenges that historic data is largely unavailable and – due to the dynamic nature of the threat landscape – of limited use in forecasts of the future risk exposure
- Ensuring awareness for cyber security risks and necessary measures to address them across the organization but with appropriate level of information for the individual’s role
- Competence management including defining the cyber security aspects of organizational roles, defining cyber security specific roles in the organization, defining necessary skills for the individual roles and finding the appropriate people to fill the roles and ensuring continuous training to build and maintain the necessary skills for these people
- Avoiding disruptive changes which would impact normal business operations while at the same time adopting cyber security practices in the organization and prioritizing on those changes which promise the biggest cyber security improvement

Among the technical challenges, the biggest ones include

- Securing an aging installed base, i.e. cyber security solutions not only need to protect systems that are commissioned or upgraded today but a strategy is required that also includes a large installed base
- Sustaining the security over time, e.g. deploying updates and patches to address newly found vulnerabilities and newly discovered emerging threats, maintaining access control to match the needs of a changing organization
- Situational awareness for cyber security, i.e. monitoring the system events for potentially suspicious events, analyzing those events and identifying cyber security incidents – in a timely fashion to allow for appropriate response before incidents can have a significant impact on the critical infrastructure operations
- Securing heterogeneous environments, i.e. finding the right technology to ensure a common security level in environments with systems from multiple vendors, systems running on multiple platforms (incl. multiple generations of the same platform), or of otherwise heterogeneous technical nature
- Efficiently (i.e. ideally automatically) documenting compliance with a variety of requirements, from internal organizational standards, external voluntary standards to enforced regulations

1.1.2 What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

Different sectors will differ in a variety of aspects. The framework to be developed by NIST will have to be flexible enough to accommodate the different needs, but at the same time effective enough to actually improve the security posture and specific enough to give actionable guidance to organizations where it is needed. The aspects in which organizations might differ include:

- Fundamental operational and design principles – different industries have different fundamental principles in terms of operational practices and technical designs which are considered proven and state-of-the-art and which may be of relevance for security as well. The framework to be developed by NIST should be compatible with these principles, but at the same time provide actionable guidance on how to address cyber security in the application of these principles.
- Maturity levels of different sectors – the maturity level between different sectors varies and any framework to be developed must ultimately have the goal that all sectors reach a similar level. However, especially in the beginning, the framework must assure that sectors with a lower maturity level are presented with an approach that is ambitious but at the same time pragmatic, not too disruptive or overwhelming. For sectors with a higher level of maturity NIST must make sure that any framework developed does not slow down or event reduce that level of maturity. As an example the NERC CIP regulation had a very positive impact on utilities that did not have a mature security program, however they left and still leave little motivation or incentives for utilities that had or have a mature program to go above and beyond the NERC CIP requirements.
- Size of the organization – small, medium and large organizations have different capabilities and different needs e.g. regarding flexibility to adopt changes or fix costs which are bearable
- Geographic distribution – local, regional, national and multi-national organizations have different needs. Organizations with a large geographical reach will likely be exposed to different legal, regulatory and cultural environments which may prevent or mandate some security measures.
- Interconnectivity – in some sectors the acting organizations inherently have a high degree of interconnectivity (e.g. the electric power grid) while in other sectors the actors are operating relatively independently from each other with rather loosely defined interfaces and dynamically changing peers they interact with.
- Differences in the scale of the societal impact of disruptions in the respective sectors – disruptions in some sectors will have a larger impact on society than other sectors and thus their risk tolerance will be different and hence the threshold for the business decision of mitigating or accepting the risk will be different. This will likely not be different in how different security controls are designed but it will be on the choice and extent of security controls chosen.

1.1.3 Describe your organization's policies and procedures governing risk generally and cyber security risk specifically. How does senior management communicate and oversee these policies and procedures?

ABB has a global enterprise risk management program. It has recently been summarized in an article in the Treasury Management International magazine [1] and has recently been recognized with the 2012 TMI Award for Innovation and Excellence in Risk Management [2]. Risks reported by various units are aggregated and consolidated in the Enterprise Risk Management team. Business managers of the different affected units remain owners of their respective risks and are asked to create a mitigation plan for their top risks.

Besides managing the risk ahead of time with the intent to minimize the likelihood of the risk materializing, ABB also considers it crucial to be prepared for the event that a risk materializes. Some incident types are relatively foreseeable and the organization can prepare for their handling. For example we have defined policies and procedures for handling incidents in our internal infrastructure, or policies and procedures for handling software vulnerabilities in our products. However, there are also incident types which are hard to foresee and for which it is impossible to prepare detailed policies and procedures. Generally, these are referred to as crises. ABB has a dedicated organization for crisis management, which is also represented in ABB's global group level cyber security organization.

1.1.4 Where do organizations locate their cyber security risk management program/office?

ABB's global cyber security organization responsible for customer related cyber security (i.e. cyber security in ABB's products, systems, services, etc.) is located in the office of the CTO, directly reporting to an Executive Committee member. The CISO is located in the Enterprise Information Systems function which in turn is part of office of the CFO. The cyber security organization has a formally established relationship with the CISO organization and collaborates frequently as topics such as the security of servers and workstations in the product development teams and in the project teams are in the scope of both organizations.

The cyber security organization spans the different hierarchy levels of the ABB group. It is headed in the office of the CTO, and consists of members at the division level (reporting to the respective division technology manager), at the business unit as well as at the product group level. Similarly, the CISO organization is organized hierarchically with global, regional and national teams.

Regional and country level organizations have cyber security resources typically located in the project execution groups and in the service delivery groups. Also, the regional and country level organizations have information security resources which report into the CISO's organization structure.

1.1.5 How do organizations define and assess risk generally and cyber security risk specifically?

ABB has defined a risk catalogue with 3 global risk categories of external, strategic and operational risks. In each of these categories, the catalogue contains 6 to 12 risk groups, each of which in turn consists of 5 to 10 risk clusters. One of these risk clusters is "Information systems & cyber security". Risk identification and assessment based on this risk catalogue is a combination of a top-down and a bottom-up approach, where global and regional functions as well as local functions are asked to report the risks from their point-of-view. Risk reporting is done using common templates which include a textual description and a qualitative valuation of the risk in a matrix of perceived likelihood (rare, unlikely, moderate, likely, almost certain) and perceived impact (insignificant, minor, moderate, major, dramatic). Based on this matrix, the risks are categorized as unimportant, less important, lower priority, higher priority and critical. Additionally, the template contains a description of existing and incremental mitigation plans.

1.1.6 To what extent is cyber security risk incorporated into organizations' overarching enterprise risk management?

As noted in 1.1.5, the ABB risk catalogue contains a risk cluster "Information systems & cyber security". All risks concerning the information security of the ABB information infrastructure as well as the cyber security risks potentially affecting our customers are reported in this cluster, following the same combined bottom-up and top-down approach described in 1.1.5. Members of the cyber security organization are primarily responsible for the identification, assessment and mitigation of these risks, however other employees are encouraged to also raise risks they perceive to the risk management team's attention.

1.1.7 What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

Generally, the mechanisms to understand, measure and manage risk are dependent on the type of risks. In the risk cluster of “Information systems and cyber security” there is a multitude of mechanisms involved.

ABB’s information security risks are managed according to an ISO 27000 information security management system operated by the CISO organization. At the management level instruments such as risk dashboards and heat maps based on a risk matrix are used to visualize the risk posture. Operationally, the plan, do, check, act cycle as described in the ISO 27000 framework is used to define, implement, monitor and improve mitigation plans for those risks that have been selected for mitigation. Other risks may be accepted, transferred or avoided.

On a technical level, in the general Enterprise Information Systems domain, we mostly use controls from the ISO 27002 catalog of controls complemented with more recent controls which have not yet been incorporated into the standard, as we see fit according to our ISO 27001 based information security management system [3].

In our cyber security organization, we use more domain specific models where available and necessary. Our product development organizations are inspired by security development lifecycle models such as the Microsoft Secure Development Lifecycle (SDL) [4], the Building Security In Maturity Model (BSIMM) [5], and the open Software Assurance Maturity Model (openSAMM) [6] and complement them with requirements specifications specific to the relevant application domain, e.g. the IEC 62351 specifications [7] in the electric sector, the ISA / IEC 62443 specifications in the process industries (and as applicable also in other industries such as discrete manufacturing).

Our system integration organizations take inspiration from industry-specific guidance such as the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), the Norwegian OLF’s security guidelines (currently OLF guidelines 104 and 110) [10] and also use specifications such as the relevant documents from the ISA / IEC 62443 standard [8]. When citing these documents, we would like to point out that the sector-specific differences often are relatively small and the sector-specific claim of these documents more often than not is primarily based on the fact that the publishing entity has some formal or informal authority for a given sector, while the concepts in the documents are mostly well applicable across different sectors of our scope.

1.1.8 What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cyber security conformity assessment?

We believe that national and international standards should define the requirements to which to conform to. These requirements should be complemented with guidance on their interpretation. However, we see different types of standards with different goals, which have an impact on conformity assessment. There are standards which aim at generally defining acceptable cyber security maturity levels in the organization as well as system and product capabilities. These standards usually define what is expected, but not how it is to be achieved (the ISA / IEC 62443 series of standards [8] is a good example in this category). Then there are standards which aim at interoperability of different solutions. These standards must be on a more higher level of technical detail and must specify exactly how the security objectives have to be met, e.g. by specifying protocols and protocol extensions (the IEC 62351 series of standards [7] is a good example in this category).

Interoperability standards should specify test cases and expected or unacceptable outcomes of the tests to define conformity. Where appropriate, different levels of conformity or different profiles of a standard may be advised, but the specification has to be transparent which requirements are applicable to each of these. Conformity assessments have to be unconditional to these levels or profiles and the requirements in the specification. If the scope of a conformity assessment is defined per assessed product or system, the comparability of these assessments is lost and their value in the economic transaction of purchasing technology is diminished.

For other standards describing meaningful conformity assessments will be much more difficult. These standards intentionally specify their requirements in fairly high-level and abstract way. This is to specifically allow different approaches to meeting the requirements. At this abstract level, it is often not possible to specify detailed test cases and expected and/or unacceptable test results. Hence, conformity assessments have to interpret the requirement when assessing whether a given implementation meets the requirement or not. This implies subjective evaluation by the assessor which impacts the comparability of different assessments and the repeatability of assessments and the predictability of their outcome for a given target of evaluation.

In either case however we strongly believe that any meaningful conformity assessment must be based on publicly available criteria. In addition conformity assessments programs must pay great attention to minimizing associated costs and time investments.

1.2 Use of Frameworks, Standards, Guidelines and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cyber security needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage.

1.2.1 What additional approaches already exist?

ISO 27000 [3], NIST 800-53 [11], IEC 62443 [8], WIB Process control Domain: security requirements for vendors [13], NERC-CIP [12], NIST 800-82 [14], DHS Cyber Security Procurement Language [15], OFL 104/110 [10], NIST IR 7628 [16], EU M490/SGCS [17], BDEW Whitepaper [18], VGB R175 [19], DoE ES-C2M2 [9], VDI 2182 [20], IEEE 1686[24], IEC 62351 [7], ERNCIP [25]

1.2.2 Which of these approaches apply across sectors?

ISO 27000 [3], NIST 800-53 [11], IEC 62443 [8], WIB Process control Domain: security requirements for vendors [13], NIST 800-82 [14], DHS Cyber Security Procurement Language [15], OFL 104/110 [10], BDEW Whitepaper [18], VGB R175 [19], DoE ES-C2M2 [9], VDI 2182 [20], ERNCIP [25]

We would like to point out that even in documents which only claim relevance for a specific sector, the content is often fairly well applicable to other sectors. This is sometimes due to the fact that the respective content is fairly high-level and abstract and thus generic. Often it is due to the fact that the cyber security challenges and approaches to address them are relatively similar across the different sectors we serve, because the base technologies used in the control systems in the different sectors are similar if not the same and also fundamental operational principles as well as design principles are very similar.

The sector-specific claim of these documents more often than not is primarily based on the fact that the publishing entity has some formal or informal authority for a given sector.

1.2.3 Which organizations use these approaches?

ISO 27000 – primarily traditional IT organizations (enterprise, e-commerce, etc.), internationally accepted (not as much in the U.S.)

NIST 800-53 – primarily US government, also similar organizations as ISO 27000 but mostly U.S. focused

ISA / IEC 62443 – industrial control systems user organizations with generally above-average security maturity (mostly because the standard is still under development), suppliers to these organizations

WIB – we currently see little adoption, suppliers of products and services (primarily system integration and maintenance) to industrial control system users are subject to the requirements specified – while it is assumed that these users actually require their suppliers to be certified towards the WIB requirements, more adoption is expected once the planned integration into the 62443 series is completed

NERC CIP – regulatory enforcement in the U.S. and Canada, but we also see European electric utilities use the NERC CIP requirements internally as a guidance

NIST 800-82 – we see little to no explicit reference to this document

DHS Cyber Security Procurement Language – we see little to no explicit reference to this document anymore

OLF 104 / 110 – primarily used by Norwegian oil & gas companies (aligned with its intended scope)

BDEW Whitepaper – we see few customers from the German energy utility sector referring to this document as guidance

VGB R175 – we see few customers operating power plants in Germany referring to this document

DoE ES-C2M2 – we see little to no reference to this document by customers

VDI 2182 – we see few customers referring to this document as a guidance

1.2.4 What, if any, are the limitations of using such approaches?

ISO 27000 – very generic, very flexible but rather unspecific, does not address specific concerns of industrial control systems

NIST 800-53 – more specific than ISO 27000, less flexible, does not address specific concerns of industrial control systems

ISA / IEC 62443 – fairly complex suite of standards, provides specific guidance within its scope, strong focus on industrial control systems and the specific context they operate in

WIB – covers diverse areas (system capabilities, project delivery, maintenance), many vague requirements which are hard to evaluate, associated certification allows for scope declaration by the applicant which is not published openly with the certificate

NERC-CIP – very focused on energy utilities,

NIST 800-82 – provides good general guidance, but is not very actionable for novice users and provides little news for expert users

DHS Cyber Security Procurement Language – provides useful procurement spec text blocks, but requires expert users to be applied properly

OLF 104 / 110 – provides specific, actionable guidance, but doesn’t go much beyond a fairly basic level, i.e. other than novice users won’t benefit much

NISTIR 7628 – Provides specific guidance to Smart grid (critical infrastructure), but overall is too big and did not get enough adoption, especially globally.

EU M490/SGCS – Mandate 490 Smart Grid Coordination Group providing guidance to architectures and relevant standards. In this sense this can be seen as a reference. Related and in support to this there is also the SGTF (Smart Grid Task Force) with its different expert groups.

BDEW Whitepaper – This is a whitepaper produced by the German energy industry association

VDI 2182 – provides a useful general framework, but is not very actionable for novice users while it provides little news for expert users, specifically the recent additions describing application examples somewhat compensate for these limitations

1.2.5 What, if any, modifications could make these approaches more useful?

In general, we would favor fewer documents which are aligned in scope and coordinated conceptually and we do believe that the approach taken by ISA / IEC 62443 is the most promising effort in this respect. As noted above, we see several documents containing very similar content conceptually. These documents often differ in structure or minor details and by the nature of their owners, focus on specific sectors. It would be desirable to have a hierarchy of documents, in which documents on the top level provide the generic guidance applicable across multiple or all sectors. Where necessary, on lower levels of the hierarchy sector-specific documents could complement or modify this guidance to express the sector specific needs. But a restatement of the same or similar guidance in different words and in a different structure is causing confusion, delay in adoption and likely unnecessary efforts in both end user and supplier organizations.

1.2.6 How do these approaches take into account sector-specific needs?

With only few exceptions, unfortunately, many approaches only mention sector-specific needs in the justification of their existence. But when carefully examined, the concepts in the approaches really do not differ much (see also 1.2.5).

1.2.7 When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

In our opinion, this is only reasonable if there are significant sector-specific needs and the sector-specific standards development process or voluntary program takes into consideration the available cross-sector content and focuses on the modifications and complements. In many cases this may be as simple as explaining the application of the cross-sector concepts in the sector-specific terminology and to possibly existing sector-specific reference architectures and models of operation.

1.2.8 What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

Such agencies should promote the use of a cross-sector approach as described in 1.2.5 and deal with the specifics in line with the cross-sector approach. They should support the development of this cross-sector approach which would help to ensure that the sector-specific extension is possible and that the scope and the concepts therein are compatible with the cross-sector approach. All this should speed up the process of development and adoption.

1.2.9 What other outreach efforts would be helpful?

As previously already state there already exists many, if not too many, efforts. Rather the starting new ones we feel it would be better to focus on the most promising ones available today and support those. These include IEC / ISA 62443, ISCJWG or ERNCIP.

1.3 Specific Industry Practices

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- *Separation of business from operational systems;*
- *Use of encryption and key management;*

- *Identification and authorization of users accessing systems;*
- *Asset identification and management;*
- *Monitoring and incident detection tools and capabilities;*
- *Incident handling policies and procedures;*
- *Mission/system resiliency practices;*
- *Security engineering practices;*
- *Privacy and civil liberties protection.*

1.3.1 Are these practices widely used throughout critical infrastructure and industry?

The adoption of these practices differs between the different sectors we serve (note: the adoption, not so much the applicability and the details of how to apply them). We see the most mature and most consistent adoption in the power transmission & distribution and generation industries as well as in the oil, gas and chemical industries. Also, we see differences in adoption geographically, where in North America and Europe the largest adoption can be observed, and parts of the Middle East are catching up quickly.

1.3.1.1 Separation of business from operational systems

Historically this has been a standard design principle. With rising adoption of COTS technologies and rising need for multi-system integration as well as integration with the enterprise architecture the separation of systems used for the operation of critical infrastructures from those used for regular business operations has been weakened in practice. However, the recognition of cyber security risks implied by this weakened separation has recently led to a return of this principle. Guidelines and standards such as the ISA/IEC 62443 (specifically the planned ISA/IEC 62443-3-2) emphasize this as well. We do encourage our customers to use network segregation and support this in our product offerings as well as in our service portfolio.

1.3.1.2 Use of encryption and key management

We would like to extend this practice to include generally the use of cryptography, not limited to encryption. Given the relatively lower importance of confidentiality in ICS environments, encryption is comparatively less relevant then cryptographic integrity mechanisms – in control systems the focus must be on the continuous operation of the underlying process and this must not be jeopardized by issues in key management. Especially for field equipment (e.g. Intelligent Electronic Devices, Remote Terminal Units etc.) cryptography and key management are not widely used in practice, largely due to the fact that historically they have not been addressed and supported in products released more than several years ago. However, these products are and will have to remain in use for a significant period of time still for economic reasons. Most industrial communication protocols today still have no specification supporting the use of encryption and key management. Several vendors and end users have started to support and use tunneling mechanisms or even proprietary extensions. However, these usually interfere with interoperability because they lack the central specification by the owner of the respective protocol specification. A notable exception is the IEC 62351 series of standards which specified security extensions for several protocols commonly used in the power systems management domain (e.g. DNP3, IEC 60870-5-*, IEC 61850).

The adoption of cryptographic functionality and key management is however increasing on larger systems such as Energy Management Systems, Distributed Control Systems etc.

1.3.1.3 Identification and authorization of users accessing systems

For larger systems (e.g. EMS, DCS) user identification and authorization is widely being used, sometimes however not on an individual user basis but using roles (e.g. Operator). We see less use of such technology in field devices (e.g. IED, RTUs, PLC) even when device already support the functionality. The main objection against its use is the need for barrier-free emergency access. However, the recognition of cyber security risks implied by too open access has recently led to a stronger emphasis of user identification and authorization. Guidelines and standards such as the ISA/IEC 62443 emphasize this as well.

1.3.1.4 Asset identification and management

Asset identification and management is becoming more and more popular, not only for reasons of cyber security. A detailed asset inventory is the basis for a variety of asset management approaches for different objectives. Asset management is often motivated by cost reasons, e.g. extending the lifetime of assets by proactive maintenance. The adoption of asset inventories and asset management approaches differs between different sectors, logically sectors which typically have large systems with a high number of assets per system more commonly use this than sectors with smaller systems with fewer assets per system. However, there is no doubt that a detailed asset inventory is also necessary for a mature cyber security management system. We do see the creation and maintenance of an asset inventory being mentioned as a recommendation or requirement in different guidelines and standards, e.g. the ISA/IEC 62443 series (specifically the -2-1 part) [8]. We do encourage our customers to deploy security monitoring and have offerings to that respect in our product and service portfolio.

1.3.1.5 Monitoring and incident detection tools and capabilities

System monitoring is a very common practice in industrial control systems. It is commonly referred to as "situational awareness" in the industrial control system community. Part of this practice is for example alarm management which helps operators to focus on the most relevant notifications from the monitoring system. Its focus is primarily on the process condition and the condition of assets, rather than on cyber security incidents. However, the recognition of cyber security risks has changed that focus to now also include cyber security. The level of security monitoring supported by products and systems released more than several years ago differs largely. While the COTS technologies adopted from general enterprise IT (e.g. operating systems, standard application, network devices) usually support the logging of security events, the industrial control specific components such as embedded PLC or IED devices offer this capability only if they are of a more recent release version. Specific details of these features ary greatly and are not necessarily consistent cross-vendor and cross-sector. Furthermore, raw events are usually not yet meaningful for incident detection, but need to be correlated and aggregated in order to reduce the volume and granularity of information to a level which a human can process. This correlation and aggregation is commonly done by SIEM (security information and event management) platforms. However, these have only been available as standard enterprise IT products for a long time and those lack the analysis capabilities specific to industrial control systems. Such analysis capabilities have only been introduced in the market in the last few years and adoption of those is still limited to the more mature sectors and the larger players therein. We do see the security monitoring being mentioned as a recommendation or requirement in different guidelines and standards, e.g. the ISA/IEC 62443 series (specifically the -2-1 part) [8]. We do encourage our customers to deploy security monitoring and have offerings to that respect in our product and service portfolio.

1.3.1.6 Incident handling policies and procedures

Similar to monitoring, incident handling as such is a common operational principle in industrial control systems. However it is primarily focused on handling incidents with the process under control (e.g. process conditions like boiler temperature or pressure reaching or exceeding limits) or safety incidents rather than on handling cyber security incidents. We do see the creation and maintenance of incident response procedures being mentioned as a recommendation or requirement in different guidelines and standards, e.g. the ISA/IEC 62443 series (specifically the -2-1 part) [8]. We do encourage our customers to develop such policies and procedures and have offerings to that respect in our service portfolio.

1.3.1.7 Mission/system resiliency practices

Similar to monitoring and incident handling, resiliency is a core design and operation practice for industrial control systems. However this has so far mostly focused on resiliency against disruptions caused e.g. by natural disasters, random equipment failure or physical sabotage. However, the recognition of cyber security risks has changed that focus to now also include cyber security. Practices such as network segmentation (not only between business and critical infrastructure systems, but also within critical systems), monitoring as well as incident detection and response all contribute to stronger system resilience against cyber security threats, as they allow for the containment of attacks if they happen, identification of attacks as they happen and response to incidents (including the prevention of severe consequences and the fast return to normal operations) as they are detected.

In some areas, we are aware of quantitative approaches to calculate reliability of alternative system designs. Specifically this is true for network reliability calculation (a summary can be found in [21]). These approaches can also be applied to critical infrastructure networks such as a substation automation system network [22]. However, these approaches are also limited to the analysis of random failures and cannot be easily applied to the analysis of resilience against an intentional attack by an intelligent threat agent. Modeling an attacker's behavior for analysis is currently still an actively discussed research problem [23].

1.3.1.8 Security engineering practices

General security engineering practices, including traceability of countermeasures to threats and risks identified in risk assessment and threat modeling, are rising in adoption, at least for new projects. We do encourage our customers to use security engineering practices and have offerings to that respect in our service portfolio.

1.3.1.9 Privacy and civil liberties protection

Privacy[1] concerns are mostly limited to the Smart Grid activities as other industrial control systems are generally not concerned with data which is relevant for privacy. Note that we consider privacy a subset of confidentiality. Industrial control systems can well contain data which is assessed confidential by their respective owner. Beyond the obvious user credentials and cryptographic keys, these are usually related to intellectual property around the configuration and operation of the process under control.

Similarly, civil liberties are usually not considered very relevant in the industrial control systems domain.

1.3.2 How do these practices relate to existing international standards and practices?

Most if not all of these practices are covered in the international or national standards and practices which we cite in this response.

1.3.3 Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

It is very difficult to give a generic answer to this question. Usually, any single countermeasure is not sufficient, but the interaction of multiples countermeasures makes up a good cyber security defense. Hence, out of this mix it is impossible to single out the importance of a given measure as the effectiveness comes from the mix. Similarly, the criticality of a given measure in the mix depends on the risks and threats the specific environment to be protected is exposed to. For example, in small systems with a low number of assets per system, an asset identification and management can be very simple or not exist as an explicit system. However, already if multiple of such small systems are operated in a fleet of systems within an organization, that may already be different.

We would however like to point out that the effectiveness of all of those practices heavily rely on a sound security program and skilled personnel. We thus strongly believe that any framework developed by NIST must set a focus on cyber security awareness, training and developing sustainable cyber security programs within all organizations.

[1] We assume that privacy refers to the confidentiality of personally identifiable information, not confidentiality in general (e.g. confidential corporate information is not addressed by privacy). In other words, we consider privacy to relate to natural persons only.

1.3.4 Are some of these practices not applicable for business or mission needs within particular sectors?

Again, it is very difficult to give a generic answer to this question. As we note above, we see large similarities in the challenges for the different sectors we serve. The differences are more significant along different dimensions, including the scale of the systems, the degree of interconnectivity of different organizations, etc. See response to question 1.1.2.

One extremely large challenge is the nature of business relations in a given sector. By business relations, we mean the way in which the sector infrastructure is built and how responsibility is allocated between the different businesses. Some sectors are very monolithic, with a few big players on both customer and equipment provider sides. Other sectors are extremely splintered, with perhaps large customers, but with thousands of small suppliers working in small temporary units to provide a solution to a large customer. In the later, there are larger challenges to interoperability, but also to defining responsibility and in dealing with responsibilities for which the assigned business is no longer in operation.

1.3.5 Which of these practices pose the most significant implementation challenge?

Again, it is very difficult to give a generic answer to this question. Implementation challenges on the technical level are mostly related to the age of the target system and thus the available technical support for these practices. This applies to both the industrial control system specific parts of the system and the generic COTS parts. One overarching challenge which the entire industrial control system security community fasces is the shortage of skilled workforce. There are only very few individuals who have a sufficient knowledge in all relevant fields, i.e. in industrial control, in computer science / IT and in information security.

1.3.5.1 Separation of business from operational systems

The deeper the networks are in the system hierarchy, the more difficult it is generally to segregate them as the interconnectivity is more critical to the operation and the more application-specific, ICS aware segregation mechanisms are necessary to effectively segregate. Those are rare on the market though.

1.3.5.2 Use of encryption and key management

Interoperability is the key challenge here. As long as the industrial protocols are not specifying a security extension similar to how IEC 62351 is doing it for most of the power systems management protocols, any attempt to doing so will be limited in utility as it will interfere with the interoperability. A notable example are OPC UA and the wireless field bus specifications (WirelessHART, ISA 100) which in fact have specified a dedicated security model and integrated the cryptographic mechanisms to ensure security in their specifications.

Furthermore, especially in real-time systems, the time synchronization for key management is very critical to ensure that all participants change their keys at the same time. While in some real-time systems times tamping is not critical, but simply the timely transmission of messages is sufficient (e.g. locally in a robot cell), with a key management system of broader scope, this will be different.

1.3.5.3 Identification and authorization of users accessing systems

Again, the complexity of implementing identification and authorization depends on where in the ICS this is to be implemented. The closer to the mission critical components it is, the more relevant it is to not only prevent unauthorized access, but at the same time to maintain barrier-free emergency access. In physically confined deployments with continuous staffing (e.g. in permanently manned operations rooms), sufficient compensating countermeasures are available (e.g. physical access control and close supervision of the equipment in question), but in more physically/geographically distributed systems these fail.

1.3.5.4 Asset identification and management

The biggest challenge in asset identification and management is the integration of heterogeneous fleets of assets, especially containing aged assets. In those cases it is difficult to automate the population and the maintenance of the asset data as there is no common interface for automatic querying, and even if there is, the semantics of the retrieved data may not be common. Especially aged equipment does not make relevant data accessible in a machine-readable format.

1.3.5.5 Monitoring and incident detection tools and capabilities

For monitoring and incident detection the biggest challenge is domain specific know-how in the analysis mechanisms. Most IDS technology (or similar approaches) available on the market has strong focus on incident types and target technologies which are dominant in the enterprise IT systems (e.g. e-mail attacks, file sharing, social media), while specific attacks against ICS are different in nature. Also, the advantage of higher determinism in ICS is rarely leveraged by commercially available analysis tools.

1.3.5.6 Incident handling policies and procedures

The biggest challenge in incident handling besides the shortage of skilled people is the conflict of interest between a proper in-depth analysis of an incident down to the root cause and the fast restoration of normal operations. Incident handling processes from the enterprise IT domain can usually live with a few hours of unavailability of affected assets while especially for assets close to the primary process under control, this is unacceptable.

1.3.5.7 Mission/system resiliency practices

As already noted in 1.3.1.7 the commonly accepted resiliency practices in the industrial control system domain are fairly sophisticated and have a strong engineering background and are quantitative in nature (e.g. in the safety world). Currently the cyber security domain is not at this stage of maturity and thus acceptance of resiliency approaches for cyber security is low as they are deemed immature. The question of quantitatively modeling cyber security risk and thus a given system's resiliency against them is an open question.

1.3.5.8 Security engineering practices

The biggest challenge in adoption of secure engineering practices is their use in "brown field" systems. Usually, it is recommended to address security concerns from the very beginning (built-in instead of bolted-on), however in the industrial control systems domain there very rarely is the situation that one starts from the beginning. Usually, all ICS projects have to build on top of or around a significant base of existing environment. This may be the interconnectivity of new systems with their existing surrounding infrastructure, this may be that projects aren't actually building new systems but are upgrading existing systems subsystem by subsystem.

1.3.5.9 Privacy and civil liberties protection.

The challenge for privacy and civil liberty concerns are primarily relevant in the Smart Grid domain, as already noted in 1.3.1.9. A challenge here is certainly the diversity in different jurisdiction's legislation around privacy, which is partially contradicting (i.e. mechanisms required in some markets are unacceptable in others).

1.3.6 How are standards or guidelines utilized by organizations in the implementation of these practices?

How ABB uses different standards and guidelines (and how we recommend their use to our customers and partners) largely depends on the type of document and its release state. We try to adopt those standards and guidelines which we identified as relevant as early as possible and to feedback our experiences in adopting them into the development process where possible. This specifically means that we are monitoring drafts of such documents and use them where we can get access. Also, our adoption and recommendation to do so depends on the type of document. Regulations and international standards which may be imposed by regulatory bodies of industry-self regulation are adopted more rigorously than documents which are intended as guidelines and recommendations for consideration.

1.3.7 Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

The ABB cyber security organization monitors different standards bodies (e.g. ISO/IEC, ISA, IEEE) for potentially relevant activities. Once such activity is identified we assess the appropriate level of involvement, which may range from simple monitoring to active contribution and leadership. Factors which influence this decision are the relevance to our business strategy, stage the activity is in when discovered, openness of the drafting team, as well as our assessment of the proposed content and concepts in terms of soundness and completeness (i.e. whether we feel our view would add a new perspective to the current drafting team's approach).

1.3.8 Do organizations have a formal escalation process to address cyber security risks that suddenly increase in severity?

As mentioned in 1.1.3, ABB has a framework of incident handling and crisis management, in which cyber security risks are fully integrated. Both the suddenly increased relevance of cyber security risk as well as the suddenly increased impact of cyber security incidents are considered in the escalation mechanisms. Specifically in crisis management, in fact the approach is rather to escalate early and scale down if appropriate, rather than to start small and escalate if necessary.

1.3.9 What risks to privacy and civil liberties do commenters perceive in the application of these practices?

As mentioned above, privacy and civil liberties are primarily applicable concerns in the Smart Grid domain, where the power consumption patterns of individual households may be revealed to a larger degree of granularity than it was previously the case.

1.3.10 What are the international implications of this Framework on your global business or in policymaking in other countries?

We already today see that NIST documents from the SP series are used and have an impact also outside of the U.S., at least in part because they are available for free and provide good guidance.

We would expect that a NIST Framework would have an impact outside the U.S. as well, e.g. because international standardization bodies or policymakers will at least use the framework as a source of inspiration.

1.3.11 How should any risks to privacy and civil liberties be managed?

Currently, privacy is not very broadly discussed other than in the Smart Grid context. Actually, we would like to see this managed, particularly guidelines that work across international boundaries and standard and recommendations that help define how long and how much personally identifiable data shall be stored in context of cyber security actions (for incident tracing and repudiation).

1.3.12 In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

Other practices not yet mentioned in this document which also support resilience include continuous training and security awareness programs, management of updates and patches, frequent backup and efficient restore capabilities, and active involvement in the industrial control system cyber security community for information sharing. The cyber security practices should be integrated into the continuous quality management and improvement program typically available in organizations.

Following up on the comment on challenges with regards to the business relationships in some sectors, defining business relations and responsibility could be a valuable contribution. For example, the construction industry has a clear and regulated way which defines how sub-suppliers work on a building project. Something similar is not existent in the Cyber Security industry, but could help in sectors, where the business relationships are of a splintered nature as described in 1.3.4.

References

[1] Tsolakas,C., "Implementing an Enterprise Risk Management Approach", Treasury Management International, Issue 207, http://www.treasury-management.com/article/1/239/1990/implementing-an-enterprise-risk-management-approach.html (full article available after free registration)

[2] Sanders, H.; „Corporate Innovation & Excellence Experiences and Insights of the 2012 Editor's Award Winners", Treasury Management International, Issue 211, http://www.treasury-management.com/showarticle.php?pubid=1&issueid=252&article=2129&page=showarticle&pageno=2

[3] ISO 27000 series of standards (not available for free), specifically ISO 27000, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56891, ISO 27001, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103 and ISO 27002, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50297.

[4] Microsoft Secure Development Lifecycle, http://www.microsoft.com/security/sdl/default.aspx.

[5] Building Security In Maturity Model, http://bsimm.com/.

[6] open Software Assurance Maturity Model, http://www.opensamm.org/.

[7] IEC 62351 series of standards (not available for free), http://www.iec.ch/dyn/www/f?p=103:91:0::::FSP_LANG_ID:25#q=62351.

[8] ISA / IEC 62443 series of standards ((not available for free)), http://isa99.isa.org/ and http://www.iec.ch/dyn/www/f?p=103:91:0::::FSP_LANG_ID:25#q=62351.

[9] Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model

[10] Norwegian Oil and Gas Association (OLF) Guidelines 104 and 110 on cyber security, http://www.norskoljeoggass.no/Documents/Retningslinjer/100-127/104%20-%20Information%20security%20baseline%20requirements.pdf and http://www.norskoljeoggass.no/Documents/Retningslinjer/100-127/110%20-%20%20Implementation%20of%20information%20security.pdf

[11] NIST 800-53v3, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[12] NERC Critical Infrastructure Protection Standards, http://www.nerc.com/page.php?cid=2%7C20

[13] WIB Process control Domain: security requirements for vendors, http://www.wib.nl/download.html (download available after registration)

[14] NIST 800-82, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[15] DHS Cyber Security Procurement Language, http://ics-cert.us-cert.gov/pdf/FINAL-Procurement_Language_Rev4_100809.pdf

[16] NIST IR 7628, Guidelines for Smart Grid Cyber Security, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf and http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

[17] EU M490/SGCS, Smart Grid Mandate –Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf

[18] BDEW Whitepaper, http://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/$file/2008-06-10_Whitepaper_Sichere%20Steuerungs-_Telekommunikationssysteme.pdf

[19] VGB R175 (now renamed to VGB S016), www.vgb.de (not available for free)

[20] VDI 2182, www.vdi.de (not available for free)

[21] Sahinoglu Mehmet, Rice Benjamin. Network reliability evaluation. WIREs Comp Stat 2010, 2: 189-211. doi: 10.1002/wics.81

[22] Sivanthi, T.; Gorlitz, O., "A systematic approach for calculating reliability of substation automation system functions," Energy Conference and Exhibition (ENERGYCON), 2012 IEEE International , vol., no., pp.957,962, 9-12 Sept. 2012, doi: 10.1109/EnergyCon.2012.6348288

[23] Sandia Report SAND2009-1673, “Impacts Analysis for Cyber Attack on Electric Power Systems”

[24] IEEE 1686 - Standard for Intelligent Electronic Devices (IEDs) Cyber Security Capabilities, http://standards.ieee.org/develop/project/1686.html

[25] ERNCIP - , https://erncip.jrc.ec.europa.eu/