CYBER SECURITY FOR ENERGY AUTOMATION SYSTEMS - NEW CHALLENGES FOR VENDORS

Bernd NARTMANN
Siemens AG - Germany
bernd.nartmann@siemens.com

Thomas BRANDSTETTER
Siemens AG - Germany
thomas.brandstetter@siemens.com

Dr. Konstantin KNORR
Siemens AG - Germany
konstantin.knorr@siemens.com

ABSTRACT

Cyber security has gained tremendous importance for energy automation systems over recent years. A lack of cyber security resilience endangers the reliability of the overall energy supply which is part of the critical infrastructure. This paper describes the new cyber security challenges which have emerged for vendors of energy automation systems and proposes solutions on how to resolve them. These range from technical, organizational to regulatory and process issues. Particular focus is brought forward on the implementation strategy, how to imbed cyber security within the products' life cycle, the implementation of IEC 62351 and cyber security assessments. This paper is based on the experience gained by the Siemens energy sector group. The authors thereby hope to support electric utilities learn from these experiences and be able to better interface their cyber security strategy with the vendor's strategy outlined in this paper.

INTRODUCTION

A global change in culture has been materializing recently in the energy automation business for electric utilities with regards to cyber security. This has accelerated rapidly in the last three years, with the culmination of new standards and mature methodologies being deployed for the energy market.

Electric utilities operate critical infrastructure in order to secure the reliability of the energy supply. Therefore the utility is focused on the uninterrupted operation and availability of the different components of the infrastructure from the control centers, substations, RTUs to the field devices.

Former energy automation systems (EAS) have not been developed with cyber security in mind. They have been operated as an "island" with "private" communication connections to other systems. Starting with the introduction of internet technology, EASs became increasingly more interconnected and emerged as targets for "hacker" groups to attack the infrastructure.

The process of awareness for cyber security issues started initially very slowly. The first attacks / incidents were not widely published and therefore not prevalently known. Nowadays the awareness of cyber security issues is growing due to the importance of energy infrastructure to be constantly in operation. The awareness of all the related cyber security topics needs to be extended in future to guarantee further smooth operation of the critical energy infrastructure. The operational failure of an EAS can have an extremely negative impact for industry, the general public and governments. Industry and households increasingly depend on electrical energy. Nobody will accept a blackout due to a cyber security attack.

The governments and large utilities of different countries are now enforcing the protection of critical energy infrastructure very seriously. Clear and detailed requirements have been defined in regulations and guidelines. The vendors are required to fulfill these requirements in order to stay in business.

Various vendors are already implementing and delivering intelligent solutions to overcome weaknesses in cyber security. The following section outlines more details concerning these challenges, especially the changes in the vulnerability landscape and standardization. The "solutions" section describes how the Siemens energy sector group counters these challenges with a detailed focus on the implementation strategy, secured process lifecycle and use of security assessments.

NEW CYBER SECURITY CHALLENGES

Changes in the vulnerability landscape

When reviewing the vulnerability landscape pertaining to EAS's over recent years, a notable change in the overall occurrence and perception of vulnerabilities can be observed. The EAS world is affected by both security events in the general IT world, as well as energy sector specific issues.

Firstly, it is noteworthy that a huge underground "hacker" internet community exists, which is currently estimated to have a turnover of around $US 7 billion [SYM2008] and is aggressively researching new vulnerabilities in common IT technologies for further exploitation or reselling. Secondly, an accelerating adoption of information technology for EASs has lead to an increased probability of security deficiencies inherent in these systems. The combination of these trends certainly affects the overall security of EASs.

Furthermore, the growing awareness and subsequent increased requirement for secure energy infrastructure significantly changed in 2007 and 2008.

Several indicators demonstrate that public attention towards automation system vulnerabilities in general, and especially the importance of EAS has increased significantly. The

Control Systems Cyber Security Report [CSSP2008] shows that the number of presentations for security in control systems alone has increased 700% from the years 2005 to 2008 and was widely spread over various countries. When reviewing the number of reported vulnerabilities, between five to ten percent of reported vulnerabilities are relevant for control systems alone.

This additional attention to EAS security has had a sudden impact for vendors of these systems, as increasing focus by research interests may lead to more vulnerabilities published, which subsequently have to be handled by the vendor. Vulnerabilities in EASs have already been reported in public forums; e.g. at the S4 SCADA security conference [S4_2008], a presentation detailed not only the technical details of two vulnerabilities, but also the vendor's inability to handle them in a timely manner.

In order to avoid future negative exposure due to such events, vendors will need to be prepared. The necessary measures range from technical and organizational changes to process issues in all stages of the product lifecycle.

Cyber security standards

Standardization in general is very important for electric utilities since it ensures aspects like independence of single suppliers, compatibility, interoperability, safety, and quality. Over recent years, the number of documents concerning the standardization and regimentation of cyber security in the energy sector has increased tremendously, cf. [DoE2005]. The following characteristics help in structuring and differentiating the documents:

- Technical document vs. management
- Who is the author? Industry bodies, operators, regulatory bodies, legislature or international standardization bodies like IEEE, ISO or IEC
- Is the document energy-specific or written with a general IT focus?
- Is the document focusing on the operation or development of the systems

For example, IEC 62351 is a technical, international, energy-specific, development oriented standard.

Vendors are challenged by identifying, adhering to and pushing the appropriate standards. A Siemens study [KRL2008] yielded ~80 different documents relevant for the energy industry with over 10.000 pages. Out of these documents, special "candidates" were identified and recommended to the different parties involved in the product development and management processes based on criteria such as importance for the customers and innovation potential. The following list gives some sample documents.

NERC CIP

NERC (North American Electric Reliability Council) has issued critical infrastructure protection (CIP) standards to address cyber security for power systems. This standard does not provide detailed technical measures, but more high level management approaches to secure electric facilities. Thus, this standard (which is and will be mandatory in the USA) is primarily relevant for the operation of such facilities, but manufacturers need to provide the required technical features, cf. [NERC].

BDEW white book

Published by the German federal energy association this white book addresses the cyber security of control and telecommunication systems and defines basic security measures and requirements for IT-based control, automation and telecommunication systems. The book takes into account general technical and operational conditions. The purpose of the security measures detailed in this white book is to assure the information security of these systems, in order to provide an adequate degree of availability, integrity, non-repudiation and confidentiality for the systems and the processed data, cf. [BDEW2008].

INL Procurement Language

The purpose of this document is to summarize security principles that should be considered when designing and procuring control systems products (software, systems, and networks) and provide example language to be incorporated into specifications. This document is a "tool kit" designed to reduce cyber security risk in control systems by requesting that technology vendors and providers, through the procurement cycle, to assist in managing known vulnerabilities and weaknesses by delivering more secure systems, cf. [PL2008].

IEC 62351

The standard IEC 62351 is pushed by IEC TC57 WG15. The 57th technical committee addresses the management of power systems and associated information exchange between appropriate devices. The scope of the work of WG15 is to develop standards that increase the informational security assurance aspects of the protocols specified within TC57 such as IEC 61850, ICCP (IEC 60870-6), DNP and IEC 60870-5-104 but also security issues related to CIM / IEC 61970. The results of these security extensions are consolidated in the standard IEC 62351. The following solution section gives more information on IEC 62351 implementation considerations.

SOLUTIONS ON RESOLVING THE CYBER SECURITY ISSUES

This section details the recommendations and measures to be utilized by vendors of the EASs to counter the aforementioned challenges.

Cyber security implementation strategy

Vendors of EASs have to handle the rapidly evolving cyber security issues that their products are facing by formulating an implementation strategy. This is especially important for vendors delivering not only single products, but entire energy automation portfolios, as they not only have to implement cyber security aspects into the products, but also harmonize them throughout the entire product portfolio.

At the beginning of the product development process an

organizational entity must be formed, which is responsible for handling and coordinating all product security activities within the business unit. This entity may be called the Product Security Group, or "PsecG", as the central coordination body for information security in energy automation products and solutions. To ensure covering all information security aspects that may occur throughout the product lifecycle, this group must be comprised of personnel from all of the product lifecycle stages. This may include system architects, development, sales and system test, but also personnel from later product lifecycle stages such as project delivery, and operation.

Once the PsecG has been established, a strategy and subsequent definition of tasks must be formulated. These tasks include:

- The creation and maintenance of mandatory security requirements for products, which shall ensure appropriate and state-of-the-art technical security controls for the products. An example herefore is the mandatory use of state of the art cryptographical algorithms and key lengths.
- The definition and enforcement of security processes and milestones such as security quality gates, e.g. application of security test tools during system test phases of each new product release (for more details see below).
- Security standardization work is done e.g. to drive future security implementations within energy automation protocols such as IEC62351.
- Another important PsecG task is to create the appropriate awareness for proper cyber security handling. This may be achieved by organizing security training, security briefings or workshops to ensure all involved participants understand cyber security issues and know how to deal with them.
- A service must be provided by the vendor which ensures integration of the products into the customer's environment. Several projects with customers have shown that a secure product alone is not sufficient, as potential vulnerabilities may arise from insecure integration into existing infrastructures, such as connectivity to partner networks for energy trading or the customer's office networks. To close these gaps, the vendor must provide additional technical consulting services including patch / update management and training to ensure appropriate understanding of IT security issues concerning the energy automation environment of the customer.

Selected cyber security "deep dives"

Due to the size and complexity of the cyber security implementation strategy only selected parts can be described in more detail in this paper. The three "deep dives" presented here will focus on (1) the process approach, (2) the implementation of IEC 62351, and (3) cyber security assessments. For more information on the cyber security activities of the Siemens energy sector please refer to [BRK2009], [EDEAMK], [KL2008], and [S2006].

Security in the product's lifecycle

In order to permanently include cyber security in a product, a process oriented approach in needed. Therefore, so-called security milestones have been defined and tied to the existing product development stages, cf. Figure 1. For the later stages in a product's life, after the product is already delivered and operated, additional processes for handling security at the utility (e.g. defects, vulnerability notifications, site acceptance tests, incidents) are established.

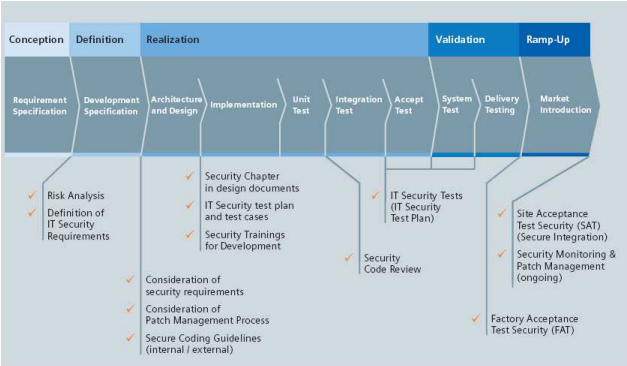

Figure 1: Security milestones in an EAS's lifecycle from a vendor's perspective

Implementation of IEC 62351

When implementing IEC 62351 major challenges for a product spanning security architecture center around authentication and authorization, especially key management & certificate handling, design of a public key infrastructure, and role based access control. The architecture team is actively forming the standard in the IEC working group and is supporting the implementation of the standard in the different products. For more information on the implementation experiences see [KFS2008].

Cyber security assessments

Security assessments are mandatory in the development and operation of EASs. During the development phase, security assessments are used to uncover security leaks and check compliance with pre-defined security requirements. During operation of an EAS, several standards such as NERC CIP and the BDEW white book define regular cyber security assessments.

Within the Siemens energy sector, the methodology presented in Figure 2 is used which consists of the following phases:

- Risk Analysis: Based on the international standard ISO 13335 a risk and threat analysis for the EAS is performed, preferably in a joint workshop with security experts from development, architecture and operation. The most important threats are identified, documented and ranked.
- Theoretical Assessment: Based on questionnaires compiled based on relevant standards like NERC CIP, BDEW white book, or the INL procurement language,

structured interviews are completed with the security experts.

- Practical Assessment (aka "Friendly Hacking"): The so-called security assessment plan lists all the practical tests which are done on the target of evaluation. Security tools such as vulnerability scanners, protocol fuzzers and port scanners are used for automation of the tasks. The assessment is done by a team specializing in this security work which is independent of the product development.

By combing the results of these three phases a broad and meaningful statement about the current security level of the EAS can be made. Possible shortcomings are identified and addressed immediately or in future product releases. More information about the assessment methodology can be found in [BKR2009].

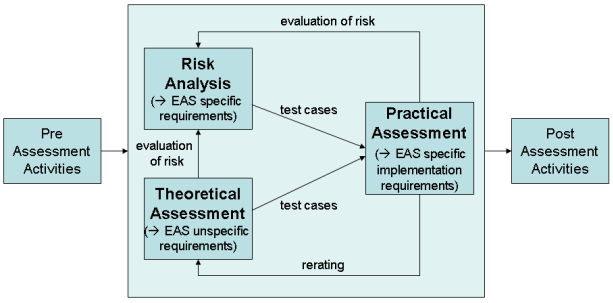

Figure 2: Cyber security assessment methodology as proposed in [BKR2009]

CONCLUSION

Different approaches have been derived by vendors to face the new challenges with regards to cyber security in the energy sector. Compliance with standards and a process oriented implementation of cyber security resilience into the products and solutions is the key factor to ensure a proper operation of EASs for energy critical infrastructure.

The definition of standards always needs to be done in close cooperation with standardization and regulation groups, utilities and vendors, because a manageable solution of high quality is required.

The implementation process starts immediately at the beginning of the product lifecycle with the definition of requirements derived from standards. The implementation of functionality also covers regular security tests and assessments, and of course a patch management process for the operational phase.

Finally, the utility's customized infrastructure needs to be included in all these approaches. Only secure products and solutions in a secure environment guarantee the success in fighting against cyber security attacks. A close cooperation between the utility and the vendor is therefore absolutely necessary. Vendors supplying the whole automation chain have the advantage to coordinate products and solutions "in-house" to limit the coordination effort and to avoid misunderstandings.

This paper presents the actions taken by the Siemens energy sector group to face cyber security issues. We thereby hope to help electric utilities learn from these experiences and be able to better interface their cyber security strategy with the Siemens one.

REFERENCES

[BDEW2008] BDEW, *White Paper Requirements for Secure Control and Telecommunication Systems*, Version 1.0, Berlin, 2008, http://www.bdew.de

[BKR2009] Th. Brandstetter, K. Knorr, Ute Rosenbaum, "A Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components", *Proc. of the IFIP SEC 2009*

[CSSP2008] Sean McBride, *CSSP Quarterly Trends and Analysis Reports*, Control Systems Security Program for US Department of Homeland Security, 2008

[DoE2005] DoE, *A Summary of Control System Security Standards Activities in the Energy Sector*, 2005

[EDEAMK] Siemens Energy Sector, Power Distribution Division, Energy Automation: Totally Integrated Energy Automation, *"Simplify your IT-Security" Brochure*, Nuremberg, October 2007 (Print version)

[KFS2008] K. Knorr, S. Fries, M. Seewald: „Informations-sicherheit für die Energieautomatisierung: IEC 62351 - Herausforderungen und Lösungsansätze", *ew Energiewirtschaft*, Jg. 107 (2008), Heft 21, S. 56 – 61 (in German)

[KL2008] K. Knorr, R. Link, "Security in the Design, Development and Testing of SCADA Systems for Energy Infrastructures: the Siemens experience", *Proc. ESTEC Workshop*, Brussels, 2008

[KRL2008] K. Knorr, U. Rosenberg, L. Nilss, *Survey of Relevant IT Security Documents, Standards & Regulations in the Energy Sector*, Version 3.0, 2008 (for Siemens internal use only)

[NERC] North American Electric Reliability Council *Critical Infrastructure Protection Standards*, http://www.nerc.com/page.php?cid=2%7C20

[PL2008] DHS, *Cyber Security Procurement Language for Control Systems*, Version 1.8, 2008, http://www.msisac.org/scada/documents/4march08scadaprocure.pdf

[S4_2008] E. Udassin, "Control System Attack Vectors and Examples: Field Site and Corporate Network", *Proc. S4 SCADA security conference, 2008*

[S2006] P. Skare, "SCADA Security Innovations", *Proc. SANS Process Control and SCADA Security Summit*, Florida, March 2006

[SYM2008] Symantec, *Symantec Report On The Underground Economy*, 2008