A Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components

Thomas Brandstetter, Dr. Konstantin Knorr, Dr. Ute Rosenbaum

{Thomas.Brandstetter, Konstantin.Knorr, Ute.Rosenbaum}@siemens.com
Siemens AG, Corporate Technology, Information and Communications
Computer Emergency Response Team (CERT)

Abstract Protecting our critical infrastructures like energy generation and distribution, telecommunication, production and traffic against cyber attacks is one of the major challenges of the new millennium. However, as security is such a complex and multilayer topic often the necessary structured foundation is missing for a manufacturer to assess the current security level of a system. This paper intro-duces a methodology for structured security assessments which has been success-fully applied during the development of several products for critical infrastruc-tures. The methodology is described in detail and the lessons learnt are given from applying it to several systems during their development.
Keywords: Cyber Security, Security Assessment Methodology, Critical Infra¬structure, NERC CIP, Security Assessment Plan, Risk Analysis

1 Introduction

Manufacturers of critical infrastructure components (CIC) like control centers for energy generation or distribution are facing increasing security demands for their products from customers and regulatory bodies. The central questions to be answered are: How good does my product rank concerning security requirements and how secure is it in a real-world operation? The fundamental dilemma here is that the manufacturer is not operating the products and that an operational CIC typically comprises – besides the base product – additional components like networks, the corresponding processes and staff which is often unaware of IT security issues. Additionally, development budgets are tight. Therefore a manufacturer is highly interested in a cost-efficient methodology to assess and subsequently improve the security level of its products extrapolating the operational challenges.

This article describes a cyber security assessment methodology (SAM) which can be used during the development of CICs. The SAM is best effort based, pragmatic, cost-efficient, generic, flexible, and built on CIC industry standards. It has been successfully applied for several Siemens CICs.

What differentiates security assessments of CICs from the "classical" office environment? Though cyber and IT security are commonly used interchangeably, they have different mentalities. The term IT security was established in and for typical office IT. We however refer to CIC systems with utmost crucial value. Besides terminology, there are also several significant technical deviations: In IT security it often is OK to shut something down to protect it (and take time to fix it), whereas CIC must stay up and running at all cost. For more information about the differences between "classical IT" and CICs see [5].

Over the last 8 years, a rapid and partly uncoordinated growth of cyber security publications can be observed. Both of the following sources [7] and [8] easily list more than 50 standards, guidelines, and regulations. To keep an overview it is important for a manufacturer to organize the publications according to the following categories:

- Who is the author? Industry bodies, customers / operators of CIC, regulatory bodies, laws, international standardization bodies?
- Technical publications vs. management
- Industry specific vs. general IT security standards
- Is the publication focusing on development or operation of the system

For example, the NERC CIP standard [6] is published by an industry regulatory body, rather management oriented, specific for the energy sector and focusing on the operation of CICs. Contrary, the procurement language [2] is published by a US information sharing center, rather technical, industry independent and focusing on the development of CICs. For an efficient and market-oriented SAM, a manufacturer must take current standardization and cyber security publications into account to determine subsequent SAM elements that suffice state-of-the-art cyber security requirements.

The remainder of the article has the following structure: After this introduction Section 2 presents SAM and its three major phases "Risk Analysis" (RA), "Theoretical Assessment" (TA) and "Practical Assessment" (PA). Examples will be given for illustration purposes. Finally, Section 3 gives conclusion, delineates SAM from related work, and discusses topics for future work.

2 Methodology

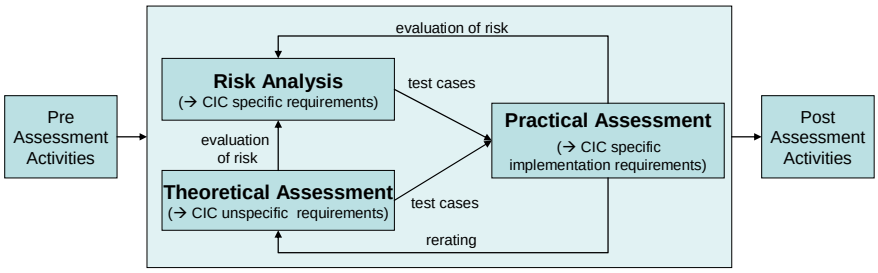
This section describes SAM and its individual phases in detail. Fig. 1 provides a high level overview.

1. Pre-assessment activities include preparation and signing of the project agreement which includes the definition of the detailed scope (CIC version and

release), milestones, location of the assessment, time line, NDA, costs, staffing, liability, etc. For our assessments we follow the existing Siemens project process and corresponding tooling which provides a suitable framework for all these aspects.

2. The RA determines the individual risk level of the CIC and subsequently derives specific security measures for the CIC (cf. Section 2.1).
3. The TA assesses in how far security measures based on a standard (e.g. [2, 6]) are implemented for the CIC. This typically includes technical, organizational and process aspects. Subsequently security measures specific for the underlying document but unspecific for the CIC are derived (cf. Section 2.2).
4. During the PA practical tests – manually and with hacker tools – are done in a suitable test environment. By this the actual exploitability of the CIC can be proven (cf. Section 2.3).
5. Post assessment activities include the communication of the findings, final reporting, issuing of a SAM confirmation, help with fixing and track fixing of security holes, and help in defining requirements for future product releases.

Fig. 1 SAM Overview: relations between the different components.



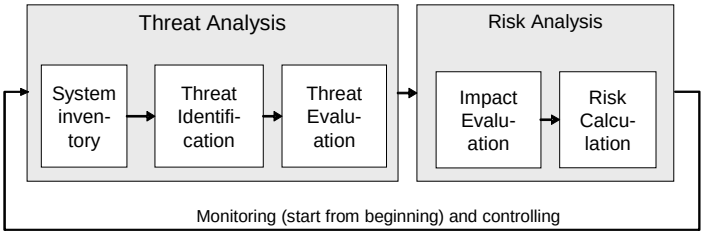
2.2 Risk Assessment

The approach we follow for the risk assessment (RA) is based on ISO/IEC TR 13335-3:1998(E) and NIST's "Risk Management Guide for Information Technology Systems" [4] and is depicted in Fig. 2. As with all other SAM phases, security efforts are balanced with economical aspects. Therefore, the RA is conducted in the form of group workshops, typically in 1-3 days depending on the complexity of CIC. By relying on a broad spectrum of participants like product development, system test, service, sales & marketing, product management and engaging in a workshop discussion accompanied by introductory interviews of participants, the know-how existing in the staff of a CIC manufacturer is being brought in. As a product usually is not developed from scratch, these parties have comprehensive experience and knowledge that can be recycled and used to create

a very efficient risk assessment process in terms of highly valuable outcome within a rather short amount of time. This process is guided by an experienced assessor who must provide both capabilities as a security expert but also as moderator.

The utmost goal of this process is to efficiently determine the adequate risks for a concrete CIC system. The output of this step also poses valuable input for the later practical assessment stage in determining attack goals.

Fig. 2 Process and phases of a risk analysis.



The output of a risk analysis is:

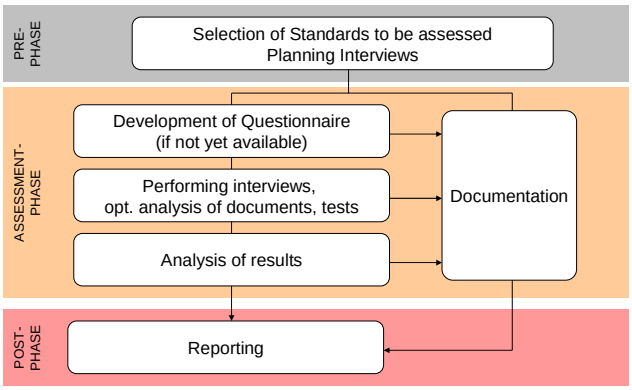
- List of critical assets: this list is the basis for the PA's SAP
- List of threats with corresponding likelihood and impact: Possibly new risks need to be added after the PA or the likelihood / impact of the threats need to be adjusted due to practical findings

2.2 Theoretical Assessment

For critical infrastructure systems (CICs) private and public operators and regulators perceived in the last years that security needs to be integrated into these systems and that a common approach ensures that enough security is realized within products and systems. This led to numerous standards and requirement documents that were published recently. For product management this is a challenge and an opportunity. They need to choose the right standards, assess their level of implementation and, based on the results, decide on further implementation steps. But many of these documents are a "pool" of agreed-upon security requirements contrasting the many customer specific requirements seen in many tenders. Therefore, in this section a method for assessing the level of implementation with regard to generic requirement documents is presented (see Fig. 3). The method has been applied using different standards for several products.

The principle assessment approach is to interview relevant persons based on a questionnaire derived from a standard and to evaluate the answers. Depending on the required assurance level, in addition to the interviews documentation is checked or the system itself is tested.

Fig. 3 Process and phases of a theoretical assessment**.**



2.2.1 Requirement documents

For each standard to be assessed, the requirements for the manufacturer need to be derived. Depending on the target group of the standard, the requirements may either be applied directly or need to be deducted in an intermediate step. As an example the aforementioned NERC CIP standard applies to operators of bulk electric systems. However for product manufacturers, requirements need to be derived. These requirements typically cover not only technical aspects, but also documentation requirements and organizational processes that are carried out by different departments – development, project groups, and support.

The requirements derivation is illustrated in an example. NERC CIP requires that the operator maintains logs of system events related to cyber security for 90 calendar days, and that these logs are reviewed regularly. Just asking if the product supports logging is not sufficient as most systems do support a basic form of logging already. Here, state-of-the-art logging technologies are asked for. Typical features are a possibility for central storage and comprehensible logging data that is stored for at least 90 days and protected against tampering. Also the review of the log data must be facilitated.

In contrast to NERC CIP, the German White Paper “Requirements for Secure Control and Telecommunication Systems“ [1] as well as the US “Cyber Security Procurement Language for Control Systems” [2] summarize security principles that should be considered when designing and procuring control system products and are for use in tenders to specify the security requirements. Therefore, both documents are well suited as direct input for an assessment of the security level of a given product. All requirements can be checked directly, but, as the scope of the documents is broad, some requirements will not be applicable for a given product and need to be marked as not applicable during the assessment.

2.2.2 Questionnaire

For the theoretical assessments (TAs), a questionnaire per standard is used. The goal of the questionnaire is to provide a tool to make the degree of compliance measurable and to yield comparable results independent on the interviewer and the product. The questionnaires have a generic structure independent of the standard, with content structured according to the pattern of the underlying standard. For each requirement one or more corresponding questions are derived with predefined answers that can be selected, and a field where additional comments and descriptions shall be inserted, to make the answers comparable.

The challenge and the effort for deriving the questionnaire lie in content and formulation of the questions, as firstly questions have to be comprehensible and secondly the answers must allow easy benchmarking. The questionnaire itself and the functionality for evaluation of the answers are generated by a tool. As far as possible the questions are formulated in such a way that they can be answered with “Yes”, “No”, or “Not Applicable”.

The experience shows that generic answers are not sufficient. For some requirements we specified “intermediate” answers out of our experience. One example is “Dependent on contract”. It expresses that some requirements are not fulfilled by the standard product offering, but, depending on the contract, can be offered as additional feature.

For automatic evaluation, the answers are mapped to a value of a predefined range. These values are used to calculate the average compliance value per section and per chapter. “Not applicable” answers are not used for calculating the average. The question arises why we did not use numerical values for answering the questions right from the beginning and give an explanation how to use the numbers. We did this for some questionnaires but experienced drawbacks with regard to comparability and traceability. Different interviewers gave different values to the same answer, e.g. if something depends on the contract, one gave full points, as the requirement can be fulfilled; the other gave no point because the standard offering did not fulfill the requirement. Both interviewers have good reasons for their rating, but the results are quite different and cannot be compared. Also during one interview, for long questionnaires, a bias can occur. At beginning the rating could be more strict whereas in the end be more “gentle”. These effects are reduced by use of the predefined, named answers. In principle the mapping is nothing else as a user friendly explanation of each answer possibility.

2.2.3 Performing the Theoretical Assessment

Based on the questionnaire the TA is done within intensive workshops with product experts answering the questions, and experienced security experts independent from product development, who are doing the interviews and guide through the questionnaire. Depending on the assessment goal different assessment depths are possible: (1) just documenting the oral statement of the interviewee(s),

(2) additionally checking / studying the document or (3) doing practical test. The assessment depth can be varied on a per requirement or per section base, e.g. to focus on more important topics.

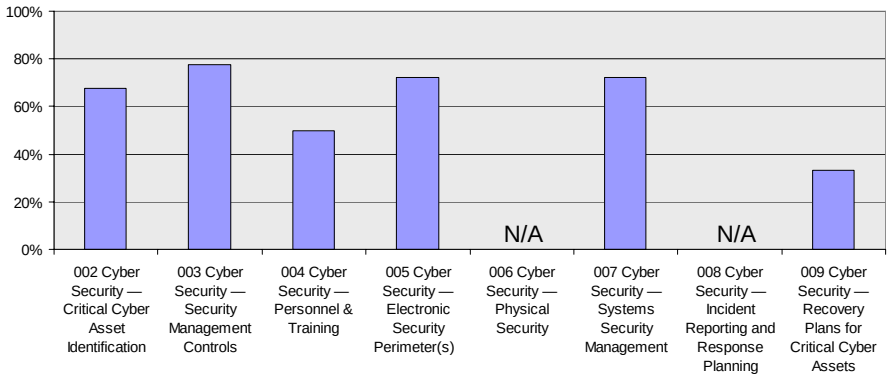
In practice we always used a compromise by doing spot tests for some topics and derived from the theoretical assessment topics for practical security assessments. This combination additionally assures that all intended security mechanisms are really implemented securely and thus raises the level of confidence.

The assessment could also be seen more comprehensive than an external audit. Here, documentation of the system and the processes are checked but also system functionality is reviewed. The scope of the checks is decided by the auditor and is limited by the defined timeframe.

2.2.4 Analysis of results

The method and the underlying tool give an instant overview about the level of compliance for the different sections. The result of the theoretical assessment is the level of compliance with the requirements and the deviations identified. Fig. 4 shows the result of a sample NERC CIP compliance TA. For CIP 009, the assessed product had functions for backup, but no documented recovery concept.

Fig. 4 Example of NERC CIP Compliance Assessment**.**



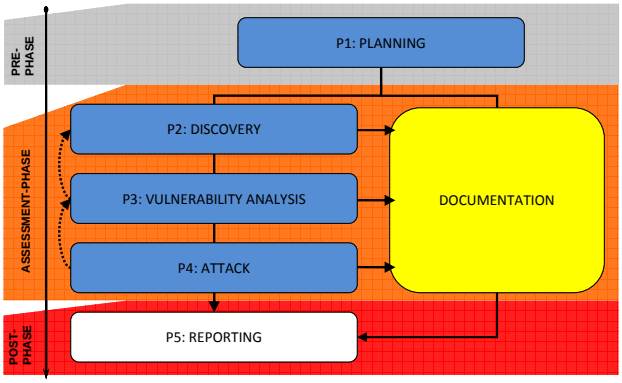
The products we assessed are sold in different regions and markets, therefore typically we checked against several standards. Some sections within different standards were covering the same topic; therefore consistency checks could easily be made.

2.3 Practical Assessment

In the next phase of the SAM, the resilience of the CIC against practical hacking-attacks is evaluated. This step is introduced in order to detect exploitable vulnerabilities and potential security flaws in a CIC, taking into account state-of-the-art hacking know-how and hacking tools. The results both from the RA and the TA are taken as input for actual attack patterns. This third step in the SAM complements the foregoing steps appropriately by verifying the actual implementation.

This is necessary because security requirements and design decisions have been made in earlier CIC development phases and flaws may have been introduced during the actual development phase. As with the whole SAM, the PA phase needs to be structured. We use the security assessment plan (SAP) process steps P1-P5 depicted in Fig. 5 for this purpose.

Fig. 5 Practical assessment process steps.



Note that there are several options for the physical location of the PA. Typically vendors maintain test centers for the unit, module and system test. These test centers can be booked and prepared to perform the PA in house. Alternatively, operational sites can be used. In this case however special care must be taken concerning the definition of the SAP and the intrusiveness of the tests.

2.3.1 Pre-Phase: Planning & SAP preparation

The assessment tasks are initially collected and categorized from former SAM phases in phase P1. In this pre-phase, the assessor decides and evaluates the scope and depth of subsequent tasks, allowing him to control the depth and intrusiveness of the assessment. The planning phase is one of the most crucial ones, as all subsequent test cases in terms of intrusion attempt tasks are decided on here. This is necessary in order to match and tailor the assessment tasks to the overall requirements of the CIC, where certain test methods may be unsuitable, e.g.

denial-of-service tests in productive environments. The actions are then arranged according to the structure of sections, modules and tasks. Fig. 6 gives an example on this task structure in a sample SAP.

Fig. 6 Sample SAP.

ID	SECTION	MODULE	TASK	TOOL	ALT TOOL	CHECKLIST / LINK	STAGE	REM	E_SL
101	network	network surveying	system enumeration	ipconfig/ifconfig	ping		1	1	basic
102	network	network surveying	system identification	nmap	nessus	http://insecure.org/nm	1	1	basic
103	network	network surveying	information leaks	wireshark		http://www.wireshark.	1	1	bronze
104	network	port scanning	service enumeration	nessus	nmap	http://www.nessus.org	1	1	bronze
105	network	port scanning	service identification	nessus	nmap	http://www.nessus.org	1	1	bronze
106	network	port scanning	error checking	hping		http://www.hping.org/	2	1	silver
107	network	port scanning	protocol response verification	nmap	nessus	http://insecure.org/nm	2	1	silver
108	network	port scanning	packet level response verification	nmap	nessus	http://insecure.org/nm	2	1	silver
109	network	port scanning	distributed tcp/ip analysis	unicornscan		http://www.unicornscr	2	1	silver
110	network	perimeter review	security analysis (level 1)	cisecurity (rat)		http://www.cisecurity.	2	1	bronze
111	network	perimeter review	network security review	checklist		http://www.nsa.gov/st	1	n/a	silver
113	network	perimeter review	switch security configuration	checklist		http://www.nsa.gov/st	3	1	silver
114	network	perimeter review	router hardening test	cisco torch	ccsat	http://www.arhont.cor	3	1	silver
115	network	perimeter review	router security configuration	checklist		http://www.nsa.gov/st	3	1	silver
116	network	perimeter review	firewall hardening test	ccsat	cisco torch	http://ccsat.sourceforg	3	1	silver
117	network	perimeter review	firewall security configuration	checklist		http://www.cisco.com/	3	1	silver
118	network	perimeter review	IDS security analysis	manual checking			2	1	silver
119	network	perimeter review	trusted systems security analysis	manual checking			2	1	silver
121	network	DoS testing	DoS vulnerability analysis	manual checking			2	1	silver
122	network	DoS testing	DoS testing	datapool 3.3	DoS test suit	http://www2.packetsto	3	1	bronze
123	network	DoS testing	DoS testing	netcat		http://sourceforge.net	3	1	silver
124	network	DoS testing	DoS risk analysis	manual checking			2	n/a	silver
201	platform	windows/all	baseline security analysis	MBSA		http://www.microsoft.	2	0	basic
202	platform	windows/all	security analysis (level 1)	cisecurity (win)	cat4win	http://www.cisecurity.	2	0	bronze
203	platform	windows/all	security testing (level 1)	manual testing			3	1	bronze
204	platform	windows/all	security analysis (level 2)	GFI languard	?	http://www.gfi.com/la	2	0	silver
205	platform	windows/server 2003	security testing (level 2)	ms scw		http://www.microsoft.	3	1	silver
208	platform	unix/all	security analysis (level 1)	cisecurity (unix)	cat4nix	http://www.cisecurity.	2	0	bronze
209	platform	unix/all	security testing (level 1)	manual testing			3	0	bronze
210	platform	unix/all	security analysis (level 2)	cops	tiger, crack, s	ftp://ftp.cerias.purdue	2	0	silver
211	platform	unix/all	security testing (level 2)	bastille		http://www.bastille-ur	3	1	silver
214	platform	all	login credentials verification	john the ripper	manual chec	http://www.openwall.	3	1	silver

2.3.2 Assessment phase: Structured execution of attacks against the system

Once task planning has finished, the actual practical assessment phase starts. The discovery stage P2 includes information retrieval from the target and passive testing using analyzing tools and techniques. The vulnerability analysis stage P3 classifies vulnerabilities and weaknesses found. Besides the threat classification, this stage requires the tester to verify a threat, to identify associated risks and to document all significant findings for later reporting. The attack stage P4 involves active testing using invasive tools and techniques, trying to successfully gain access to the target or to crash a certain service or function. Strong dependencies exist between phases P2-P4, as newly gained findings are fed back into appropriate tasks.

Typical activities here include port and security scanning, service verification, account brute-forcing, utilization of commercial and self-developed protocol fuzzers, packet spoofing attempts, operating system and database hardening checks, patch level verification, denial-of-service attacks and web-application specific attacks like cross-site-request-forgery, sql injection and HTTP response splitting.

2.3.3 Post-assessment phase: Reporting phase

The reporting stage finally corresponds to the post assessment phase. A report documents all findings produced throughout the assessment phase and forms the base for potential workarounds or mitigation concepts; for an example see Fig. 7. The report also demonstrates and ensures that all sections chosen during the planning phase have actually been covered during the practical assessment phase and proves the scope of the PA phase.

Fig. 7 Sample finding of the PA.

[F1]RSH service detected	
Criticality	HIGH
Vulnerability Location	The service was detected on port 514 TCP on the management server host.
Description	The host provides a remoteshell (RSH) daemon that allows operating system command execution with system privileges from remote without prior authentication. This is highly critical as it immediately gives a remote attacker full system access.
Prerequisites	An attacker with network access can immediately detect and connect to the rsh port.
Counter Measures	Remove the RSH service or replace it with its secure variant SSH.

2.4 Related work and delimitation

There are several approaches in the greater field of SAM that have been studied and evaluated for the purposes of application by a CIC manufacturer. The results are summarized here:

SAM vs. ISO 27002: While ISO 27002 is a management standard SAM is more on a technical level. SAM focuses on the ISO sections 7 and 8, requiring other sections like 1, 2, 3, and 4 as a basis. Other sections like 6 are entirely out-of-scope for SAM. The ISO risk assessment approach is a good way to map the potential exploitation of vulnerabilities identified by SAM to their financial impact.

SAM vs. OSSTMM: The hierarchical structure section / module / task and the process phases are shared between OSSTMM [3] and SAM. However, OSSTMM lacks SAM's RA and TA phases.

SAM vs. IEC/ISO 15408: SAM's scope and depth concept is similar to the common criteria[1]: (CC) approach, standardized in IEC/ISO 15408, but by far shorter and more pragmatic. CC defines the „Target of Evaluation" (scope) and

[1] http://www.commoncriteriaportal.org/

"Evaluation Assurance Level" (EAL) (depth). Also, the mapping of specific tasks to certain inspection depths is shared between the two approaches.

CC provides a certification done by external bodies for external parties while SAM is mainly a manufacturer internal methodology. SAM helps the manufacturer to identify additionally relevant security measures for its CIC and is more oriented on practical aspects that are typically found in bids / tenders. Another difference is the typical size of corresponding projects – CC projects especially for higher EALs require a huge effort. Also CC is much more "paper / process" based than SAM which stresses the practical tests.

SAM can easily be "aligned" with other manufacturer-based certification programs like the one announced by the ISA Security Compliance Institute[2]

3 Conclusion

In this article a SAM for CICs was presented. The major advantages of the SAM are:

- Security level of the CIC can be measured & quantified. This provides an excellent input for subsequent security decisions e.g. on which security requirements to focus in future CIC versions.
- SAM has a broad basis as a practical and theoretical phase is included. Different techniques like interviews, document reviews and practical tests provide a broad insight into the security level of the CIC.
- SAM is flexible and generic since it can be adjusted to different CICs by using different cyber security standards as the basis and adopting the SAP to the CIC's needs, taking into account any concerns or restrictions.
- SAM is cost effective and has been successfully used for different CICs. Typically 1-3 assessors work for a few weeks on the SAM for a CIC.
- The theoretical assessments revealed missing technical features, but surprisingly also security deficiencies with regard to documentation and the processes along the complete product lifecycle, starting from the bidding process, where critical customer information needs to be protected to service during operation.

Over the last years many major IT manufacturers like Microsoft and SAP have started to tie their security activities to the product development process. Also SAM follows this approach. The different SAM phases can be done at different development milestones of the CIC. Risk Assessment (RA) should be done as early as possible (e.g. during plan / design). For Practical Assessment (PA) the product must be in a "testable" state, i.e. the required SW and HW modules must be available in a suitable test environment (e.g. during the "realization" phase). It

[2] http://www.isa.org/Content/NavigationMenu/Technical_Information/ASCI/ISCI/ISCI.htm

should be noted that it is possible (but not recommended as important synergies get lost) to perform only selected parts of the entire SAM, e.g. (RA) + (PA) or (TA) + (PA).

The advantage of combining the three major SAM phases can finally be demonstrated by the catchy example patch management: Most cyber security standards ask for patch management and the corresponding processes and organization. With SAM, these requirements are checked via interviews and review of the corresponding documents in the TA. The actual patch level of the CIC and the implications of missing patches on CIC are tested in the PA. The risk of not applying required patches or late application of a patch is addressed in the RA.

SAM has been developed based on the experiences of security analysis of CICs and CIC security needs. It has been applied successfully to various CIC systems. As the method is generic, it could in principle be applied to other systems, e.g. standard office and IT systems. As a prerequisite, a set of relevant security standards for these systems need to be identified to be able to choose the most appropriate standards for the actual security analysis. Also, the practical assessment tools used need to be chosen in accordance with the new application fields.

References

1. Bundesverband der Energie- und Wasserwirtschaft: White Paper Requirements for Secure Control and Telecommunication Systems, Berlin, June 2008 http://www.bdew.de/bdew.nsf/id/A975B8333599F9B0C12574B400348E7A/$file/Whitepaper_Secure_Systems_Vedis_1.0final.pdf
2. Idaho National Laboratory: Cyber Security Procurement Language for Control Systems. February 2008. Version 1.8, on http://www.msisac.org/scada/
3. ISECOM: Open Source Software Testing Methodology, 2007, http://www.isecom.org/osstmm/
4. National Institute of Standards and Technology Special Publication 800-30, Natl. Inst. Stand. Technol. Spec. Publ. 800-30, 54 pages (July 2002), http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
5. National Institute of Standards and Technology Special Publication 800-82 (FINAL PUBLIC DRAFT) Natl. Inst. Stand. Technol. Spec. Publ. 800-82, 156 pages (September 2008), http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf
6. North American Electric Reliability Council: Critical Infrastructure Protection (CIP), http://www.nerc.com/
7. US-CERT: Standards & References Web Site of the Control System Security Program of the US CERT, http://www.us-cert.gov/control_systems/csstandards.html
8. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability: National SCADA Test Bed, A Summary of Control System Security Standards Activities in the Energy Sector, October 2005, http://www.inl.gov/scada/publications/d/a_summary_of_control_system_security_standards_activities_in_the_energy_sector.pdf