Chapter 16

A MANUFACTURER-SPECIFIC SECURITY ASSESSMENT METHODOLOGY FOR CRITICAL INFRASTRUCTURE COMPONENTS

Thomas Brandstetter, Konstantin Knorr and Ute Rosenbaum

Abstract Protecting critical infrastructure assets such as telecommunications networks and energy generation and distribution facilities from cyber attacks is a major challenge. However, because security is a complex and multi-layered topic, a foundation for manufacturers to assess the security of products used in critical infrastructures is often missing. This paper describes a structured security assessment methodology that is specifically designed for use by manufacturers during product development. The methodology, which incorporates risk analysis, theoretical assessment and practical assessment, anticipates operational security challenges before products are deployed in critical infrastructures.

Keywords: Critical infrastructure components, security assessment, risk analysis

1. Introduction

Security assessments of critical infrastructure components (CICs) differ from those of classical IT systems in that availability and integrity of the components trump confidentiality [18]. Also, it is often impossible to perform regular patching for these components; consequently, the patching cycles typically follow planned maintenance schedules.

Manufacturers of CICs such as control systems for energy generation are facing increasing security demands for their products from customers and regulatory bodies. The central question to be answered is: what security problems related to the products should be remediated? This paper describes a three-step security assessment methodology to help answer this question. The steps are: (i) evaluate the individual security risks associated with the design and architecture of the product, and identify the risks that cannot be tolerated and

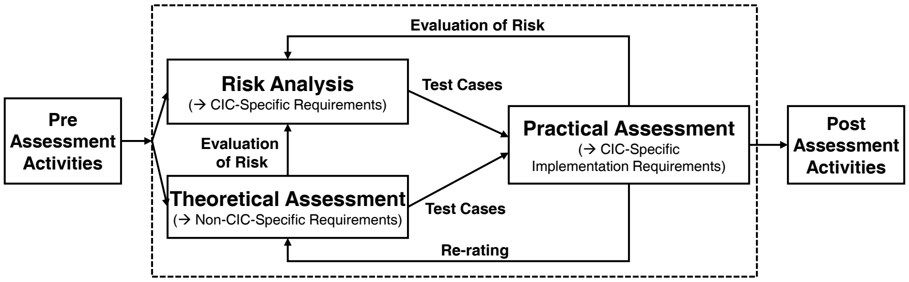

Pre Assessment Activities
Risk Analysis
(→ CIC-Specific Requirements)
Evaluation of Risk
Theoretical Assessment
(→ Non-CIC-Specific Requirements)
Evaluation of Risk
Test Cases
Test Cases
Practical Assessment
(→ CIC-Specific Implementation Requirements)
Re-rating
Post Assessment Activities

Figure 1. Security assessment methodology phases.

must be mitigated, accepted or transferred; (ii) determine how the product ranks with regard to security requirements published by potential customers and regulatory bodies; and (iii) perform practical tests of the CIC in operational environments to uncover implementation and configuration flaws.

The security assessment methodology described in this paper is intended to address the needs of manufacturers during the development of CICs. The methodology, which is pragmatic, cost-effective, generic, flexible and built on CIC industry standards, has been successfully applied to several CICs.

2. Security Assessment Methodology

Figure 1 presents a high-level overview of the security assessment methodology. The methodology starts with the pre-assessment phase, which involves the preparation and signing of the project agreement, and includes a definition of the assessment scope (CIC version and release), milestones, location, timeline, costs, staffing, liability, etc. The subsequent risk analysis phase determines the individual information security risk levels arising from the technical design and architecture of the CIC by performing a risk analysis and deriving specific security measures for the CIC. The theoretical assessment phase examines how far security measures mandated by standards, regulatory requirements and generic customer requirements are implemented in the CIC. This typically includes technical, organizational and process aspects. Security measures specific to the standard, but not specific to the component under test, are checked. The practical assessment phase involves the application of manual procedures and automated tools in a suitable testing environment to determine the potential for exploiting vulnerabilities. The final post-assessment activities involve presenting a final report to the product manager, issuing a security assessment methodology confirmation and suggesting solutions for the security flaws.

In recent years, many manufacturers have begun to tie security activities to the product development process. Our security assessment methodology follows this approach. The various phases can be performed during different development milestones of a CIC. Risk analysis and theoretical assessment should be completed as early as possible (e.g., during product planning or design). In the case of a practical assessment, the product must be in a "testable" state, i.e., a suitable test environment must be available. Note that it is possible to perform only selected parts of the methodology, e.g., risk analysis and practical assessment, or theoretical assessment and practical assessment. However, partial assessment is not recommended because important synergies are lost.

2.1 Pre-Assessment

The pre-assessment phase is the preparatory phase of a security assessment. During this phase, the various participants agree on the project details. After an initial discussion and using a predefined questionnaire, the proposed target of evaluation (TOE) is briefly analyzed. This analysis identifies the security goals and the scope and depth of the assessment, which must be agreed upon by all the involved parties. The detailed specifications of all the subsequent assessment phases are determined in this initial analysis. Depending on the security goals of the TOE and its market placement, it is necessary to decide on the standards to be included in the theoretical assessment and the tests to be included in the practical assessment. This helps determine the overall effort for conducting the assessment and a realistic cost estimate and timeline, all of which assist in planning the subsequent phases.

2.2 Risk Analysis

ISO/IEC 27005:2008(E) defines information security risk as the potential that a given threat will exploit vulnerabilities in an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and its consequence. Risk analysis is the practice of determining the threats to which an organization or system is exposed and the potential harm. The risk analysis approach in our security assessment methodology is based on established risk analysis techniques [9, 17], but is adapted to the specific needs of CIC manufacturers by defining a risk management framework that is designed to be cost-effective by using a workshop to conduct the analysis.

Risk Analysis Steps The risk analysis steps follow the ISO and NIST standards [9, 17]. First, the CIC assets are identified. Next, threats that exploit asset vulnerabilities are determined and the probability of a successful attack is estimated. Finally, the impact of an attack is described and classified. The associated risk is computed by combining the probability of a successful attack and its impact.

During these steps, the CIC risk must be seen from two points of view. First, what risks does the CIC pose to the manufacturer's business model? Second, what risks arise during CIC operation due to its technical architecture?

Both views have to be considered during risk analysis. Depending on the point of view, the assets are quite different. To the manufacturer, the assets may represent intellectual property and licensing schemes; often, considerable threats and associated risks can be identified for these assets. To the operator,

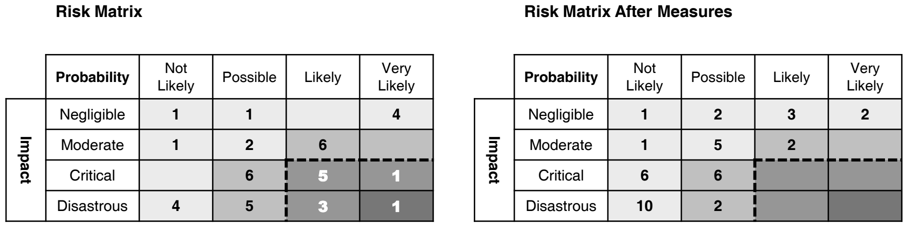
Table 1. List of potential attackers.

Attacker	Comment
Third-party consulting vendor	Attacks against licensing scheme, e.g., by selling high-end products to the customer but ordering and paying for low-end products with less functionality.
Competitor	Competitor seeks proprietary information about a product, e.g., to better position his products, or to copy the product or some of its functionality.
Hacker (organized)	Hacker attempts to control a CIC on behalf of a third party.
Hacker (curious)	Hacker accidentally breaks into a system and tries to gather information.
Malware	Malware infects a CIC network accidentally or intentionally.
Employee (manufacturer)	Employee with access to confidential development data steals or destroys the data.
Cyberterrorist	Cyberterrorist disrupts CIC service to cause panic or to extort money.

the assets are quite different; they may, for example, correspond to personal data that has to be kept confidential or systems whose availability must be maintained. Because the risk analysis is performed by the manufacturer and not by the system operator, several deployment scenarios may have to be analyzed to determine the possible impact to an operator.

Practical Risk Analysis As with all the phases of the security assessment methodology, security efforts are balanced with economic aspects. Therefore, the risk analysis is conducted in the form of a group workshop, which is typically one to three days long, depending on the complexity of the CIC. The workshop is conducted by an experienced assessor who is a security expert and can serve effectively as a moderator. The workshop participants represent all the various phases of the product lifecycle, e.g., product development, system testing, service, sales and marketing, and product management. Ideal participants would have comprehensive knowledge and significant experience in product design and architecture (product development); use cases and deployment in customer environments (service); and competitors and sales channels (sales and marketing) necessary to understand the risks related to intellectual property and license fraud related risks.

Predefined lists of potential attackers, targets, threats and impacts are used to provide examples, raise discussion and check for completeness. The list in Table 1 is derived from generic lists [9, 11] that are adapted to CIC needs.



Risk Matrix

	Probability	Not Likely	Possible	Likely	Very Likely
Impact	Negligible	1	1		4
	Moderate	1	2	6	
	Critical		6	5	1
	Disastrous	4	5	3	1

Risk Matrix After Measures

	Probability	Not Likely	Possible	Likely	Very Likely
Impact	Negligible	1	2	3	2
	Moderate	1	5	2	
	Critical	6	6		
	Disastrous	10	2		

Figure 2. Sample risk analysis results.

Experience has shown that this approach yields an efficient and useful risk analysis in a relatively short amount of time.

Risk Management In order to reduce the effort involved in risk analysis, a predefined risk management model is used following a qualitative rating. Four categories are defined for rating the probability of a successful attack and the impact; these categories take into account CIC-specific aspects such as availability. If necessary, the descriptions of the categories may be clarified and amended by product-specific aspects during the workshop. The results of the risk analysis are presented as a 4 × 4 risk matrix. The ratings of the risks, i.e., the definitions of the risks that are considered to be acceptable and those that need to be mitigated, are also predefined.

Figure 2 shows the results of a threat analysis of an energy management system. Initially, several non-acceptable risks were identified, one is classified as “Probability: Very Likely” and “Harm: Disastrous.” However, the risk may be reduced to an acceptable level after selecting and implementing countermeasures. The initial analysis can be completed in a two-day workshop.

Four categories for the probability of a successful attack and the resulting impact are offered. Using an even number of values ensures that no midpoint value can be chosen, which eliminates indecision in arriving at an assessment.

Risk Analysis Results For the workshop participants, the immediate results provide a better understanding of the threats to which the CIC is exposed, because the participants themselves “discover” the threats to the CIC. They gain understanding of the need for security measures and learn to act accordingly. The workshop gives them a forum to discuss security aspects. Also, the workshop provides training and awareness opportunities for non-expert participants. The overall effect of the workshop is far superior to that of a risk assessment conducted by an external consultant, which is based entirely on technical input from the development team.

The risk analysis provides the project manager with a list of the identified risks along with their ratings, identifying the risks that must be mitigated according to their priority. The risk analysis also provides valuable inputs to the other phases of the security assessment (e.g., the list of critical assets and identified risks that form the basis of the practical assessment). Note, however, that it is sometimes the case that the threats identified by the theoretical assessment and the practical assessment have to be added to the risk analysis.

2.3 Theoretical Assessment

This section discusses the theoretical assessment approach, which is designed to assess the security level of CICs with regard to generic security standards. Note that the term "standard" does not accurately fit the documents (guidelines, recommendations, regulatory documents and laws) referred to in this work. However, for the sake of simplicity we use this term throughout the paper.

In general, customers who operate critical infrastructure assets have published their own generic security requirements; sometimes based on regulatory requirements for operation, sometimes directly referring to existing standards. Fulfilling customer requirements is a prerequisite for selling products. Consequently, it is important for a manufacturer to know how well its products satisfy the requirements. The first step in the theoretical assessment approach is to decide which standard is relevant to the CIC. Next, a questionnaire is created based on the selected security standard if one is not yet available. Finally, the approach uses the results of the interviews of CIC experts based on the questionnaire to arrive at a security assessment.

Selecting Standards Numerous CIC-related security standards have been published (see, e.g., [5, 21] for a list of more than 50 important standards). For example, the NERC CIP standard [10] is published by an industry regulatory body and focuses on the operation of CICs. A U.S. information sharing center has published a "procurement language" [8] that focuses on the development of CICs. From the point of view of product management, the diversity of security documents presents a challenge and an opportunity. On the one hand, it complicates the task of selecting the standards used in an assessment. On the other hand, many of the documents contain agreed-upon security requirements that are seen in many tenders.

Developing Questionnaires A theoretical assessment uses one questionnaire per standard. A questionnaire has a generic structure that is independent of the standard, but its content is structured according to the pattern of the underlying standard. The content reflects the requirements of the standard being assessed.

Relevant requirements have to be derived when a standard does not specifically address a manufacturer's product. For example, NERC CIP [10], a standard for operators of bulk electric systems, requires that operators maintain logs of security events for 90 calendar days and that these logs be reviewed regularly. Merely checking if a product supports logging is insufficient because most systems already support logging. The intent of the standard is for products to incorporate state-of-the-art logging technology.

In contrast with the NERC CIP standard, the U.S. Cyber Security Procurement Language for Control Systems [8] summarizes security principles that should be considered when designing and procuring control system products. Therefore, it is well-suited as direct input for a questionnaire. Because the scope of the document is broad, some requirements will not be applicable to a given product and have to be marked as not applicable during the assessment. For each requirement of the selected standard, one or more corresponding questions are derived so that they can be answered with "Yes," "No" or "Not Applicable." Predefined intermediate answers such as "Dependent on Contract" are also permitted. It expresses the fact that a requirement is not fulfilled by the default product offering but, depending on the contract, can be offered as an additional feature. Without this option, different answers are possible: the answer "Yes" because the requirement can be fulfilled, and "No" because the standard offering does not fulfill the requirement. In the case of automatic evaluation, the predefined answers are mapped to a value in a predefined range and are used to calculate the "average compliance." Additionally, a comments field is provided for each question to enable respondents to clarify their answers.

Conducting Interviews The theoretical assessment is conducted in a workshop environment where experienced security assessors (who are not involved product development) conduct interviews of product experts and guide them through the questionnaire. Depending on the goal, different assessment depths are possible: (i) merely documenting the oral statements of the interviewees; (ii) checking and analyzing the available documentation; or (iii) deriving tests for the subsequent practical assessment phase. The assessment depth can be varied on a per-requirement or per-section basis.

In practice, we perform spot tests for some topics and also use some of the theoretical assessment topics to derive topics for the practical security assessment. This combination ensures that all the intended security mechanisms exist and are implemented securely, thereby raising the level of confidence of the assessment.

Analyzing and Reporting Results The results of the theoretical assessment include the level of compliance with the requirements and the identified deviations. The results support a detailed analysis of the shortcomings of the product, and are suitable for presentation to management. The degree of deviation is apparent without delving into the technical details; also, security becomes measurable.

Figure 3 shows the results for a NERC CIP benchmark of two versions of a CIC. The initial version of the product incorporates backup functionality without a documented recovery concept. The new version incorporates additional security functionality and documentation, with the documentation, in particular, improving the CIP 009 rating.

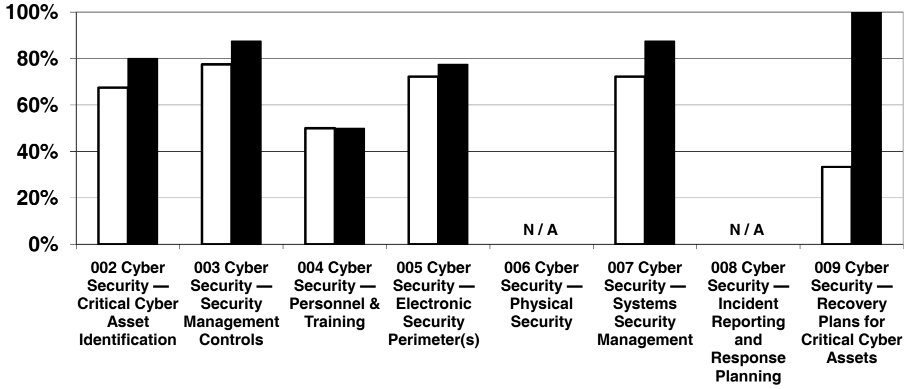


Figure 3. Sample NERC CIP compliance theoretical assessment results.

2.4 Practical Assessment

Practical assessment, the next phase of the security assessment methodology, evaluates the resilience of a CIC to hacking attacks. This phase is introduced to detect exploitable vulnerabilities and potential security flaws in a CIC taking into account state-of-the-art hacking techniques and tools. The results of the risk analysis and theoretical assessment phases are used as input when generating attack patterns and testing tasks. Practical assessment complements these phases by verifying the actual implementation of the security features.

We begin by discussing a sample test task to explain how a practical assessment works. NERC CIP 005-1 R4 requires a review of controls for default accounts, passwords and network management community strings. The first task is to identify the credentials in a target system; this is typically performed using an automated tool (e.g., Nessus Security Scanner [19]) or by manually reviewing the credential store on the system. Next, the credentials are reviewed for known default values or easily guessed credentials. Insecure credential combinations are then documented. Finally, the identified username/password combinations are tested to determine if they permit access to the system.

A suitable test system is necessary to conduct a practical assessment. A test system at a manufacturer is suitable for conducting in-house tests. Factory and site acceptance tests are typically performed during the handover of a CIC from the manufacturer to the customer; these tests also provide an excellent environment for a practical assessment. Alternatively, a practical assessment can be performed at the customer site. In this case, special care must be taken to define the testing tasks as they must not affect normal operations. As with the entire security assessment methodology, the practical assessment follows a structured process, which is presented in Figure 4.

Planning and Preparation The practical assessment test tasks are initially collected and categorized based on input from the preceding risk analysis and theoretical assessment phases, and on an agreement between the project

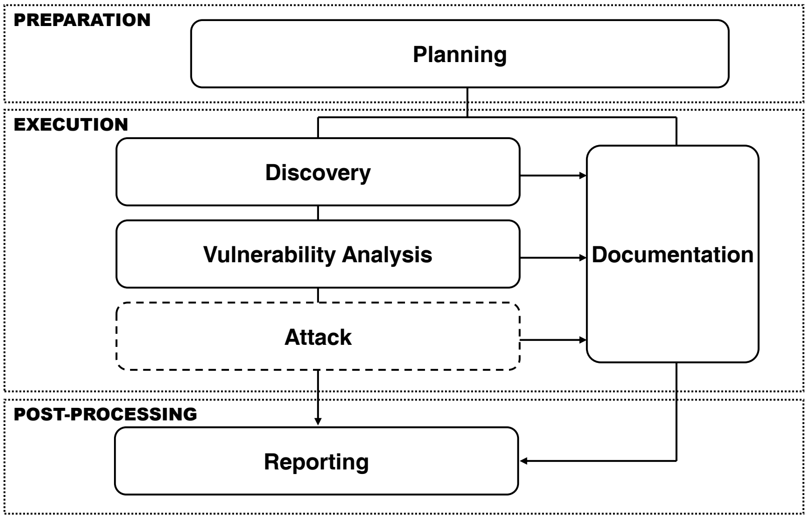


Figure 4. Practical assessment steps (with optional attack step).

manager and the assessment team. In this step, the assessor uses a structured assessment plan (Table 2) to evaluate the scope of the subsequent tasks, enabling the depth and intrusiveness of the assessment to be controlled.

Assessment The practical assessment process closely follows the steps used by real hackers. A hacker initially tries to gather information about the target via discovery and reconnaissance activities. This information is reviewed and analyzed for potential vulnerabilities during the vulnerability analysis phase. Finally, in the attack step, the hacker attempts to exploit certain vulnerabilities and launch real attacks against the system.

A practical assessment begins with the discovery step, where information gathering tasks are carried out to collect information about the target using active or passive tools. A vulnerability analysis is conducted using the collected information; this is done by manually reviewing the information for indications of potential flaws. For each flaw, the assessor attempts to estimate the potential of successful exploitation and the criticality. This must be done because hackers typically work their way from "low hanging fruit" to more complex attacks. The review helps identify the most promising entry points for further attacks.

In the practical attack step, the assessor attempts to exploit an identified vulnerability and document the extent to which the intrusion attempt is successful. The attack step involves both active and passive testing. Active testing uses invasive tools and techniques to gain access to the target or to crash a certain service. Passive testing mainly involves a configuration review (invasive tools may not be used because they can impact system availability). Strong dependencies exist between all the steps as new findings are fed back into succeeding test activities. The practical attack step is optional because it may be

Table 2. Sample practical assessment plan (N: network; P: platform).

ID	Sect.	Module	Task	Tool
101	N	Network survey	System enumeration	ipconfig/ifconfig
102	N	Network survey	System identification	nmap
103	N	Network survey	Information leaks	Wireshark
104	N	Port scan	Service enumeration	Nessus
105	N	Port scan	Service identification	Nessus
106	N	Port scan	Error checking	hping
107	N	Port scan	Protocol response verification	nmap
108	N	Port scan	Packet response verification	nmap
109	N	Port scan	Distributed TCP/IP analysis	Unicornscan
110	N	Perimeter review	Security analysis (Level 1)	cisecurity (rat)
111	N	Perimeter review	Network security review	Checklist
113	N	Perimeter review	Switch security configuration	Checklist
114	N	Perimeter review	Router hardening test	Cisco Torch
115	N	Perimeter review	Router security configuration	Checklist
116	N	Perimeter review	Firewall hardening test	ccsat
117	N	Perimeter review	Firewall security configuration	Checklist
118	N	Perimeter review	IDS security analysis	Manual checking
119	N	Perimeter review	Trusted sys. security analysis	Manual checking
121	N	DoS test	DoS vulnerability analysis	Manual checking
122	N	DoS test	DoS testing	datapool 3.3
123	N	DoS test	DoS testing	netcat
124	N	DoS test	DoS risk analysis	Manual checking
201	P	Windows/all	Baseline security analysis	MBSA
202	P	Windows/all	Security analysis (Level 1)	cisecurity (win)
203	P	Windows/all	Security testing (Level 1)	Manual testing
204	P	Windows/all	Security analysis (Level 2)	GFI Languard
205	P	Windows/Svr2003	Security testing (Level 2)	MS SCW
208	P	Unix/all	Security analysis (Level 1)	cisecurity (Unix)
209	P	Unix/all	Security testing (Level 1)	Manual testing
210	P	Unix/all	Security analysis (Level 2)	COPS
211	P	Unix/all	Security testing (Level 2)	Bastille
214	P	All	Login credential verification	John the Ripper

sufficient to gather information about the target and review it for indications of vulnerabilities rather than executing an attack.

Finally, note that each test task has two possible outcomes: the intrusion attempt either succeeds or it fails. Both outcomes must be noted to comprehensively document the test; this also gives product developers a better view of the security aspects of the product that have been addressed properly.

Reporting The findings (i.e., discovered security flaws) are documented in a report using a predefined structure. Table 3 presents example findings from the energy management system assessment described above. The example focuses on a test of the ability to log security-relevant information such as brute-force attacks on accounts at the operating system level. During the discovery phase, a port scan revealed typical server message block (SMB) ports in the TCP range of 135–139 and 445. During the subsequent vulnerability analysis phase, the ports were tested for the null-session feature, which enables an attacker

Table 3. Sample practical assessment finding.

Headline	Account login auditing disabled on application server.
Criticality	HIGH
Vulnerability Location	Windows OS auditing policy of application server with hostname `appserver.localdomain`.
Description	Logging and auditing settings at the OS level were reviewed to check for proper audit trail generation. During the review it was noted that login attempts at the OS level were not audited, regardless of whether they were successful or not. This enables an attacker to conduct a brute-force attack on an account without being detected. If security-critical information is not recorded, there is no trail for forensic analysis. Discovering the cause of problem or the source of the attack may become more difficult or impossible.
Prerequisites	For an actual attack (e.g., brute-forcing an account), the attacker would need network access to the system.
Standards Violated	NERC CIP 007-1 R 5.1.2; NERC CIP 007-1 R 6.3
CWE	778
Countermeasure	The logging level must be set appropriately for security-relevant items like account login activity. Enable account logging at the OS level.

to gather information about user account names and other account details at the operating system level. With this information, a brute-force attack for determining the passwords of existing user accounts was started, upon which the log entries were reviewed for appropriate tracking details. In the example, the logging subsystem failed to document the existence of the attack because of an inappropriate configuration.

The report is an important tool for quality control because it verifiably demonstrates that all the sections chosen in the planning step have been covered during the practical assessment. Also, it proves that the entire scope of the practical assessment phase has been completed.

2.5 Post-Assessment

The post-assessment activities of the security assessment methodology include, but are not limited to, the final report, the communication of the findings, the issuance of a security assessment methodology confirmation, and support for addressing the security flaws identified in the assessment. The security assessment methodology results are documented in a final report comprising the three sub-reports from the risk analysis, theoretical assessment and practical assessment phases along with their relationships. The content of the final report is typically confidential and is, therefore, delivered only to the project manager, who then becomes the owner of the report. If required, a confirmation about the assessment is generated for the project manager that states the detailed CIC version, size and date of the assessment, and confirms that the CIC was assessed and describes the security issues addressed in the product.

The next step for the project manager is to decide how to proceed with the results of the security assessment, especially the identified risks, the shortcomings related to the standards, and the implementation and configuration flaws. Entries in the error tracking database corresponding to the product have been successfully used for emergency (short-term) mitigation projects. Other findings can be addressed via change requests and subsequently by new security requirements for the product. Support for these activities is not part of the security assessment methodology, but they are, nevertheless, very important to enhance product security.

3. Discussion

This section discusses the applicability of the security assessment methodology to CICs, compares the methodology with related work in the field and identifies future areas of research.

3.1 CIC Applicability

The risk analysis phase of the security assessment methodology uses generic security standards (e.g., [9, 17]). This has been done on purpose because the generic method described in these standards is well-suited to CICs. The general principle followed in designing the security assessment methodology was to re-use as much as possible of existing methodologies and adapt them to CIC needs where necessary. The adaptations for the three phases of the security assessment methodology are:

- **Risk Analysis:** While the risk analysis phase is based on [9, 17], the workshop and, in particular, its inclusion of participants with experience in CIC development and management are CIC-specific.

- **Theoretical Assessment:** The use of CIC-related standards [4, 8, 10] in the questionnaires makes this phase CIC-specific. In most critical infrastructure domains, the main standardization bodies have decided not to use generic security standards such as the ISO 2700x series, but to adapt these standards to reflect specific domain requirements.

- **Practical Assessment:** The tools and test cases are, by necessity, CIC-specific. For example, CIC-specific protocol fuzzers have to be used because CICs engage proprietary protocols.

3.2 Related Work

To our knowledge, this is the first security assessment methodology that combines the three phases, risk analysis, theoretical assessment and practical assessment, in a pragmatic and cost-effective manner for use by CIC manufacturers.

Risk analysis is a fairly mature area (see, e.g., [9, 17]). The main focus of risk analysis as used in our work is to identify risks stemming from the design and architecture of a product. This is in contrast to other published methodologies, such as OCTAVE [1] and CRAMM [16], which deal with the risks faced by organizations that operate IT systems. Some risk assessment approaches created for operators of critical infrastructures (e.g., [12]) share the basic aspects of our risk analysis approach, but they cannot be directly applied by CIC manufacturers.

With regard to the theoretical assessment phase, certain parallels exist with the recommended use of the Control System Cyber Security Self-Assessment Tool (CS2SAT) [20], which includes a self-assessment step based on a questionnaire using recommended standards. Note, however, that CS2SAT is designed primarily for use by operators, and cannot be directly applied by CIC manufacturers.

Considerable work has been performed in the area of practical assessment. Several approaches either compete with or overlap with our practical assessment approach. Interested readers are referred to [2] for a detailed discussion of practical assessment approaches.

3.3 Future Work

Future work related to the security assessment methodology will focus on enhancing the risk analysis, theoretical assessment and practical assessment phases. The current risk analysis approach is relatively stable, but the opportunity exists to streamline and optimize the underlying process. Our future work related to theoretical assessment will address the identification and inclusion of new standards, and corresponding updates to the questionnaire; another research thrust is to devise approaches for leveraging the synergies existing in overlapping standards. Refinements to the practical assessment phase will concentrate on extending the assessment plan with new attacks and tools, and improving the test task descriptions.

Deficiencies identified by the security assessment methodology create new security requirements for the CIC, which should be implemented according to a requirements engineering process. Our future work will attempt to align the security assessment methodology findings with those obtained using common requirements engineering methods.

The security assessment methodology has been developed based on our experience with security assessments of CICs and CIC security needs. The methodology has been applied successfully to several CIC products. Because the methodology is generic, it can, in principle, be applied to other systems (e.g., corporate IT systems). However, it will be necessary to identify relevant security standards for these systems before the security assessment methodology can be applied.

4. Conclusions

The security assessment methodology presented in this paper has been applied to more than fifty products, including control systems, substation automation devices, and field devices in industrial and energy environments. The results indicate that the methodology is flexible and well-suited to assessing the security levels of CICs within a matter of man-days as opposed to man-weeks.

A key advantage of the methodology is that the security level of a CIC can be measured and quantified. This is accomplished by constructing a risk matrix. Changes to the risk matrix caused by implementing countermeasures as a result of risk analysis quantifies the resilience against the documented risks. Also, security capabilities are measured in the form of a benchmark against the requirements derived from relevant industry standards. This provides excellent input for subsequent security decisions.

The security assessment methodology is generic and can be adjusted to different CICs by using the relevant CIC security standards as the basis and applying the methodology to the CIC specifics. Finally, the security assessment methodology is lightweight and cost-effective in comparison with evaluation methods such as the Common Criteria [6]. In most cases, one to three assessors require a few weeks to complete a security assessment of a large CIC.

References

[1] C. Alberts, A. Dorofee, J. Stevens and C. Woody, Introduction to the OCTAVE Approach, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania (www.cert.org/octave/approach_intro.pdf), 2003.

[2] M. Braun, Process Optimization of Practical Security Assessments, Master's Thesis, University of Applied Sciences, Augsburg, Germany, 2008.

[3] Bundesamt fuer Sicherheit in der Informationstechnik, Durchfuehrung fuer Penetrationstests, Bonn, Germany (www.bsi.bund.de/cae/servlet/contentblob/487300/publicationFile/30684/penetrationstest_pdf.pdf), 2003.

[4] Bundesverband der Energie und Wasserwirtschaft, White Paper: Requirements for Secure Control and Telecommunication Systems, Version 1.0, Berlin, Germany (branchenkommunikation-energie.bdew.de/bdew.nsf/id/52929DBC7CEEED1EC125766C000588AD/$file/Whitepaper_Secure_Systems_Vedis_1.0final.pdf), 2008.

[5] R. Carlson, J. Dagle, S. Shamsuddin and R. Evans, A Summary of Control System Security Standards Activities in the Energy Sector, National SCADA Test Bed, U.S. Department of Energy, Washington, DC, 2005.

[6] Common Criteria Recognition Agreement Members, Common Criteria v3.1. Release 3, National Information Assurance Partnership, U.S. Department of Defense, Fort George Meade, Maryland (www.commoncriteriaportal.org/thecc.html), 2009.

[7] P. Herzog, OSSTMM – Open Source Software Testing Methodology, Institute for Security and Open Methodologies, New York (www.isecom.org /osstmm).

[8] Idaho National Laboratory, Cyber Security Procurement Language for Control Systems, Version 1.8, Technical Report INL/EXT-06-11516, Revision 3, Idaho Falls, Idaho (www.msisac.org/scada/documents/4march08 scadaprocure.pdf), 2008.

[9] International Organization for Standardization, ISO/IEC 27005:2008(E), Information Technology – Security Techniques – Information Security Risk Management, Geneva, Switzerland, 2008.

[10] North American Electric Reliability Corporation, Critical Infrastructure Protection Program, Princeton, New Jersey (www.nerc.com/page.php?cid = 6—69).

[11] North American Electric Reliability Corporation, Security Guideline for the Electricity Sector: Identifying Critical Assets, Version 1.0, Princeton, New Jersey (www.nerc.com/docs/cip/sgwg/Critcal%20Asset_ID_Final_Clean.pdf), 2009.

[12] Office of Energy Assurance, Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities, U.S. Department of Energy, Washington, DC (www.esisac.com/publicdocs/assessment _methods/Risk_Management_Checklist_Small_Facilities.pdf), 2002.

[13] Open Information Systems Security Group, Information Systems Security Assessment Framework (ISSAF), Draft 0.2.1B, Colorado Springs, Colorado (www.oissg.org/downloads/issaf-0.2/information-systems-security-assessment-framework-issaf-draft-0.2.1b/download.html), 2006.

[14] OWASP Foundation, Open Web Application Security Project Testing Guide, Version 3.0, Columbia, Maryland (www.owasp.org/images/5/56 /OWASP_Testing_Guide_v3.pdf), 2008.

[15] K. Scarfone, M. Souppaya, A. Cody and A. Orebaugh, Technical Guide to Information Security Testing and Assessment, NIST Special Publication 800-115, National Institute of Standards and Technology, Gaithersburg, Maryland (csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf), 2008.

[16] Siemens Enterprise Communications, CCTA Risk Analysis and Management Method (CRAMM), Milton Keynes, United Kingdom (www.cramm .com/overview/howitworks.htm), 2009.

[17] G. Stoneburner, A. Goguen and A. Feringa, Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30, National Institute of Standards and Technology, Gaithersburg, Maryland (csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf), 2002.

[18] K. Stouffer, J. Falco and K. Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, Maryland (csrc.nist .gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf), 2008.

[19] Tenable Network Security, Nessus – The network vulnerability scanner, Columbia, Maryland (www.nessus.org/nessus).

[20] US-CERT, Cyber Security Self-Assessment Tool, Control System Security Program, U.S. Department of Homeland Security, Washington, DC (www.us-cert.gov/control_systems/satool.html).

[21] US-CERT, Standards and References, Control System Security Program, U.S. Department of Homeland Security, Washington, DC (www.us-cert.gov/control_systems/csstandards.html).