Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems

Guillermo A. Francia, III, David Thornton, and Joshua Dawson
Jacksonville State University
Jacksonville, AL 36265 USA

Abstract - *The nation's critical infrastructures, such as those found in Supervisory Control and Data Acquisition (SCADA) and industrial control systems (ICS), are increasingly at risk and vulnerable to internal and external threats. Security best practices on these systems come at a very opportune time. Further, the value of risk assessment of these systems is something that cannot just be relegated as irrelevant. In this paper, we present a review of security best practices and risk assessment of SCADA and ICS and report our research findings on an on-going risk modeling of a prototypical industrial control system using the CORAS framework tool.*

Keywords: Security Best Practices, Risk Assessment, SCADA, Industrial Control Systems.

1 Introduction

The nation's critical infrastructures, such as those found in SCADA and industrial control systems (ICS), are increasingly at risk and vulnerable to internal and external threats. These are ushered by insecure connectivity to traditional network systems for the purposes of convenience and also by the vulnerabilities typically found in control system devices and applications. Simply stated, these devices are not ready to be publicly exposed on the Internet.

Security best practices on these systems come at a very opportune time. Further, the value of risk assessment of these systems is something that cannot just be relegated as irrelevant. In this paper, we present a review of security best practices and risk assessment of SCADA and ICS and report our research findings on an on-going risk modeling of a prototypical industrial control system using the CORAS framework tool.

In recent years, the recognition of critical infrastructure vulnerabilities and the consequences of successful attacks have garnered increasing attention. Fortunately, this has led to an ever-growing corpus of best practices and security guides published by governmental and industrial entities.

The rest of the paper is organized into four parts. First, we present a concise overview of security guidelines and best practices for protecting critical infrastructures. Second, we cover risk assessment tools and models. In the third section, we describe the CORAS framework and our motivation in using it. Finally, we present our work in developing a risk assessment model for SCADA and industrial control systems.

2 Security Guidelines and Best Practices

Pointers to the set of guidelines, best practices, security tools and new technologies developed by governmental agencies and industrial associations are provided by Ralston, et al. [20].

NIST has published a guideline for security best practices for Information Technology [17]. The NIST has established the Industrial Control System Security Project to research, among its other objectives, the applicability of the NIST SP800-53 recommendations to ICS [12]. The report concluded that an organization, conforming with the baseline sets of security controls in SP 800-53, will also comply with the NERC CIP requirements with regard to the management, operational and technical controls. However, the report pointed out that the so called “business risk reduction” requirements of NERC CIP are not being met because of SP 800-53 is solely focused on information security controls.

Like many information security documents, NIST SP800-53 divides security controls into three categories – technical, management, and operational. These are further subdivided into eighteen families, as shown in Table 1 below.

This set of controls does not represent an exhaustive list, but rather a fundamental set for most practitioners. An additional, much larger list can be found in the appendices and then customized for an individual information security program.

NIST has also released a more targeted security guide [18] which focuses on industrial control systems (ICS) security. This includes the subcategories of SCADA, distributed control systems (DCS), and other control systems like the programmable logic controller (PLC). It contrasts ICS with the more common IT system, underlining threats that are particular to ICS. The broad categories of these threats include policy and procedure vulnerabilities, (such as lack of personnel training and awareness), platform vulnerabilities (such as delayed patching and lack of configuration), and network vulnerabilities (such as weak encryption and lack of redundant hardware). It also explains some of the major risk factors relevant to ICS, including standardized protocols, increased network connectivity, rogue connections, and (somewhat ironically) public information. A cautionary section on documented incidents of attack and hypothetical attack scenarios provides concrete examples of the aforementioned security vulnerabilities.

The President's Critical Infrastructure Protection Board released a concise and approachable overview of key SCADA security concerns in their document, "21 Steps to Improve Cyber Security of SCADA Networks" [19]. Though it was first published in 2002, its content is still relevant today. It represents a good entry point for industry professionals who are taking initial steps toward addressing information security. For more in-depth coverage, the Center for Protection of National Infrastructure's 2010 guide "Configuring and Managing Remote Access for Industrial Control Systems" pairs practical security adjustments with solid justifications for implementing them [4]. It outlines the host of stakeholders related to ICS and the ramifications of attacks on each of them.

In "Best Practices for Government to Enhance the Security of National Critical Infrastructures" [16], the National Infrastructure Advisory Council addresses the need for government to intervene in some markets where the risk of attack and the concordant damage are high. They provide useful advice for managing security in specific industry sectors, and they advocate maintaining high security standards through peer pressure or market competition whenever possible.

Another excellent source for industrial control systems managers was released in 2009 by the Department of Homeland Security [8]. In "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies", the authors provide a comprehensive explanation of technical security vulnerabilities along with strategies to mitigate or eliminate them. It also includes a brief coverage of management techniques and operational security controls.

Technical	**Operational**
Access Control	Awareness and Training
Audit and Accountability	Configuration Management
Identification and Authentication	Contingency Planning
System and Communications Protection	Incident Response
Management	Maintenance
Security Assessment and Authorization	Media Protection
Planning	Physical and Environmental Protection
Risk Assessment	Personnel Security
System and Services Acquisition	System and Information Integrity
Program Management	

Table 1. The NIST Security Controls

In January of 2009, the Department of Homeland Security also released the latest version of its National Infrastructure Protection Plan (NIPP), which aims to unify critical infrastructure and key resources (CIKR) security concepts [8]. The NIPP is written for a wide audience, including government personnel, CIKR owners, and academia. As such, it provides a broad understanding of the vulnerabilities and repercussions of successful attacks against CIKR.

3 Risk Assessment

Risk management is the process of finding the best among many alternatives in order to minimize the impact of uncertain events [5]. It may also be considered as an assessment process used to determine the controls that are needed to adequately and cost effectively protect critical assets. The five main factors involved in the process are:

- value of assets to be protected;
- threats to these assets;
- vulnerabilities of these assets;
- types of losses that these threats would inflict; and
- controls that will mitigate these threats.

For general risk assessment, the ASIS International Guidelines Commission recommended the following general security risk assessment steps [1]:

1. Understanding of the organization, its people and assets at risk;
2. Specifying risks and vulnerabilities;
3. Establishing the probability of risks and frequency of events;
4. Determining impacts;
5. Developing mitigation;
6. Considering the options; and
7. Performing cost and benefit analysis.

Advances in probabilistic risk assessment that can be applied to estimate the risk from SCADA and DCS installations are described in [20]. Also, in the same paper, the authors provided a comparison of approaches to quantifying the risk, threat impact and cyber-security on SCADA and DCS networks.

Previous work on risk assessment studies specifically for the SCADA systems are found in [6], and [10].

3.1 Risk Assessment Tools

The Carnegie Mellon University's CERT Coordination Center developed the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [2], which is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning. It uses the event/fault tree model to analyze threats to critical assets.

A freely available model-driven risk analysis tool, Cost of Risk Analysis System (CORAS), is available for download at http://coras.sourceforge.net/. A guided tour of the CORAS method can be located at the website and at the CORAS book [13]. The CORAS tool is a computerized implementation tool which is designed to support documenting, maintaining and reporting the analysis resulting from the CORAS risk modeling.

Risk Watch for Critical Infrastructure **(**Nuclear Power compliant) is a commercial product that provides compliance and risk assessments for critical infrastructure entities, more specifically the nuclear power sector. It is based on the new Nuclear Energy Institute guidelines contained in the NEI 04-04 Revision 1: "Cyber Security Program for Nuclear Power Reactors". Both the Nuclear Regulatory Commission and the Nuclear Energy Institute participated in the development of this software, which was funded by the U.S. Department of Defense through the Technical Support Working Group [21].

3.2 Risk Models and Methodologies

Perhaps, one of the earliest quantitative risk assessment methodologies uses the Annualized Loss Expectancy (ALE) model. The ALE is calculated by multiplying the Single Loss Expectancy (SLE) by the Annualized Rate of Occurrence (ARO), the expected frequency of the event.

The eight-stage security risk assessment model proposed by Drake and Morse [9] includes the following stages: 1) threat obstruction; 2) threat occurrence; 3) detection threat occurrence; 4) recovery from threat occurrence; 5) security breach; 6) detection of breach; 7) damage elimination; and 8) identifying external losses. The external losses include mission failure, personnel loss, loss of resources, revenue loss, and time loss.

The Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM) [11], developed by the UK Security Service, is based on the matrix method to assess risk based on data gathered from questionnaires. It consists of three stages: 1) Asset identification; 2) Vulnerability identification; and 3) Counter-measure installation.

The Quantitative Threat-Risk Index Model (QTRIM) [3] is used to predict the risk of a terrorist attack against a national infrastructure. It is built and tested at the Idaho National Engineering and Environmental Laboratory (INEEL) and calculates risk using terrorist specific constraints, objectives, value systems, logistics, and opportunities on a balance scorecard framework.

The Fault Tree Analysis (FTA) [25] method uses a deductive, failure-based approach. While the leaf node represents the triggering event, the root node represents an unwanted event, or failure, and the different events that may lead to the top event are modeled as branches of nodes.

Attack trees [22] provide a formal way of describing the security of a system by using the FTA model and replacing the fault as the attack goal and event probabilities for failure rates. The capability of attack trees to represent a highly comprehensive attack sequences are highly dependent on the experience of the security analysts that build them [14].

McQueen, et al, [15] developed quantitative techniques to calculate risk reduction estimates for a small SCADA control system. Directed graph structures, wherein nodes represent stages of a potential attack and edges represent the expected time-to-compromise for different attacker skill levels, are used as framework model.

4 The CORAS Framework

The CORAS framework is made up of a methodology for model-based risk assessment, a Unified Modeling Language (UML) based specification language, a library of reusable packages, an integrated platform for data repository, and a risk assessment reporting system.

The following objectives of the CORAS project [13] are:

- To develop a practical framework for risk analysis;
- To assess the applicability, usability, and efficiency of the framework; and
- To investigate its commercial viability.

The CORAS platform is an open-source and data-portable tool for risk assessment. It was developed in 2002 by a consortium of partners from four European countries.

The CORAS method is divided into two major groups of procedures. The first group establishes a common understanding of the target for analysis as well the documentation of assumptions and constraints needed for the subsequent risk analysis. The second group is focused on the actual risk analysis [13].

We opted to use this tool primarily because it is open-source, system independent and very user friendly for rapid risk model development.

5 Risk Modeling of an Industrial Control System

In this paper, we assume that the initial steps of initial discussions on the target, preparatory analysis, and documentations of the CORAS method have been completed. We start with asset identification.

5.1 Assets

We identify and classify each asset with a corresponding degree of importance (1=most important and 5=least important). Table 2 depicts a partial list of assets using the management view of business objectives.

Asset	*Importance*	*Type*
Safe Operation	2	Direct
Regulatory Compliant	3	Direct
Company Reputation	2	Indirect
Customer Service	4	Direct
Company Information	5	Direct
Profitability	1	Indirect

Table 2. Asset Table

5.2 Threats

Next, in Table 3 we list the threats and possible scenarios that may affect the identified assets.

Threat	*Scenario/Incident*
Employee	Intended/unintended service disruption
System Failure	Power outage
Network Failure	Denial of Service
Hacker	Intrusion or Service Disruption
Malware	Disruption
Eavesdropper	Listening on communication channels
Natural disaster	Tornado, flood, earthquake

Table 3. Threat Table

5.3 Vulnerabilities

Vulnerabilities are security weaknesses that could be exploited or inadvertently triggered. Table 4 depicts some of the control system vulnerabilities.

Area	*Vulnerability*
System	Misconfiguration, Missing anti-virus software, Outdate patch, Weak authentication, Web server flaws, Database system flaws.
Network	Firewall misconfiguration, rogue access points, unrestricted personal device access, weak authentication.
Physical	Unlocked facilities, weak entry authentication, Record access unrestricted
Employee	No training, undisciplined web access, unrestricted system access, social engineering
Information	Unrestricted access, unencrypted transmission, lack of data duplication policy, improper media disposal.

Table 4. Vulnerability Table

5.4 CORAS Snapshots

The symbols used in the CORAS framework include an accidental human threat (e.g. an untrained technical staff), a deliberate human threat (e.g. a hacker), a vulnerability (e.g. an unpatched system), a direct asset (e.g. company information), an indirect asset (e.g. the company reputation), a non-human threat (e.g. natural phenomenon), an unwanted incident (e.g. disclosure of company secrets), and a threat scenario (e.g. a rogue access point connected to the company network). The symbols are shown in Figure 1.

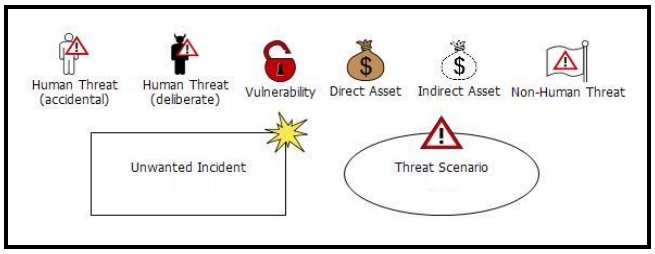

Figure 1. CORAS Symbols [13]

Initial threat diagrams are developed during a brainstorming session participated by stakeholders, security professionals, and risk modelers. Preliminary threat diagrams are developed during the initial stage of the brain storming sessions. A sample initial threat diagram is shown in Figure 2. In this preliminary threat diagram two non-human threats are modeled with respective vulnerabilities. This causes a threat scenario in which the system becomes inaccessible and thereby causing an unwanted incident (service disruption). Finally, the service disruption event is triggered and thereby affecting safe operation, a direct asset of the industrial control system.

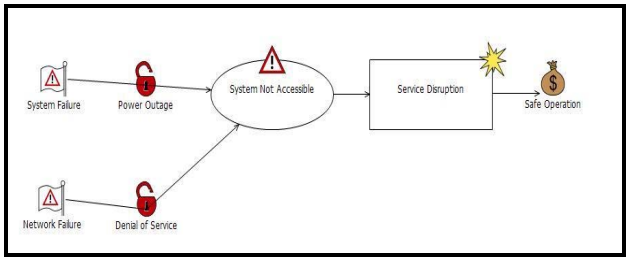

Figure 2. Non-Human Threat Diagram

An example of one of our final threat diagrams is depicted in Figure 3. In this final threat diagram we looked at three different actors, ICS Technician, Hacker and an Eavesdropper.

The ICS Technician introduced various vulnerabilities into the ICS system. These vulnerabilities are then exploited by the hacker or eavesdropper to gain access to the ICS system or compromise the confidentiality of the system. In this scenario, the ICS technician receives no training which leads to a misconfiguration of the ICS system and also the introduction of a rogue access point in the ICS network. Another vulnerability associated with the ICS technician is giving the technician unrestricted system access. In this scenario a hacker can attack the ICS system by means of social engineering, where the hacker tricks the ICS technician into releasing information, or discovering the rogue access point and using that to gain access to the network.

The hacker can compromise access to the ICS system which leads to an ICS system disruption. The diagram shows that a disruption in service affects two direct assets: customer service and safe operation as well as two indirect assets: profitability and company reputation. Another route the hacker can take is to compromise the commands issued to the ICS system which leads to compromise the ICS's data integrity. This affects the direct assets: safe operation, company information, and regulatory compliance as well as the indirect assets: profitability and company reputation. The hacker may also pose a threat to the ICS system by using the rogue access point introduced by the ICS technician. The hacker bypasses the network authentication and is able to access the network which, in effect, affecting the direct assets: safe operation and customer service as well as the indirect assets: profitability and company reputation.

The eavesdropper will use the rogue access point to access the network. The ICS system has the vulnerability of unencrypted transmissions so the eavesdropper can compromise the confidentiality of the ICS system resulting in the loss of company information. This diagram shows the various vulnerabilities in the ICS system, how these vulnerabilities can lead to threats, and finally how deliberate actions by humans can lead to these vulnerabilities being exploited resulting in damage to the direct and indirect assets of the company.

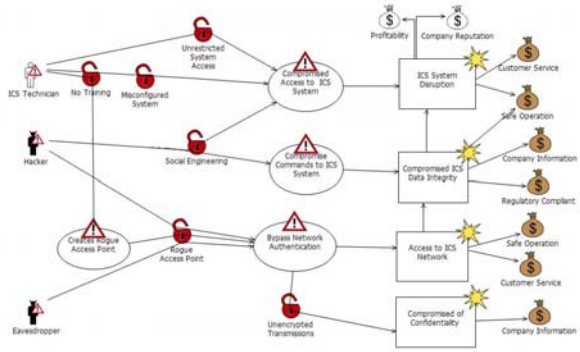

Figure 3. Final Threat Diagram

6 Conclusions and Future Plans

This paper presented a review of security best practices and risk assessment of SCADA and ICS systems. We also presented our research findings on an on-going risk modeling of a prototypical industrial control system using the CORAS framework tool

The challenge for the authors will be in the continual development of the SCADA and ICS system risk model. Future plans include:

- Development of a risk simulation model that mimics the actual risks endemic to SCADA and ICS systems; and
- Expansion of the current risk model to include parameters representing additional assets, risks, and vulnerabilities.

7 Acknowledgements

This paper is based upon a project partly supported by the National Science Foundation under grant awards DUE-0726486 and OCI-0959687. Opinions expressed are those of the authors and not necessarily of the Foundation.

8 References

[1] ASIS International. 2004. General Security Risk Assessment Guidelines. www.tisp.org/index.cfm?pk=download&id=10948&pid=10261

[2] Alberts, Christopher and Dorofee, Audrey. 2003. Managing Information Security Risks: The OCTAVE (SM) Approach. Addison-Wesley Professional Publishing. 2003.

[3] Beitel, G.A., Gertman, D. I., and Plum, M.M. 2004. Balanced Scorecard Method for Predicting the Probability of a Terrorist Attack. Risk Analysis IV:581-592, WIT Press, Brebbia, C.A., ed..

[4] Center for the Protection of National Infrastructure. 2010. Configuring and Managing Remote Access for Industrial Control Systems. http://www.us-cert.gov/control_systems/pdf/Recommended_Practice-Remote_Access_1-6-2011.pdf

[5] Cardenas, A., Amin, S., Lin, Z., Huang, Y., Huang, C., and Sastry, S. Attacks Against Process Control Systems: Risk Assessment, Detection, and Response. In Proceeding of the ASIACCS'11 Conference, (March, 2011). ACM, DOI 978-1-4503-0564-8-8/11/03.

[6] Craig,P., Mortensen, J., and Dagle. J.E. 2008. Metrics for the National SCADA Test Bed Program. Technical Report. PNNL-18031, Pacific Northwest National Laboratory (PNNL), Richland, WA.

[7] Department of Homeland Security. 2009. National Infrastructure Protection Plan http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[8] Department of Homeland Security. 2009 Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf.

[9] Drake, D.L. and Morse, K.L. 1994. The Security-specific Eight Stage Risk Assessment Methodology. In Proceedings of the 17th National Computer Security Conference (San Diego, CA).

[10] Hamoud, G., Chen, R.L., and Bradley, I. 2003. Risk assessment of power systems SCADA. In IEEE Power Engineering Society General Meeting, 2003, volume 2.

[11] Jones, Andy, and Ashenden, Debi. 2005. Risk Management for Computer Security: Protecting Your Network and Information Assets. Butterworth-Heinemann, UK.

[12] Katze, S., Stouffer, K., Abrams, M., Norton, D., and Weiss, J. 2006. Applying NIST SP 800-53 to Industrial Control Systems, NIST 2006. http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/Apply-SP-800-53-ICS-final-22Aug06.pdf.

[13] Lund, M. S., Solhaug, B. and Stolen K. Model-Driven Risk Analysis. 2011. The CORAS Approach. Springer-Verlag Berlin Heidelberg .

[14] McQueen, M., Boyer, W., Flynn, M., Alessi, S. Quantitative Risk Reduction Estimation Tool for Control Systems, Suggested Approach and Research Needs. Idaho National Laboratory. International Workshop On Complex Network and Infrastructure Protection (2006A).

[15] McQueen, M., Boyer, W., Flynn, M., Beitek, G. Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System, In Proceedings of the 39th Hawaii International Conference on System Science, Kauai, Hawaii. (2006B).

[16] National Infrastructure Advisory Council. 2004. Best Practices for Government to Enhance the Security of National Critical Infrastructures. http://www.dhs.gov/xlibrary/assets/niac/NIAC_BestPracticesSecurityInfrastructures_0404.pdf.

[17] National Institute of Standards and Technology (NIST), SP 800-53, "Guide to Industrial Control Systems (ICS) Security," Website: http://csrc.nist.gov/publications/nistpubs/800-53-

Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[18] National Institute of Standards and Technology (NIST), SP 800-82, "Guide to Industrial Control Systems (ICS) Security," Website: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, September 2008.

[19] President's Critical Infrastructure Protection Board. 2002. 21 Steps to Improve Cyber Security of SCADA Networks. http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf.

[20] Ralston, P.,Graham, J., and Hieb, J. 2007. Cyber security risk assessment for SCADA and DCS networks. ISA Transactions, 46(4), 583–594.

[21] Risk Watch for NEI. Website: http://www.riskwatch.com/index.php/nei-compliance. Last access: March 06, 2012.

[22] Schneier, Bruce. 1999. Attack trees: Modeling security threats. Dr. Dobb's Journal of Software Tools, 24(12), 21-29.

[23] Stølen, Ketin. 2001. CORAS-A Framework for Risk Analysis of Security Critical Systems. In supplement of the 2001 International Conference on Dependable Systems and Networks, pages D4 - D11, July 2-4, 2001, Gothenburg, Sweden.

[24] Stouffer, K., Falco, J., Scarfone, K. 2006. Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security: Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology (2006). http://www.cyber.st.dhs.gov/docs/NIST%20Guide%20to%20Supervisory%20and%20Data%20Acquisition-SCADA%20and%20Industrial%20Control%20Systems%20Security%20(2007).pdf.

[25] Vesely W. Fault Tree Analysis (FTA): Concepts and Applications. Website: http://www.hq.nasa.gov/office/codeq/risk/docs/ftacourse.pdf. Access date: March 05, 2012.