SANDIA REPORT
SAND2018 - 7592
Unlimited Release
Printed July, 2018

Industrial Control Systems Cyber Security Risk Candidate Methods Analysis

Armida Carbajal, Christopher Lamb, Lon Dawson

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

SAND2018-7592
Printed July 2018
Unlimited Release

Industrial Control Systems Cyber Security Risk Candidate Methods Analysis

Armida Carbajal, Christopher Lamb, Lon Dawson
Risk and Reliability Analysis
Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-MS0748

Abstract

In recognition of their mission and in response to continuously evolving cyber threats against nuclear facilities, Department of Energy – Nuclear Energy (DOE-NE) is building the Nuclear Energy Cyber security Research, Development, and Demonstration (RD&D) Program, which includes a cyber risk management thrust. This report supports the cyber risk management thrust objective which is to deliver "Standardized methodologies for credible risk-based identification, evaluation and prioritization of digital components." In a previous task, the Sandia National Laboratories (SNL) team presented evaluation criteria and a survey to review methods to determine the most suitable techniques [1]. In this task we will identify and evaluate a series of candidate methodologies.

In this report, 10 distinct methodologies are evaluated. The overall goal of this effort was to identify the current range of risk analysis techniques that were currently available, and how they could be applied, with an focus on industrial control systems (ICS). Overall, most of the techniques identified did fall into accepted risk analysis practices, though they generally addressed only one step of the multi-step risk management process. A few addressed multiple steps, but generally their treatment was superficial.

This study revealed that the current state of security risk analysis in digital control systems was not comprehensive and did not support a science-based evaluation. The papers surveyed did use mathematical formulation to describe the addressed problems, and tied the models to some kind of experimental or experiential evidence as support. Most of the papers, however, did not use a rigorous approach to experimentally support the proposed models, nor did they have enough evidence supporting the efficacy of the models to statistically analyze model impact. Both of these issues stem from the difficulty and expense associated with collecting experimental data in this domain.

TABLE OF CONTENTS

FIGURES

TABLES

NOMENCLATURE

Abbreviation	Definition
ARO	Annual Rate of Occurrence
API	Application Programming Interface
CPE	Common Platform Enumeration
CVE	Common Vulnerability and Exposure
CVSS	Common Vulnerability Scoring System
DCS	Distributed Control System
DNS	Domain Name System
ES	Exploitability Score
ICAT	Internet Catalog (a previous NIST project, replaced by NVD)
ICS	Industrial Control System
IP	Internet Protocol
IS	Impact Score
ISMS	Information Security Management System
IT	Information Technology
LAN	Local Area Network
MTU	Master Terminal Unit
NVD	National Vulnerability Database
ROSI	Return on Security Investment
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SME	Subject Matter Expert
RD&D	Research, Development, and Demonstration

1. INTRODUCTION

1.1. Background

Cyber-attacks are increasing in frequency, sophistication and breadth of targets. Control systems have been successfully targeted [2] and have become increasingly vulnerable as analog and/or unconnected systems are replaced by modern digital systems. Historically, control systems were designed to provide a control function, and the user was more interested in function availability than system security. As industry began to use more digital assets, processes were incorporated with the end goal to reduce the response and repair time. Problem solving became easier, as many solutions no longer required an operator to physically visit the asset location. The physical proximity from which information can be obtained and resultant corrective action taken allows many issues to be resolved without travel, for example: from the company control room, remotely at the operator's desk, or from the operator's home via an smartphone app. No one imagined that these simplified solutions would result in enabling increased access for malicious threat actors.

Given this context of important, complex industrial control systems coming under evolving and sophisticated cyber-attack, cyber-risk management methods are needed for assessing the cyber security posture and improving defense. This research develops and proposes a methodology for assisting industry in selecting or evaluating competing methods or models to assess or improve the cyber security risk posture in an industrial facility.

1.2. Emerging Cyber Threat Risk

Sophisticated attacks on critical infrastructure facilities are increasingly well-executed, well-engineered, and well-funded. The first attack, on Iranian nuclear production facilities, was discovered in 2010 and reverse engineered by Kaspersky and Symantec [3] [4]. Since then, there have been attacks on energy infrastructure in the US [5], the Ukraine [6] [7], and other targets [8] [9]. The level of activity over the last five years shows that these kinds of targets are of strong interest to malware developers.

1.3. Metrics and Methods

To evaluate the efficacy of cyber security features in a design or controls in an operational system, a way to measure the effectiveness of those features or controls is needed. Work has been ongoing in this field over the past decade in a variety of contexts. To evaluate the security posture of a given system, one of these methods, or some as-of-yet undiscovered method, needs to be used to determine overall security strength. These kinds of measures are also needed to determine if the security posture of a system is improved via a proposed change or security control.

In many cases today, the inputs for cyber-risk models are not based on quantitative data, but rather on subject matter expertise (SME) and evaluation. This leads to situations in which a model will produce different output from very similar input—when the only difference is the inclusion of a new expert. This variability makes evaluating risks difficult to reproduce, and more challenging to evaluate. Likewise, more quantitative model inputs can also provide a false feeling of rigor. Common quantitative inputs to risk models involve the Common Vulnerability Scoring System (CVSS) [(CVSS Special Interest Group, 2018)] data, for example, with no experimental evidence that the CVSS data accurately reflects real system risk.

Establishing repeatable, end-to-end verifiable, and experimentally validated risk measures and models with respect to cyber-risk evaluation is vital to prioritizing system defense and verifying secure system designs.

2. REVIEW CRITERIA AND METHODOLOGY

This effort seeks to both understand and inform the state-of-the-art for control system cyber-risk management. The effort started with a literature survey of existing, well-known related references. The team found many potential methods, with varying degrees of development. Compounding the complexity, the various papers were incomplete or inconsistent in the definition of cyber-risk management steps. As the team began to organize its findings, this variability caused the evaluation of competing techniques to become difficult and cumbersome—it became necessary to adopt standard step definitions and define relevant criteria. Figure 2-1 shows the step definitions adopted from traditional risk management guidance [10]. These same step definitions are used to organize the analysis.

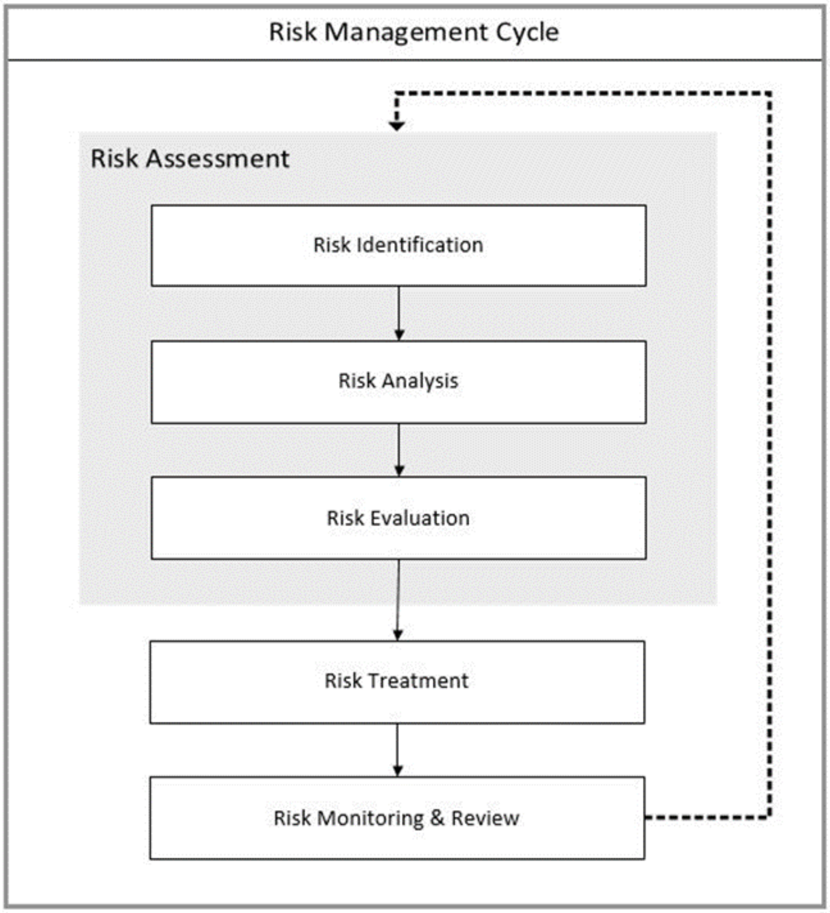

Figure 2-1. Risk Management Model[1]

[1] Figure 2-1 adapted from ISO/IEC 27005, Cherdantseva et al. (2016), AlencarRigon, et al. (2014), Kriaa et al. (2015), Toosarvandani et al (2012)

2.1. Evaluation Methods and Criteria

A detailed overview of the evaluation methods and criteria is the subject of a previous SAND report [1]. In summary, the review evaluated each methodology for the following criteria:

1. **Steps of Cyber-Risk Assessment & Cyber-Risk Management**. Preference is given to complete methods—ones that address all steps of the risk assessment & management cycle. However, there is value in methodologies that robustly address individual steps of risk and this analysis will seek to identify which steps candidate methods adequately cover.

2. **Utility**. Utility of the candidate method considers the specifics of where the method could be used. For example, if a method could be used in multiple domains, it was considered to be of higher utility.

    a. **Level of Implementation**. This component of the *utility* criterion scores the extent of implementation of the candidate method.

    b. **Scalability.** The ability to change in size or scale; as well as flexibility of usage and application.

    c. **Automation**. Methods supported by tools or that yield an automated process.

3. **Measurability.** Quantitative versus Qualitative results with preference given to quantitative techniques that offer a continuous metric (i.e., a probability, unlike High, Medium, Low qualitative categorical scales) for risk analysis to systems. Rank-order and categorical scales used in methods that provide valid and reliable results will be considered equally as preferential as interval or ratio scales of measurement.

4. **Reproducibility**. This criterion is a measure of precision for the ability of the candidate method's tools, metrics, techniques, etc. to provide the same measurement or output, consistently across iterations. The technique must not be operator or user dependent and the result should not vary depending on the expertise level of the user. Preference was given to methods that have minimal reliance on expert judgement.

5. **Validity**. This criterion is a measure of verifiable accuracy of the method's results. Preference was given to methods that can be or have been independently validated.

3. ANALYSIS OF CANDIDATE METHODS

Ten papers are included for this application, Table 3-1. This particular set of candidate methodologies were selected because of their emphasis on using a quantitative approach to their process. Five of the articles were selected based on the findings in Cherdantseva et al [11].

Table 3-1. Summary of Criterion for the Reviewed References

Reference	Utility	Ease of Implementation [1-5]	Risk Identification	Risk Analysis	Risk Evaluation	Risk Treatment	Risk Monitoring
Genge, B., Graur, F., & Enachescu, C. (2015)	Broadly Applicable	2	Yes	x*	-	-	-
McQueen et al. (2006)	Broadly Applicable	2	x*	Yes	x*	-	-
Ten, C., Govindarasu, M. & Liu, C. (2010)	Specific	2	x*	x*	Yes	x*	x*
Huang et al. (2015	Specific	2	-	Yes	-	-	-
Gallon, L., & Bascou, J. J. (2011)	Specific	2	-	Yes	-	-	-
Cohen, F. (1998)	Specific	2	-	Yes	-	-	-
Patel, S., Graham, J.H., & Ralston, P.A.S. (2008)	Broadly Applicable	2	-	x*	Yes	x*	-
Teixeira, A., Sou, K.C., Sandberg, H. & Johansson, K.H. (2015).	Broadly Applicable	2	-	x*	x*	x*	Yes
Patel, S. & Zaver J. (2010)	Broadly Applicable	3	-	-	Yes	-	-
Markovic-Petrovic & Stojanovic, (2014)	Broadly Applicable	1	-	-	Yes	-	-

**This step includes a reference or generalized technique however; the methodology for its use in the paper is not well developed.*

Even though there exists commonly referenced guidance for cyber-risk management, there is inconsistent usage of the terminology, resulting in unreliable summaries and findings. Although there are relevant guides, they are not prescriptive in standardization of methods or of terms. As a result, there was a lot of inter-rater variability in the categorization of the papers reviewed in the Cherdantseva et al article [11].

The factor of inter-rater variation was mentioned as one of the limitations in their methodology for reviewing the articles. However, it can be assumed that an analysis of inter-rater variation would have resulted with the discovery of inconsistent usage of terminology not only in the guidance documentation but also between other publications. This problem exists systemically in all areas that use the varying sets of guides, methods, and terminology for their applications.

This became the motivation behind using criterion for improving how information is evaluated for further usage. For this reason, the papers were still effective samples for evaluation using the questionnaire developed for this process. A summary of advantages and disadvantages of each of these methods is included, in addition to highlights of the technical details of the methods with respect to this application.

Most of these proposed methodologies only focused on one step from the risk assessment/management cycle shown in Figure 3-1. Whenever a methodology included multiple steps, the steps were typically embedded within another step of coverage, or as a minor subject reference. In situations when the multiple steps were addressed, it was done relatively superficially.

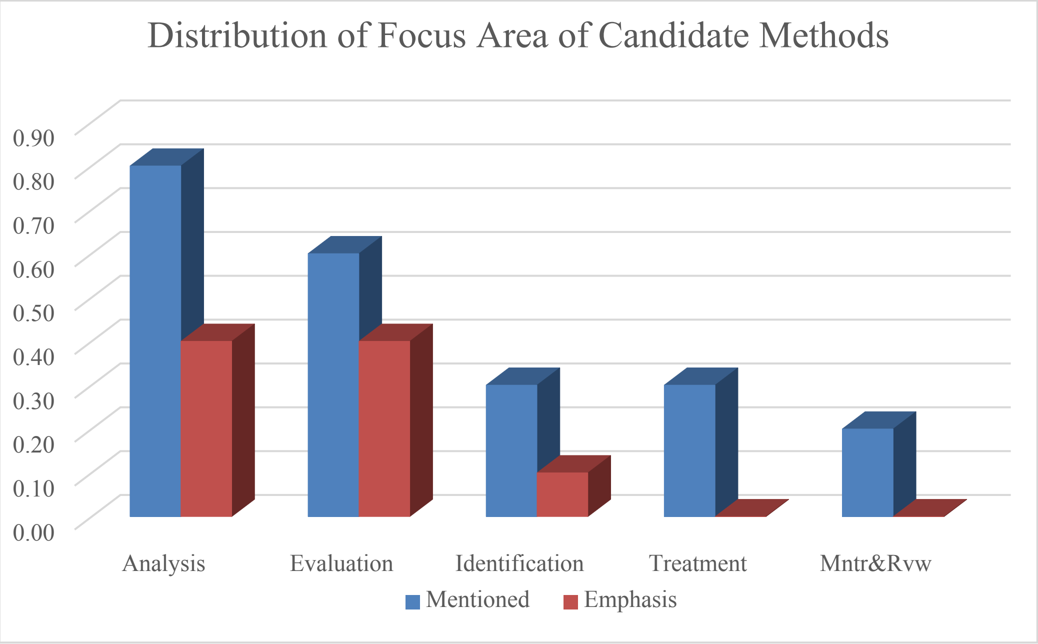

Figure 3-1. Distribution of Focus Area of Candidate Methods
Note: The blue series-labeled as “Mentioned” displays the fraction of candidate methods that mentioned or briefly discussed the Risk Management Step in their methodology. In orange, the series label as “Emphasis,” is the area in which a candidate method went into great detail and was the emphasis of their methodology. Some steps are not emphasized in any of the candidate methods, but instead just discussed briefly.

3.1. Emphasis on Risk Identification

Risk identification of targets of interest is one of the main challenges in the risk management cycle. The step of defining and characterizing the assets in an ICS is very challenging. Also, in an established ICS, system availability is crucial, so using scanning and probing techniques as well as conducting regular security updates is not always feasible as they may interrupt critical functions of the devices. As a result, discovering these systems within networks alone would place a challenge on the energy industry.

The following two papers propose potential techniques for network asset discovery and vulnerability identification. One non-intrusive technique uses the Shodan application programming interface (API) to conduct the asset discovery [12]. The identified assets are automatically screened using the National Vulnerability Database (NVD) for existing vulnerabilities, producing automated CVSS scoring for systems and devices. These authors combine the three steps of risk assessment (identification, analysis and evaluation) within one tool.

The second approach [13] uses the signals from an infrastructure reporting system combined with information received from control and monitoring systems to infer a network mapping. The resulting system was evaluated for a security control method (implementation of a strong password) which resulted in a 84% improvement in intrusion defense.

3.1.1. *Non-Intrusive Techniques for Vulnerability Assessment Services in Distributed Systems (Genge & Enachescu, 2015)*

In this paper, the authors propose using the Shodan search engine in combination with NVD to conduct a non-intrusive vulnerability assessment of internet-facing services. Identifying the targets of interest in order to identify risks and vulnerabilities is very challenging in ICS. Without identifying the targets of interest, vulnerabilities cannot be identified, nor can threats be characterized. The concept of physically conducting a walk-through in order to inventory the number of systems that could potentially be vulnerable to cyber-attacks is daunting and unrealistic. The manual processes required to review documentation quickly becomes a labor intensive task in asset identification.

Genge et al. [12] shows that this can be done via automated means, and in ways that do not require the physical and manual inventory of these systems and their documentation. Instead, Shodan is used to assist in gathering the system information needed to conduct a vulnerability assessment.

The combination of Shodan and the NVD result in automatic vulnerability metrics for systems that would otherwise be difficult to scan, probe, or penetrate. The authors combined information from several sources, but their technique assumes access to internal network traffic, Domain Name System (DNS) queries, and additional information about the systems in order to complete the network topology.

The network asset discovery process uses the Shodan API to acquire target information with a specified IP address range [14]. Once the device information is obtained, then the NVD is queried to conduct a vulnerability assessment automatically. Finally, it generates a report automatically which provides a summary for the discovered services, vulnerabilities and metrics including the Common Vulnerability and Exposure (CVE) scores using the CVSS included for each CVE entry. Their technique enhances the information that Shodan gathers by having an automated process to match the Common Platform Enumeration (CPE) name reconstructed to match it to the correct CVE entry. Furthermore, they provide a generous amount of details, including pseudo-code to replicate the process.

The availability and usage of these resources is not uncommon to penetration testers and adversaries interested in conducting reconnaissance on a target device. Combining the two available resources with their vulnerability assessment tool allows for passive vulnerability assessment.

This is done without compromising the devices with port scanning, which can disrupt device service. The NVD developers of the CVSS scoring system state that the CVSS is not intended to be used as vulnerability database or for overall risk management. The information gathered by this process is highly dependent on the set of vulnerabilities that are available at the time of the query. Nonetheless, the CVSS does provide a framework for communicating characteristics and impacts of IT vulnerabilities.

The authors state [12] that coupling additional resources like event logs from hosts, network traffic analysis, and network topology mapping can greatly improve the information obtained from the vulnerability assessment.

3.1.2. *Cyber Security for Critical Infrastructures: Attack and Defense Modeling (Ten, 2010)*

This methodology was based on a test platform at Iowa State University emulating an electric power plant. The problem space is based exclusively on techniques for assessing access points of a power system control network. This included a primary control center, backup control center, substations or process control networks, the power plant control and monitoring features of the network, and Web-based Supervisory Control and Data Acquisition (SCADA) which includes both remote access by plant operators or third-party vendors.

In this paper, the authors emphasize the importance of identifying system components and using the Energy Management System (EMS), the network used by the facility, to access system information. The authors also introduced the concept of conditional connectivity to consider assets that are not on the network, but are occasionally connected to either a network, vendor laptop, or other peripheral for maintenance, updates, or data capture.

This method provides a technique for determining a probability-like value of an attack by proposing a calculation of leaf vulnerability where

$v(G) = x \cdot max < v_{\alpha}, v_{\beta} >$

$where\ v_{\alpha}$, is port audit results andv_{β} is password strength, given that x is identified first. Then the product of the group of leaves that make up a group that represents an attack scenario produces the value of the system vulnerability.

Ten et al., (2010), created a Vulnerability Index based on three conditions (Ci), for i=[1,3].

Table 3-2. Rules for Conditions 1, 2, and 3

C1	system is free of intrusion attempts | electronic evidence
C2	1 or more countermeasures to protect an attack leaf is in place
C3	at least 1 or more password policies are enforced corresponding to each attack leaf

The vulnerability analysis is based on the product of the Vulnerability Index ***X***, and the maximum value between the port and password vulnerability. ***X*** is obtained using the following criteria.

Table 3-3. Value of X given Conditions

X	**Conditions to Calculate System Vulnerability**
.33	*if C1 and C2 and C3 are satisfied*
.67	*if C1 and C2 OR C1 and C3 OR C2 and C3, in other words any 2 conditions are satisfied*
1	*if C1 OR C2 OR C3 OR None of the conditions are met*

A unique application is the concept of using EMS information to collect electronic evidence of intrusions or attacks using anomaly detection. The second is the use of real-time monitoring by port scanning to audit the strength of passwords. Changing the password from the default to something else is a minimal treatment. However, the results they obtained from their analysis displayed at least a 50% reduction in system vulnerability just by strengthening passwords alone.

The focus was limited to port access and passwords on the system. However, it is not unheard of for plants to have the passwords set to defaults from the manufacturer, so this alone could be very useful. In fact, [15] found that it is a very common occurrence in SCADA systems. The approach included an algorithm to evaluate both of these conditions and supplies vulnerability indices.

The authors' risk treatment approach to reduce the vulnerability of these systems was to improve the password policy from the factory defaults to at least eight characters and four different character types. The authors did not provide a treatment for the two backdoors revealed in their port auditing process.

This paper is strong in risk concepts and mathematical relationships but specific to a system level interaction and treatment. The algorithm they developed for improving may not be generally applicable, and the understanding of a network architecture of a plant may not be an existing operator capability. However, this type of specific technique would be useful as a simplified first level of assessment approach that does not depend completely on expert opinion. The authors demonstrate that intrusion detection can be conducted through algorithms. Most distributed control system related papers reject this being a plausible option.

3.2. Emphasis on Risk Analysis

3.2.1. *Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System(McQueen, Boyer, Flynn, & Beitel, 2006)*

This paper proposes a risk assessment methodology based on a real-life case study and uses a quantitative approach. The proposed risk assessment methodology decomposes an attack in the form of reconnaissance, breach, penetrate, escalate, and damage, to categorize the path of a given exploit for a specific asset in a system.

The paper is based on the CS60 system, and is limited to a single system assessment. The method requires experts to understand the system configuration and to identify the possible vulnerabilities to create attack paths. The vulnerabilities are characterized according to CVE. If the vulnerability information was not available in CVE, then expert panels were used to feed the model.

This methodology uses some basis for threat level by adding variability based on the attacker's skill level instead of using a fixed value. They populate an attack graph by breaking down a cyber-attack using the cyber-kill-chain-like steps previously described. Although this is done, only a summary of this process is provided. Several formulas for calculating metrics to obtain results are provided as well. The methodology does have a quantitative component even though it requires SME input.

This methodology does not provide any true suggestions for assessing a plant, but instead, a unified process for an attack of a specific system or device in the network. One benefit was an estimate for what integrating a new security control will yield to potentially prevent, detect, or stop an attack.

3.2.2. *Difficulty-Level Metric for Cyber Security Training (Z Huang, 2015)*

This methodology addresses attack graphs, how they are built, how they could be analyzed, and how they can be scored. The key contribution of this methodology is the application of a Bayesian Network to propagate probabilities by converting cyclic attack graphs (i.e. multi-pathway to satisfy a node of a graph) to a directed acyclic attack graphs.

The application of their technique was based on training cyber analysts using adaptive learning modules. However, part of the definition for risk analysis included looking for techniques that quantify a probability of a cyber-attack or difficulty of a cyber-attack based on the current state of the target of interest. The authors needed to measure the knowledge gained based on performance of the analyst as well as the level of difficulty each attack graph presented to subjects in order to design an adaptive learning platform.

The techniques were valuable to the risk management cycle to protect SCADA and industrial control systems. Attack graphs are often used as a technique in vulnerability assessment by creating potential adversarial attack scenarios. Most methodologies seek to score the attack graphs, trees or paths in order to understand the vulnerabilities and in some cases also the improvements gained with protections that are implemented post-analysis.

This technique offers an approach to use Bayesian Networks by accounting for the constraints this technique has converting otherwise undirected attack graphs to directed graphs and supplying probabilities by simply dividing CVSS scores by 10 in order to define a probability between [0,1].

Furthermore, by using a Bayesian process, if the distribution of probabilities isn't normal, the sampling techniques can be fitted with prior distributions that better define the quantitative space that the spread of CVSS scores will create.

The Bayesian Network process is partially automated, that is once the attack graph scenario has been defined, a proposed set of automated steps are followed. The authors use of CVSS scores as probability values is a modification of this scoring technique that is widely used in the IT community.

3.2.3. *Using CVSS in Attack Graphs (Gallon & Bascou, 2011)*

Gallon enhanced CVSS scores to propagate metrics through Attack Graphs [16]. They defined the concept of host damage (*hd*), which represented the cumulative security damage of corresponding security impacts of all vulnerabilities exploited on the target host and the corresponding network. They did this by modifying the CVSS Impact calculation to:

$$hd_i = 10.41[1 - (1 - CD_i)(1 - ID_i)(1 - AD_i)]$$

$$\text{for } i = 1, \dots, k$$

Where k is the previous attack damage for the host relationship to the network and other terms retain standard CVSS definitions. This accounts for the cumulative security damage to other hosts on the network that trusted the target host. The score obtained from hd_i ranges from [0,10], preserving the original CVSS scaling.

They also proposed a network damage (*nd*) calculation to vary the usage of how an attack graph is summarized. The authors claim varying techniques reveal all the subtleties of a multistage attack. The main limitation, mentioned within the paper, is their current formulation does not consider the security policy of the network or the target host. The final CVSS score ranges from 0 -10.

The scoring techniques reviewed used, at some level, a portion of calculations or numerical values that could be perceived as qualitative, arbitrary, or otherwise categorical to obtain a probability-like value to insert into their risk, probability and impact calculations. The CVSS suffers from this limitation as well, see [17].

For example, the CVSS calculation includes a Base Score (BS) which is composed of an Exploitability Score (ES) and an Impact Score (IS). To calculate the IS, obtain a Confidentiality Impact, Integrity Impact, and Availability Impact score which they defined as summarized in Table 3-4:

Table 3-4. Impact Score Components and Their Designated Scores

	Confidentiality	Integrity	Availability
None	0	0	0
Partial	.275	.275	.275
Complete	.66	.66	.66

where none, partial, and complete are considered with respect to the loss or as a proportion of exposure or loss of trust based on adversarial action or system exposure. These values are then used in the following equation:

$$Impact = 10.41[1 - (1 - Impact_c)(1 - Impact_i)(1 - Impact_a)]$$

The values in the Impact Score Components table are identical for Confidentiality, Integrity, and Availability. The values used for these calculations may appear to be arbitrary, but are easy to use, comprehensive, and provide overall accurate results that have continued to be used through time.

3.2.4. *Simulating Cyber Attacks, Defenses, and Consequences (Cohen, 1997)*

The Cohen model was developed and designed for simulation and analysis of cyber-attacks by using a classification schemes and techniques to describe the process of an attack and develop cause and effect chains. Cohen, when describing the challenges of a quantitative technique, expressed that quantitative methods for risk assessment would be challenging to obtain and limited by the data that researchers are able to acquire. As a result, he expressed that cyber-risk assessment had historically been marked by a qualitative approach.

Cohen placed a considerable amount of research into this model. It is based on a set of 37 classes of threats, 94 classes of attack mechanisms, and about 140 classes of protective mechanisms. These are interlinked by a database that associates threats with attacks and attacks with applicable defenses.

In addition, the database associates these with other characteristics such as their impact on integrity, availability, access, and leakage; the sophistication level of the attackers; and their use in prevention, detection, and reaction.

They cross-reference data with 15,000 pieces of relational data. In addition to the preexisting data, they added 20,000 new pieces of data to provide metrics that would allow for the simulation to proceed in a meaningful manner. They also introduced the time required for each attack and each defense to operate and the effectiveness of each defense against each attack as well as how these factors were effected by attacker and defender skill levels. The work from Cohen is a pivotal in the area of cyber-risk assessment, as well as modeling cyber-attacks and defense techniques.

3.3. Emphasis on Risk Evaluation

This section include articles with descriptions of risk evaluation techniques.

3.3.1. *A Risk Assessment Model for Cyber-Attacks on Information Systems (Patel & Zaveri, 2010)*

This risk assessment model delivers a risk evaluation for a limited number of proposed cyber-attacks. It can be broadly applied to different industries to estimate financial damages from a limited set of ICS cyber-attacks. However, no insight is included regarding cyber vulnerabilities or potential defense mitigations. This work was conducted in a test-bed at the University of Louisiana modeling a chemical plant. There are many available publications using this testbed by multiple authors including Patel and Zaveri. The testbed was designed with actual SCADA software and hardware, although it is not an actual plant.

Patel and Zaveri did not specifically define a technique for identifying digital assets and their vulnerabilities. Although the paper includes a block diagram of the plant communication architecture, the focus is on MTU and RTU capability. Attacks are limited to a compact list of seven types of real-time (or active) attacks:

Table 3-5. Patel & Zaveri Attack Type Descriptions

Type of Attacks	Description
Replay	Capture a message and resend it at a later point one or more times
Spoofing	Pretend to be an MTU or RTU
Denial of Service	Send very large number of spurious messages so that RTU is unable to fulfill a valid request
Control message modification	Capture a request, modify some of its parameters and send it to RTU
Write to MTU	Add or modify files on MTU
RTU-response alteration	Capture a response, modify some of its parameters and send it to RTU
Write to RTU	Add or modify values on RTU

Other types of attacks are ignored. The attack probabilities are based on several papers that analyzed real-time or short-term loss attacks.

The only section that relied on expert opinion were the financial impacts used in damage calculations. The main result obtained from this model provides the financial impacts and consequences in terms of a dollar value as the method to inform decision makers of the cost to implement security measures in comparison to experiencing a loss due to a cyber-attack.

This work provides equations that can estimate the effects of an attack which results in financial loss. From a financial perspective, this risk evaluation model can be useful in presenting decision makers with a simple bottom-line fiscal value. Such a high-level approach could be used to evaluate equally high-level decisions.

3.3.2. *Quantitatively Assessing the Vulnerability of Critical Information Systems: A New Method for Evaluating Security Enhancements (Patel, Graham, & Ralston, 2008)*

This paper describes how to create a vulnerability assessment scoring system by constructing a vulnerability tree. The work is based on a University of Kentucky testbed, but does not explain, identify, or characterize the systems, components, and devices used. Patel, Graham, Ralston, & Tantalean [18] is referenced for additional network and system layout details. This model can be considered the exemplar of the Patel and Zaveri risk evaluation work.

The authors used a pre-determined system topology. No techniques were provided for risk identification, which included asset identification and vulnerability identification. The vulnerability assessment provided is based on a set of seven specific attacks, seen previously in Table 3-5*,* where the probability of each attack was taken from Cohen [19].

They then proposed two indices that range from 0 - 100:

- ***Threat Impact:*** A proposed value quantifying the impact of a cyber threat.
- ***Cyber-Vulnerability:*** The threat-impact index is equally divided among all the base events (attacks) at the same level.

The threat-impact values are taken from the last column of their damage analysis table. The total of all the threat-impact indices represents the threat-impact index for the entire information system, which is listed for the top event. A system without any implemented security has the threat-impact index of 100. After security enhancements are applied, this index should fall if the enhancement eliminates attacks.

Although it walks through the scoring processes that would be exercised in the steps of risk identification and risk analysis, the result is based on risk evaluation, which gives a scoring for the amount damage given a certain attack has occurred. This paper combines expert opinion to develop metrics and historical data to develop values. The authors list the use of operationally critical threat, asset, and vulnerability evaluation results for identifying and classifying assets. Next, they use ranking methodologies as a filter to prioritize the items in the system. They finally apply a Markov and semi-Markov process model to account for existing interdependencies that may not have been accounted for in the networked links.

The emphasis was intended to be the cyber vulnerability score obtained by producing a vulnerability tree. The authors display the current vs. improved state post application of the security enhancements found in Patel (2006) for the risk treatment step as a proposed treatment technique. Fully attempting to replicate this process would require a significant investment from experts in several areas, and automation may prove difficult.

3.3.3. *An Improved Risk Assessment Method for SCADA Information Security (Markovic-Petrovic & Stojanovic, 2014)*

This method was developed to help optimize the level of security investment and define different levels of acceptable risk. The proposed method provides an equation to assist with a quantitative semi-automated process for calculating risk in ICS, though the authors did not provide guidance to ease the implementation of this process.

Their quantitative model is reduced to a categorical model using three impact weights: W_A, the probability of an attack; W_E, the penalties for not delivering energy; and W_H, the losses created by excess hydro potential (the example is a hydroelectric plant). They inferred probabilities of detection from multiple sources for the following equation:

$$ALE = W_A W_E W_H P(t_A + W_A t_{Rmax}) c_e \times ARO$$

The remaining values in the formula are t_A, the duration of the attack; P, the time required for system recovery; c_e, the unit price of electric energy; and t_{Rmax}, a weighting factor with recovery time after a maximum strength attack. This result is then multiplied by the Annual Rate of Occurrence (ARO), which is not fully explained in the paper, but is correlated to a Return on Security Investment (ROSI*)* value.

The authors proposed using pre-existing research to model the system impact and extended consequences of the attack. The down-time of the system, the duration of the attack, and the company’s key performance indictors used to model the impact of the attack were all obtained from specific system-level research. These values were then used in updating the proposed equation. As an example, they show the different levels of impact depending on each level of their proposed weighting scale.

The authors also mention that the weights would have to be developed through a site-specific process, susceptible to subjectivity, and subjected to a lengthy risk assessment process.

This model may be applied to multiple ICS/SCADA facilities, with an emphasis on electric energy producing plants. This paper offers a conceptual risk framework that describes the main factors of consideration but it did not include specifics resulting in an implicit need for SMEs in order to obtain company-specific information. This may lead to a subjective analysis reducing the likelihood that the same result would be obtained for the identical company-specific information if a different set of SMEs performing a given analysis.

3.4. Emphasis on Risk Treatment

There were no candidate methods in the included sample set or additional resources in which risk treatment was the emphasis of their methodology. However, three papers did mention a technique that they recommended for the problem they were discussing. As an overview of the proposed techniques, in Ten et al. [13] the authors scanned network ports to check for authentication requirements. In most cases, the ports were not password protected or only required a default password or an easy-to-guess or acquire shared password. They modeled a risk treatment to increase the system security by implementing more stringent password controls.

The second paper uses channel encryption as their risk treatment technique and is discussed in Section 3.5.1.

3.5. Emphasis on Risk Monitoring & Review

3.5.1. *Secure Control Systems: A Quantitative Risk Management Approach (Teixeira, 2015)*

Teixiera et al. [20] emphasized that security at both the cyber and physical level is necessary for a complete system solution. While fail-safe failure conditions are in place for critical control systems, they may not protect from techniques executed with malicious intent. The authors prioritized threats using risk management methods to propose a design framework to protect these systems.

Their model was based on Confidentiality, Integrity, and Availability. However, they did not use a categorical variable delimiter as seen in other approaches [13] [16]. Instead, statistical techniques for anomaly detection were applied to measure state signal changes in the energy systems indicative of an attack or compromise.

The Teixiera et al. methodology focused on the foundation of risk monitoring, followed by risk treatment. They used everything the system could supply as a signal, from voltage phases, to DC power flow, to water levels in a quadruple tank process. They propose an optimization calculation that considers the limited resources available to a plant for protecting equipment. Teixiera et al. optimize to the minimum number of channels and devices requiring encryption in an attempt to obtain the maximum level of protection. Their max-impact/minimum-resources attack analysis, termed a Data Protection Strategy, considers both the adversary resources and the system impact and resources available or affected in the plant, yielding a maximum impact resources-constrained attack policy.

The risk treatment of choice in Teixiera et al. was focused on encryption. There are limitations to encryption in that it only protects during data transmission and not at communication endpoints. They proposed noise injection to develop different techniques to detect and protect encrypted traffic from cryptanalysis.

Teixiera et al. did an excellent job at proposing computationally efficient methods and mathematically sound techniques from an algorithmic approach to monitor and protect a large scale electric power network. They provided a complete layout of techniques to use various parts of the system information to run diverse types of security analysis on both static and dynamic models in multiple ways.

3.5.2. *Additional Resources*

The following candidate methods were considered but not used for the sample set. For the most part, these papers provided an overview of possible techniques but were not focused on risk analysis, or were significantly similar to other reviewed work.

Table 3-6. Additional Candidate Methods Reviewed

Candidate Method	Description OF Use for Analysis
Byres, 2004 [21]	An early account of tracking the occurrences of cyber-security risks with respect to industrial control systems.
Genge et al., 2016 [14]	Technical detail article on ShoVAT
Cohen, 1997 [19]	Cohen's perspective on Risk Management or Risk Analysis for network security strategies.
Sommestad, 2010 [15]	An interesting comparison of cyber-security standards.
Kesler, 2011 [2]	Overview of four cyber incidents important to nuclear facilities and critical infrastructure and the importance of regulations.
Kriaa, 2015 [22]	FAIR –The Open Group ISO/IEC 27005 Cook Book recommendation. As well as, review a different interpretation of the Risk Management Process.
Toosarvandani, 2012 [23]	Overview of ISMS Standards with respect to LAN Security
Alencar, 2014 [24]	Considered their interpretation in aligning our adaption of the risk management process with their nested approach.
Maynard, 2016 [25]	Explain the limitations of CVE and CVSS information not being useful in identifying future OR existing attacks, then model DUQU 2.0 using attack trees.
Woo, 2017 [26]	Similar to Ten, et al. (2010) in using the EMS to understand cyber threat via analysis of the power flow. The level of similarity did not warrant analyzing the two.
Lopez, 2013 [27]	A general overview of how to Use ISO 27001 and other guidance documentation.
Francia III, 2012 [28]	A General overview of guidance publications, (i.e. NIST, NERC, ISO, etc.) and using CORAS framework to categorize.
Taylor, 2002 [29]	A review of how to apply Probability Risk Assessment for the purposes of cyber-attacks in critical infrastructure.

4. CONCLUSIONS

The current state of security risk in digital control systems is an active area of research, though until recently it has been overshadowed by more common information technology systems. The surveyed papers span a period of 20 years, with the majority of the reviewed work produced in the last 10. Much of the work was produced in the United States, with a substantial number of foreign collaborators involved.

Overall, the digital control systems security risk evaluation area is in need of additional ideas and resources to help experimentally support proposed risk evaluation models. While all the evaluated models were internally consistent and logically sound based on presented preconditions and assumptions, they were uniformly supported by scant or weak experimental evidence. Many of the evaluation schemes still depended on SMEs as well, further eroding the reproducibility of findings.

The presented methods were all useful and provided insight into risk of a given system. Some attempted to evaluate risk based on known system flaws tied to internet-based system identification [14], while others attempted to explicitly evaluate the change in security based on incorporating new security controls [20].

The state of research into these kinds of methods could benefit from a common, validated, and accepted simulation platform. Few of the authors had access to platforms to allow them to run experiments over systems to validate proposed models, and even then they were unable to run enough experiments to show that the models did, in fact, evaluate *real* cyber risk via rigorous, controlled, structured, and reproducible experimentation. Those that did not explored other approaches to validate presented work. In order to build valid models of security risk, efforts should be made to establish accurate, low-cost ways to evaluate and prove the accuracy of those models, which the community, as of yet, has failed to do.

5. REFERENCES

[1] L. D. C. C. L. Armida Carbajal, "Proposed Process for Evaluating Candidate Methods for Control System Cyber Risk Management," Sandia National Laboratories, Albuquerque, NM, 2017.

[2] B. Kesler, "The vulnerability of nuclear facilities to cyber-attack," *Strategic Insights*, Spring 2011 Volume 10, Issue 1, 2011.

[3] D. Kushner, "The Real Story of Stuxnet," 26 February 2013. [Online]. Available: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. [Accessed 21 September 2017].

[4] N. Falliere, L. O Murchu and E. Chien, "W32.Stuxnet Dossier," Symantec.

[5] Symantec Security Response, "Dragonfly: Cyberespionage Attacks Against Energy Suppliers," Symantec, 2014.

[6] Dragos, "CrashOverride: Analysis of the Threat to Electric Grid Operations," Dragos, 2017.

[7] F-Secure, "Blackenergy & Quedagh: The Convergence of Crimeware and APT Attacks," F-Secure, 2014.

[8] CyberX Labs, "BlackEnergy 3 - Exfiltration of Data in ICS Networks," CyberX Labs, 2015.

[9] F-Secure, "News from the Lab," 23 June 2014. [Online]. Available: https://www.f-secure.com/weblog/archives/00002718.html. [Accessed 21 September 2017].

[10] ISO/IEC, "ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management," ISO/IEC, 2011 (Second Edition).

[11] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Computers & Security,* pp. 1-27, 2016.

[12] B. G. F. Genge and C. Enachescu, "Non-intrusive techniques for vulnerability assessment services in distributed systems," in *8th International Conference Interdisciplinarity in Engineering*, Tirgu-Mures, Romania, 2015.

[13] C.-W. Ten, "Cybersecurity for Critical Infrastructures:," *IEEE Transactions on Systems, Man, and Cybernetics--Part A: Systems and Humans,* vol. 40, no. 4, pp. 853-865, 2010.

[14] B. Genge and C. Enăchescu, "ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services," *Security and communication networks,* vol. 9, no. 15, pp. 2696-2714, 2016.

[15] G. N. E. a. J. N. T. Sommestad, "SCADA system cyber security — A comparison of standards," IEEE PES General Meeting, Minneapolis, 2010.

[16] L. Gallon and J. Bascou, "Using CVSS in attack graphs," in *2011 Sixth International Conference on Availability, Reliability and Security*, 2011.

[17] P. Mell, K. Scarfone and S. Romanosky, "A Complete Guide to the Common Vulnerability Scoring System (CVSS) version 2.0," in *Forum of Incident Response and Security Teams*, 2007.

[18] S. Patel, J. Graham and P. Ralston, "Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements," *International Journal of Information Management,* pp. 483-491, 2008.

[19] F. Cohen, "Managing network security—Part 5: Risk management or risk analysis 15-19.," *Network Security,* vol. 1997, no. 4, pp. 15-19, 1997.

[20] A. S. K. S. H. &. J. K. Teixeira, "Secure Control Systems: A Quantitative Risk Management Approach," *IEEE Control Systems magazine,* pp. 24-45, 2015.

[21] E. &. L. J. Byres, "The myths and facts behind cyber security risks for industrial control systems.," in *In Proceedings of the VDE Kongress*, 2004.

[22] S. P.-C. L. B. M. &. H. Y. Kriaa, "A survey of approaches combining safety and security for industrial control systems," *Reliability Engineering & System Safety,* vol. 139, pp. 156-178, 2015.

[23] M. S. M. N. &. A. M. Toosarvandani, "The risk assessment and treatment approach in order to provide lan security based on isms standard," *International Journal Foundations of Computer Science & Technology,* vol. 2, no. 6, pp. 15-36, 2012.

[24] E. M. W. C. R. d. S. D. &. B. W. C. Alencar Rigon, " A cyclical evaluation model of information security maturity," *Information Management & Computer Security,* vol. 22, no. 3, pp. 265-278, 2014.

[25] P. M. K. &. S. S. Maynard, "Modelling Duqu 2.0 Malware using Attack Trees with Sequential Conjunction. In ICISSP (pp. 465-472).," in *In Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, 2016.

[26] P. S. &. K. B. H. Woo, "Methodology of Cyber Security Assessment in the Smart Grid," *Journal of Electrical Engineering & Technology,* vol. 12, no. 2, pp. 495-501, 2017.

[27] D. V. O. &. G. L. J. López, "Dynamic risk assessment in information systems: state-of-the-art," in *In Proceedings of the 6th International Conference on Information Technology*, Amman, 2013.

[28] G. A. T. D. &. D. J. Francia III, "Security best practices and risk assessment of SCADA and industrial control systems.," in *In Proceedings of International Conference on Security and Management (SAM)*, 2012.

[29] C. K. A. &. A.-F. J. Taylor, "Risk analysis and probabilistic survivability assessment (RAPSA): An assessment approach for power substation hardening," in *In Proc. ACM Workshop on Scientific Aspects of Cyber Terrorism,(SACT)*, Washington DC, 2002.

[30] J. Markovic-Petrovic and M. Stojanovic, "An Improved Risk Assessment Method for SCADA Information Security," *Elektronika Ir Electrotechnika,* vol. 20, no. 7, pp. 69-72, 2014.

[31] M. McQueen, W. Boyer, M. Flynn and G. Beitel, "Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System," in *Proceedings of the 39th Hawaii International Conference on System Sciences*, 2006.

[32] S. Patel and J. Zaveri, "A Risk-Assessment Model for Cyber Attacks on Information Systems," *Journal of Computers,* vol. 5, no. 3, pp. 352-359, March 2010.

[33] C. S. S. D. N. T. H. D. Z Huang, "Difficulty-Level Metric for Cyber Security Training," IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, 2015.

DISTRIBUTION

1 DOE-NE Sponsor – Trevor Cook, by electronic delivery

1	MS0748	Lon Dawson	08851
1	MS0748	Mitch McCrory	08851
1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories