Cyber security risk assessment for SCADA and DCS networks

ARTICLE *in* ISA TRANSACTIONS · NOVEMBER 2007

Impact Factor: 2.98 · DOI: 10.1016/j.isatra.2007.04.003 · Source: PubMed

Jeffrey L. Hieb
University of Louisville

Available online at www.sciencedirect.com
ScienceDirect
ISA Transactions 46 (2007) 583–594
www.elsevier.com/locate/isatrans

Cyber security risk assessment for SCADA and DCS networks

P.A.S. Ralston[a,*], J.H. Graham[b], J.L. Hieb[b]

[a] University of Louisville, JB Speed School of Engineering, 40292 Louisville, KY, United States
[b] Department of Computer Engineering and Computer Science, University of Louisville, Louisville, KY 40292, United States

Received 13 October 2006; accepted 22 April 2007
Available online 10 July 2007

Abstract

The growing dependence of critical infrastructures and industrial automation on interconnected physical and cyber-based control systems has resulted in a growing and previously unforeseen cyber security threat to supervisory control and data acquisition (SCADA) and distributed control systems (DCSs). It is critical that engineers and managers understand these issues and know how to locate the information they need. This paper provides a broad overview of cyber security and risk assessment for SCADA and DCS, introduces the main industry organizations and government groups working in this area, and gives a comprehensive review of the literature to date. Major concepts related to the risk assessment methods are introduced with references cited for more detail. Included are risk assessment methods such as HHM, IIM, and RFRM which have been applied successfully to SCADA systems with many interdependencies and have highlighted the need for quantifiable metrics. Presented in broad terms is probability risk analysis (PRA) which includes methods such as FTA, ETA, and FEMA. The paper concludes with a general discussion of two recent methods (one based on compromise graphs and one on augmented vulnerability trees) that quantitatively determine the probability of an attack, the impact of the attack, and the reduction in risk associated with a particular countermeasure.

Keywords: SCADA; DCS; Risk analysis; Vulnerability assessment; Control systems

1. Critical infrastructure protection: SCADA and DCS cyber security

Critical infrastructures (CIs) are physical and cyber-based systems that are essential for day-to-day operation of the economy and government. Electric power production and distribution, water treatment and supply, gas and oil production and distribution, and telecommunications are excellent examples of CI. Protecting and assuring the availability of CI is vital to both the US and world economies. CI assets are often privately held and can cross international borders. The August 2003 northeast blackout, which also affected Canada, shows how CI crosses international boundaries. The President's Report on Critical Infrastructure Protection [1] and Presidential Directive 63 (PDD 63) acknowledged and highlighted that computer-based control systems, supervisory control and data acquisition (SCADA) and distributed control systems (DCSs), were vital to the daily operation of many CIs and were susceptible to both cyber and physical attacks.

The Homeland Security Act of 2002 assigned to the Department of Homeland Security (DHS) the responsibility for developing a comprehensive national plan for critical infrastructure protection. As part of its infrastructure protection mission, DHS is focusing on risk management and analysis through the risk management division (RMD) and office of risk management and analysis (RMA), which is leading the department's efforts to create a framework for overall management and analysis of risks to homeland security. A national asset database (NADB) is being compiled and overseen by RMD that will serve as a national list of critical resources, such as the number and location of dams, power plants, and other assets. The NADB is not yet complete [2].

Within DHS there are programs and groups that are looking specifically at SCADA control systems security. The National Infrastructure Advisory Council (NIAC) convergence work group is investigating the cyber security of SCADA and process control systems and will eventually make recommendations regarding their protection. The National Communication System (NCS), a federal agency transferred to DHS, focuses exclusively on communication systems including SCADA systems. The Department of Homeland Security Science

* Tel.: +1 502 852 0479; fax: +1 502 852 6355.
E-mail address: parals01@louisville.edu (P.A.S. Ralston).

0019-0578/$ - see front matter
doi:10.1016/j.isatra.2007.04.003

and Technology Directorate conducts and funds research in many areas including cyber security; part of their mission is to lead the development of robust process control and SCADA systems. The Control Systems Security Program (CSSP) of the National Cyber Security Division (NCSD) of DHS leads an initiative to secure our nation's critical infrastructure by identifying, analyzing, and reducing cyber risks associated with the control systems that govern our infrastructures [3]. Established in 2003 as the operational arm of the NCSD to protect the nation's Internet infrastructure, US-CERT (Computer Emergency Readiness Team) coordinates defenses against and responses to cyber attacks across the nation. For control system security, US-CERT publishes documents to assist in determining vulnerabilities and improving control system security [4,5] including vendor specific vulnerabilities and solutions. Worldwide, there are more than 250 organizations that use the name "CERT" related to cyber security response; US-CERT is independent of these but may coordinate with them on security incidents. The CERT® Coordination Center (CERT/CC), established at Carnegie Mellon University in 1988 and working jointly with DHS, contributes expertise for protecting the nation's information infrastructure by coordinating defense against and response to cyber attacks.

The objectives of the most recent National Infrastructure Protection Plan [6] include building security partnerships to implement critical infrastructure protection programs, assessing risk, implementing risk reduction programs, and maximizing use of resources. Risk assessment for all cyber systems including SCADA and DCS are an integral part of the document that aims to provide a national unifying structure to all protection efforts. Until recently, there has been little specific guidance on the actual analysis of risk assessment, specifically as it relates to SCADA and DCS and the risk of cyber-based attacks on these systems. What is necessary, and what is occurring, is a cooperative effort between government, industry, and academia to address critical infrastructure security, including cyber security and risk management for SCADA and DCS.

1.1. Government and industry groups contributions

Information Sharing and Analysis Centers (ISACs, http://www.ni2ciel.org/ISACs) were created by Presidential Directive 63 (http://www.fas.org/irp/offdocs/pdd/pdd-63.htm), and are private, independent organizations designed to share important information about cyber vulnerabilities, threats, intrusions and anomalies within and between industry sectors and the government. Recently, a government organization, the Multi-State Information Sharing and Analysis Center (MS-ISAC, http://www.msisac.org/) has been created as the central resource for gathering and sharing information on cyber threats between states and local government and is recognized by DHS as the national center for coordination of cyber readiness and response. This site has links to almost all national initiatives.

The Idaho National Laboratory (INL, http://www.inl.gov) in conjunction with the Sandia National Lab, Argon National Lab, Oak Ridge National Lab, and Pacific Northwest National Lab have created the National SCADA Test Bed in a setting that includes a functioning power grid and synergistic cyber and wireless test beds. Sandia National Laboratory (http://www.sandia.gov) has created The Center for SCADA Security where SCADA research, training, red teams, and standards development takes place. In addition to pure research, the National SCADA Testbed (NTSB) Program work includes supporting the development of industry standards covering cyber security of control systems. Two reports [7,8] summarize these activities to date. Researchers at Sandia have also recently developed and published a SCADA Security Policy Framework [9] which ensures that all critical topics have been adequately addressed by specific policy rather than by relying on standard IT security policy.

In addition to full-fledged research activities such as those at national laboratories, standards bodies and industry groups are working to address the needs of control system security [10]. These include, but are not limited to: ISA (Instrumentation, Systems, and Automation Society), NIST (National Institute for Standards and Technology), Chemical Sector Cyber Security Program organized by the Chemical Information Technology Council (ChemITC), which absorbed the CIDX (Chemical Industry Data Exchange) Cyber Security Initiative in January 2006, IEC (International Electrotechnical Commission), CIGRE (International Council on Large Electric Systems), AGA (American Gas Association), and NERC (North American Electric Reliability Council). All have published documents on cyber security and risk assessment for control systems, with links provided to these documents at the websites for these organizations.

Some important contributions by these groups include two published technical reports by ISA that cover security technologies and how to apply them to control systems [11, 12], and AGA documents on communications encryption [13]. AGA's ongoing work is focused on encryption for legacy systems, networked systems, and eventually for embedding developed technologies into devices during the manufacturing process. NERC has finalized cyber security standards [14] that will establish the requirements for security management programs, electronic and physical protection, personnel, incident reporting, and recovery plans. The National Institute of Standards and Technology (NIST) through its Process Control Security Requirements Forum (PCSRF) has defined a cohesive, cross-industry, baseline set of common security requirements for existing and new control systems [15–17] for various industries as well as a comprehensive guide to SCADA system security [18].

Perhaps the most ambitious group created and funded by the Department of Homeland Security/Homeland Security Advanced Research Projects Agency (DHS/HSARPA) is called the Process Control Systems Forum, https://www.pcsforum.org. Established in February 2005 the PCSF mission is to accelerate the design, development, and deployment of more secure control and legacy systems that are crucial to securing critical infrastructures. This group is not a standards body; its purpose is to provide the opportunity for technical exchange with a

focus on common needs, practices, and consensus architectures in order to accelerate the development and implementation of more secure process control systems (PCS). One goal of the PCSF is to provide communication and information dissemination capabilities that extend beyond the current boundaries of other organizations that are working on control systems issues. Through "working groups", it interfaces with other organizations including international groups.

The Institute for Information Infrastructure Protection (I3P), http://www.thei3p.org/ was founded in 2001 by the Department of Homeland Security (DHS) as a consortium of government, academic, and nonprofit organizations to coordinate fundamental research and development efforts in information infrastructure protection. The I3P funded a research endeavor "Unifying Stakeholders and Security Programs to Address SCADA Vulnerability and Infrastructure Interdependencies" [19], a SCADA project that is investigating ways to advance the security of process control systems. A main task is to develop a risk assessment methodology and tool to support the development of inherently secure SCADA and PCS systems, [20]. Another report [21] identified existing security metrics tools and their applicability to PCS and an overview of risk analysis. This report also included an extensive bibliography of cyber security documents.

A concise and informative history of critical infrastructure concerns through mid 2005, with emphasis on security of SCADA, is found in a System Administration Audit Network Security (SANS) Institute paper [22]. The SANS Institute (http://www.sans.org/) created in 1989, provides training and performs research in information security. The British Columbia Institute of Technology Industrial Security Incident Database reported in 2004 [23] that there was a sharp increase in events around 2001, and that the source of cyber-attacks shifted from internal attacks to 70% external attacks, reinforcing the need for SCADA and DCS cyber security.

1.2. SCADA and DCS cyber security concerns

Early digital communication in SCADA and DCS systems was achieved using serial networks and the ubiquitous RS-232, RS-422, and RS-485 standards. This meant that while networks were still relatively isolated, there was consolidation of both communications channels and communication standards [24]. Due to low fidelity and limited channel capacity of early serial communications, these protocols supported only the minimal functionality needed to achieve reliable scanning and control of points within a remote device [25], with little or no attention to security. For example, data messages sent as clear text and operating and control commands accepted without any authentication [26]. Today SCADA and DCS communication is carried through a variety of media: Ethernet, wireless, shared leased lines, and even the Internet. These communication channels are increasingly less isolated, leaving SCADA and DCS vulnerable to the forgery of commands and status data [26]. In addition to this threat, SCADA and DCS are now built from commercial off-the-shelf (COTS) components including commercial operating systems that have known security vulnerabilities. When combined with increased network convergence and connectivity, the use of COTS components makes SCADA and DCS vulnerable to common cyber attacks.

Recognition of the threat created by the lack of authentication in SCADA and DCS protocols and the use of COTS components is described in a number of recent publications [15,27–31]. Exploiting the vulnerabilities in SCADA systems can have serious consequences [32] which can result in loss of service to utility customers, financial loss to service providers due to damaged equipment and corruption of metering information, and finally environmental damage and potential loss of human life. Several sections of a National Academy of Science publication "Making the Nation Safer" [26] describe in greater detail security vulnerabilities in SCADA systems, their relation to different critical infrastructures, and the potential devastating consequences of successful attacks.

Numerous articles and guides have been published recently to aid SCADA and DCS users and vendors. The President's Critical Infrastructure Protection Board, and the Department of Energy, has developed 21 steps to help any organization improve the security of its SCADA networks [33]. The United Kingdom has a similar guide provided by the National Infrastructure Security Coordination Centre (NISCC) [34]. The Chemical Industry Data Exchange has guidance documents posted [35], and other papers available for download at the Chemical Sector Cyber Security Program website (http://www.chemicalcybersecurity.com). The General Accounting Office in 1999 issued a guide [36] to help federal managers implement information security risk assessments by providing case studies. Many in the industrial community have been slow to accept the problem with SCADA and DCS systems because such systems were historically stand alone and isolated. Emphasis was on reliability and performance, not security. Because of connections to company networks and the Internet, these systems are now vulnerable to typical network threats. This is exacerbated by the fact that SCADA systems are now tightly integrated into business and economic processes [37]. A more recent guide [38] with information to enhance industrial control systems security provides a foundation to help implement secure systems, secure existing systems, and make security a process. Many current references and links to related standards guides are provided.

A General Accounting Office Report [39] succinctly identified the trends that have escalated the risks to SCADA systems: adoption of standardized technologies with known vulnerabilities, connectivity of control systems to other networks, constraints on the use of existing security technologies and practices, insecure remote connections, and widespread availability of technical information about control systems. These trends have moved SCADA systems from proprietary, closed networks to systems with security challenges comparable to enterprise Information Technology (IT) systems. The PCS community will need to find compensating security controls until inherently secure systems are available and insecure legacy systems replaced. Since

control systems last 15 years or longer, securing legacy systems will require hardware and software retrofit solutions to become commercially available [40].

Much information has focused on becoming aware of the growing problem of securing SCADA and DCS systems, recognizing the threats, and learning how to find solutions [10, 41–46]. Several introduce and explain applicable security technology such as vulnerability testing and assessment [47,48] intrusion detection and security monitoring of networks [49], and encryption, network architecture and system hardware hardening [50], and hardening operating systems [51]. Geer's article [51] points out that hardening operating systems could close network access to systems that some control applications require for proper functioning. He further notes that improperly implemented security could fail by making control systems difficult to use; employees will circumvent security in such situations. The article concludes with an important warning to users, that they should not spend time worrying about an ideal approach to security to adopt, but rather take the available and effective interim steps now. A recent survey article summarizes many of these issues and provides an overview of research issues related to strengthening cyber security [28].

DHS sees a need for commercial owners of critical infrastructure to invest in more secure networks and encouragement for SCADA system vendors to build security into their products [52]. Some initial response to this need is now appearing on the market. Honeywell's Experion Process Knowledge System R300 now includes embedded cyber security that protects against denial of service attacks and message flooding by protecting the controller network [53]. Plantdata Technologies [54] has recently developed a new type of firewall designed to be distributed throughout the SCADA environment and is said to deliver a higher level of network segmentation and defense. The SCADA Procurement Project, established in March 2006, is a joint effort among public and private sectors focused on development of a common procurement language with a goal of federal, state and local asset owners and regulators to use these procurement requirements to maximize the collective buying power to help ensure that security is integrated into SCADA systems. The most recent version is available [55]. As standards bodies, vendors, and users cooperate and acquire more experience with proper security expectation and testing, it can become an embedded and expected quality assurance issue.

Byres and Franz [47] point out that security vulnerability in control hardware is as important as software and communication vulnerability. They state that many industrial control system vulnerabilities are the result of procedural or administrative security failings rather than software failings. They suggest classifying vulnerabilities by where or how they enter into a product's life cycle: inherent protocol vulnerabilities, product design vulnerabilities, implementation vulnerabilities, and mis-configuration vulnerabilities.

2. Risk assessment for SCADA and DCS systems

Miller and Byres [56] point out that the many papers discussing vulnerabilities of control systems neglect the articulation of relative risk of particular implementations. All resources that need protection and the vulnerabilities that can become threats must be identified. Then, policy, procedures, or technology for protection can be determined. The general area of risk assessment is vast, with many methods and tools available to use for assessing risk of various environments including SCADA and PCS systems. A non-exhaustive list of available tools can be found from Riskworld [57].

Commercial systems such as RiskWatch provide an automated tool to perform qualitative or quantitative risk analyses and vulnerability assessments. This tool employs user friendly interfaces, comprehensive knowledge databases, predefined risk analysis templates, data linking functions, and proven risk analysis analytic techniques [58].

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [59], is a framework for identifying and managing information security risks developed at Carnegie Mellon University's CERT Coordination Center. It is a self-directed activity by a team that draws on the knowledge of many employees to define the current state of security, identify risks to critical assets, and set a security strategy. It also uses event/fault tree analyses to model threats to critical assets.

CORAS [60] is a tool-supported methodology for model-based risk analysis of security-critical systems developed under the European Information Society Technologies Programme. It was completed in 2003, and a website (http://coras.sourceforge.net/) is maintained where one can download the tool, receive updates, and locate the many related papers. Unlike many of the commercial tools, CORAS documents clearly explain what methods are used for risk assessment, such as fault tree analysis (FTA) and failure mode effect criticality analysis (FMECA), though few quantitative results are presented.

As part of their participation in DOE response to PDD 63 Lawrence Livermore National Laboratory (LLNL) began assessing vulnerabilities and risk in the electric power infrastructure in 1998 [61]. The discussion of their activities indicated a focus on cyber security, particularly for SCADA, but specific analytical techniques were not discussed. Identification of vulnerabilities was a major focus of the assessment processes, and grew to include live penetration testing, "zero-knowledge" attacks, and crossover attacks that included physical stages and cyber stages. Lopez [61] points out that the most difficult portion of the assessment was the analysis or risk characterization.

After the creation of DHS and the shift in critical infrastructure protection to new departments within DHS, LLNL and other national labs began performing vulnerability and risk assessment for other critical infrastructures and for entire regions of the US. A recent Sandia National Laboratories report [62] attempted to classify risk assessment methods, (primarily available risk assessment tools) according to level of detail and approach in order for users to be able to select the most appropriate method.

2.1. Published research on overall risk assessment

Published work related to risk assessment is very difficult to categorize. Several different aspects define the research, primarily how much of the overall process is tackled. Risk assessment is a multiphase process: it starts with risk identification, proceeds to risk analysis, follows with risk evaluation and ranking, and ends with the management and treatment phases.

Many of the government guidelines and industry publications mentioned previously describe qualitative risk assessment approaches. Researchers at Georgia Institute of Technology [63] present a qualitative, but very systematic approach to overall risk assessment for information systems. Especially helpful is their development of a three axis view of the threat space which organizes the problem of risk management and the presentation of a procedure for computing losses due to threats and benefits of countermeasures.

The next articles discussed are holistic in their approach and are studies of huge, interdependent systems. The research includes the risk analysis phase, but the exact details of the risk analysis methods will be discussed separately in the following section. These are noted separately because of their large scope and the massive effort involved in the risk identification phase.

A number of modeling and simulation approaches under development at Sandia National Laboratories directly address interdependencies and offer insight into the operational and behavioral characteristics of critical infrastructures. Detailed interdependency models and simulations of the following categories have been made: (1) aggregate supply and demand tools which evaluate the total demand for an infrastructure service and the ability to provide it, (2) dynamic simulations to examine infrastructure operations, disruption effects, and downstream consequences, (3) agent-based models which model physical components and their interactions and operational characteristics, (4) physics-based models that analyze aspects of infrastructure with standard engineering techniques, (5) population mobility models primarily for transportation and social network study, and (6) Leontif Input–Output models which provide an aggregated, time-independent analysis of generation, flow, and consumption of commodities among infrastructure sectors [64]. Such modeling and simulation abilities are integral to infrastructure risk analyses.

The most comprehensive risk identification methodology to address interdependencies is hierarchical holographic modeling (HHM), [65,66]. Chittester and Haimes described HHM as a method that "can identify all conceivable sources of risk to SCADA systems and to the utilities and infrastructure that uses them" [67]. The method aims to represent the diverse characteristics and attributes of a system. HHM has the ability to facilitate the evaluation of subsystem risks and their corresponding contributions to risks in the total system. This makes it the ideal application for SCADA systems and their associated interdependent and interconnected infrastructures [68]. This method has been used to identify sources of risk to SCADA systems in the railroad sector [67].

Haimes, Kaplan, and Lambert [69] describe the risk filtering, ranking, and management method (RFRM) which builds on HHM to identify risks, but then filters and ranks the risks so that the risks can be addressed in order of priority. RFRM is an eight phase process that begins with HHM for risk identification, progresses through various phases of filtered risk scenarios with quantitative ranking to the final phases of management and feedback.

Many critical infrastructures are coupled and their interdependencies render them at great risk to cyber attacks. They are often remotely controlled and managed by SCADA systems. Hierarchical holographic modeling can identify the sources of risk, but to quantify the efficacy of risk management, inoperability input–output modeling (IIM) is needed. This is a Leontief-based model that enables accounting for both intra and interconnectedness with each infrastructure. The input to the system is an initial perturbation triggered by an attack, and the outputs are resulting risks of inoperability. The outputs are represented in two different metrics, economic inoperability measured in dollars lost and percentage of dysfunctionality. Haimes and Chittester [70] use this method to quantify economic losses and their propagation through the various economic sectors for large scale civil infrastructures controlled by SCADA systems over IP based communication networks. They present a case study demonstrating the effects of a perturbation to the telecommunications sector by way of cyber intrusion. Additional case studies and more description of IIM can be found in [71].

Crowther et al. [72] applied the methods of HHM, RFRM, and IIM to assess and manage risk of terrorism to Virginia's interdependent transportation system. They developed a methodology and computer tool for assessing the consequences of a failure in the transportation infrastructure and how this failure propagates into interdependent sectors.

All of this research on interdependent systems has stressed the need for metrics that characterize the condition and performance of the infrastructures. Recent work [73,74] focused on representing interdependent infrastructure networks using Markov and semi-Markov processes to reflect uncertain capacity on network links. The Markov-based approach allows analysis of both transient and steady-state concerns regarding availability of service. They demonstrated their approach on a small-scale SCADA system. Their model structure is dependent on good estimates of parameters and these estimates have to come from empirical data, which is often difficult to obtain.

2.2. Risk Analysis – quantifying, filtering, and ranking risk – probabilistic risk assessment

Quantitative risk analysis methods fall under the broad category of probabilistic risk assessment (PRA). A generally accepted definition of PRA is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological entity. Although PRA technically includes the risk identification phase, it does not provide the guidance of methods such as HHM, but rather assumes that the designer can identify the risks. PRA includes all

fault/attack (FTA) tree analyses, event tree analysis (ETA), failure mode and effect analysis (FMEA) or failure mode effect and criticality analysis (FMECA), and cause/consequence analysis (CCA), as well as methods that use directed graphs and logic diagrams [75]. Most other methods are extensions or combinations of these. Many of the tools mentioned earlier incorporate these methods to varying degrees.

Risk is characterized by the severity (or magnitude) of an adverse consequence that can result from an action and the likelihood of occurrence of the given adverse consequence. In probabilistic risk assessment, consequences are expressed numerically and their likelihoods of occurrence are expressed as probabilities or frequencies. Determining risk is generally accepted as answering the three questions: What can go wrong? How likely is it? What are the consequences? [76] In PRA, these are answered by developing a set of scenarios or initiating events to answer what can go wrong, then evaluating the probability of the these scenarios, and finally estimating their consequences. The PRA ultimately presents a set of scenarios, frequencies, and associated consequences developed in a way to make informed decisions. PRA quantifies "risk metrics", a term that refers to a consequence-oriented figure of merit, such as the probability of the top event [77]. Determination of needed basic event probabilities is the most difficult task in applying this technique and can limit the effectiveness of PRA if realistic and meaningful probabilities and frequencies cannot be estimated. Many references explain all aspects of PRA in great detail [75, 77].

2.3. Fault tree analysis (FTA), failure mode effect analysis (FMEA)

FTA (fault tree analysis) [78,79], is a deductive, failure-based approach. It starts with an undesired event, and then deduces event causes using a systematic backward reasoning process. A fault tree is constructed as a logical illustration of the events and their relationships necessary and sufficient to result in the undesired (top or root) event. The symbols used indicate the types of event and relationship involved such as AND gates (output of gate occurs if all inputs occur) and OR gates (output of gate occurs if any of the inputs occur). The fault tree displays the stepwise cause resolution using formal logic symbols. To evaluate the fault tree and calculate a top event probability, it has to be transformed into an equivalent set of logic equations. By successive substitution, each gate event is expressed in terms of basic events. The qualitative results obtained from FTA are "minimal cut sets", the smallest combination of basic events that result in the top event (fault). Each minimal cut set is a combination of basic events. The set of minimal cut sets for the top event represents all the ways that basic events can cause the fault or top event. Quantification of FTA happens when top event probability is determined from basic event information by assigning probabilities to the basic events. Uncertainties in any quantified result can be determined. These top event probabilities can be used to calculate risk in financial or other terms. Several importance measures can be calculated to determine the change in the risk metric of interest such as the change in the top event probability when a basic event probability is set to zero [77].

Inductive approaches such as FMEA and FMECA are forward stepping and begin with an initiating event, then induce the end effects [78]. It is important to note that these methods analyze single component faults and their system effects and do not consider combinations of faults. Walker [80], makes a strong case for using FMEA in the early design phase of all engineering projects to determine the project's technical risk.

The basic difference between FTA and inductive methods is the direction of the analysis. FTA starts with the undesired event and traces backward to causes, whereas inductive methods start with an initiating event and trace forward to consequences. Thus, FTA is the appropriate analysis to carry out if a given undesired event is defined and the goal is to determine its cause. Inductive approaches should be used if a given set of causes are identified and the goal is to determine the consequences. A comprehensive PRA might use both inductive and deductive approaches to obtain a complete set of accident sequences, depending on the complexity of the system.

2.4. PRA extensions or modifications

Yacoub and Ammar [81] present a methodology for architecture-level risk analysis. Their approach is based on dynamic risk metrics [82] that define complexity factors for architecture elements obtained from simulation of the software architecture specifications. FMEA is used with simulation to determine the effects of a failure, and these results are used to develop heuristic risk factors for all components and connectors. The risk factors are aggregated and used with component dependency graphs to analyze the overall risk for the architecture.

Wyss et al. [83] describe how features of event tree analysis and Monte-Carlo discrete event simulation can be combined with concepts of object-oriented analysis to form a new risk assessment technique (OBEST, object-based event scenario tree), though related to PRA. This OBEST method was developed to enable risk assessment study of systems and scenarios that exhibit strong time dependence (not a characteristic of SCADA systems).

Madan et al. [84] applied a stochastic model to a computer network system to capture attacker behavior and analyze and quantify the security attributes. They determined steady-state availability of quality of service requirements and mean times to security failures based on probabilities of failure due to violations of different security attributes.

Taylor et al. [85] merged PRA with survivability system analysis (SSA) with minor modification of what would be considered traditional PRA, but it is still dependent on obtaining estimates of probabilities.

A natural extension to PRA involves the use of fuzzy concepts, though this approach has not been published for use in SCADA system security risk assessment. Early in the study of risk analysis related to computer security, fuzzy modeling was used to analyze and rank risks in a computing facility [86]. The authors created a set of fuzzy rules describing likely

vulnerabilities such as "if the hard drive is old, then the customer database loss risk factor is increased". These rules are combined to produce a total risk factor associated with the loss of the customer database. Similar rule sets and associated risk factors can be calculated for all computer facility assets. A similar procedure was used to calculate a severity of loss for different components and then a total project risk in electronic commerce development [87].

Fuzzy concepts provide a way to deal with uncertainty in both the probabilistic parameter estimates and subjective judgments. This method was recently applied to risk assessment of a subway construction project in Korea [88].

Pillay and Wang [89] used fuzzy concepts to model the occurrence likelihood and consequences of failure for the identified hazards on a fishing vessel. They used FTA to calculate a "fuzzy" probability of the system failure. The consequences of failure for each basic event within the fault tree are considered for the four categories of negligible, marginal, critical, or catastrophic. The risk of the basic events is determined by combining the likelihood of occurrence and consequences of failure in linguistic terms via a fuzzy rule set. The output, once "defuzzified", produces a risk ranking.

3. Attack trees and vulnerability trees

Attack trees were introduced by Schneier [90] as a way of formally analyzing the security of systems and subsystems based on varying attacks. This is basically FTA with the attack goal in place of a fault and basic event probabilities in place of failure rates. Schneier's work is notable because he was the first to apply this approach to the area of information security. The attack goal is the root of the tree and the different ways of accomplishing the attack are the leaves, with connections via AND and OR nodes.

Moore et al. [91] describe and illustrate an approach for documenting attacks on software systems using attack tree information in a structured and reusable form. Analysts can then use the approach to document and identify commonly occurring attack patterns and then modify attack trees to enhance security development.

Most recently, attack trees have been applied to a SCADA communication system [92]. The authors identified eleven attacker goals and associated security vulnerabilities in the specifications and development of typical SCADA systems. They were then used to suggest best practices for SCADA operators and improvements to the MODBUS standard. Their application was qualitative in that attack tree analysis was used only to identify paths and qualify the severity of impact, probability of detection, and level of difficulty. They did not calculate the probability of an actual attack being successful.

A related approach that arose in the computer and information security literature is vulnerability tree analysis. Vulnerability trees are hierarchy trees constructed as a result of the relationship between one vulnerability and another vulnerability and or steps that a threat agent has to carry out to reach the top of the tree [93]. Vulnerability trees help security analysts understand and analyze different attack scenarios that a threat agent might follow to exploit a vulnerability. With this understanding, more effective countermeasures can be taken.

4. Cyber security risk reduction for SCADA and DCS

The ability to determine whether or not risk reduction is achieved when modifications are made is critical for effectively planning and implementing security enhancements. Simple calculations for risk reduction were published by Tolbert [94] in 2005. In this paper, a risk metric was calculated which was simply the product of the frequency, likelihood of occurrence, and severity according to an arbitrarily selected 1–5 scale for the three factors. The calculation is made before and after a system modification is made. This simple method of risk assessment would be a good start for initial investigation of a planned security upgrade.

In 2006, McQueen et al. [95] published results of a promising method to calculate a quantitative risk reduction estimate of security enhancements applied to a specific SCADA system. A case study of the use of the method was carried out on a small SCADA system that consisted of eight generic machine types connected to a local Ethernet LAN that did not include a firewall. The method employs a directed graph (compromise graph) where the nodes represent different potential attack states for each device on the SCADA network. Edges represent transitions from one attack state to another and the value associated with each edge is an estimate of the time required to make the transition. Time-to-compromise for each edge is modeled as a function of the device vulnerabilities and attacker skill level. The total time-to-compromise the SCADA system is the shortest path to the primary security target(s). Total time-to-compromise is calculated both before and after security enhancements and the quantitative risk reduction associated with a security enhancement is measured by the increase in time-to-compromise of the enhanced system.

The proposed methodology begins by analyzing the system configuration to identify primary target(s) and perimeter devices. Next, the security requirements of the primary target(s) are identified and prioritized; for SCADA systems high priority attacks would be unauthorized control and denial of service. Once the primary target(s) have been identified the vulnerabilities of each system device are identified through testing and search of online vulnerability databases. Then, all device vulnerabilities are assigned one or more compromise types. Next, the time to compromise each device is estimated based on the attacker skill level and device vulnerabilities. Now the compromise graph(s) can be generated and the dominant attack path(s), the path with the minimum weight, can be assigned an overall time-to-compromise. Risk reduction is estimated by using time-to-compromise (of the dominant attack path(s)) as the primary measure of risk, assuming that risk is inversely proportional to time-to-compromise. Values for the baseline and enhanced system are compared with risk reduction calculated as 1-(expected time-to-compromise for dominant attack path of baseline system)/(expected time-to-compromise for dominant attack path of enhanced system). Results reinforced the selection of the basic security enhancements such

as hardening the weakest link in the attack path, use of firewalls, and network partitioning.

Probabilistic Risk Assessment provides a foundation for the calculation of risk reduction when applied to SCADA security. In 2006, Graham, Patel, and Ralston [96] described a new risk modeling tool, augmented vulnerability trees, and two new indices for quantifying the risk.

In this approach, augmented vulnerability trees are used to combine attack tree and vulnerability tree methods. All of the tree analysis methods are very similar and are analyzed similarly; they differ in what defines the top event. The fault tree/attack tree/vulnerability tree method is a deductive process where the topmost undesirable event is postulated. Then, the ways for this event to occur are deduced. The deduction process results in a tree that includes all components that could contribute in causing the top event. Thus, a vulnerability tree is a logical model representing the logic of system-failures qualitatively. A tree diagram is often constructed as a graphical illustration showing the stepwise cause resolution using formal logic symbols.

Two indices representing the vulnerability for an information system are presented. The threat-impact index is a value between 0 and 100 showing the economical impact of a probable threat; the lower the value, the smaller the impact from a successful attack. The cyber-vulnerability index, also a value between 0 and 100, is a numerical value representing vulnerabilities or undesirable events that would help an intruder launch attacks. A lower value represents a more secure system which implies fewer security flaws. The following steps summarize the proposed method.

Step 1: *Construct the base-level and expanded vulnerability trees*

To construct a vulnerability tree, the top undesirable event is first postulated which represents a pivotal event for a particular failure scenario. The possible means (attacks) for this event to occur are systematically deduced. These attack paths can result in a failure (the top event). Then, each situation (base-events) that could cause an attack is added to the tree as a series of logical expressions. Thus, the intermediate failure events ("attacks") are connected to the top event and basic events with logic gates, the most common of which are "AND" gates and "OR" gates. In a vulnerability tree, the AND gate is used when all the base-events connected by this gate must happen to launch an attack. The OR gate is used when any one of the base-events connected by this gate is sufficient for an intruder to launch an attack.

Step 2: *Construct effect analysis table and calculate threat-impact*

From the vulnerability tree a list of all threat types is created. Each of these threats is considered one at a time and a list of various effects, or types of damage, is constructed. Using these effects, a table showing effects for each attack is created. Then, using the attack history/logs, the frequency of attacks is calculated. A damage/impact dollar value for each event is calculated by interviewing the operators, engineers, accountants, and managers. The probabilities and the impacts (listed in dollar amount) are normalized so that the values range from 0 to 100. The probability of each attack is multiplied by the total maximum damage amount caused by the attack. Methods such as [97] can be used to get probability data. Costs could be estimated using the data in [98].

Step 3: *Add threat-impact index values to vulnerability tree*

The threat-impact values from the effect analysis table are marked on the vulnerability tree. The top event of a system without any implemented security (base vulnerability tree) will have the threat impact index of 100. After security enhancements are applied, this value is expected to be reduced in the new vulnerability tree.

Step 4: *Calculate the vulnerability index values*

The cyber-vulnerability indices are assigned to all the base-events by using the threat-impact index of their parent event in a vulnerability tree. The threat-impact index is equally divided among all the base-events at the same level. AND and OR are treated the same way while dividing the parent-level values. Once all the base-events have the cyber-vulnerability indices assigned to them, the cyber-vulnerability index for the attack tree is calculated by summing up all the cyber-vulnerability indices.

Step 5: *Complete augmented vulnerability tree by adding vulnerability index values*

The expanded tree now has graphical information about threats, the impact of these threats, and the vulnerability of the system to electronically launched attacks.

Step 6: *Repeat steps 2 to 5 for proposed security enhancements*

Security enhancement should lead to lower threat impact index and cyber-vulnerability index values. However, some security enhancements may not result in lower values if other vulnerabilities continue to enable a threat.

Using data from a SCADA system testbed implemented at the University of Louisville as a case study, the use of these proposed vulnerability and risk assessment tools was illustrated [96]. The revised augmented vulnerability tree for the security enhanced system is shown in Fig. 4.1. By comparing the indices for threat impact and vulnerability on SCADA communication protocols with, and without, security enhancements, risk and vulnerability were quantified for the system, and the improvement produced by the protocol security enhancements was demonstrated. Without security enhancements the TI index and CV index are 100. The revised augmented vulnerability tree in Fig. 4.1 shows the reduced TI and CV indices the result from the security enhancements.

5. Conclusions

This paper has discussed a number of important real-life issues in the cyber-security of the SCADA and DCS networks that control much of the critical infrastructure of countries around the world. Many of the current vulnerabilities in these systems are due to the transition of older computer networks into newer networks that are accessible, either directly or indirectly, through the public Internet. This paper attempts to provide two significant resources for engineers who now struggle to cope with this worsened security situation: (1)

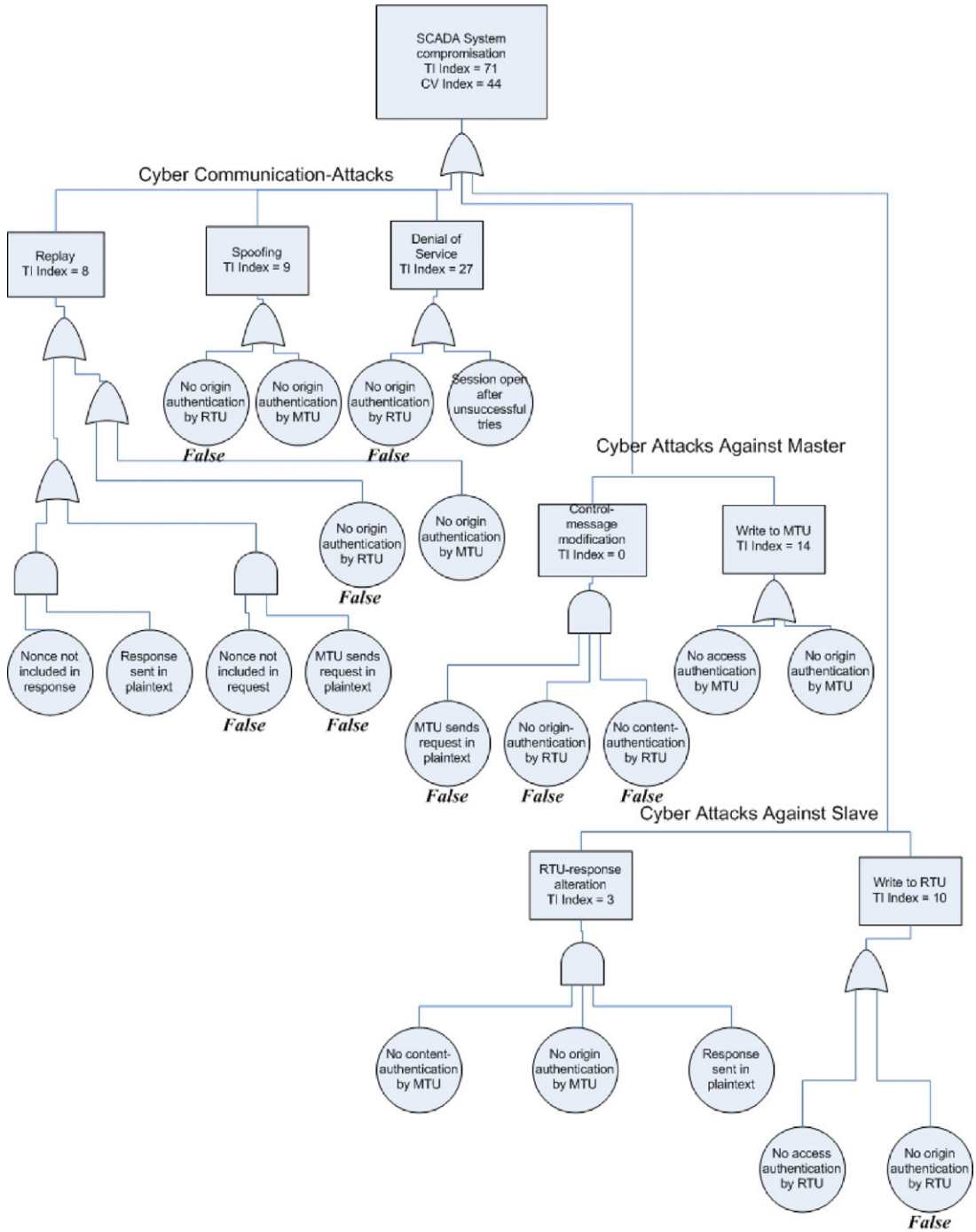

Fig. 4.1. Augmented vulnerability tree from case study [96].

it provides pointers to the set of guidelines, best practices, security tools and new technologies developed by governmental agencies (NIST, Sandia and Dept. of Homeland Security) and industrial associations (NERC, AGA and others), and (2) it provides an update on the advances in probabilistic risk assessment that can be applied to estimate the risk (exposure or expected loss) from SCADA and DCS installations. The paper also discusses and compares recently published approaches for quantifying the risk, threat impact and cyber-security of these networks.

Acknowledgments

This work was supported, in part, by a grant from the Dept. of Homeland Security through the Kentucky Critical Infrastructure Protection program. The authors would like to acknowledge comments and suggestions made by Dr. John Hoyt, Dr. Benjamin Arazi, Dr. Sandip Patel and Dr. Mostafa S. Mostafa. Any conclusions or opinions expressed in this paper are solely those of the authors.

References

[1] Critical Foundations—Protecting America's Infrastructures. Report of the president's commission on critical infrastructure protection, http://www.fas.org/sgp/library/pccip.pdf; 1997 [accessed 4.8.2006].

[2] Progress in Developing the National Asset Database. Office of the Inspector General, OIG-06-40. 2006.

[3] US-CERT (United States Computer Emergency Readiness Team) Control System Documents. US-CERT, http://www.us-cert.gov/control_systems/csdocuments.html; 2006 [accessed 2.5.2006].

[4] Nash T. An undirected attack against critical infrastructure, a case study for improving your control system security. US-CERT, http://www.us-cert.gov/control_systems/pdf/undirected_attack0905.pdf; 2005 [accessed 2006].

[5] Nelson T. Common control system vulnerability. US-CERT, http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf; 2005 [accessed 2.2006].

[6] National Infrastructure Protection Plan. DHS, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf; 2006 [accessed 11.1.2006].

[7] Carlson RE, Dagle JE, Shamsuddin SA, Evans RP. National SCADA testbed. A summary of control system security standards activities in the energy sector. National Laboratories, https://www.pcsforum.org/news/NSTB%20Security%20Standards%20Report.pdf; 2005 [accessed 2006].

[8] Evans RP, Hill RC, Rodriquez JG. A comparison of cross-sector cyber security standards. Idaho national laboratories, INL/EXT-05-00656, http://www.inl.gov/scada/publications/d/a_comparison_of_cross-sector_cyber_security_standards.pdf; 2005 [accessed 4.23.2006].

[9] Kilman D, Stamp J. Framework for SCADA security policy. Sandia national laboratories, SAND 2005-1002C, http://www.sandia.gov/scada/documents/sand_2005_1002C.pdf; 2005 [accessed 11.1.2006].

[10] Singer B, Weiss J. Control systems cyber security. Control Engineering, http://www.manufacturing.net/ctl/index.asp?layout=articlePrint%26articleID=CA501039; 2005 [accessed 2.4.2006].

[11] ANSI/ISA-TR99.00.01-2004. Security Technologies for Manufacturing and Control Systems. Instrument society of America, http://www.isa.org/Template.cfm?Section=Find_Standards%26template=/Ecommerce/ProductDisplay.cfm%26ProductID=7372; 2004 [accessed 4.21.2006].

[12] Instrument Society of America, ANSI/ISA-TR99.00.02-2004. Integrating electronic security into the manufacturing and control systems environment. Instrument Society of America, http://www.isa.org/Template.cfm?Section=Standards2%26template=/Ecommerce/ProductDisplay.cfm%26ProductID=7380; 2004 [accessed 4.11.2006].

[13] Cryptographic Protection of SCADA Communications, Part 1: Background, Policies, and Test Plan. AGA 12 Part 1. American Gas Association, http://www.aga.org/Template.cfm?Section=Operations_and_Engineering%26template=/ContentManagement/ContentDisplay.cfm%26ContentID=19329; 2006 [accessed 4.7.2006].

[14] Cyber Security Standards, CIP -002-1 – CIP-009-1. North American electric reliability council, http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html; 2006 [accessed 10.3.2006].

[15] Falco J, Stouffer K, Wavering A, Proctor F. IT Security for Industrial Control Systems. Intelligent Systems Division, National Institute of Standards and Technology (NIST) Gaithersburg, MD, in coordination with the Process Control Security Requirements Forum(PCSRF), http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf; 2006 [accessed 10.23.2006].

[16] Stouffer, Keith, Joe Falco, Fred Proctor. The NIST Process Control Security Requirements Forum (PCSRF) and the future of industrial control system security (2004 TAPPI paper summit—spring technical and international environmental conference). Atlanta (GA 30348-5113, United States): TAPPI Press; 2004.

[17] Melton R, Fletcher T, Earley M. System protection profile-industrial control systems (SPP-ICS) Version 1.0. NIST process control security requirements forum (PCSRF), http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.pdf; 2004 [accessed 10.23.2006].

[18] Stouffer K, Falco J, Kent K. NIST Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. NIST Process Control Security Requirements Forum (PCSRF), http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf; 2006.

[19] Trellue R. I3P Scada Security Research Plan Summary. I3P, 5-20-2005. http://www.thei3p.org/research/scada/scadasecresearchplan606.pdf; [accessed 2006].

[20] Kertzner P, Bodeau D, Nitschke R, Watters J, Young M, Stoddard M. Process control system security technical risk assessment: Analysis of problem domain. I3P, Research report No.3, www.thei3p.org; 2006 [accessed 2006].

[21] Stoddard M, Bodeau D, Carlson R, Glantz C, Haimes Y, Lian C, et al. Process control system security metrics-state of practice. I3P Research report No. 1, www.thei3p.org; 2005 [accessed 2.11.2006].

[22] Hildick-Smith A. Security for Critical Infrastructure SCADA Systems. SANS Institute White Paper, http://www.sans.org/reading_room/whitepapers/warfare/1644.php; 2005 [accessed 11.19.2006].

[23] Byres E, Lowe J. The Myths and facts behind cyber security risks for industrial control systems. Berlin (Germany): VDE Kongress; 2004.

[24] Brown T. Security in SCADA systems: How to handle the growing menace to process automation. Computing and Control Engineering 2005; 16(3):42–7.

[25] Supervisory Control and Data Acquisition (SCADA) Systems. National Communications System, Technical bulletin 04-1, http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf; 2006 [accessed 3.15.2007].

[26] Making the nation safer: The role of science and technology in countering terrorism. National Research Council; 2002.

[27] Fernandez JD, Fernandez AE. SCADA systems: Vulnerabilities and remediation. Journal of Computing Sciences in Colleges 2005;20(4): 160–8.

[28] Igure VM, Laughter SA, Williams RD. Security issues in SCADA networks. Computers & Security 2006;25(7):1–9.

[29] Kropp T. System threats and vulnerabilities [power system protection]. Power and Energy Magazine 2006;4(2):46–50.

[30] Smith C. Connection to public communications increases danger of cyber-attacks. Pipeline and Gas Journal 2003;230(2):20–4.

[31] Watts D. Security & vulnerability in electric power systems. In: 35th North American Power Symposium. 2003. p. 559–66.

[32] Oman P, Schweitzer E, Roberts J. Safeguarding IEDs, substations, and SCADA systems against electronic intrusions. In: Proceedings of the 2001 western power delivery automation conference. 2001. p. 9–12.

[33] 21 Steps to Improve Cyber Security of SCADA Networks. President's critical infrastructure protection board and department of energy report, http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf; 2002 [accessed 2.15.2006].

[34] Good Practice Guide for Process Control and SCADA Security. National infrastructure security coordination centre (NISCC) and PA consulting group, http://www.niscc.gov.uk/niscc/docs/re-20051025-00940.pdf?lang=en; 2005 [accessed 3.21.2006].

[35] Guidance for Addressing Cyber security in the Chemical Sector. Chemical industry data exchange (CIDX) report. Version 2.1, http://www.chemicalcybersecurity.com/cybersecurity_tools/CyberSecurityGuidanceMaster2_1.pdf; 2005 [accessed 4.18.2006].

[36] Information Security Risk Assessment Practices of Leading Organizations, A Supplement to GAO's May 1998 Executive Guide on Information Security Management. United states general accounting office (GAO) report GAO/AIMD-00-33, http://www.gao.gov/special.pubs/ai00033.pdf; 1999 [accessed 4.1.2006].

[37] Novak Russ. Merging SCADA and business processes. Plant Engineering 2005;59(5):35–6.

[38] Securing your SCADA and Industrial Control Systems. Version 1. Technical support working group guide, http://www.tswg.gov/tswg/ip/SCADA_GB_Short.pdf; 2005 [accessed 5.10.2006].

[39] Dacey RF. Critical infrastructure protection, challenges and efforts to secure control systems. United States general accounting office, GAO-04-354, http://www.gao.gov/new.items/d04354.pdf; 2004 [accessed 2.10.2006].

[40] Asenjo J. Cybersecurity for legacy SCADA systems. Utility Automation and Engineering T&D 2005;10(6):48–52.

[41] Battling the cyber menace. PEI Power Engineering International 2005; 13(6):123–5.

[42] Blume R. Mitigating Security Risks in SCADA/DCS System Environments. DYONYX, http://www.dyonyx.com/documents/SCADA_security.pdf; 2006 [accessed 2.4.2006].
[43] SAAD AY. Securing supervisory control and data acquisition systems: Plant utilities: A special report. Hydrocarbon processing (International Ed.) 2002; 81(7); 55–6.
[44] Miller A. Trends in process control systems security. Security & Privacy Magazine, IEEE 2005;3(5):57–60.
[45] Byres Eric, Lowe Justin. Insidious threat to control systems. InTech 2005; 52(1):28–31.
[46] Alper A. SCADA Security-Closing a Pandora's Box. Managing automation, http://www.managingautomation.com/maonline/channel/exclusive/read/5111813; 2005 [accessed 3.8.2006].
[47] Byres E, Franz M. Uncovering cyber flaws. InTech 2006;53(1):20–5.
[48] Strickles RP, Ozog H, Mohindra S. Security Vulnerability Assessment (SVA) Revealed. ioMosiac Corporation White Paper, http://archives1.iomosaic.com/whitepapers/SVA.pdf; 2003 [accessed 2.5.2006].
[49] Peterson D. Intrusion detection and cyber security monitoring of SCADA and DCS Networks. ISA: ISA Automation West; 2004.
[50] Creery A, Byres EJ. Industrial Cybersecurity for Power System and SCADA Networks. In: Industry applications society 52nd annual petroleum and chemical industry conference. 2005. p. 303–9.
[51] Geer D. Security of critical control systems sparks concern. Computer 2006;39(1):20–3.
[52] Carlson C. DHS to state its case to business. Eweek 2005;42:20.
[53] Honeywell reshapes industrial control world. Manufacturing Computer Solutions 2005;37.
[54] Pollett J. patriotSCADA Distributed Firewall for SCADA and Industrial Networks. Plantdata technologies whitepaper, http://www.controlglobal.com/whitepapers/wp_001_SCADApollet.pdf; 2006 [accessed 4.5.2006].
[55] Assante M, Pelgrin W, Wells R. Cyber security procurement language for control systems, Draft Version 1.4. Idaho National Laboratory National & Homeland Security Division, http://www.msisac.org/scada/documents/1-aug-06-scada-procurement-draft-1.4.pdf; 2006 [accessed 10.22.2006].
[56] Miller D, Byres E. Risk assessment: The first step. InTech 2005;52(3):68.
[57] RiskWorld list of software for risk assessment and management. Risk World, http://www.riskworld.com/SOFTWARE/SW5SW001.HTM; 2006 [accessed 4.10.2006].
[58] How to do a Complete Automated Risk Assessment: A Methodology Review. Riskwatch White Paper, http://www.riskwatch.com/news/whitepapers/How_To_Do_A_Complete_Automated_Risk_Assessment_10-02RW.pdf; 2002 [accessed 4.1.2006].
[59] Alberts C, Dorofee A, Stevens J, Woody C. Introduction to the OCTAVE Approach. CERT Coordination Center, http://www.cert.org/octave/approach_intro.pdf; 2003 [accessed 4.9.2006].
[60] Aagedal J, den Braber F, Dimitrakos T, Gran BA, Raptis D, Stolen K. Model-based risk assessment to improve enterprise security. In: Proceedings of the sixth international distributed object computing conference. 2002.
[61] Auerswald PhilipE, Branscomb LewisM, La Porte ToddM, Michel-Kerjan ErwanO. Seeds of disaster, roots of response. New York: Cambridge University Press; 2006.
[62] Campbell P, Stamp J. A classification scheme for risk assessment methods. Sandia National Laboratory, SAND2004-4233. 2004.
[63] Farahmand F, Navathe SB, Enslow PH, Sharp GP. Managing vulnerabilities of information systems to security incidents. In: Proceedings of the 5th international conference on electronic commerce. ACM Press; 2003.
[64] Rinaldi Steven M. Modeling and simulating critical infrastructures and their interdependencies. In: Proceedings of the Hawaii international conference on system sciences. Piscataway (Piscataway, NJ): Institute of Electrical and Electronics Engineers Computer Society; 2004.
[65] Haimes YY. Hierarchical holographic modeling. IEEE Transactions on Systems, Man, and Cybernetics 1981;11(9):606–17.
[66] Haimes YY. Risk modeling, assessment, and management. 1st ed. New York: John Wiley and Sons; 1998.
[67] Chittester CG, Haimes YY. Risks of terrorism to information technology and to critical interdependent infrastructures. Journal of Homeland Security and Emergency Management 2004;1(4).
[68] Ezell BC. Thesis/dissertation. University of Virginia: Systems Engineering Department; 1998.
[69] Haimes YY, Kaplan S, Lambert JH. Risk filtering, ranking, and management framework using hierarchical holographic modeling. Risk Analysis 2002;22(2):381–95.
[70] Haimes YY, Chittester CG. A roadmap for quantifying the efficacy of risk management of information security and interdependent scada systems. Journal of Homeland Security and Emergency Management 2005;2(2): Article 12.
[71] Crowther KennethG, Haimes YacovY. Application of the inoperability input–output model (IIM) for systemic risk assessment and management of interdependent infrastructures. Systems Engineering 2005;8(4): 323–41.
[72] Crowther KG, Dicdican RY, Leung MF, Lian C, Haimes YY, Lambert JH, et al. Assessing and Managing Risk of Terrorism to Virginia's Interdependent Transportation Systems. Virginia Transportation Research Council, VTRC 05-CR6, http://virginiadot.org/vtrc/main/online_reports/pdf/05-cr6.pdf; 2004 [accessed 3.15.2006].
[73] Nozick LindaK, Turnquist MarkA, Jones DeanA, Davis JenniferR, Lawton CraigR. Assessing the performance of interdependent infrastructures and optimizing investments. In: Proceedings of the hawaii international conference on system sciences. Piscataway (NJ 08855-1331, United States): Institute of Electrical and Electronics Engineers Computer Society; 2004. Big Island, HI., United States.
[74] Nozick LK, Turnquist MA, Jones DA, Davis JR. Assessing the performance of interdependent infrastructures and optimizing investments. International Journal of Critical Infrastructures 2005;1(2):144–54.
[75] Kumamoto H, Henley EJ. Probabilistic risk assessment and management for engineers and scientists. 2nd ed. New York: IEEE Press; 1996.
[76] Kaplan Stanley, Garrick B John. On the quantitative definition of risk. Risk Analysis 1981;1(1):11–37.
[77] Stamatelalos M. Probabilistic risk assessment procedure guide for NASA managers and practitioners. NASA office of safety and mission assurance, http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf; 2002 [accessed 4.18.2006].
[78] Vesely W, Stamatelalos M, Dugan J, Fragola J, Minarick J. Fault tree handbook with aerospace applications. Report by NASA Office of Safety and Mission Assurance, http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf; 2002 [accessed 2006].
[79] Vesely W. Fault Tree Analysis (FTA): Concepts and Applications. http://www.hq.nasa.gov/office/codeq/risk/ftacourse.pdf; 1998 [accessed 2006].
[80] Walker RW. Assessment of technical risks. In: Proceedings of the 2000 IEEE international conference on management of innovation and technology. 2000.
[81] Yacoub SherifM, Ammar HanyH. A methodology for architecture-level reliability risk analysis. IEEE Transactions on Software Engineering 2002;28(6):529–47.
[82] Yacoub Sherif M, Ammar Hany H, Robinson Tom. Methodology for architectural-level risk assessment using dynamic metrics. In: Proceedings of the international symposium on software reliability engineering, ISSRE. Los Alamitos (San Jose, CA, USA): Institute of Electrical and Electronics Engineers Computer Society; 2000.
[83] Wyss GregoryD, Duran FeliciaA, Dandini VincentJ. An object-oriented approach to risk and reliability analysis: Methodology and aviation safety applications. Simulation 2004;80(1):33–43.
[84] Madan BharatB, Goseva-Popstojanova Katerina, Vaidyanathan Kalyanaraman, Trivedi KishorS. Modeling and quantification of security attributes of software systems. In: Proceedings of the 2002 international conference on dependable systems and networks. Washington (DC, United States): IEEE Computer Society; 2002.
[85] Taylor C, Krings A, Alves-Foss J. Risk analysis and probabilistic survivability assessment (RAPSA): An assessment approach for power substation hardening. In: Proc. ACM workshop on scientific aspects of cyber terrorism. 2002. p. 1–9.
[86] de Ru WG, Eloff JHP. Risk analysis modeling with the use of fuzzy logic. Computers & Security 1996;15(3):239–48.
[87] Wat FKT, Ngai EWT. Risk analysis in electronic commerce development

using fuzzy set. In: Annual conference of the north american fuzzy information processing society. Vancouver (BC, Canada): Institute of Electrical and Electronics Engineers Inc.; 2001.

[88] Choi HyunHo, Cho HyoNam, Seo JW. Risk assessment methodology for underground construction projects. Journal of Construction Engineering and Management 2004;130(2):258–72.

[89] Pillay A, Wang J. Risk assessment of fishing vessels using fuzzy set approach. International Journal of Reliability, Quality and Safety Engineering 2002;9(2):163–81.

[90] Schneier B. Attack Trees. Dr. Dobb's Journal 1999;24(12):21–9.

[91] Moore A, Ellison R, Linger R. Attack modeling for information security and survivability. Technical note, CMU/SEI-2001-TN-001, 3-15-2001. Software Engineering Institute, Carnegie Mellon University.

[92] Byres EJ, Franz M, Miller D. The use of attack trees in assessing vulnerabilities in SCADA systems. In: International infrastructure survivability workshop. Lisbon (Portugal): IEEE; 2004.

[93] Vidalis S, Jones A. Using vulnerability trees for decision making in threat assessment. University of Glamorgan, School of Computing Technical report CS-03-2, http://www.glam.ac.uk/socschool/research/publications/technical/CS-03-2.pdf; 2003 [accessed 2006].

[94] Tolbert GD. Residual risk reduction. Professional Safety. 2005. p. 25–33.

[95] McQueen MA, Boyer WF, Flynn MA, Beitel GA. quantitative cyber risk reduction estimation methodology for a Small SCADA control system. In: Proceedings of the 39th annual hawaii international conference on system sciences. 2006.

[96] Graham J, Patel S, Ralston P. Security enhancement for scada communication protocols using augmented vulnerability trees. In: 19th international conference on computer applications in industry and engineering. 2006.

[97] Cohen F. Simulating cyber attacks, defenses, and consequences. Computers & Security 1999;18(6):479–518.

[98] Rakaczky E. Building a Security Business Case. Invensys, https://www.pcsforum.org/events/2005/fall/pdf/Building%20a%20Security%20Business%20Case2a.pdf; 2005.

Patricia A.S. Ralston is Professor and Acting Chair of the Department of Engineering Fundamentals and an Associate in Chemical Engineering at the J. B. Speed School of Engineering at the University of Louisville. She received her Master of Engineering and Ph.D. degrees in Chemical Engineering from the University of Louisville in 1980 and 1983 respectively. Her fields of expertise include process modeling, simulation, and process control. She has specific research interests in process monitoring, fault detection, and security of SCADA systems. Dr. Ralston also teaches mathematics courses for all engineering undergraduates.

James H. Graham is the Henry Vogt Professor of Computer Science and Engineering at the University of Louisville. He has over thirty years of experience in computing and electrical engineering. Prof. Graham has served as a faculty member at Rensselaer Polytechnic Institute and as a product engineer with General Motors Corporation. He received his M.S. and Ph.D. from Purdue University in 1978 and 1980 respectively. He is a senior member of the IEEE and a registered professional engineer. His research interests involve information security, algorithms for computational science, intelligent systems, distributed computing, and computer simulation applications.

Jeffrey L. Hieb is a doctoral candidate in computer science and engineering and a graduate research assistant at the University of Louisville. His research interests include Honeypots, security for process control systems, and operating system. Hieb received a B.S. in computer science from Furman University and an M.S. in computer science from the University of Louisville. He is a student member of the IEEE and the ACM.