Intelligent Systems Research Laboratory

Technical Report TR-ISRL-06-01

Dept. of Computer Engineering and Computer Science
University of Louisville
Louisville, KY 40292

July 2006

Literature Review of Security and Risk Assessment of SCADA and DCS Systems

Dr. Patricia A. Ralston, Dr. James H. Graham and Dr. Sandip C. Patel.

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 SCADA and DCS systems. Industry organizations such as NERC and AGA as well as government organizations like NIST and SANDIA are responding to the cyber security threat faced by control systems and critical infrastructure through the development of guidelines, best practices, test beds, security tools and new technology. Published papers such as (Byres and Lowe, 2005; Miller, 2005; and Greer, 2006) describe the threats and vulnerabilities faced by SCADA and DCS systems and the challenges presented in attempting to secure these systems. Other papers, such as (Byres and Franz, 2006, Strickles, et al 2003) describe the application of existing security technologies and security practices. The articulation of risk is an important component of a comprehensive, realistic, and long term commitment to securing SCADA and DCS systems. Risk assessment methods such as HHM, IIM, and RFRM have been successfully applied to SCADA systems and have highlighted the need for quantifiable metrics. Quantifiable risk analysis falls under the general category of probability risk analysis (PRA) which includes methods like FTA, ETA, and FEMA. What is needed for SCADA and DCS cyber security risk analysis is to quantitatively determine the probability of an attack, the impact of the attack, and the reduction in risk associated with a particular countermeasure. Two recent methods, one based on compromise graphs and one on augmented vulnerability trees, have specifically targeted SCADA security.

Keywords: SCADA, DCS, risk analysis, vulnerability.

Overview and Historical Perspective

Protecting the critical infrastructure of the United States is essential for physical and economic security of its citizens. Beginning with the report from the President's Commission on Critical Infrastructure Protection, the government recognized that the country relied on increasingly vulnerable, interconnected physical and cyber infrastructures (Commission Report, Oct. 1997).

The Department of Homeland Security (DHS), through various agencies and groups, is primarily responsible for all aspects of infrastructure protection. The Control Systems Security Program (CSSP) of the National Cyber Security Division (NCSD) of DHS leads the comprehensive national initiative to secure our nation's critical infrastructure by identifying, analyzing, and reducing cyber risks associated with the control systems that govern our infrastructures http://www.us-cert.gov/control_systems/. Established in 2003 to protect the nation's Internet infrastructure, US-CERT (Computer Emergency Readiness Team) coordinates defense against and responses to cyber attacks across the nation. It is the operational arm of the National Cyber Security Division at DHS and publishes documents to assist in determining vulnerabilities and improving control system security (Nash, 2005, Nelson, 2005). 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, contributes expertise for protecting the nation's information infrastructure by coordinating defense against and response to cyber attacks working jointly with DHS.

The objectives of the most recent National Infrastructure Protection Plan (NIPP v.2, Jan. 2006) include building security partnerships to implement critical infrastructure protection programs, assess risk and implement risk reduction programs, and maximize use of resources. Risk assessment for all cyber systems including SCADA and DCS systems are an integral part of the document that aims to provide a national unifying structure to all protection efforts. What is necessary, and what is occurring, is a cooperative effort between government, industry, and academia to address all issues related to securing our infrastructures.

Government and Industry Groups: Research/Guideline Contributions

Information Sharing and Analysis Centers (ISACs, http://www.ni2ciel.org/ISACs) were created by the Presidential Directive 63 (http://www.fas.org/irp/offdocs/pdd/pdd-63.htm, but are independent organizations. They were designed to share important information about vulnerabilities, threats, intrusions and anomalies within and between industry sectors and the government.

The Idaho National Engineering and Environmental Laboratory (INEEL) in conjunction with the Sandia National Laboratory have created the National SCADA Test Bed in a setting that includes a functioning power grid and synergistic cyber and wireless test beds, http://www.inl.gov/nationalsecurity/capabilities/security/index.shtml. Sandia National Laboratory has created The Center for SCADA Security (http://www.sandia.gov/scada/home.htm), where SCADA research, training, red teams, and standards development takes place. In addition to pure research, the National SCADA Testbed Program work includes supporting the development of industry standards covering cyber

security of control systems. Two reports summarize these activities to date, (Carlson, et al, 2005 and Evans, et al, 2005). Researchers at Sandia recently developed and published a SCADA Security Policy Framework (Kilman and Stamp, 2005) which ensures all critical topics have been adequately addressed by specific policy rather than relying on standard IT security policy.

In addition to full-fledged research activities like those at national laboratories, standards bodies and industry groups are working to address the needs of control system security (Singer and Weiss, 2005). 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 Engineering Consortium), 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. Links are provided to 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 (ANSI/ISA-TR99.00.01-2004, ANSI/ISA-TR99.00.02-2004), and AGA documents on communications encryption (AGA 12, Part 1, 2006, final document, and ongoing work parts 2, 3 and 4 which extend encryption to legacy systems, networked systems, and embedding capabilities during the manufacturing process). NERC has finalized cyber security standards (CIP-002-1 – CIP-009-1, 2006) that will establish the requirements for security management programs, electronic and physical protection, personnel, incident reporting, and recovery plans (2006), and 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 for various industries (Falco, et al), (Stouffer et al, 2004), (Melton et al, 2004).

Perhaps the most ambitious group created and funded by the 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 in response to the growing vulnerability of infrastructure control systems in the increasingly computerized, automated and interdependent operating environment, it is managed by a public/private Interim Governing Board. 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. https://www.pcsforum.org/news/SCADAwg.pdf. 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 PCS and SCADA systems. 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. All of these groups’ reports and guidelines highlight the need for risk analysis and assessment, however, guidance on the actual analysis of the risk assessment is not always specific.

The Institute for Information Infrastructure Protection (I3P) 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 (Trellue et al, I3P SCADA Security Research Plan Summary, May 2005), a SCADA project that is investigating ways to advance the security of process control systems (PCS). A main task is to develop a risk assessment methodology and tool to support development of inherently secure SCADA and PCS systems. (Kertzner, et al, Research Report No.3, Jan. 2006). Another report (Stoddard et al, Research Report No. 1, August 2005) 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 Supervisory Control And Data Acquisition systems (SCADA), is found in a SANS Institute paper (Hildick-Smith 2005). The SANS (System Administration Audit Network Security) Institute, created in 1989, provides training and performs research in information security. The British Columbia Institute of Technology Industrial Security Incident Database reported in 2004 (Byres and Lowe, 2004) 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.

Awareness of the Issues

Numerous articles and guides have been published recently to aid SCADA and PCS 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 (DOE white paper 2002). The United Kingdom has a similar guide, the National Infrastructure Security Coordination Centre (NISCC) Good practice guide (2005) and other SCADA security documents available at http://www.niscc.gov.uk/niscc/scada-en.html. The Chemical Industry Data Exchange has many guidance documents (May 2005) and white papers available at http://www.chemicalcybersecurity.com/online_information/whitepapers.cfm, and other papers are available for download at the Chemical Sector Cyber Security Program website http://www.chemicalcybersecurity.com/cybersecurity_tools/whitepapers.cfm.
With the widespread use of the internet, SCADA and Distributed Control Systems (DCS) are more vulnerable to attack. Many papers, reports, and discussions from system vendors, security experts, industry, and the government have recognized this and alerted researchers and plant managers. The General Accounting Office in 1999 issued a guide (GAO/AIMD-00-33) 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 PCS 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 (Novak, 2005). A more recent guide (2005) 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 http://www.tswg.gov/tswg/ip/SCADA_GB_Short.pdf

A General Accounting Office Report (2003) most succinctly identified the trends that have escalated the risks to these systems: adoption of standardized technologies with known vulnerabilities, connectivity of control systems to other networks, constraints on 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 security challenges comparable to 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 (Asenjo, 2005).

Much information has focused on becoming aware of the growing problem of securing SCADA and PCS systems, recognizing the threats, and learning how to find solutions (Anonymous, June 2005, Blume, DYONYX white paper, Saad, 2002, Singer and Weiss, 2005, Miller 2005, Byres and Lowe, 2005, Alper 2005). Several introduce and explain applicable security technology like vulnerability testing and assessment (Byres and Franz, 2006, Strickles, et al 2003), intrusion detection and security monitoring of networks (Peterson, 2004), and encryption, network architecture and system hardware hardening (Creery and Byres, 2005), and hardening operating systems (Geer, 2006). Geer's article 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.

DHS sees a need for commercial owners of critical infrastructure to invest in more secure networks and SCADA system vendors should be encouraged to build security in to their products (C. Carlson, 2005). Some of these are 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 (Anonymous, May 2005). Plantdata Technologies (Pollett, 2006) 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. Byres and Franz (2006) 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. As standards bodies, vendors, and users cooperate and get more experience with proper security expectation and testing, it can become an embedded and expected quality assurance issue.

Overview of Risk Assessment

Miller and Byres, (2005), 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 at the Riskworld website http://www.riskworld.com/SOFTWARE/SW5SW001.HTM.

Commercial systems like 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 (RiskWatch white paper, 2002).

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) , (Alberts, et al, 2003) 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 (Aagedal, et al, 2002) 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 is maintained http://coras.sourceforge.net/ 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).

A Sandia National Laboratories report (Campbell and Stamp, 2004) 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.

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 multi-phase 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 (2003), present a qualitative, but very systematic approach to overall risk assessment for information systems. Especially helpful is their development of a 3 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 evaluates 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 (Rinaldi, 2004). Such modeling and simulation abilities are integral to infrastructure risk analyses.

In such cases, the most comprehensive risk identification methodology is hierarchical holographic modeling (HHM), (Haimes, 1981, 1998). This method is described as one that can identify all conceivable sources of risk to SCADA systems and to any infrastructure that uses them. 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 (Ezell, 1998). This method has been used to identify sources of risk to SCADA systems in the railroad sector (Chittester and Haimes, 2004).

Haimes, Kaplan, and Lambert (2002) 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,

(2005), 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 internet protocol 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 Crowther and Haimes, 2005.

Crowther, et al, (2004) 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 (Nozich, et al, 2005) 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.

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 like HHM, but rather assumes 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 (Henley and Kumamoto, 1996). 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 3 questions: What can go wrong? How likely is it? What are the consequences? (Kaplan and Barrick,1981). 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. RPA quantifies "risk metrics", a term that refers to a consequence-oriented figure of merit, such as the probability of the top event (Stamatelalos, 2002). Determination of needed basic event probabilities is the most difficult task in applying this technique. Many references explain all aspects of PRA in great detail (Stamatelalos, 2002, Henley and Kumamoto, 1996).

Fault Tree Analysis, Failure Mode Effect Analysis – FTA, FMEA

FTA (fault tree analysis), (Vesely, et al, 2002), 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 type of events and relationships 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 (Stamatelalos, 2002).

Inductive approaches such as FMEA and FMECA are forward stepping and begin with an initiating event then induce the end effects (Vesely, et al, 2002) It is important to note that theses methods analyze single component faults and their system effects and do not consider combinations of faults. Walker, (2000), 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 get a complete set of accident sequences depending on the complexity of the system.

PRA Extensions or Modifications

Yacoub and Ammar (2002), present a methodology for architecture-level risk analysis. Their approach is based on dynamic risk metrics (Yacoub, et al, 2000) that define complexity factors for architecture elements obtained from simulation of the software architecture specifications. FMEA is used with simulation to determine effects of a failure, and these results 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 (2004) 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, (2002), 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, (2002), 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 studies of risk analysis related to computer security, fuzzy modeling was used to analyze and rank risks in a computing facility, (de Ru and Eloff, 1996). 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 calculate a severity of loss for different components and then a total project risk in electronic commerce development (Wat and Ngai, 2001).

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 (Choi, et al, 2004).

Pillay and Wang, (2002) 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.

Attack Trees and Vulnerability Trees

Attack trees were introduced by Schneier (1999) 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 are not failure rates. Schneier's work is notable because it 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, (2001) 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 (Byres, et al, 2004). 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 (Vidalis and Jones, 2003). Vulnerability trees help security analysts understand and analyze different attack scenarios that a threat agent might follow to exploit a vulnerability. With this understanding, countermeasures can be taken.

Risk Reduction

What is needed is a way to quantitatively determine the probability of a particular attack, the impact of that attack, and a way to determine the reduction in risk if a particular countermeasure is taken.

The ability to determine whether or not risk reduction is achieved when modifications are made is important. Simple calculations for risk reduction have been published (Tolbert, 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.

McQueen, et al, (2006) recently published results of a promising method to calculate risk reduction estimates for a SCADA system and a set of control system remedial actions. The method employed a directed graph (compromise graph) where the nodes represent stages of a potential attack and the edges represent expected time-to-compromise for differing attacker skill levels.

Probabilistic Risk Assessment provides for calculation of risk reduction when applied to SCADA security. If a lower event probability of a specific threat can be set to zero by the addition of a security enhancement, the effect on the top event probability of an overall attack can be computed. Graham, Patel, and Ralston (2006) have recently developed a risk modeling tool with two indices for quantifying risk associated with SCADA systems. Their work makes use of augmented vulnerability trees which combine attack tree and vulnerability tree methods.

References

J. Aagedal, F. den Braber, T. Dimitrakos, B.A. Gran, D. Raptis, K. Stolen, "Model-based Risk Assessment to Improve Enterprise Security," Proceedings of the Sixth International Distributed Object Computing Conference, 2002, 12 pages.

J. Abshier, "Ten Principles for Securing Control Systems," ControlGlobal.com, October 2005, http://www.controlglobal.com/articles/2005/498.html, accessed February 2006.

A. Alper, "SCADA Security – Closing a Pandora's Box," http://www.managingautomation.com/maonline/channel/exclusive/read/5111813, posted September 2005, accessed March 2006.

C. Alberts, A. Dorofee, J. Stevens, C. Woody, "Introduction to the OCTAVE Approach," CERT-CC white paper, August 2003, 37 pages, http://www.cert.org/octave/approach_intro.pdf, accessed April 2006.

American Gas Association (AGA), "Cryptographic Protection of SCADA Communications, Part 1: Background, Policies, and Test Plan, AGA 12 Part 1," March 14, 2006, 123 pages, http://www.aga.org/Template.cfm?Section=Operations_and_Engineering&template=/ContentManagement/ContentDisplay.cfm&ContentID=19329, accessed April 2006.

ANSI/ISA-TR99.00.01-2004 Security Technologies for Manufacturing and Control Systems," ISA, http://www.isa.org/Template.cfm?Section=Find_Standards&template=/Ecommerce/ProductDisplay.cfm&ProductID=7372, accessed April 2006.

ANSI/ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment," ISA, http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=7380, accessed April. 2006.

Anonymous, "Battling the Cyber Menace," Power Engineering International, Vol. 13, No. 6, June 2005, p.123.

Anonymous, "Honeywell Reshapes Industrial Control World," Manufacturing Computer Solutions, May 2005, p. 37.

J. Asenjo, "Cybersecurity for Legacy SCADA Systems," Utility Automation and Engineering T&D, Vol. 10, no. 6, Sep/Oct 2005, pp. 48-52.

A. Baker et al, "A Scalable Systems Approach for Critical Infrastructure Security," Sandia Laboratories Report, April 2002, 54 pages, http://www.sandia.gov/scada/documents/020877.pdf, accessed April 2006.

R. Blume, “Mitigating Security Risks in SCADA/DCS System Environments,” Dyonyx White Paper, http://www.dyonyx.com/documents/SCADA_security.pdf, accessed February 2006.

S. Butler, “Security Attribute Evaluation Method: A Cost-Benefit Approach,” Proceedings of the 24th International Conference on Software Engineering, Orlando Florida, 2002, pp. 232-240.

E. Byres, J. Lowe, “The Myths and Facts behind Cyber Security Risks for Industrial Control Systems,” VDE Congress, Berlin, October 2004, 5 pages.

E. Byres, M. Franz, D. Miller, “The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems,” International Infrastructure Survivability Workshop (IISW’04), IEEE, Lisbon, Portugal, Dec. 4, 2004, 9 pages.

E. Byres, “Who Turned Out the Lights?,” http://www.pnwer.org/meetings/Summer2005/Presentations/HLS/HLS_Byres Lights.pdf, accessed April 2006.

E. Byres, M. Franz, “Uncovering Cyber Flaws,” http://www.isa.org/InTechTemplate.cfm?Section=Article_Index1&template=/ContentManagement/ContentDisplay.cfm&ContentID=50583, January 1, 2006, accessed March 2006.

E. Byres, J. Lowe, “Insidious Threat to Control Systems,” InTech, Vol. 52, no.1, 2005, p.28.

P. Campbell, J. Stamp, “A Classification Scheme for Risk Assessment Methods,” Sandia National Laboratory Report August 2004, SAND2004-4233.

C. Carlson, “DHS to state its case to business,” eweek, Issue 42, October 31, 2005, p. 20.

R.E. Carlson, J.E. Dagle, S.A. Shamsuddin, R.P. Evans, “National SCADA Testbed, A Summary of Control System Security Standards Activities in the Energy Sector,” October 2005, 48 page report by National Laboratories, https://www.pcsforum.org/news/NSTB%20Security%20Standards%20Report.pdf, accessed February, 2006.

C.G. Chittester, Y.Y. Haimes, “Risks of Terrorism to Information Technology and to Critical Interdependent Infrastructures,” Journal of Homeland Security and Emergency Management, Vol.1, Issue 4, 2004, article 402.

H.Choi, H. Cho, J. W. Seo, “Risk Assessment Methodology for Underground Construction Projects,” Journal of Construction Engineering and Management, March/April 2004, pp. 258-272.

A. Creery, E.J. Byres, “Industrial Cybersecurity for Power System and SCADA Networks, IEEE paper PCIC-2005-34, pp. 303-309.

"Critical Foundations – Protecting America's Infrastructures," Report of the President's Commission on Critical Infrastructure Protection, October 1997, 192 pages, http://www.tsa.gov/interweb/assetlibrary/Infrastructure.pdf, accessed April 2006.

K.G. Crowther, R.Y. Dicdican, M.F. Leung, C. Lian, Y.Y. Haimes, J.H. Lambert, B.M. Horowitz, J.R. Santos, "Assessing and Managing Risk of Terrorism to Virginia's Interdependent Transportation Systems," Final Contract Report to Virginia Transportation Research Council (VTRC 05-CR6), Center for Risk Management of Engineering Systems, University of Virginia, Charlottesville, VA (October 2004), 56 pages, http://virginiadot.org/vtrc/main/online_reports/pdf/05-cr6.pdf, accessed March 2006.

K.G. Crowther, Y.Y. Haimes, "Application of the Inoperability Input-Output Model (IIM) for Systemic Risk Assessment and Management of Interdependent Infrastructures," Systems Engineering, Vol. 8, No. 4, 2005, pp. 323-341.

R.F. Dacey, "Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems," GAO Report, March 2004, 47 pages, http://www.gao.gov/new.items/d04354.pdf, accessed February 2006.

W.G. de Ru, J. H. P. Eloff, "Risk Analysis Modelling with the Use of Fuzzy Logic," Computers and Security, Vol. 15, No. 3, 1996, pp. 239-248.

J. Eisenhauer, P. Donnelly, M. Ellis, M. O'Brien, "Roadmap to Secure Control Systems in the Energy Sector," Report sponsored by US DOE and DHS, January 2006, 58 pages, http://www.controlsystemsroadmap.net/pdfs/roadmap.pdf, accessed February 2006.

R.P. Evans, R.C. Hill, J.G. Rodriquez, "A Comparison of Cross-Sector Cyber Security Standards," Idaho National Laboratories Report, September 2005, 36 pages, http://www.inl.gov/scada/publications/d/a_comparison_of_cross-sector_cyber_security_standards.pdf, accessed April 2006.

S. Evans, D. Heinbuch, E. Kyle, J. Piorkowski, J. Wallner, "Risk-Based Systems Security Engineering: Stopping Attacks with Intention," IEEE Security and Privacy, November/December 2004, pp.59-62.

B.C. Ezell, "Risks of Cyber Attacks to Supervisory Control and Data Acquisition for Water Supply," Thesis, University of Virginia, May 1988, http://www.riskinfo.com/cyberisk/Watersupply/SCADA-thesis.html accessed online March 2006.

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

F. Faramand, S. Navathe, G. Sharp, P. Enslow, "Managing Vulnerabilities of Information Systems to Security Incidents," ACM Intl. Conf. Proceedings Series, Vol. 50, ICEC, 2003, pp. 348-354.

C. Gan, E. Scharf, "Building an Experience Factory for a Model-based Risk Analysis Framework," http://sunsite.informatik.rwth-aachen.de/Publications/CEUR-WS//Vol-67/gwem2003-GS.pdf, accessed March 2006.

D. Geer, "Security of Critical Control Systems Sparks Concern," Computer, January, 2006, pp. 20-23.

"Good Practice Guide for Process Control and SCADA Security," National Infrastructure Security Coordination Centre (NISCC) and PA Consulting Group, October 2005, 20 pages, http://www.niscc.gov.uk/niscc/docs/re-20051025-00940.pdf?lang=en, accessed February 2006.

J. Graham, S. Patel, P. Ralston, "Security Enhancement for SCADA Communication Protocols using Augmented Vulnerability Trees," submitted to CAINE 2006.

"Guidance for Addressing Cyber security in the Chemical Sector," Chemical Industry Data Exchange (CIDX) Report, Version 2.1, May 2005, http://www.chemicalcybersecurity.com/cybersecurity_tools/CyberSecurityGuidanceMaster2_1.pdf, accessed April 2006.

Y. Y. Haimes, "Hierarchical Holographic Modeling," IEEE Transactions on Systems, Man, and Cybernetics, Vol. 11, No. 9, pp. 606-617, 1981.

Y. Y. Haimes, Risk Modeling, Assessment, and Management, First Edition, New York: John Wiley and Sons, 1998.

Y.Y. Haimes, C.G. Chittester, "A Roadmap for Quantifying the Efficacy of Risk Management of Information Security and Interdependent SCADA Systems," Journal of Homeland Security and Emergency Management, Vol. 2, Issue 2, 2005, article 12.

Y.Y. Haimes, S. Kaplan, J.H. Lambert, "Risk Filtering, Ranking, and Management Framework using Hierarchical Holographic Modeling," Risk Analysis, Vol. 22, No. 2, pp. 381-395, 2002.

Y.Y. Haimes, J. H. Lambert, B.M. Horowitz, J.R. Santos, "Assessing and Managing Risk of Terrorism to Virginia's Interdependent Transportation Systems," Virginia Transportation Research Council Final Contract Report, VTRC 05-CR6, October 2004.

E. Henley, H. Kumamoto, Probabilistic Risk Assessment, 2nd edition, IEEE Press, New York, 1996.

A. Hildick-Smith, "Security for Critical Infrastructure SCADA Systems," SANS Institute White Paper, February 2005, 19 pages.

B. Hope, “Using Fault Tree Analysis to Assess Bioterrorist Risks to the U.S. Food Supply,” Human and Ecological Risk Assessment, Vol. 10, 2004, pp. 327-347.

Idaho National Laboratory National Test Bed Program, http://www.inl.gov/scada/standards/index.shtml, updated April 2006, accessed April 2006.

S. Kaplan, B. J. Garrick, “On the Quantitative Definition of Risk,” Risk Analysis, Vol. 1, No. 1, 1981, pp. 11-37.

P. Kertzner, D. Bodeau, R. Nitschke, J Watters, M. Young, M. Stoddard, “Process Control System Security Technical Risk Assessment: Analysis of Problem Domain,” Research Report No. 3, January 2006, I3P, www.thei3p.org, accessed Feb. 2006.

D. Kilman, J. Stamp, “Framework for SCADA Security Policy,” http://www.sandia.gov/scada/documents/sand_2005_1002C.pdf, accessed April 2006.

M. Lathrop, J.M.D. Hill, J.R. Surdu, “Modeling Network Attacks,” http://www.itoc.usma.edu/surdu/Documents/BRIMSMAADNET.pdf, accessed April 2006.

L. Liu, S.Y. Cheng, H.G. Guo, “A Simulation-Assessment Modeling Approach for Analyzing Environmental Risks of Groundwater Contamination at Waste Landfill Sites,” Human and Ecological Risk Assessment, Vol. 10, 2004, pp. 373-388.

B.B. Madan, K. Goseva-Popstojavova, K. Vaidyanathan, K.S. Trivedi, “Modeling and Quantification of Security Attributes of Software Systems,” Proceedings of the International Conference on Dependable Systems and Networks, Washington, D.C., 2002, 10 pages, http://srel.ee.duke.edu/PAPERS/revised-paper.pdf, accessed April 2006.

M. A. McQueen, W.F. Boyer, M.A. Flynn, G.A. Beitel, “Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System,” Proceedings of the 39th Hawaii International Conference on System Sciences, January, 2006. http://csdl2.computer.org/comp/proceedings/hicss/2006/2507/09/250790226.pdf.

R. Melton, T. Fletcher, M. Earley, “System Protection Profile-Industrial Control Systems (SPP-ICS) Version 1.0, April 14, 2004, 151 pages,” http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.pdf, accessed April 2006.

R. Merritt, “A Word About Cyber Security,” ControlGlobal.com, January 2006, http://www.controlglobal.com/articles/2006/004.html, accessed April 2006.

A. Miller, “Trends in Process Control Systems Security,” IEEE Security and Privacy, September/October 2005, pp.57-60.

D. Miller, E. Byres, “Risk Assessment: The First Step,” InTech, Vol. 52, no. 3, 2005, p. 68.

A. Moore, R. Ellison, R. Linger, "Attack Modeling for Information Security and Survivability," Technical Note, CMU/SEI-2001-TN-001, Software Engineering Institute, Carnegie Mellon University, March 2001.

J. Murdock, "Security Measurement," White Paper prepared by Practical Software and Systems Measurement, July 2005, http://www.psmsc.com/Downloads/Other/Security%20White%20Paper%202.0.pdf, accessed March 2006.

D. Mussington, "Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development," monograph published by RAND, Santa Monica, CA, 2002, 100 pages, http://www.rand.org/pubs/monograph_reports/2005/MR1259.pdf, accessed April 2006.

T. Nash, "An Undirected Attack against Critical Infrastructure, A Case Study for Improving Your Control System Security," US-CERT Control Systems Security Center Document, September 2005, 11 pages, http://www.us-cert.gov/control_systems/pdf/undirected_attack0905.pdf, accessed April 2006.

National Infrastructure Protection Plan, Base Plan, Revised Draft V2, January 2006, 213 pages, http://www.ni2ciel.org/NIPC/Revised-Draft-NIPP-v2.0.pdf, accessed February 2006.

T. Nelson, "Common Control System Vulnerability," US-CERT Document, November 2005, 7 pages, http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf, accessed February 2006.

North American Electric Reliability Council, "Cyber Security Standards, CIP -002-1 – CIP-009-1," to be approved by Board of Trustees May 2006, http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html, accessed April 2006.

L. K. Nozick, M.A. Turnquist, D. A. Jones, J. R. Davis, C. R. Lawton, "Assessing the Performance of Interdependent Infrastructures and Optimizing Investments, International Journal of Critical Infrastructures, Vol. 1, Nov. 2/3, 2005, pp. 144-154.

R. Novac, "Merging SCADA and business processes," Plant Engineering, May 2005, pp. 35-36.

T. Paukatong, "SCADA Security: A New Concerning Issue of an In-house EGAT-SCADA," Proceedings of the IEEE/PES Transmission and Distribution Conference, Dalian, China, paper 0-7803-9114-4/05, 2005, 5 pages.

D. Peterson, "DHS Funds DCS/SCADA Security Research," http://www.digitalbond.com/SCADA_security/Final%20DHS%20Article.pdf, accessed March 2006.

D. Peterson, "Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks, Presented at ISA Automation West, 2004, http://www.isa.org, accessed February 2006.

A. Pillay, J. Wang, "Risk Assessment of Fishing Vessels Using Fuzzy Set Approach," International Journal of Reliability, Quality, and Safety Engineering, Vol. 9, No. 2, 2002, pp. 163-181.

J. Pollet, "patriotSCADA Distributed Firewall for SCADA and Industrial Networks," plantdata technologies Whitepaper, April 2006, 13 pages, http://www.controlglobal.com/whitepapers/wp_001_SCADApollet.pdf, accessed April 2006.

E. Rakaczky, "Building a Security Business Case," Presentation at the Chicago PCSF Meeting, October 27, 2005, https://www.pcsforum.org/events/2005/fall/pdf/Building%20a%20Security%20Business%20Case2a.pdf, accessed May 2006.

S.M. Rinaldi, "Modeling and Simulating Critical Infrastructures and Interdependencies," Proceedings of the 37th Hawaii International Conference on System Sciences, 2004, http://csdl2.computer.org/comp/proceedings/hicss/2004/2056/02/205620054a.pdf, accessed April 2006.

Riskwatch, "How to do a Complete Automated Risk Assessment: A Methodology Review," a White Paper (2002) available at http://www.riskwatch.com/news/whitepapers/How_To_Do_A_Complete_Automated_Risk_Assessment_10-02RW.pdf, accessed April 2006.

RiskWorld list of software for risk assessment and management, http://www.riskworld.com/SOFTWARE/SW5SW001.HTM, accessed April 2006.

"Risk Assessment Methodologies for Use in the Electric Utility Industry," September 2005, prepared by the Risk Assessment Working Group of the North American Reliability Council's Critical Infrastructure Protection Committee, http://www.esisac.com/publicdocs/assessment_methods/RiskAsmntWP_09sept2005.pdf, accessed April 2006.

C. Roth, K. Farley, "SCADA and Enterprise Security," Pipeline and GasTechnology, Vol. 4, no. 1, Jan/Feb 2005, p. 38.

A. Y. Saad, "Securing Supervisory Control and Data Acquisition Systems," Hydrocarbon Processing, July 2002, pp. 56-57.

B. Schneier, "Attack Trees," Dr. Dobb's Journal, December 1999, http://www.schneier.com/paper-attacktrees-ddj-ft.html, accessed March 2006.

"Securing your SCADA and Industrial Control Systems, Version 1," Technical Support Working Group Guide, 2005, 43 pages, http://www.tswg.gov/tswg/ip/SCADA_GB_Short.pdf, accessed May 2006.

N. Sheble, "SCADA Security Groups Follow ISA," InTech, Vol. 52, no. 5, May 2005, p. 87.

B. Singer, J. Weiss, "Control Systems Cyber Security," Control Engineering, http://www.manufacturing.net/ctl/index.asp?layout=articlePrint&articleID=CA501039, accessed February 2006.

M. Stamatelalos, "Probabilistic Risk Assessment Procedure Guide for NASA Managers and Practitioners," Report by NASA Office of Safety and Mission Assurance, August 2002, 323 pages, http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf, accessed April 2006.

M. Stoddard, D. Bodeau, R. Carlson, C. Glantz, Y. Haimes, C. Lian, J. Santos, J. Shaw, "Process Control System Security Metrics-State of Practice," I3P Research Report No.1, August 2005, I3P, www.thei3p.org, accessed February 2006.

K. Stouffer, J. Falco, F. Proctor, "The NIST Process Control Security Requirements Forum (PCSRF) and the Future of Industrial Control System Security," Proceedings of the 2004 TAPPI Summit, Atlanta, Georgia, May 2004, 7 pages, http://www.isd.mel.nist.gov/documents/stouffer/TAPPI.pdf, accessed April 2006.

R.P. Strickles, H. Ozog, S. Mohindra, "Security Vulnerability Assessment," ioMosaic Corporation White Paper, 2003, 10 pages.

C. Taylor, A. Krings, J. Alves-Foss, "Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening," Proceedings of the ACM Workshop on Scientific Aspects of Cyber Terrorism, (SACT), Washington D.C., November 2002, 9 pages, http://www.cs.uidaho.edu/~krings/publications/SACT-2002-T.pdf, accessed April 2006.

G. D. Tolbert, "Residual Risk Reduction," Professional Safety, November 2005, pp. 25-33.

R. Trellue, I3P Scada Security Research Plan Summary, May 20, 2005, http://www.thei3p.org/research/scada/scadasecresearchplan606.pdf, accessed February 2006.

21 Steps to Improve Cyber Security of SCADA Networks, President's Critical Infrastructure Protection Board and Department of Energy Report, September 2002, http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf, accessed February 2006.

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

US-CERT Informational Focus Paper, "Control Systems Cyber Security Awareness," July 7, 2005, 5 pages, http://www.us-cert.gov/reading_room/Control_System_Security.pdf, accessed February 2006.

United States General Accounting Office (GAO) Report GAO/AIMD-00-33, "Information Security Risk Assessment Practices of Leading Organizations, A Supplement to GAO's May

1998 Executive Guide on Information Security Management," November 1999, 50 pages, http://www.gao.gov/special.pubs/ai00033.pdf, accessed April 2006.

W. Vesely, M. Stamatelalos, J. Dugan, J. Fragola, J. Minarick, "Fault Tree Handbook with Aerospace Applications," Report by NASA Office of Safety and Mission Assurance, August 2002, 218 pages, http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf, accessed April 2006.

W. Vesely, "Fault Tree Analysis (FTA): Concepts and Applications," NASA document, http://www.hq.nasa.gov/office/codeq/risk/ftacourse.pdf, accessed April 2006.

S. Vidalis, A. Jones, "Using Vulnerability Trees for Decision Making in Threat Assessment," School of Computing Technical Report CS-03-2, School of Computing, University of Glamorgan, Pontypridd, CF37, 1DL, Wales, UK, June 2003, 13 pages. http://www.glam.ac.uk/socschool/research/publications/technical/CS-03-2.pdf accessed June 2006.

R. Walker, "Assessment of Technical Risks," Proceedings of the 2000 IEEE International Conference on Management of Innovation and Technology, Vol. 1, No. 12-15, 2000, pp. 402-406.

F.K.T. Wat, E.W.T. Ngai, "Risk Analysis in Electronic Commerce Development Using Fuzzy Sets," Proceedings of the North American Fuzzy Information Processing Society, NAFIPS, Vol. 2, 2001, pp. 807-811.

G. D. Wyss, F. A. Duran, V. J. Dandini, "An Object-Oriented Approach to Risk and Reliability Analysis: Methodology and Aviation Safety Applications," Simulation, Vol. 80 Issue 1, January 2004, pp. 33-43.

S.M. Yacoub, H.H. Ammar, T. Robinson, "A Methodology for Architectural-Level Risk Assessment Using Dynamic Metrics," 11th International Symposium on Software Reliability Engineering (ISSRE'00), 2000, *issre*, p.210-221.

S.M. Yacoub, H.H. Ammar, "A Methodology for Architecture-Level Reliability Risk Analysis," IEEE Transactions on Software Engineering, Vol. 28, No. 6, June 2002, pp. 529-547.