Cyber Security Risk Management in the SCADA Critical Infrastructure Environment

Morgan Henrie, MH Consulting, Inc.

Abstract: Engineering managers are responsible for ensuring the safe, efficient, and effective operation of process control systems which monitor and control the nations critical infrastructures. These systems are subject to increasing risks based on technology vulnerabilities, cyber-threats, and system consequences. Critical infrastructure cyber-threats are expanding at a rapid rate and pose new challenges to the engineering manager's role. This paper presents a short historical view of the risks, types of systems which are involved, and additional information from which the engineering manager may use to make informed decisions on how to develop and maintain a robust process control system in regards to the cyber-threat envelope.

Keywords: Risk Management, Cyber Security, Critical Infrastructure, SCADA

EMJ Focus Areas: Risk Management, Quantitative Methods and Models, Operations Management

Headlines:

- "FBI: Cyber threat might surpass terror threat" (Budich, 2013)
- "Computer-based attacks emerge as threat of future …" (Gertz, 2011), and
- "Saudi Arabia's national oil company, Aramco, said… that a cyber attack against it…that damaged some 30,000 computers was aimed at stopping oil and gas production…" (Reuters, 2012)

Cyber-threats carry the very real potential for remote and anonymous entities to incapacitate or destroy a company's, city's, state's or nation's operations (McIntyre, 2009; Henrie, 2006; Zubairi and Mahboob, 2012). As the global economy continues to leverage automation, through computer based process control systems or *Supervisory Control and Data Acquisition* (*SCADA*) systems, cyber-risks will also continue to increase (Byres, 2000). (Note: Here forward this article will use SCADA to be inclusive of computer based process control system as well as supervisory control and data acquisition systems.)

Engineering managers face expanding and daunting cyber-threats across a broad industry base that includes manufacturing as well as local, state, and national systems. This ever-increasing risk is associated with keeping SCADA systems safe from internal and/or external agent cyber attacks and threats. Threats take many forms: computer viruses, Trojan horses, zombie attacks, or even "… ongoing series of attacks targeting SCADA security companies… use[ing] customized malicious files…" (Farrell, 2012).

While all SCADA utilizing organizations should take proactive steps to secure those systems, engineering managers who are responsible for national critical infrastructures have an even higher level of responsibility. These individuals are responsible for the safe, efficient, and effective operation of systems that support society's infrastructures as we know it. National critical infrastructure is defined as "…infrastructure so vital that the incapacity or destruction would have a debilitating impact on the defense or economic security of the United States" (Executive, 1996). The literature is clear that society, as we know it, could be significantly impacted if a wide spread, long duration, outage of critical infrastructures were to occur.

This article utilizes an exploratory case study approach to identify and discuss SCADA systems cyber security challenges. It is intended to provide engineering managers, as well as senior management, engineers, and technical analysts, deeper understanding of cyber-threats and suggestions on how to mitigate this expanding risk.

The Research

During 2010 and 2011, the author participated in an extensive review of oil and gas (O&G) critical infrastructure SCADA system cyber security programs. The results of this research were presented at the 2010 and 2011 American Petroleum Institute (API) November Information Technology Security Conferences.

The nature of this research was contextual with the intent of extending the industry's knowledge of critical infrastructure cyber security, the associated risks, and the proposed risk-based performance method. The research output is intended to provide engineering managers additional information that can be used to make informed decisions on how organizations should allocate resources to mitigate this expanding risk map. As noted by the Baker Institute Policy Report, SCADA system cyber security risks are a recent phenomenon where "…energy companies…are facing this new risk…," and the risk nature is rapidly evolving (Baker, 2012).

In order to develop a contextual-based understanding of the targeted, diverse industry participants' views, experiences, and knowledge base, an exploratory case study method, patterned after Yin's (2003) case study methods, was applied. According to Yin, an exploratory case study approach is typically used as an initial research effort that is intended to develop a theoretical understanding of the topic matter. One method to achieve this includes direct interaction between the survey population and the researcher – in the form of semi-guided interviews. The semi-guided interviews, in the form of individual interviews, workshops, and breakout focus group meetings, were based on the following set of open ended questions:

- Based on experiences and expectations, what should industry consider to be the appropriate documentation to use when performing system risk and performance financial audits?
- Given the myriad federal agencies currently generating, establishing, and tasked with implementing cyber security,

Refereed Research Manuscript. Accepted by Special Issue Editors Pinto and Bozkurt

who, from industry's perspective, is best suited to advance, promote, and improve cyber security?
- What top three issues keep you up or concern you when it comes to cyber security?
- Where is the marriage between existing technology and the need to create the next generation of cyber security experts?
- What is the current state of industry cyber security threat landscape?
- What is your organization's approach to SCADA system cyber security?

The intent of these questions was to foster a dialogue between the researchers and industry participants so a deeper understanding of SCADA cyber security issues could be developed and elaborated on. Specific to this article's topic, that research developed a general view of the O&G industry and implementation of SCADA cyber security, including:
- Organizational policy, standards, and supply chain issues
- Identification of most pertinent risk and most critical areas of the architecture
- Identification of risk mitigation approaches and processes

The researcher initially engaged with, interviewed, and received input from:
- 47 O&G industry members
- 8 O&G operating companies
- 14 O&G industry security consulting firms
- 19 O&G industry process control hardware/software vendors
- 9 government agencies
- 4 academic research entities

Interactive participation and further data collection occurred during two follow-up workshops that included 94 additional participants, representing 68 O&G related organizations. The breadth of entities included represents a significant portion of the United States O&G industry, several SCADA system vendors, as well as cyber security-involved government agencies, security consulting firms, and academic researchers. A key element of this research and intent of the open ended questions was to determine key decision factors and interdependencies associated with policies, technology drivers, economic factors, operational concerns, and risk and cost-benefit trade-offs.

Based on data and information obtained during the open-ended research question interview sessions, the research identified eight key findings. First, the organizations utilize a variety of risk evaluation methods. Second, public information and research clearly shows SCADA cyber security risks are escalating. The third key finding is that a universal and consistent cyber security program is not applied across various organizations. This finding is supported by the factors that each SCADA system is unique based on its physical, operational, and environmental context (Zhu, Joseph, and Sastry, 2011). A key fourth finding is that a system of systems view (holistic view) is required by all key personnel involved with SCADA cyber security. The system must be the focus to avoid sub-optimization of one component or subsystem to the detriment of the overall system. Tightly coupled with the fourth finding is the fifth key point that merging control system cyber security with the overall company security system is needed and should occur. The SCADA cyber security system must start with the company's strategic plan and propagate throughout the organization. The sixth key finding is that senior management must support the overall system by starting with a clear control system cyber security policy statement in the company security policy. From the company security policy, the seventh key finding is that the company should then develop and deploy specific plans and procedures that support the policy. Eighth, it is imperative that the company develop and deploy training programs for the individuals directly involved and the organization in general (Henrie, 2010 and 2011).

The research provides further support that SCADA system cyber security threats are real and expanding. Engineering managers must ensure that they are adequately reducing their cyber risk to meet organizational needs. Yet, what are SCADA systems? What is a cyber security risk map? How can engineering managers utilize risk maps to make informed decisions? Each of these questions is explored below.

SCADA Systems

SCADA (supervisory control and data acquisition) "…systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste water control, energy, oil and gas refining, and transportation" (NCS, 2004). Also, SCADA systems are one form of automation, that are widely used in manufacturing processes as "…automation often is looked upon as the 'silver bullet' that can drive down operational expenses and improve productivity. For these reasons, automation has been used extensively in manufacturing" (Starovasnik, 2012).

While the SCADA acronym first appeared in use during the early 1960s (NTSB, 2005), the forerunner of today's technically sophisticated SCADA systems was the 1912 Chicago power industry. The Chicago power industry implemented a telephone line and voice communication (Zubairi and Mahboob, 2012) rudimentary SCADA system. This elementary system allowed a centrally located control room supervisor or operator the ability to obtain remote power station status and direct control functions. Using this technical innovation, the early day SCADA system made the power grid's operation more effective and efficient. The next evolutionary SCADA system progression occurred in 1959 with the application of an industrial control computer in the Texaco Port Arthur refinery (ComputerHistory, 2012). Since this time, technological advances continue to expand and facilitate enhanced capabilities but, in general, today's systems continue to be grounded in the 1960's utilities industry (NCS, 2004; Shaw, 2006).

SCADA systems have evolved into sophisticated technology enablers, which allow operation of virtually every type of process, automation, or manufacturing system. These systems provide the capability of ensuring a steady source of reliable electrical power, a steady supply of natural gas to factories, hospitals, and homes as well as enhanced pipeline infrastructure monitoring and control. Many processes now operate at a level of safety, effectiveness, and efficiency never before achieved. These proficiencies are specifically due to the technologically advanced SCADA system capabilities. Technological progress made it possible to design, engineer, deploy, and operate high speed, near real time, remote monitoring and control systems that contribute to higher standards of living.

Modern day, highly advanced technology-based SCADA systems are the result of evolutionary change. Beginning with people talking on the phone, the technology advanced to proprietary electronic controls systems that operated over dedicated telecommunication systems. The next major evolutionary step resulted in today's highly sophisticated and advanced process control networked-based environment. Each step in this evolution brought forth greater process monitoring and control capabilities, safer and more efficient operations,

as well as enhanced business opportunities. Yet, as the systems evolve, new and different levels of associated risks also occur.

The risks this article considers are based on sophisticated and advanced process control, network-based SCADA systems. These systems are found throughout the world and are used in critical infrastructure process control system. As noted by the Transportation Security Administration:

> The [SCADA] control systems used by operators to manage their infrastructure and products are vital to the pipeline's safe and efficient operation. The growing convergence of information technology (IT) and control systems brings with it increased capabilities, but also increased exposure to cyber attacks against the infrastructure (TSA, 2010).

The increasing SCADA system cyber attack risks are a result of several contributing factors such as the systems evolutionary change and how organizations are leveraging them to enhance overall operations. Also, greater system utilization and application raises the company's risk factors. The increased risk is also a factor of the commonality of information technology, SCADA systems hardware, system software, networks, and shared use of telecommunication infrastructures.

The evolutionary process has resulted in systems that utilize common information technology and process control computer operating systems, common technology standards, and common hardware infrastructures. The commonality of hardware, software, interconnections across the company's intranet, and global internet creates new SCADA system vulnerabilities and subsequently increased cyber security threats. SCADA system cyber threats are global issues and, since Sept. 11, 2001, are escalating (Henrie, 2008). As Secretary of Defense Leon E. Panetta states:

> As director of the CIA and now Secretary of Defense, I have understood that cyber attacks are every bit as real as the more well-known threats like terrorism, nuclear weapons… And the cyber threats facing the country are growing. With dramatic advances… (Panetta, 2012).

In an effort to mitigate these increasing risks, engineering managers must proactively manage these new vulnerabilities as they have no direct means to address the threats that may exist. This article first presents what a risk map looks like and what key risk variables are involved in developing a comprehensive risk mitigation plan. The article then suggests a method for addressing organizational challenges resulting from these risks. The ultimate objective of this article is to provide engineering managers, engineers, and technicians an increased understanding of SCADA systems cyber security risk maps, and concepts on how to mitigate the overall risk using a risk-based performance approach. Ultimately, following this approach can enable a more robust critical infrastructure control system.

Cyber Security Risk Maps

SCADA systems are the automation heart and brains for all critical infrastructure systems. SCADA systems merge the ability to monitor remote location physical states, relay human initiated controls to remote field devices, and, frequently, take autonomous action to control processes based on field device states and established algorithms. These actions happen in near real time where the time delay between event and response may be microseconds or less. The potential of significant, negative cascading impacts associated with nearly instantaneous reaction times and potential severe system impacts set the decision risk map analysis stage. Defining or describing an overall risk map involves the development of an organizational understanding of three key variables including threat, system vulnerabilities, and event consequences.

In an attempt to provide industry a standard method by which to quantify critical infrastructure cyber security risks, "In April, 2007, the Department of Homeland Security (DHS) released a risk-based performance standard…for security of chemical facilities…[that]…estimates risks by means of the following formula" (Cox, 2008; see Exhibit 1). This risk quantification approach is in alignment with the various literature sources that clearly identify risk as a function of potential *threats, vulnerabilities, and consequences* (Bahill and Smith, 2009; Patil, Grantham, and Steele, 2012). Threats, vulnerabilities, and consequences are discussed below.

In general, a threat is someone or something that intends to do harm. In the context of cyber security, a threat can be described by its type and its originating source. For example, one type of threat is an unintentional threat. Unintentional threats occur when the threat initiator did not introduce the cyber attack on purpose, i.e. "… unintended modifications as those that represent a violation of the intended behavior…" (Stolfo, Bellovin, Hershkop, and Keromytis, 2008). The unintentional threat is very different from a financial gain threat. As implied, a cyber security financial gain threat targets an opportunity to obtain some financial benefit. The objective is monetary versus malicious (Diaz-Gomez, ValleCarcamo, and Jones, 2011). Malicious intent is the third type of threat and "…usually involves malicious code used as a weapon to infect enemy computers to exploit a weakness…" (Wilson, 2005).

Exhibit 1. Risk Equation

Risk = Threat * Vulnerability * Consequences

Threat – internal or external agents intended to disrupt or cause harm to the organization
Vulnerability – a weakness in the SCADA system that can be exploited
Consequences – result on the system if the threat has successfully exploited vulnerability
Risk – impact to the organization

Regardless of the type of threat, the source of threats are either internal or external to the company. A company's internal agent threat is "…an employee of the company that has greater access to sensitive information, a better understanding of internal processes, and knowledge of high-value targets and potential weaknesses in security," (Ruppert, 2009). Internal agent attacks are also called internal penetration (Diaz-Gomez, ValleCarcamo, and Jones, 2011) or insider attacks (Ruppert, 2009). This article standardizes the use of internal agent for those attacks initiated by an employee or agent who works within the company. The external agent threat is "…one that has no permission to use computer resources…[or] someone that has never been granted computer and network access privileges of an organization," (Diaz-Gomez, ValleCarcamo, and Jones, 2011).

Exhibit 2 is a simplified matrix that relates the type of *threat* and *threat sources* to probability levels. Exhibit 2 shows that both

internal and external *threats* are common across the risk map; yet, the intended purpose of the threat probability changes based on the interaction of the source and threat type.

Exhibit 2. Threat and Source Probability Matrix

	Unintentional	Financial Gain	Malicious
Internal Agent Threat	High	Moderate	Low
External Agent Threat	Low	High	High

The literature identifies that internal agent attacks "…are more frequent than external attacks" (Diaz-Gomez, ValleCarcamo, and Jones, 2011); involve, among other types of attacks "making an unintentional mistake" (Ruppert, 2009); and, in general, do not account for much of the company losses due to cyber crimes (Richardson, 2011). Also, "by most accounts…unintentional human actions (or omissions) cause a large fraction of system incidents that are not explained by natural events and accidents" (Brown, 2006). These sources identify that internal agent *threats* of an unintentional nature are more frequent, i.e. high, yet do not result in a major financial impact to the organization.

For external agent attacks, unintended mistakes, similar to that of internal agent attacks, are considered extremely unlikely. These attack scenarios and processes are different, so the probability that an external agent would make an unintended mistake, as previously defined, was rated low. Moving from unintended mistakes to *threats* associated with purposeful intent, there are two questions of interest. First, what are the key motivators? Second, are internal and external threat motivators different?

The literature identifies that intentional internal agent attacks "…are least frequently [to] occur" (Tsang, 2011), and are often motivated by financial gain or malicious intent. Specifically, "In an insider threat study…analysis of validated cases of insider attack indicated that "…motivation was financial gain" (Diaz-Gomez, ValleCarcamo, and Jones, 2011). Another example is the often cited Australian 2011 waste water attack, that was initiated by an " …ex-employee [who] was trying to convince the water treatment company to hire him to solve the problems he was creating" (Tsang, 2011). Thus, for intentional insider attacks, financial gain is identified as a key motivator, but the frequency of occurrence is lower than unintentional insider attacks, so a probability of moderate was assigned.

Further, external agent threat motivation may be the desire to obtain system command and control capability, providing remote data access, data exfiltration, data manipulation, or activity monitoring (Mateski et al., 2012). While there may be a financial component to the external agent threat, it may be a secondary intent, rather than the primary intent, to cause system disruption, take over system control, or to cause significant negative operational impacts through the use of malicious cyber attacks.

Malicious cyber attack intent is defined, for this article, as the application of a cyber attack to steal, destroy, or modify information used on critical infrastructure. This article specifically delineates malicious intent from financial gain as the attacker intends to cause harm for some reason, such as ideology, rather than financial gain. One literature source identifies that the percentage of "…inside malicious [attacks is] 23.83% [while]… inside accidental [events]…is [a] bigger threat…with 68.82%" (Diaz-Gomez, ValleCarcamo, and Jones, 2011). Insider malicious cyber attacks do occur, but at a frequency level lower than for financial gain, thus the assignment of low to this category.

External agent malicious cyber security attacks or malware infection, on the other hand, have a high probability of occurring. For example, the 2012 Saudi Arabia cyber attack was specifically designed to damage computers and shut down that petroleum industry source. "Malware infection continued to be the most commonly seen attack…" (Richardson, 2011).

Exhibit 2 also demonstrates that the interaction of a threat source and intended results have a probability of occurring. One cannot rule any possibility out just because it has a lower probability than a corresponding intent.

As shown in Exhibit 1, *threat* is one of three variables in organizational risk indicators. Yet, it is the one term that the organization has lowest ability to control. What this means is that an engineering manager can try and minimize internal threats through human resource policies and procedures, such as background checks, operating policies and procedures, and quality control procedures, but experience demonstrates that even these methods can and are circumvented. A classic example is the release of thousands of confidential U.S. Government documents by what appeared to be a trusted insider, i.e., WikiLeaks.

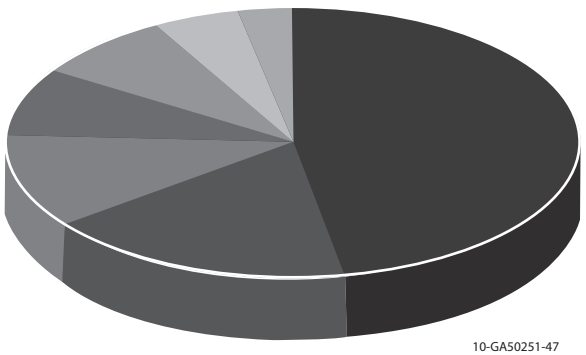
For external agent threats, the organization generally has no means to mitigate or eliminate this type of threat. It is virtually impossible for an engineering manager to identify the external agent threat or to effect any action that would eliminate or mitigate the threat. The inability to alter the *threa*t variable restricts the organization to focusing on the risk formula *vulnerability* and *consequences* variables.

Vulnerabilities are one part of the risk equation where engineering managers have the ability to reduce an organization's risk and to ensure the highest probability of continuous operation. As previously defined, *vulnerabilities* are weaknesses in the SCADA system that can be exploited. Exhibit 3 identifies and quantifies some of the vulnerabilities that exist within SCADA systems (Homeland Security).

SCADA system *vulnerabilities* encompass the areas of hardware, software, communication networks, system design, as well as policies and procedures. The breadth and depth of known *vulnerabilities* requires a corresponding range of mitigating effort to reduce overall system risk through a comprehensive process.

Consequences, the third risk equation variable, are the results or outcomes of a successfully exploited vulnerability.

Exhibit 3. Categories of Vulnerabilities



Organizational consequences range from minor nuisance to full system, organizational failure, up to and including national security consequences. When a successful vulnerability exploit involves national critical infrastructure, the very fabric of the nation is at risk.

Exhibit 4 provides a view of an organizational risk profile that assumes the organization has a 100% threat level. This means there is a threat agent that is intending to launch a cyber attack. Exhibit 4 is also based on the assumption that a vulnerability or set of vulnerabilities exists within the infrastructure, as shown on the x-axis. The final aspect of this plot is the range of probabilities that the cyber attack will be successful. The full spectrum of probable success is provided, in 10% increments, to demonstrate how the overall organization risk factor increases, based on the combination that a vulnerability exists and that the attacker is successful.

Exhibit 4 illustrates one approach for quantifying an organization's risk level based on the combined variables of the probability that a vulnerability is present and that the vulnerability is successfully exploited by a threat agent. In this example, the organization risk level is about 56%. This is based on a 70% probability that a vulnerability exists and the assumption that an attacker has an 80% probability of succeeding. The intersection of these two probabilities results in a 56% organization risk level. Exhibit 4 shows that as the probability of a successful event (vulnerability exploit) declines, there is a subsequent reduction in the organization risk profile for any given vulnerability probability level (Cox, 2008).

Exhibit 5 provides a different critical infrastructure risk quantification/consequence matrix. This method reduces the analysis to qualitative terms that are usually assigned based on input from subject matter experts. A risk quantification/consequence matrix provides the organization a mechanism for assigning an assessed state to the question of the organization's overall cyber security risk.

There are several other risk analysis techniques that can be applied to determining risk level; however, "Published work related to risk assessment is very difficult to categorize" (Ralston, Graham and Hieb, 2007). Ultimately, as Bahill and Smith (2009) state, "Risk is an expression of the potential harm or loss associated with an activity executed in an uncertain environment," and which risk analysis technique is applied can factor into the final outcome. An essential first step is to understand the risk methodological mistakes and limitations before the tool is applied.

One weakness of some risk analysis approaches is classification of low probability but catastrophic consequence events. Examples of this include the successful exploitation of a low probability event that results in drastic organizational, state, or national consequences, such as the organization going out of business or millions of electrical or gas users who lose access to electric or gas grids in the middle of winter.

A consistent weakness of the risk mapping methods presented in this article is that they fail to adequately quantify a profile that reflects the occurrence of a very low probability threat that results in catastrophic consequences. This observation is supported by research such as that conducted by the United Kingdom Cabinet Office and Ministry of Defence, Blackett Review of High Impact

Exhibit 4. Successful Exploit Plot

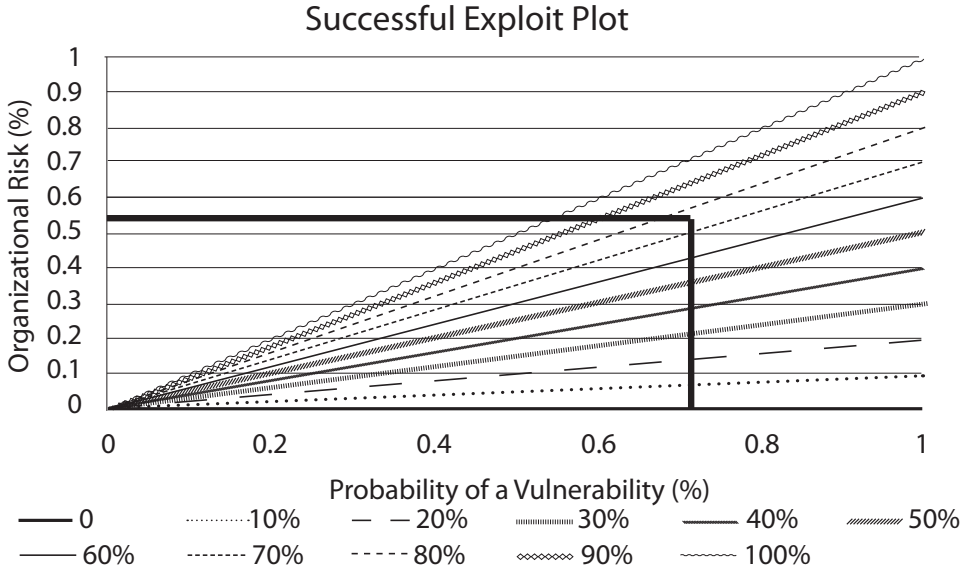


Exhibit 5. Risk Quantification/Consequence Matrix

Consequences						
	High	L	M	H-	H	H+
	Medium	L	L+	M	M+	M+
	Low	L	L+	L	L	L
		Very Low	Low	Medium	Elevated	High
		Threat * Vulnerability				

Low Probability Risks, (U.K., 2011) as well as Pinto et al. who state that, "A constant challenge in risk assessment is the proper representation of catastrophic incidents… [as] averaging out rare but catastrophic events with frequent but inconsequential events, [which may produce] disastrous consequences have the potential to be neglected in the [overall] analysis" (Pinto et al., 2006).

While it is critical to identify and quantify risk profile, this is only part of the overall effort that must occur to increase a company's cybersecurity position. A key activity that must occur before the overall SCADA cybersecurity position is enhanced is development and implementation of a risk mitigation plan.

A Mitigation Approach

A comprehensive SCADA cybersecurity mitigation program is required to provide organizations with the required level of cybersecurity tailored to a company's risk matrix (Zhu, Joseph, and Sastry, 2011). The comprehensive vulnerability reduction process must incorporate, as identified in the following standards and best practices, activities that include company policies, procedures, purchasing requirements, technological solutions, and adherence to applicable standards such as the American Petroleum Institute (API 1164), Interstate Natural Gas Association of America (INGAA), and American National Standards Institute (ANSI), as well as implementing industry best cybersecurity practices through a companywide cybersecurity program. Exhibit 6 provides a general roadmap, applicable to any organization interested in mitigating SCADA system cybersecurity risks.

As shown in Exhibit 6, and supported by previous research (Lebanidze, 2011), a sound SCADA cybersecurity program must start with inclusion in the company's policy statement. The inclusion provides both internal and external individuals and entities a clear understanding of the importance the company places on this activity, as well as provides the foundation for future funding decisions.

Policy statements also provide the scope and overarching guidelines for decisions that can be made by subordinates. Ultimately, company policy statements guide final funding allocations as virtually all companies face the dilemma of insufficient funds to support all requests. Including SCADA cybersecurity within policy statements provides an overall organizational guideline for deciding how funding should be applied.

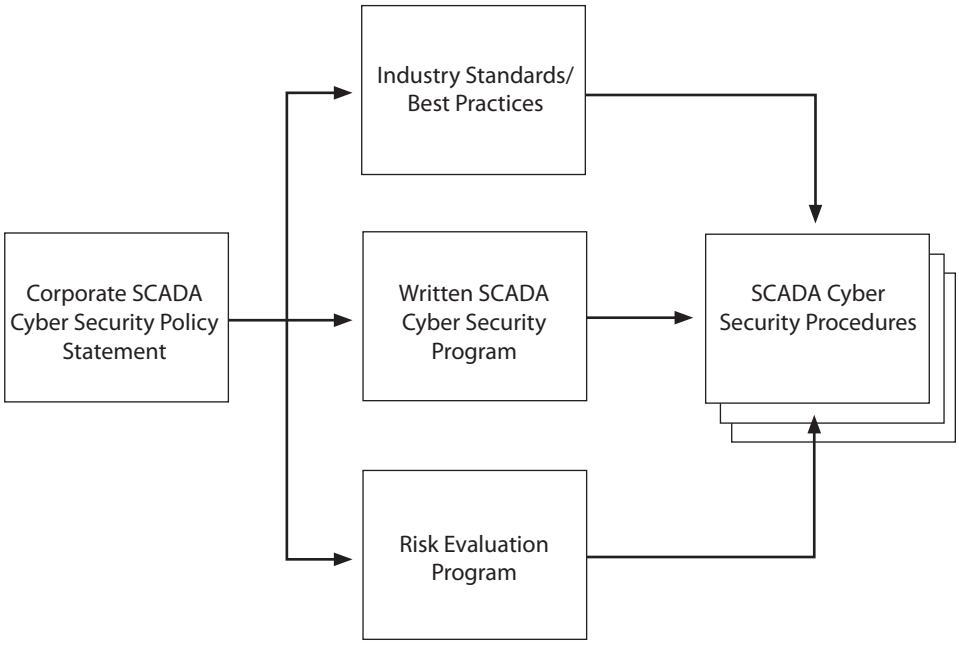
Based on the company policy statement, the organization can move forward with implementation of the program. Implementation involves development of a detailed program with supporting procedures. Inputs to the program and detailed procedures originate from various inputs such as industry standards, best practices, and a risk evaluation program. An example of one input would be incorporation of a cyber incident management system. The cyber incident management system fits within Homeland Security Presidential Directive 5 which outlines the "… development and administration of [a National Incident Management System] NIMS to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies" (Anderson, Compton, and Mason, 2004).

In fact, using formalized risk assessment methods to evaluate an overall cybersecurity program as well as the SCADA system architecture is a vital, recurring practice to planning, achieving, and maintaining an appropriate level of system security and assurance. Risk based assessment findings are essential to developing operational and cybersecurity policies, developing a secure design, fortifying a network, and life-cycle planning. A key outcome of the risk assessments is to provide input to the proper allocation of limited resources for maximum company benefit (Clemen, 1997; Cox, 2008). Below risk based asset allocation is discussed.

Risk Based Asset Allocation

One outcome of a risk based assessment is to provide input to the limited resource allocation decision process. A common and often applied concept is to rank order the risks and then allocate resources from the highest risk to lower risks until the limited resources are consumed. Exhibit 7 is an example of such an approach. The bar height indicates not only the cost to mitigate the risk but the level of risk that has been assigned to the specific category. Based on the level of available funds, the organization can select where the greatest reduction in risk can be obtained for the available funding. This risk mitigation method is supported by many sources including the Department of Homeland

Exhibit 6. SCADA Cybersecurity Program Roadmap



Security, which identifies that, "Comparing the risk faced by different entities helps identify where risk mitigation is needed and to subsequently determine and help justify the most cost-effective risk management options" (DHS, 2007). Further, "In practical terms, a risk-based approach to security is recognizing that there are too many risk scenarios to protect all risks equally, so we have to establish priorities and allocate security resources accordingly" (DOE, 2007). In order to overcome these challenges, the engineering manager must select and implement a risk-based assessment method that supports their unique environment.

In relationship to business or information technology cybersecurity, SCADA cybersecurity is a recent phenomenon. As stated by the United States Transportation Security Administration, "Prior to the terrorist attacks of September 11, 2001, safety concerns took priority over security interests in the pipeline industry" (TSA, 2010). Engineering managers are on the forefront of this expanding risk as they are often the individuals who are responsible for ensuring the SCADA system operates correctly to provide a safe, effective, and efficient process. The benefits of good cybersecurity are well documented (DHS, 2007; DOE, 2007; Shaw, 2006), but the processes to achieve it can be daunting and a significant managerial task (Layton and van Helten, 2013). This article addresses the organizational level challenges of developing and implementing a SCADA cybersecurity program. An essential element and key factor in the program is selection and implementation of a risk based assessment method. Utilizing a risk based assessment method provides engineering managers and decision makers critical input regarding where the highest return on investment can be achieved.

References

Anderson, Anice I., Dennis Compton, and Tom Mason, "Managing in a Dangerous World – the National Incident Management System," *Engineering Management Journal*, *16*:4 (December 2004), pp. 3-9.

American Petroleum Institute "Pipeline SCADA Security," (June 2009).

Bahill, A. Terry, and Eric D. Smith, "An Industry Standard Risk Analysis Technique," *Engineering Management Journal*, *21*:4 (December 2009), pp. 16-29.

Baker Institute Policy Report, "Cybersecurity Issues and Policy Options for the U.S. Energy Industry," (September 2012).

Brown, Kathi Ann, *A Brief History of Critical Infrastructure Protection in the United States*, Spectrum Publishing Group, Inc. (2006).

Budich, Alicia, "FBI: Cyber Threat Might Surpass Terror Threat," (February 2, 2012), available at: http://www.cbsnews.com/8301-3460_162-57370682/fbi-cyber-threat-might-surpass-terror-threat/.

Byres, Eric, J., "Protect That Network: Designing Secure Networks for Industrial Control," *Institute of Electrical and Electronic Engineers Industrial Applications Magazine*, (September/October 2006), pp. 33-39.

Clemen, Robert T., *Making Hard Decisions: An Introduction to Decision Analysis*, Duxbury Press (1997).

Cox, Jr., Louis Anthony, "Some Limitations of 'Risk = Threat x Vulnerability x Consequence' for Risk Analysis of Terrorist Attacks," *Risk Analysis*, *28*:6 (October 2008).

Computerhistory.org, "Texaco Refinery, Port Arthur, Texas," (October 18, 2012), available at: http://www.computerhistory.org/revolution/real-time-computing/6/130/543.

Department of Homeland Security, "National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency," (2007).

Department of Energy, "Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plans Input to the National Infrastructure Protection Plan," (May 2007).

Diaz-Gomez, Gilberto ValleCarcamo, and Douglas Jones, "Internal vs. External Penetrations: A Computer Security Dilemma" *WorldComp 2011, The 2011 World Congress in Computer Science, Computer Engineering and Applied Computing*, (July 19, 2011).

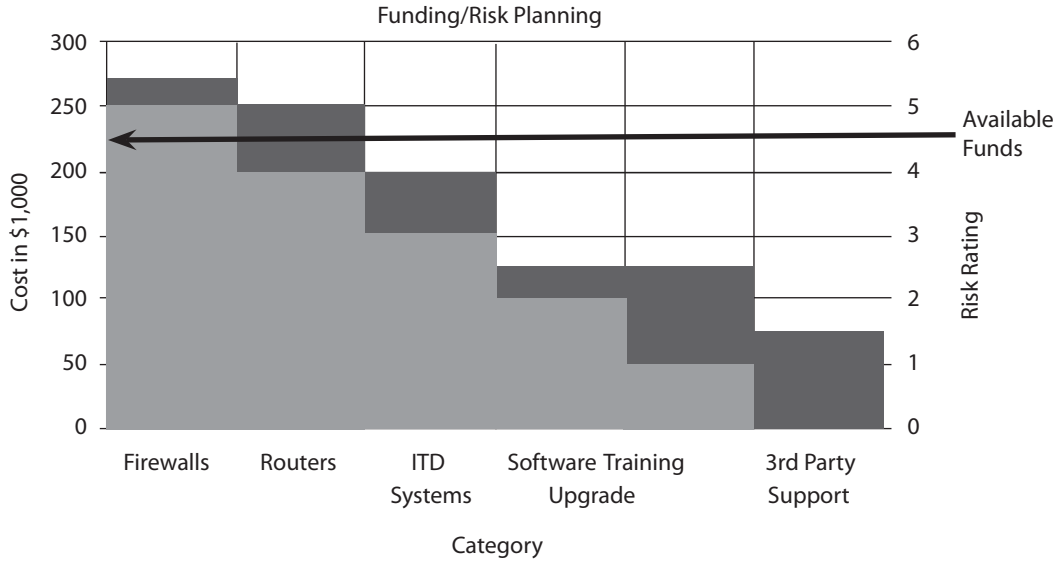
Executive Order 13010, "Critical Infrastructure Protection," (July 17, 1996), available at: http://www.gpo.gov/fdsys/pkg/FR-1996-07-17/html/96-18351.htm

Farrell, Nick, "Chinese Servers Attack Top U.S. Websites," TechEYE.net (2012), available at: http://news.techeye.net/security/chinese-servers-attack-top-us-websites.

Gertz, Bill, "Computer-Based Attacks Emerge as Threat of Future, General Says," (September 12, 2011), available at: http://www.washingtontimes.com/news/2011/sep/13/computer-based-attacks-emerge-as-threat-of-future-/?page=all.

Henrie, Morgan, and Philip Carpenter, "Process Control Cyber-Security: A Case-Study with Design Proposals," *Industrial*

Exhibit 7. Funding Request and Risk Ranking to Available Funding Chart



and Commercial Power Systems Technical Conference, IEEE, (April 2006-May 2006).

Henrie, Morgan, and Paul Liddell, "Quantifying Cyber Security Risk," *Control Engineering*, *55*:3 (March 1, 2008) pp. 12-16.

Henrie, Morgan, and Annie McIntyre, "Critical Issues in Process Control system Security: DHS Spares Project," *Sandia Cyber Security Workshop, API IT Security Conference*, (November 8, 2010).

Homeland Security, "Common CyberSecurity Vulnerabilities in Industrial Control Systems," Control Systems Security Program, National Cyber Security Division, (May 2011), available at: http://ics-cert.us-cert.gov/pdf/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf.

Interstate Natural Gas Association of America, "Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry," (January 2011).

Layton, Gary, and Marcel van Helten, "High Security," *Power and Energy*, *6* (January 16, 2013).

Lebanidze, Evgeny, "Guide to Developing a Cyber Security and Risk Mitigation Plan," The National Rural Electric Research Network (2011).

Mateski, Mark, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Mauuoka, and Jason Frye, "Cyber Threat Metrics," Sandia Report, Sand2012-2427, (March 2012), available at: http://www.fas.org/irp/eprint/metrics.pdf.

McIntyre, Annie, "Process Control System Security: Risks and Mitigations," *IDGA: Cyber Security for National Defense Conference* (May 21, 2009).

McIntyre, Annie, and Morgan Henrie, "Good Operational Security: The Integration of Technology, Policies, and Controls," *Cyber Workshop, API IT Security Conference*, (November 1, 2011).

National Transportation Safety Board, *Supervisory Control and Data Acquisition (SCADA) in Liquid Pipelines, Safety Study NTSB/SS-05/02, PB2005-917005*, (November, 29, 2005), available at: http://www.ntsb.gov/doclib/safetystudies/SS0502.pdf.

Office of the Manager National Communications System, "Technical Information Bulleting 04-1: Supervisory Control and Data Acquisition (SCADA) Systems," (October 2004), available at: http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf.

Panetta, Leon E., "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," U.S. Department of Defense News Transcript, (October 11, 2012), available at: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Patil, Rahul, Katie Grantham, and David Steele, "Business Risk in Early Design: A Business Risk Assessment Approach," *Engineering Management Journal*, *24*:1, (March 2012), pp. 35-46.

Pinto, C. Ariel, Ashish Arora, Dennis Hall, and Edward Schmitz, "Challenges to Sustainable Risk Management: Case Example in Information Network Security," *Engineering Management Journal*, *18*:1 (March 2006), pp. 17-23.

Ralston, Patricia A.S., James H. Graham, and Jefferey L. Hieb. "Cyber Security Risk Assessment for SCADA and DCS Networks," *ISA Transactions*, *46:*4 (2007), pp. 583-594.

Reuters, "Aramco Says Cyberattack Was Aimed at Production," (December 9, 2012), available at: http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0.

Richardson, Robert, "2010/2011 CSI Computer Crime and Security Survey," Computer Security Institute, GoCSI.Com, (2011).

Ruppert, Brad, "Protecting Against Insider Attacks," SANS Institute InfoSec Reading Room, (April 2, 2009), available at: http://www.sans.org/reading_room/whitepapers/incident/protecting-insider-attacks_33168.

Shaw, William T., *Cybersecurity For SCADA Systems*, PennWell (2006).

Singer, Bryan L., and Joe Weiss, "Control Systems Cyber Security," *Control Engineering*, *52*:2 (Feb 2005), pp. 26-31.

Starovasnik, Dean M., "Know the Automation Situation," *Industrial Engineering, 44*:2 (February 2012), pp. 44-48.

Stolfo, Salvatore J., Steven M. Bellovin, Shlomo Hershkop, and Angelos D. Keromytis, *Insider Attack and Cyber Security: Beyond the Hacker*, Springer (2008).

Transportation Security Administration TSA, "Pipeline Security Guidelines," (December, 2010).

Tsang, Rose, "Cyberthreats, Vulnerabilities and Attacks on SCADA Networks," University of California, Berkeley, Working Paper, http://gspp. berkeley. edu/iths/Tsang_SCADA% 20Attacks.pdf (as of Dec. 28, 2011).

U.K. Cabinet Office and Ministry of Defence, "Blackett Review of High Impact Low Probability Risks," Department of Business, Innovation and Skills, (2011), available at: http://www.bis.gov.uk/assets/goscience/docs/b/12-519-blackett-review-high-impact-low-probability-risks.

Wilson, Clay, "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," The Navy Department Library, Order Code RL32114, (April 1, 2005), available at: http://digital.library.unt.edu/ark:/67531/metacrs6315/.

Yin, R.K., *Case Study Research, Design and Methods*, Sage Publications (2003).

Zubaire, Junaid Ahmed,, and Athar Mahboob, *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies,* Information Science Reference (2012).

Zhu, Bonne, Anthony Joseph, and Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," *2011 International Conference on Internet of Things*, (2011), pp. 380-388.

About the Author

Dr. Morgan Henrie is the president of MH Consulting, Inc., providing international support to critical infrastructure industries. Support includes systems analysis, project management, contract negotiations, contract monitoring and management, and assessments of process control cyber security. Dr. Henrie has a PhD in engineering management and systems science from Old Dominion University. Areas of research and publications include multinational project team communication, crisis team communication, process control cyber systems, and liquid pipeline leak detection systems.

Contact: Dr. Morgan Henrie, MH Consulting, Inc., 2103 Sorbus Way, Anchorage, AK 99508; phone: 907-229-5469; fax: 907-344-6361; mhenrie@mhcinc.net