SAND2015-3667C

Supply Chain Risk Management: The Challenge in a Digital World

F. Mitch McCrory, Gio K. Kao, PhD, Dianna S. Blair, PhD

Sandia National Laboratories, Albuquerque, NM, USA*

fmmccro@sandia.gov

Abstract

The increased presence of digital systems in critical safety, security, and emergency planning systems for nuclear power plants presents a complex security risk challenge. The increased functionality of hardware and the length of software code make adequate inspection problematic. This paper addresses one approach to addressing the risks related to this challenge by recommending a systems approach to managing the security risks associated with the supply chain by recognizing that security risks can occur anywhere in the supply chain lifecycle. It expands Supply Chain Risk Management (SCRM) from the acquisition process to the lifecycle process and highlights some of the potential risks with the sub phases associated with the Create and Deploy trust phases. The paper also presents a modified security risk methodology that, unlike other more traditional methods, uses a cost-benefit approach to addressing system risks.

Key Words: Supply Chain Risk Management, Nuclear Power Plant, Supply Chain Lifecycle, Malicious Intent

1. Introduction

Supply Chain Risk Management (SCRM) is well recognized as a critical element of any comprehensive cybersecurity system [1,2]. As the presence of digital systems, encompassing the electronics and information technologies that handle digital signals, continues to expand, SCRM should be applied to address current and future security risks. Whereas there are no global statistics on the percentage of nuclear power plants (NPPs) with digital instrument and control systems it is recognized that both existing and new NPPs will modernize to include more digital technologies [3] in critical safety, security, and emergency planning systems. Concomitant with the increased reliability and performance of digital systems are the increased complexity of devices and systems. This makes their inspection for security difficult to impossible, resulting in new attack vectors that a malicious actor could leverage. This paper frames some of the security issues related to digital SCRM, gives a potential reframing of risk to account for malicious intent as applied to the supply chain, and presents a framework for assessing risk.

2. Framing the Challenge

2.1 Complexity and Inspectability

Hardware and software complexity present critical quality, reliability, and security issues for NPP SCRM. Due in part to decreased device feature sizes [4] and increased lines of code [5], the confluence of such advances have resulted in digital systems that are impossible to

*Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

adequately inspect. For example, security tools are needed to adequately inspect today's generation of FPGAs with up to 2 x 10^{10} transistors and software systems with more than 10^{8} source lines of code. This is illustrated for software code with software security patches issued after software release.

Whereas the economic advantages of incorporating Commercial Off-the-Shelf (COTS) products in digital systems continues to support industry growth they present a security challenge. Pre-engineered with little or no oversight by the COTS integrator, much less the end-user, many COTS parts with simple functions have highly complex designs utilizing on-board central processing units (CPUs) and memory to facilitate the operation of the device. This highlights the inspection challenge of today's digital systems composed of hundreds to thousands of COTS components.

2.2 Globalization

Globalization of commodity items such as FPGAs, microprocessors, software, and other items used in digital systems has decreased their costs and increased their availability. However, globalization has introduced additional issues that make SCRM challenging. From components to sub-systems, a digital system can be the product of multiple teams in multiple locations. In addition, these teams can change during development and manufacturing. An end user would have no way of knowing the composition and worker changeover of the product team. For example, a laptop computer has multiple sub-systems with various firmware storage device sources. The amount of memory, the pedigree of the firmware, the different touch points (foreign or otherwise) that occurred during manufacturing and delivering of the computer, the configuration(s) of the computer for the intended environment, and many other unknowns present challenges for any quality or reliability program to determine the security for items used on critical systems.

Events highlight that adversaries are capable of altering digital products. In 2008, PC World reported [6] that many CDs shipped with digital picture frames from a prominent manufacturer were shipped with a software Trojan virus. More recently hundreds of Europay, Mastercard, Visa (EMV) card readers were tampered somewhere in their supply chain. PINs of credit and debit cards were stolen, and tens of millions of pound sterling are believed to have been stolen [7].

3. Addressing Supply Chain Risk

Supply chain risk from a security perspective has been studied, and standards by various bodies have been published. The United States National Institute for Standards and Technology (NIST) Special Publication (SP), 800-161 [8], identifies nineteen security control families that describe a SCRM program for an information system bounded by the intersection of security, integrity, resilience and quality. Additionally, NIST SP 800-161 provides a significant number of reference documents that can be used to both understand the issue and implement the controls.

Security of digital systems is a lifecycle challenge and therefore any SCRM program needs to be comprehensive in addressing this. Treating SCRM holistically by understanding the supply chain from an adversary's perspective, taking into consideration the entire system lifecycle, and utilizing a risk methodology that accounts for the malicious intent of an adversary in prioritizing controls provides for a robust and effective SCRM.

3.1 Attack Scenarios

A useful framework for understanding the security challenge is to divide potential SCRM attacks into three categories: whole supply chain, subset of the supply chain, and a specific system. While any of these attacks, if successful, might cause unacceptable consequences to a NPP, looking at the relative merits of each type of potential attack could inform the NPPs cybersecurity design basis threat (DBT).

A supply chain attack that targets all components or systems from a single manufacturing facility runs the risk of detection due to the probability presented by the relatively large number of items being available for inspection, random, statistical or ad hoc. Further, it does not provide the attacker the opportunity to track the attack to the intended target. Scenarios of this nature typically do not present consequences of concern for NPP and are therefore more of an inconvenience than a safety concern.

If the attack focuses on the distributor of digital technology it reduces the number of items with the exploit and thus the probability of detection. Such attacks require more information regarding the NPP systems, how they are used, and their providers.

A targeted attacked of a specific component or set of components presents the greatest concern for a NPP. It is the most challenging scenario to plan and execute because it requires detailed information about the NPP. Such an attack should be included in a NPPs DBTs due to its potential consequences. Limiting the distribution of information on the system architecture to keep it away from potential adversaries is the most effective defense for this type of scenario.

3.2 Lifecycle

SCRM should not be viewed as an acquisition process but rather a lifecycle process. This perspective is critical to building a robust program that addresses the diverse threat vectors a system can encounter throughout its lifecycle. For example, a component that is already fielded and thought to be secure can potentially be compromised overnight with a simple firmware update. Figure 1 shows a typical lifecycle for a system and its two trust phases: Create and Deploy. In the creation phase, most of SCRM is focused on tamper *prevention*. When the finished product is delivered and installed (or integrated into an existing system), the focus shifts from tamper *prevention* to tamper *resistance and detection*.

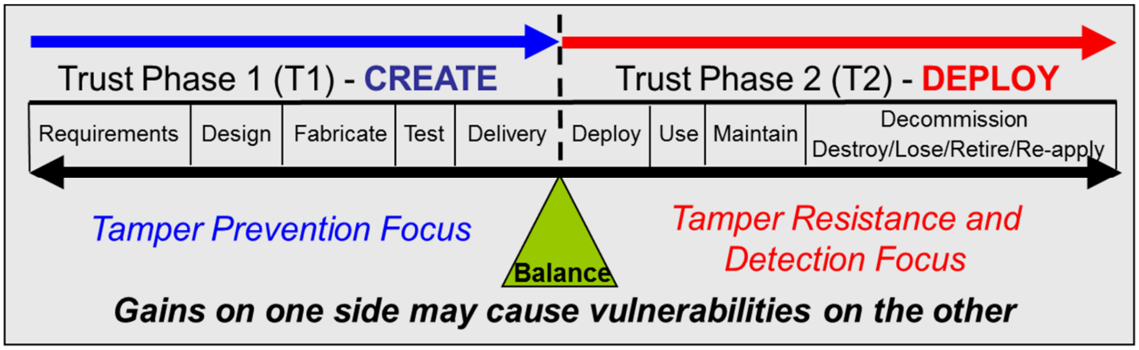
Trust Phase 1 (T1) - CREATE
Trust Phase 2 (T2) - DEPLOY
Requirements
Design
Fabricate
Test
Delivery
Deploy
Use
Maintain
Decommission
Destroy/Lose/Retire/Re-apply
Tamper Prevention Focus
Balance
Tamper Resistance and Detection Focus
Gains on one side may cause vulnerabilities on the other

Figure 1 SCRM Lifecycle

Each of these phases, as well as the various sub phases, can have different SCRM controls and mitigations. A key perspective that this figure illustrates is that SCRM is a systems problem during the lifecycle of a digital system and should be treated as such. For example, implementing controls late in the Create phase provides exploit opportunities to the adversary earlier in the phase and relaxing controls after it is deployed leaves it unprotected.

Below is a brief discussion regarding SCRM concerns to be considered when identifying controls for particular sub phases. It is not intended to be an exhaustive discussion but merely to highlight some issues.

3.2.1 Requirements

Requirements are specifications for system, sub-system, or component performance. SCRM should be incorporated into the overall security requirements for the system and should begin at this sub phase. Requirements such as system elements having inspectability throughout their lifecycle can go far in reducing risk of exploitation. Whereas requirments typically focus on what a system should do, from a SCRM perspective it is also important to provide requirements on what the system **should not** do. This is especially important in the digital COTS era where components can have a vast array of capabilities, but only a subset of those might be used for the system. These extra functions could be a path into the system or enable an otherwise unobtainable consequence.

3.2.2 Design

The system design sub phase is an important element of the system lifecycle for SCRM and presents multiple challenges. For example, inspectability and security robustness are often in the same trade space as cost, schedule and performance. Also it is important to identify the critical safety, security, emergency preparedness components so they can be used in developing SCRM controls for use in the follow-on sub phases of the lifecycle.

Protection of design information is critical throughout the lifecycle of a system and needs to begin during this sub phase. Release of design information provides an adversary with critical information that allows a system defeat to be deployed. A recent high profile attack highlights this point. Figure 2 below shows a simplistic view of how digital information flows in an operating facility. While Stuxnet is not often viewed as a supply chain event, this computer worm illustrates the importance of lifecycle information protection for critical systems. Open source analysis of the attack suggests that the Stuxnet attack would not have been accomplished if the worm designers did not have detailed information related to the process it attacked [13].

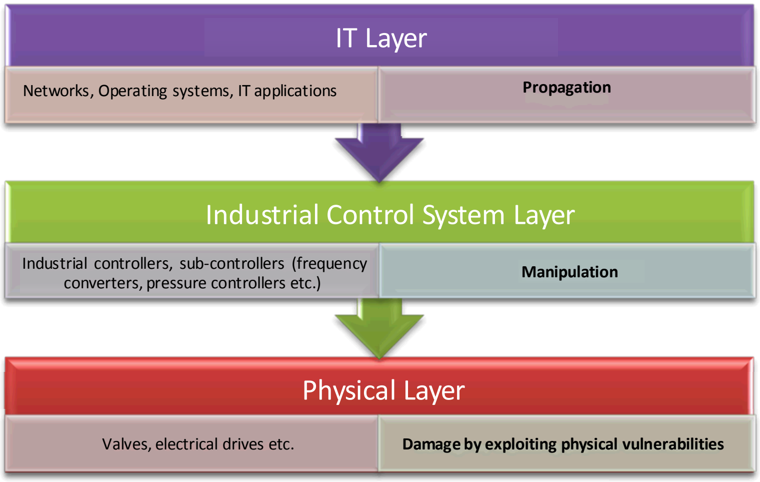
IT Layer
Networks, Operating systems, IT applications
Propagation
Industrial Control System Layer
Industrial controllers, sub-controllers (frequency converters, pressure controllers etc.)
Manipulation
Physical Layer
Valves, electrical drives etc.
Damage by exploiting physical vulnerabilities

Figure 2 Schematic of Stuxnet worm flow [13]

3.2.3 Fabricate

Fabrication, including assembly, of systems can be a complex operation with many components and subassemblies coming together to create the final product. In today's global economy parts/subassemblies originate across the global. It is challenging to identify where hardware, electronics, and software are manufactured and who has potential access to the supply chain. Within the overall SCRM program, this is potentially the most vulnerable time for introduction of malicious content. There are measures that can be taken depending on the risk perceived by the end user. These include blind buys, using multiple vendors to procure the same component, developing a list of trusted suppliers and creating uncertainty about where/when components or systems will be procured. Note: determining the attributes of what makes a supplier trusted can be challenging and will not be explored in this paper.

3.2.4 Test

Testing is often a portion of the lifecycle not accounted for in a SCRM program, yet in this stage, an adversary could mask a supply chain modification by also corrupting the testing program. Additionally, in this sub phase, malicious modification of the testing program could result in accepting bad parts that would have otherwise been rejected.

3.2.5 Deliver

Supply chain attacks between fabrication and delivery can provide an opportunity to add additional malicious functionality. Ways to counter supply chain attacks for critical components in this sub phase include protecting information about how that component will be used and/or buying critical systems, such as a workstation laptop, from several vendors, with the intent that one laptop goes into a control system and the others are used in noncritical systems.

3.2.6 Deploy/Use

This sub phase is probably the safest part of SCRM, but it does present potential exposure to the insider threat. This paper does not intend to discuss insider threat, as this is an area where significant research is being conducted.

3.2.7 Maintain

Once a system is fielded, the maintenance sub phase presents an often overlooked opportunity for a malicious hardware or software insertion. It is during this sub phase when the chain of custody can be lost, original overarching security design requirements can be missed, and the system can be exposed to expert personnel from vendors that may not have adequate facility system access authorizations. In this sub phase vendor supplied experts can be provided access to the critical system without adequate oversight by the facility. It is important that escorts assigned to accompany the expert have the appropriate system knowledge to detect tampering. This sub phase is also where refurbishment/upgrades (technology refresh) of systems take place. Because new technologies may be introduced into the system this results in a branch back to earlier in the SCRM lifecycle. Due to the ever decreasing lifespan of digital systems a digital sub-system replacement can introduce different technologies into the critical system. Such changes need to be taken into consideration when planning technology refreshes. For existing analog NPPs that intend to update to digital components, it is imperative that the security requirements for the lifecycle be revisited.

3.2.8 Decommission/Lose/Retire/Reapply

When decommissioning a system, sub-system, or component, it is important to consider if there is any information contained within the retired technology that would enable an attacker to gain knowledge of the system for use in a supply chain interdiction. A good SCRM program includes how to properly disposition technology so that there is no useful information for a would-be attacker.

3.3 Adversary's Perspective

When developing a SCRM program taking the adversary's perspective into consideration can help to inform and rank controls. For NPPs and nuclear facilities, developing a threat utilizing the DBT or by developing a threat assessment is useful. The International Atomic Energy Agency (IAEA) has published technical guidance on physical [9] and computer security [10] at nuclear facilities that recommends development of these threat models. The United States Nuclear Regulatory Commission (NRC) has codified these requirements [11],[12] and requires that cyber threat be included in the DBT. SCRM of digital systems clearly falls into these guidance documents since it presents a potential threat to digital control and information systems.

The Stuxnet worm illustrated the importance of the adversary having detailed knowledge of the system in order to engineer the attack [13]. In general an adversary, to be successful in engineering a digital attack through the supply chain, would need information about the target system, access to that system (physically or virtually), and knowledge of vulnerabilities within the targeted system. Figure 3 is a simplified view of these three considerations. The intersection of these three sets provides a qualitative, illustrative view of the risk SCRM programs are trying to reduce. Understanding how an applied control reduces this intersection helps to determine the importance of the control.

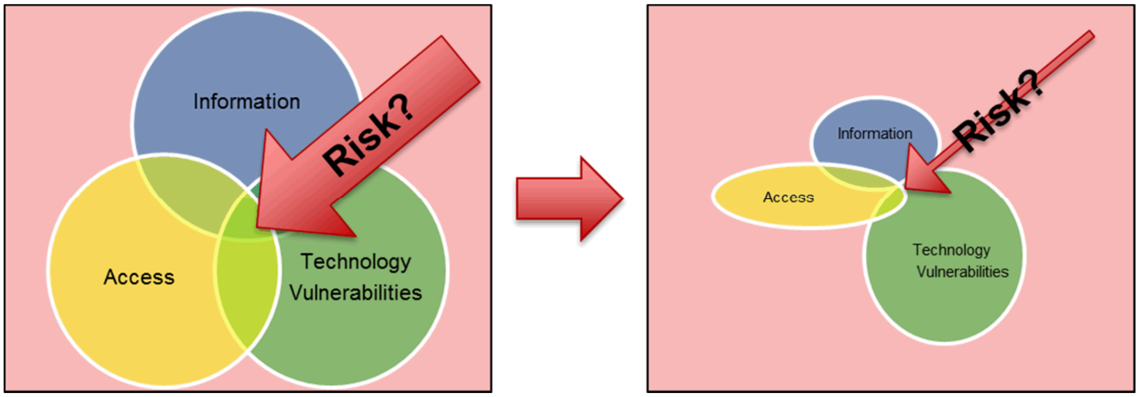

Figure 3 SCRM Venn Diagram

For example, many NPPs limit connectivity (Access) to safety systems through data diodes, but may not adequately protect the information on the critical system itself. This information can be publicly available or otherwise easily obtained, helping an adversary craft an attack.

An operational plant has regulatory obligations to build and maintain a robust physical security program for the plant, but critical components outside of the physical security boundary, present an opportunity for an adversary to insert malicious content, especially if they have information about the system. Access controls, physical or digital, for critical components outside of the Deploy, Use, and Maintain sub phases as shown in Figure 1, need to be considered.

Once a system is designed and installed, it is very difficult to reduce the technology vulnerabilities – they are inherent in the technology selected. This illustrates the importance of the Requirements and Design sub phases of the lifecycle. Mandating security requirements in the systems requirements and choosing technologies that limit vulnerabilities in the Design sub phases are critical to reducing exposure once the system is operational. For example, utilizing a multipurpose microprocessor for an embedded system may provide more security exposure than utilization of an FPGA. For mitigating "Technology Vulnerabilities", another design option that could be considered, preferably in the initial Design sub phase but also possible once fielded, would be to add a sensor to the system that could indicate the system has been modified.

Understanding how the controls to be implemented impact the convergence of the three sets in Figure 3 can assist in qualitatively evaluating the effectiveness or importance of the control. For example, choosing a technology that cannot be normally accessed remotely that is also robust to digital vulnerabilities impacts two of the three circles in the Venn diagram and helps build a robust system. Evaluating the difficulty of exploiting vulnerabilities also helps in prioritizing the controls. Placing controls on all critical digital assets may or may not be economically possible. If the difficulty in exploiting a critical digital asset (CDA) is high and the impact of exploitation is low, then prioritizing controls on easier to exploit CDAs that have higher impact would be beneficial. This thought is explored in a little more detail below.

3.4 Risk Methodology

Traditional techniques to calculate security risk do not translate effectively in digital systems for SCRM. This is due to the complexity and interdependence of such systems and their functions. The inability to adequately inspect the system for all functions and the potential malicious intent of an adversary further complicate the task. A security risk formula: *Risk = Threat · Vulnerability · Consequences* may appear simple but in reality calculating these components of risk can be difficult and imprecise. In particular "*Threat*" is not well defined, and due to its qualitative nature, it is very difficult to quantify. It is dynamic and changes frequently. Furthermore, the three components cannot be treated as independent variables which is required for the risk formula to be valid. This section will provide a brief overview of a variation to the traditional risk equation that overcomes the shortcomings of such an approach, providing an outline of a SCRM framework that utilizes this risk calculation method.

Wyss, et al. [14] propose a modification to the risk equation which can be used to provide insight and help prioritize the list of controls to ensure that NPP critical digital assets procurement processes have the proper controls identified and implemented. Traditional methods attempt to calculate the likelihood of an attack and assume that threat is constant. However, the revised approach calculates the degree of difficulty for an adversary to successfully accomplish the attack. It is possible to assume that difficulty is positively correlated to threat capabilities and negatively correlated to the probability of attack. For example an easier attack in comparison to a harder attack with the same consequences will have a higher likelihood of occurring. Instead of estimating an adversary's probability of attack, it is more manageable to assess difficulty of a successful attack based on the defenders' own knowledge of their security systems. To facilitate difficulty assessments, metrics have been developed to capture both qualitative and quantitative factors. These metrics are categorized into 12 dimensions for assessment which account for attack preparations such as outsider support, insider support, supporting infrastructure, tools and technology requirements, in addition to attack execution strategies, such as situation exploitation, covertness capability, outsider support, and insider support. For a more in-depth discussion of this security risk evaluation methodology, please refer to [14].

Sandia National Laboratories have developed a SCRM framework that leverages this modified security risk evaluation. The Supply Chain Lifecycle Decision Analytic Framework [15] is a supply chain risk assessment tool that provides decision-support technologies which enable decision-makers to perform risk-based cost-benefit prioritization of security investments in managing supply chain integrity and risk. This framework is different from other approaches (which often only focus on performing supplier reviews). Sandia's SCRM framework has a lifecycle process focus, which considers both information and material flows, the internal and external entities involvement, and supporting infrastructure. In addition, this repeatable and structured framework helps analysts and decision makers organize the risk assessment process in order to better understand areas of risk.

One key challenge in evaluating supply chain risk is the complexity of the problem. The end-to-end supply chain lifecycle problem is large and complex. To approach the problem we recommend examining and addressing SCRM with the following framework: 1. Supply Chain Lifecycle Representation, 2. Supply Chain Vulnerability and Mitigation Assessment, 3. Supply Chain Risk Assessment, and 4. Decision and Optimization Support.

Supply Chain Lifecycle Representation – provides a systematic way to capture the end-to-end lifecycle supply chain. This component hierarchically models the supply chain by mapping the information and material flow. It also provides the flexibility to scale the problem as needed by evaluating the supply chain at various depths while addressing the complexity of representation.

Supply Chain Vulnerability and Mitigation Assessment — provides taxonomy to map adversarial action to the supply chain lifecycle representation. Vulnerability and mitigation assessment can be a highly subjective process, and the adversarial action mapping attempts to reduce subjectivity and increase objectivity while streamlining the process to improve the efficiency of SMEs. This component helps to holistically understand their vulnerability space.

Supply Chain Risk Assessment — provides evaluation of potential adversarial attacks based on the supply chain vulnerability and mitigation assessment. This component leverages the consequence- and difficulty-based Sandia Risk Methodology proposed in [14]. It provides a pragmatic platform that has been used in security assessment.

Decision and Optimization Support — provides the technology for decision makers to perform risk-based cost-benefit prioritization of security investments to manage supply chain integrity. Optimization models have been developed to help determine best mitigation impacts. This enables decision-makers to consider constraints such as cost, time and influence. Together with the other components of the framework, this enables decision makers to assess their return-on-investment.

This framework helps to lay foundational analytics for supply chain risk assessment and provides a systematic approach to SCRM.

4. Conclusion

The growing use of digital equipment in critical systems for NPPs presents a security, integrity and quality challenge for plants. Ensuring that systems perform as expected and do not present a threat vector for an adversary should be seen as a system problem framed by the lifecycle of the system and each component and sub system in it. From establishing requirements to final decommissioning, the lifecycle presents opportunities for both the security team and the adversaries. Whether updating technology to remove discovered vulnerabilities or unknowingly introducing new risks, SCRM is a process that continues to support digital systems throughout their life cycle. Recognizing that security risks exist in all systems we recommend the adoption of a modified security risk methodology that utilizes the defender's knowledge of the system to eliminate those attacks that could be viewed as easy, with resources applied based on risk-based cost-benefit prioritization. The Supply Chain Lifecycle Decision Analytic Framework embraces this approach modified and bounds the problem space, allowing for analytics and subsequent prioritization.

REFERENCES

[1] The Comprehensive National Cybersecurity Initiative, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

[2] Chabinsky, S. R. (2010). Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line. *Journal of National Security Law & Policy [Vol. 4:27 2010] A Primer On Cybersecurity Strategy*. Retrieved from http://jnslp.com/wp-content/uploads/2010/08/04_Chabinsky.pdf

[3] "Instrument and Control (I&C) Systems in Nuclear Power Plants: A Time of Transition," 52nd IAEA General Conference, 9/29-10/4/2008. Retrieved from http://www.iaea.org/About/Policy/GC/GC52/GC52InfDocuments/English/gc52inf-3-att5_en.pdf

[4] Xcell Journal, Issue 86, First Quarter 2014, page 14: http://www.xilinx.com/publications/archives/xcell/Xcell86.pdf.

[5] Source lines of code, (n.d.). Retrieve April 26, 2015 from Wikipedia: http://en.wikipedia.org/wiki/Source_lines_of_code

[6] Agam Shah, IDG News Service, (Dec. 24, 2008). "Samsung Shipped Infected Digital Picture Frames." Retrieve from: http://www.pcworld.com/article/156050/samsung_infected_cds.html

[7] Online source: http://en.wikipedia.org/wiki/EMV#Successful_attacks

[8] Jon Boyens, et al., NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations." April 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities

(INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011)

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011)

[11] US Code of Federal Regulations, Title 10, Part 73.1, Purpose and scope, November 28, 1979

[12] US Code of Federal Regulations, Title 10, Part 73.54, Protection of digital computer and communication systems and networks, March 27, 2009

[13] Langner, Ralph. *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. The Langner Group, November 2013. <http://www.langner.com>

[14] Wyss, G., et al., "Risk-Based Cost-Benefit Analysis for Security Assessment Problems", 44th IEEE Annual International Carnahan Conference on Security Technology, San Jose, CA, October 2010

[15] Kao, G. et al., "Supply Chain Lifecycle Decision Analytics", 48th IEEE Annual International Carnahan Conference on Security Technology, Rome, October 2014