CYBERSECURITY FOR SAFEGUARDS:

A TECHNOLOGY LIFECYCLE DEVELOPMENT APPROACH

Risa Haddal[1], Sharon DeLand[1], Dianna Blair[1], Phil Turner[1], Mitch McCrory[1]
[1]Sandia National Laboratories
P.O. Box 5800, MS-1371, Albuquerque, NM, 87185-1371 USA
rhaddal@sandia.gov

ABSTRACT

International nuclear safeguards are technical measures implemented by the International Atomic Energy Agency (IAEA) to verify the correctness and completeness of declarations made by States about their nuclear material activities. Based, in part, on information provided by safeguards equipment, the IAEA relies on the integrity of the information to make accurate conclusions. Most safeguards equipment contains digital systems that collect, process, analyze, store and transmit data. Despite increasing efforts to protect digital systems against unauthorized access and modification of information or equipment, cyber adversaries are becoming more sophisticated and more persistent. Cyber security is a challenging problem due to its breadth and complexity. We have chosen a framework that applies especially well to the equipment-based environment of safeguards. Specifically, we use the lifecycle of safeguards technology development (requirements, design, manufacture, test, review, authorize, deliver, use, decommission) as a framework to examine potential risks and preventive measures based on best practices to address cybersecurity challenges. This paper will explore how the lifecycle framework might be applied generally to safeguards technology to reduce risks from cyber attack.

INTRODUCTION

International nuclear safeguards are technical measures implemented by the International Atomic Energy Agency (IAEA) to verify the correctness and completeness of declarations made by States about their nuclear material activities. Based, in part, on information provided by safeguards equipment, the IAEA relies on the integrity of its information to make accurate conclusions. Most safeguards equipment contains digital systems that collect, process, analyze, store and transmit data. Despite increasing efforts to protect digital systems against unauthorized access and modification of information or equipment, cyber adversaries are becoming more sophisticated and more persistent. The presence of digital systems in safeguards equipment inherently puts that equipment at risk for a cyber-based attack.

This paper describes an analytical framework for analyzing cybersecurity risks of safeguards equipment. Cybersecurity analyses typically consider risks during equipment operation. This framework considers the full equipment lifecycle in order to capture risks that may be incurred during design, manufacture, acquisition, and disposition of equipment. The framework leverages previous research at Sandia on supply chain risk management;[1] however it has been adapted to address unique features of the safeguards equipment lifecycle. At each stage of the lifecycle, the framework identifies potential risks and preventive measures based on best practices to address

[1] McCrory, M. F., Gio K. Kao, Dianna S. Blair. *Supply Chain Risk Management: The Challenge in a Digital World*. SAND2015-3667. Sandia National Laboratories. Albuquerque, NM, USA.

cybersecurity challenges. This paper will explore how the lifecycle framework might be applied generally to safeguards technology to reduce risks from cyber attack.

CONTEXT

Cybersecurity is recognized as a key component of any comprehensive security plan. It focuses on ensuring protection of digital systems from malicious attack that can include anything from interruption of operations to insertion of malicious code that alters information and/or changes operations. For international nuclear safeguards, attack goals could include changes to data and information, falsification of state of health information for systems and sensors, or interception of sensitive communications and data. Successful attacks could result in invalid safeguards conclusions, increased allocation of resources to resolve inconsistencies, or embarrassment to the IAEA, all of which undermine its mission.

While cybersecurity is a challenge in many areas, the safeguards equipment lifecycle itself presents a unique set of risks. Typically, the deployment and use lifecycle phases are seen as relatively low-risk cybersecurity periods for systems in which access is controlled by the equipment owner. However, for safeguards, deployment and use occurs in operator facilities, making these phases potentially high risk for cybersecurity. In addition, the safeguards procurement process identifies the end user in a certain niche market, thereby increasing the targetability and cybersecurity risk for this phase. Given these important differences from many technology applications, it is important to perform cybersecurity analysis specific to safeguards applications. The open source framework described in this paper is one potential tool for doing so.

METHODOLOGY

The cybersecurity for safeguards analytical framework examines the entire equipment lifecycle from source through delivery and installation and ultimately decommissioning, or equipment retirement. This approach takes into account the fact that potential adversary access vectors exist at nearly every lifecycle stage for any equipment with electronic and digital hardware and software components capable of data collection, processing, analysis, storage and transmission. The framework is a tool that could be used to reduce risks to safeguards equipment, such as manipulation or exploitation that may compromise their integrity and reliability.

Figure 1 describes the methodology for analyzing the cyber security risks for a piece of monitoring equipment. This methodology was developed using expertise at Sandia for conducting cyber assessments and is based on knowledge gained from similar projects performed for other domains. The process steps used in this study include:

- Data collection;
- System characterization;
- Lifecycle analysis;
- Mitigation strategy(ies) identification and prioritization

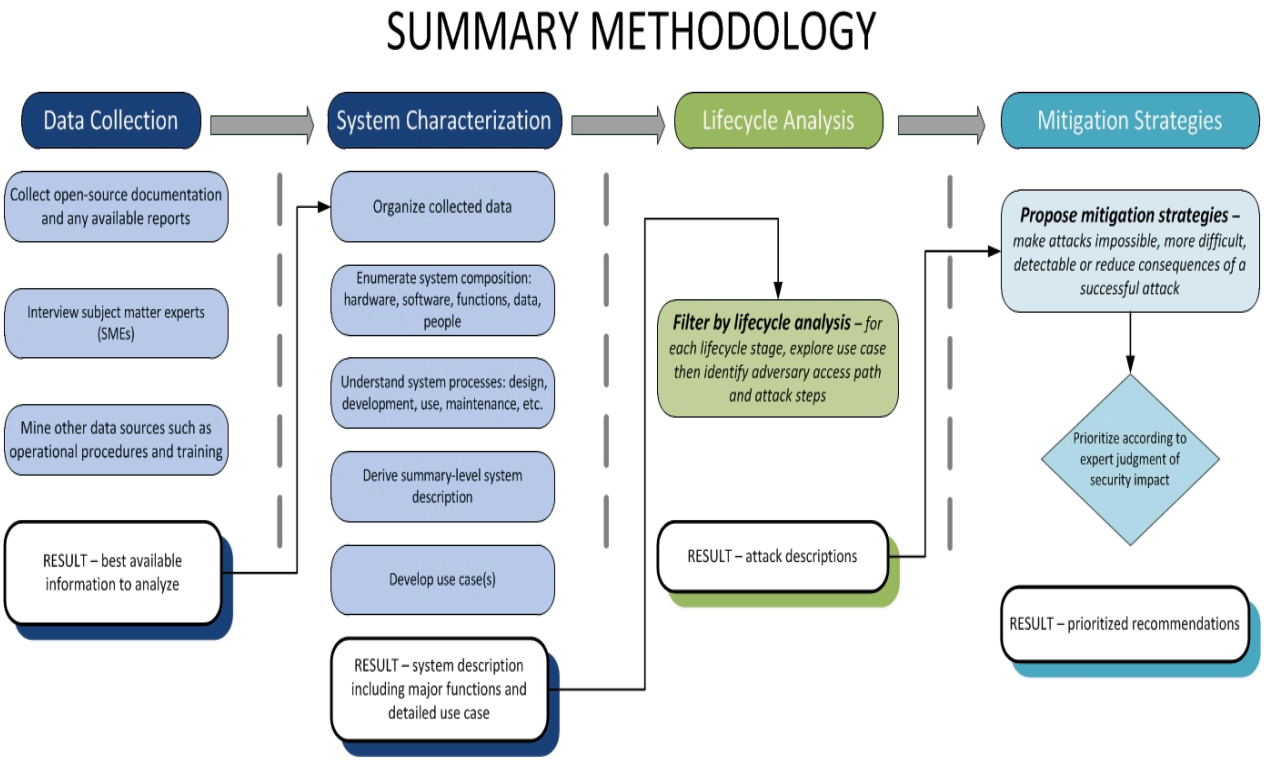

Figure 1. Methodology for equipment analysis.

Data collection draws on open source information, subject matter expertise, and other available data sources to collect information about the equipment or instrument, including its functionality, how it is used, operational procedures and user training as input for characterizing the equipment. An important element of the system characterization is a set of use cases describing who has access to the instrument and how it is handled or used at each stage of its lifecycle. In the case of safeguards equipment, sources of information for developing use cases could include SME input e.g., former IAEA safeguards inspectors, publicly available user's guides, and knowledge relative to the specific system. Given the set of use cases, each stage of the system lifecycle is individually analyzed as described below to understand how the equipment could be accessed and attacked. During attack development, it is common to identify key information that can enable or prevent an attack, resulting in further data collection or refinement of the equipment description. For each attack, mitigations are developed and prioritized based on cost and effectiveness.

In an equipment-focused analysis, the attacks and recommended mitigations would be as specific as possible in order to be actionable. The focus of the overview in this paper is to illustrate the types of attacks and mitigations that might be considered and how these are adapted for the safeguards domain. While it does not identify exact vulnerabilities in specific IAEA safeguards equipment, the overview does list generic risks and preventive measures that could be considered.

Attacks and mitigation measures are linked to phases of the equipment's lifecycle. Lifecycle phases are typically given as requirements, design, manufacture, test, acquisition, deployment/operation, and decommission/disposition. In order to apply this framework to safeguards equipment, we determined how the safeguards equipment lifecycle may differ from the generic lifecycle and identified additional attacks or mitigations specific to safeguards. The resulting high-level lifecycle framework is described in the sections below.

FRAMEWORK APPROACH

While the development of safeguards equipment is similar to other generic COTS systems, there are three key differences. First, the safeguards equipment development process includes a "Safeguards Authorization" step and a "Vulnerability Review" which are unique to safeguards. The authorization process is an established quality assurance procedure employed by the IAEA to verify that equipment and software is acceptable for safeguards use. The "Vulnerability Review" consists of an assessment for vulnerabilities conducted by an independent entity to ensure that weaknesses are mitigated. Second, while the IAEA continues to place importance on the use of COTS equipment for the purposes of more efficient, cost effective safeguards, the use of this type of equipment for conducting nuclear material measurements or remote monitoring could introduce information security risks. Third, the amount of time it takes for safeguards equipment to go from the requirements stage to deployment and use is extensive and does not keep pace with technology development in industry. As such, equipment may not have the appropriate security-by-design incorporated today that is necessary to address the cybersecurity challenges five to ten years from now.

The safeguards technology development lifecycle, including these unique stages, are depicted in Figure 2 below.

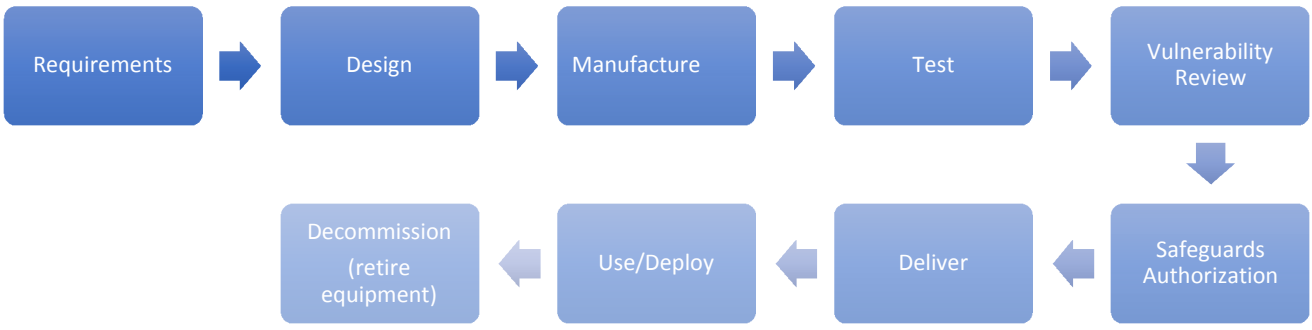

Figure 2. Safeguards technology development lifecycle.

In addition to understanding the safeguards technology development lifecycle, other factors that inform a cyber analysis include:

- How the equipment is used;
- Knowledge about the supply chain;

- Electronics (digital, analog, etc.);
- Complexity of the instrument;
- Fuel cycle stage in which equipment is used; and
- Use by IAEA and/or other inspectorates.

LIFECYCLE STAGE ANALYSIS

This section describes the activities at each stage of the safeguards system lifecycle, potential opportunities for cyber access or attack, and possible preventive measures. Detailed analysis of costs and effectiveness of these measures with respect to a specific piece of equipment would allow these measures to be prioritized. Since this paper focuses on the methodology, it does not include prioritization.

Requirements

System requirements are developed with the specific uses in mind – that is, what features should the device have to facilitate its intended use? Also, requirements are typically dictated by designers who are expert in the specific technical area of the intended use. However, considering an unprotected and open supply chain, an opposing perspective is necessary – what features must the device not have to block malicious functionality? Safeguards equipment designers who are not knowledgeable in information security will need to consult with security experts to determine likely attack paths and malicious functions. For example, can/will the device have hardware features that are disabled through software? This is a common process but any features that can be easily disabled can also be enabled, perhaps without knowledge of the user.

Requirements Access Vectors

- Insiders could request functionality that would make exploitation easier, wittingly or unwittingly, due to influence from an adversary.
- Requirements could be modified either in stored documents or in transit on networks where they are held either remotely or locally.

Requirements Preventive Measures

- Review requirements to ensure there are no nonessential access vectors such as Bluetooth and USB.
- Validate that the capabilities are tied to a current need and that the process could not be performed by another means.
- Put processes and security measures in place which require appropriate configuration control and protection software.
- Consider adding requirements that will enhance security. Limit information that will allow the adversary specific context as to why a requirement is necessary or how the component will be used – this extends throughout the lifecycle.
- Protect the network and communications channels where requirements documents exist.

Design

In the design stage, the system manufacturer designs a system to accomplish the intended requirements. It is unlikely, although not impossible, that a single customer will be targeted by a system designer in this phase. In fact, design is often iterative – using a previous system as a

starting point and evolving it for new requirements or uses. The system designer often leverages subcomponents of existing COTS products which can be integrated into the final system.

Design Access Vectors
Design documents on a safeguards equipment developer's network could be modified through the network, either locally or remotely, perhaps by a trusted insider at the development facility and provide the hardware and software access vectors to the system that could later be exploited by an adversary.

Design Preventive Measures
- Use trusted designer;
- Place contractual security requirements on development network e.g., disconnected from the internet, media scanning process.
- Place requirements on vendors for auditing of design facilities.

Manufacture
In the product manufacture stage, subcomponents are integrated into a final product and it is likely that software and firmware will be used. Lacking specific requirements for supply chain security, manufacturers typically rely on convenient or inexpensive building blocks and software/firmware development is likely targeted to system function rather than security. While our knowledge of the safeguards equipment manufacturing process was limited, we do know that the manufacture of some components are outsourced to external facilities or suppliers, which introduces information security challenges.

Manufacture Access Vectors
- Hardware designs or software code held on networks or in transit may be susceptible to manipulation.
- Insiders at a fabrication facility could change designs or code.
- Compromised components that come in through the manufacturer's supply chain could be added to hardware.
- Some or all manufacturing may be outsourced to another facility.

Manufacture Preventive Measures
- Use trusted manufacturer.
- Place contractual security requirements on network that holds designs e.g., disconnected from the internet, media scanning process.
- Require vetting of all outsourcing for fabrication of hardware and software.
- Place requirements on vendors for auditing of manufacture facilities.

Vulnerability Review
As unique elements of the safeguards equipment lifecycle, the vulnerability review and safeguards authorization process consists of a series of steps used to carefully assess various aspects of the equipment. Through an iterative prototype development and assessment process, the IAEA ensures end products meet safeguards needs and standards. Prototypes undergo field testing in operational facilities to assess usability, operational impact and operator concerns. As designs mature through the prototype and field testing process, they are subject to *vulnerability*

reviews (VRs) conducted by an independent third party, using a Member State Support Program (MSSP) that is different from the one that is developing the technology.

Vulnerability Review Access Vectors

- Modifications to safeguards equipment made after the VR could introduce risks.

Vulnerability Review Preventive Measures

- Conduct additional VRs following any equipment modifications and prior to deployment and use.

Safeguards Authorization

Once equipment has successfully completed the vulnerability review and is deemed "mature", it undergoes a final authorization process before general commercialization and acquisition by the IAEA begins. Overall, the *safeguards authorization process*[2] ensures, among other things, that (1) compliance with user requirements is verified and the instrument is fully characterized, (2) vulnerability, data security, usability and expected reliability have been assessed, (3) appropriate user documentation has been prepared, and (4) training needs have been identified and addressed. This includes analysis of expected performance, usability and affordability, followed by successful field testing. Often, it can take several years for a new piece of safeguards equipment to be authorized which, as previously mentioned, could introduce vulnerabilities. While potential cyber risks could be introduced during these stages, the vulnerability review and authorization process are logical points in the safeguards technology development lifecycle that subject matter experts (SMEs) could leverage for analysis and the development of risk mitigation recommendations.

Test

System testing ensures the product performs reliably and meets the intended functions. In the safeguards equipment lifecycle, all systems are carefully tested at IAEA Headquarters prior to field installation. For example, a test period for unattended systems typically lasts 90 days to represent the current unattended period between in situ visits by inspectors. Early component failure, configuration errors and manufacturing defects can be eliminated during the test phase, while the system and its components are easily accessible. Once the system has operated successfully (without failure) for a full inspection period, it is ready for field installation. However, even at this late stage in product supply, all aspects of security may not be considered, so analysis for malicious insertion before or during the testing process may not be performed. An adversary may use the testing phase to hide the presence of compromised systems. This would provide an opportunity to instill a measure of confidence or trust with the owner of the system that it executes its function as intended and provides the level of security desired.

Test Access Vectors

- Insider may change procedures, data, or test equipment.
- Test equipment supply chain attack opportunities may exist that could allow for faulty testing.

---

[2] *IAEA Equipment Authorization for Safeguards Use*. IAEA Department of Safeguards, Division of Scientific and Technical Services (SGTS). May 2015. IAEA.

- Outsourcing of testing may provide opportunities for an adversary.
- Local and remote access to networks that hold test documentation and data.

Test Preventive Measures

- Inspect for additional or altered elements that were not a part of the design.
- Inspect for counterfeit components.
- Perform testing as close to real world conditions and environment as possible.
- Place requirements on vendors for auditing of test facilities.

Deliver

As a system is delivered from the manufacturing facility its custody transfers to the delivery organization and an adversary might use this opportunity. As the adversary gets closer to the end user of the system, the attack can be much more targeted to that specific user. This affords an adversary the opportunity to modify the system to add exploits or access vectors into the system, either in transit or in the software/firmware or updates that exist on the organization's network. Our knowledge of the safeguards equipment chain of custody was limited. However, we assume that safeguards equipment is typically shipped either to IAEA Headquarters or directly to the facility where it will be installed and used. If strict security measures are not maintained on the equipment during delivery, cyber challenges could arise.

Deliver Access Vectors

- Insiders at the manufacturer, shipping company, or in the receiving organization could modify or replace system or software code.
- Package could be intercepted and modified in transit (e.g., delay points, Customs).
- Software can be modified on vendor network locally or remotely
- User might download compromised software through redirected website or altered communication stream.
- Organization's network could be compromised through local or remote vectors or through an insider.

Deliver Preventive Measures

- Pick up system directly from manufacturer.
- Use trusted carrier for delivery.
- Perform hash validation of all software, whether mailed, shipped, or downloaded, using a robust, cryptographic hashing function[3] (e.g., SHA-2 family) when obtained from the vendor and when installed on the system. Obtain the hash through a different channel from which the software was obtained, e.g., mail or phone for downloaded software. Avoid using CRC or MD5 hashes as these have been susceptible to exploit for some time. SHA-1 has also recently had a successful collision attack performed on it and should be avoided, if possible.
- Limit information available on delivery procedures and timeframes.

[3] A cryptographic hash function is similar to a digital fingerprint. It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash function) which is designed to also be a one-way function. That is, a function which is infeasible to invert. The only way to recreate the input data from an ideal cryptographic hash function's output is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes. https://en.wikipedia.org/wiki/Cryptographic_hash_function

- Maintain offline secure copies of software and a record of printed hash values.
- Use encryption for software delivery and storage.
- Implement password protection on devices or other authentication mechanism and change default passwords.

Use

The use phase is likely the best defended stage of the system lifecycle. However, at this point the specific user is well known and targeted attacks are straight forward. In this stage an adversary could delete or corrupt data during collection, transfer, storage, or analysis. The adversary could also embed exploits during system use, resulting in loss of data integrity and/or confidentiality. System access vectors may have been disabled by the organization but re-enabled through an insider or exploit.

As with the delivery stage, the system custody will likely change during installation. This affords an adversary the opportunity to modify the system to add exploits or access vectors into the system. An adversary could modify or replace the system or software in transit or trigger embedded exploits during deployment. Triggering could be carried out on the system that would begin execution of an embedded exploit. This could potentially circumvent any testing that may have been performed prior to deployment. Data loaded onto the system could be manipulated by an adversary.

During the deploy/use phase, an adversary could modify the device during maintenance activities but also the system owner may not detect software updates that may have been modified for an adversary's purpose allowing for malicious activity. Hardware could be modified if units are sent back to the vendor, allowing for malicious activity.

Use Access Vectors

- Insiders within the organization could modify or replace the system, software, or data.
- If shipping mechanisms or Customs are involved, see Delivery.
- The organization's network could be compromised locally or remotely allowing for data or software modification.
- Insider with direct system access.
- Other personnel that have access to the system during use.
- Access to the organization's network, locally or remotely.
- Access vectors within the system itself, e.g., Bluetooth, USB.
- Triggering mechanisms can include a specific signatures detected by or present to the system from various environmental factors, GPS coordinates, Bluetooth signal, etc.

Use Preventive Measures

- Maintain strict physical custody and protection during transit, while going through customs, in hotel, etc. This will reduce opportunities for exploitation.
- If not essential to power up while in transit to final location, keep equipment powered off.
- Limit information available on deployment schedules and procedures.
- Ensure robust cybersecurity on the network where the software and data reside.
- Implement password protection on devices or other authentication mechanism and change default passwords.
- Use encryption for data in transit and at rest.

- Protect systems where data and software is stored.
- Ensure features such as GPS and Bluetooth are disabled if not needed. Hardware disablement is preferred.
- Disable USB ports on devices, if possible, or require authentication for writing of firmware. Use USB devices that are not susceptible to BadUSB.[4]
- Robust testing procedures at use location may help detect potential exploitation.
- Use of multiple capabilities with different systems may help detect/defeat exploitation.
- Avoid sending equipment back to the vendor, if possible.

Decommission (retire equipment)

Although a system is no longer used during the decommission (equipment retirement) phase, it may still have important information that allows for development and/or implementation of future exploits and/or loss of data confidentiality. An adversary can gain insights in physical security measures, e.g. tamper seals, system configuration, and equipment types used that could allow them to carryout future attacks. Also, an adversary may gain key insights into whether prior exploits were effective or detected. Access is much easier, perhaps trivial because the system is no longer in use. As with other phases of the safeguards equipment lifecycle, our knowledge of the decommissioning phase was limited. However, there may be similarities to generic equipment decommissioning processes. Therefore, certain general assumptions were made about access vectors and preventive measures.

Decommission Access Vectors

If a system is disposed without controls i.e., in the trash, even a low-level adversary could gain access. Alternatively, an adversary can leverage insiders or trusted disposal organizations. Disposal schedules and procedures are likely considered unimportant and can be accessed via local or remote access to an organization's network.

Decommission Preventive Measures

- Develop procedures for end-of-life processing, including erasing all data and software.
- Maintain custody of equipment until controlled destruction is performed.

CONCLUSION

This study was conducted as a scoping effort that would also assess the applicability of a lifecycle-based cyber risk identification and assessment methodology for application to safeguards (Figure 1). The methodology can be applied to identify specific risks for equipment. It also successfully identified risk factors that may be broadly applicable to the safeguards domain. While cyber challenges exist at nearly every phase of the safeguards equipment lifecycle, security measures can be implemented throughout that help prevent the compromise of data and the loss of credibility of the IAEA. Specifically, vulnerability reviews and safeguards authorization processes should be leveraged to maintain the security of international nuclear safeguards equipment.

[4] BadUSB is a malware capability installed on USB drives that is capable of taking over PCs, invisibly altering files, or redirecting internet traffic. Greenberg, A. *Why the Security of USB is Fundamentally Broken*. Wired Magazine. July 31, 2014. https://www.wired.com/2014/07/usb-security/