Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

A novel approach for analyzing the nuclear supply chain cyber-attack surface

Shannon Eggers*

Idaho National Laboratory, Idaho Falls, ID, 83415, United States

ARTICLE INFO

Article history:
Received 19 February 2020
Received in revised form
23 July 2020
Accepted 24 August 2020
Available online 7 September 2020

Keywords:
I&C
supply chain
cyber-attack surface

ABSTRACT

The nuclear supply chain attack surface is a large, complex network of interconnected stakeholders and activities. The global economy has widened and deepened the supply chain, resulting in larger numbers of geographically dispersed locations and increased difficulty ensuring the authenticity and security of critical digital assets. Although the nuclear industry has made significant strides in securing facilities from cyber-attacks, the supply chain remains vulnerable. This paper discusses supply chain threats and vulnerabilities that are often overlooked in nuclear cyber supply chain risk analysis. A novel supply chain cyber-attack surface diagram is provided to assist with enumeration of risks and to examine the complex issues surrounding the requirements for securing hardware, firmware, software, and system information throughout the entire supply chain lifecycle. This supply chain cyber-attack surface diagram provides a dashboard that security practitioners and researchers can use to identify gaps in current cyber supply chain practices and develop new risk-informed, cyber supply chain tools and processes.

1. Introduction

Due in part to obsolescence, technology advancements, and economic factors, the U.S. nuclear industry is gradually modernizing instrumentation and control (I&C) systems on existing nuclear power plants (NPPs). For example, intelligent transmitters and digital controllers are replacing analog sensors and actuators; digital indicators and recorders are replacing analog indicators and pen-based chart recorders; and digital non-safety-related control systems, such as turbine control systems and feedwater control systems, are replacing analog control systems. Replacement of safety-related control systems, such as reactor protection systems (RPSs), is less common in the current U.S. nuclear fleet, partly due to a lengthy and uncertain licensing process.

New and advanced reactors, such as generation III+ reactors and small modular reactors (SMRs), deploy hybrid approaches incorporating analog transmitters and actuators in addition to digital I&C systems [1]. Furthermore, it is anticipated that new microreactors designed for autonomous, remote control will primarily use digital technology. While digital I&C provides increased flexibility, better performance, and improved reliability for an NPP [1], the expanded digital footprint increases the cyber-attack surface which subsequently increases cybersecurity risk.

Adversaries intent on malicious activity often use the easiest and most accessible attack pathway. Although the U.S. nuclear fleet has made significant progress in securing NPPs against cyber-attacks by implementing Cyber Security Plans (CSPs) in accordance with the Nuclear Regulatory Commission's (NRC) Cyber Rule, 10 CFR 73.54, "Protection of digital computer and communication systems and networks" [2], the supply chain pathway remains a weak link. Ongoing vulnerability of the nuclear supply chain is influenced by the following factors: (1) the ubiquitous nature of NPP digital instrumentation, (2) the increasing sophistication of malicious cyber actors, (3) the expanded global supply chain and limited production capabilities within the U.S., and (4) the difficulty assuring provenance and trustworthiness within the complex relationship of vendors, suppliers, fabricators, integrators, and contractors that make up the various supply chain stakeholders.

For example, a notional block diagram identifying subcomponents of an intelligent transmitter is shown in Fig. 1. These smart transmitters, installed throughout the nuclear fleet, use hardware, firmware, and software to receive analog process signals and convert the analog signal to a digital signal for mathematical transformation prior to conversion to a 4–20 mA output signal. Although these transmitters are relatively simple digital devices, over a dozen globally dispersed stakeholders might be involved in

* Corresponding author.
E-mail addresses: shannon.eggers@inl.gov, shannon.eggers@inl.gov.

https://doi.org/10.1016/j.net.2020.08.021

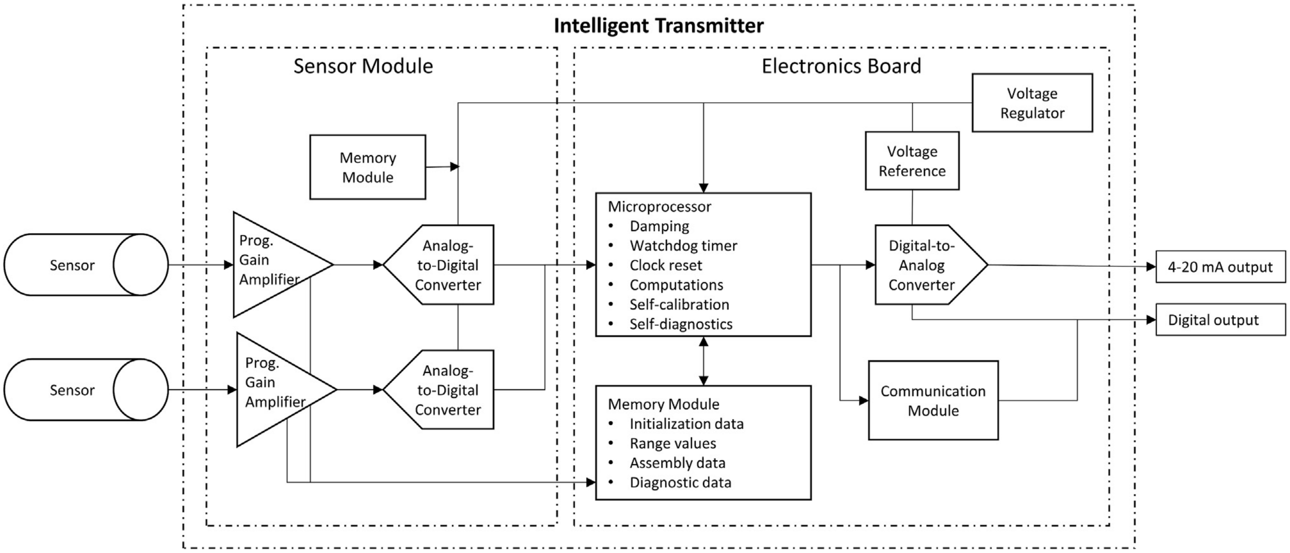

Fig. 1. Notional block diagram of an intelligent transmitter illustrating the number of subcomponents in a simple device. Not shown is the associated liquid crystal display, firmware, and software.

their end-to-end supply chain, including those who are involved in design, fabrication, manufacturing, programming, integration, and/or testing activities.

A goal of cybersecurity is to protect the confidentiality, integrity, and availability (C–I-A) of a system or component during operation. Maintaining confidentiality assures that sensitive information remains private and is only available to authorized users and devices. Although confidentiality is the least important goal in a digital I&C system, reconnaissance attacks enable adversaries to gather information about a system for development of future attacks. Maintaining integrity assures that accurate and complete data is used by the system. Data integrity attacks affect the truthfulness of the system by injecting false data, modifying commands, or altering system parameters. Adverse impacts from data integrity attacks include operator misdirection that leads to improper operator action or adverse system function. Maintaining availability assures there are no disruptions in systems or functions. Availability attacks, such as denial of service (DoS) or distributed denial of service (DDoS) attacks, may disrupt communication or data flow in a control system network to cause timing issues, unstable operation, or system shutdown.

Cyber-attacks may impact confidentiality, integrity, or availability during plant operations regardless of whether the attack is initiated via the internet or the supply chain. The adversarial goal for any cyber-attack is to exploit a system and then control, execute, and maintain a presence [3]. Exploits that result in loss of a digital I&C system's integrity, availability, or safety function are often categorized as malware insertion, hardware tainting, component substitution or corruption, information falsification, or component modification [3]. When a hardware, firmware, software, or system information attack occurs within the supply chain, it establishes an early presence in an asset's lifecycle such that it can remain persistent and unidentified by traditional information communication technology (ICT) perimeter defenses. For instance, if an adversary maliciously modifies the firmware of the intelligent transmitter shown in Fig. 1 during supply chain activities, installation of the transmitter in the plant will bypass system architecture security controls and the malware may remain undetected until it is triggered by pre-defined events or conditions.

In comparison to operational cybersecurity goals, the goals for supply chain cybersecurity are to protect the confidentiality, integrity, authenticity, and exclusivity of components (i.e., hardware, firmware, software, and system information) throughout the supply chain lifecycle [4]. Similar to maintaining confidentiality in an operational environment, maintaining confidentiality throughout the supply chain lifecycle assures that components remain private with no unauthorized transfer of data or secrets. Maintaining integrity throughout the supply chain lifecycle assures that components remain trustworthy, untainted, and uncompromised. Maintaining authenticity assures that components are genuine and not substituted or counterfeit. And, finally, maintaining supply chain exclusivity assures limited possession, control, or use of components by authorized and trusted stakeholders to reduce the number of cyber-attack entry points [4]. Improving the assurance of NPP supply chain confidentiality, integrity, authenticity, and exclusivity begins with understanding the entire supply chain cyber-attack surface. This knowledge can then be used to enhance cyber supply chain risk analysis, identify supply chain cybersecurity vulnerabilities, and develop mitigations or solutions.

The remainder of this paper is organized as follows: section 1 provides a background describing the digital footprint and cyber threat at NPPs. Section 2 identifies vulnerabilities for hardware, firmware, software, and system information within nuclear supply chains. Section 3 describes the digital I&C supply chain cyber-attack surface diagram. A discussion is provided in section 4 prior to ending the paper with conclusions and future work in sections 5 and 6. The intelligent transmitter illustrated in Fig. 1 will be referenced throughout the paper.

2. Background

2.1. *Digital footprint*

The digital footprint in an NPP includes ICT and operational technology (OT) equipment. Business systems used at an NPP include the desktop computing, enterprise applications, and network infrastructure used to enable corporate computing and communication requirements. Business systems are segregated from plant systems by maintaining a secure network architecture. An NPP's defensive architecture establishes strict and formal communication between network levels such that traffic from more secure control system levels (e.g., safety control system network) can only move outward toward less secure levels (e.g., plant network) as shown in Fig. 2 where Level 4 is the control system network. Communication between business system networks and less secure plant system networks may allow bidirectional traffic controlled by boundary protection devices, such as firewalls, intrusion prevention systems (IPSs), and intrusion detection systems (IDSs).

Digital assets in plant systems, structures, and components (SSCs) are used for the operation, safety, and security of the facility. SSCs in U.S. NPPs are considered digital assets (DAs) if they contain any combination of hardware, firmware, and/or software to execute internally stored programs or algorithms without operator action [6]. Furthermore, DAs are assessed as critical digital assets (CDAs) if they are components in systems (or support systems) providing safety-related, important-to-safety, security, or emergency preparedness functions [2]. The number of CDAs in a plant depends on the plant's design basis and how the CSP is implemented. On average, there are 2000 CDAs per NPP in the current U.S. nuclear fleet [7]. Due to increased use of digital technology, generation III+ reactors will have increased numbers of DAs.

CDAs are used in digital I&C systems, such as RPSs, engineered safety feature actuation systems, distributed control systems (DCSs), feedwater control systems, turbine control systems, and emergency diesel generator systems. CDAs used in I&C applications can include pressure, temperature, level, or flow transmitters, programmable logic controllers (PLCs), data recorders, computers, and data displays. CDAs may also be used in metrology, chemistry, and dose assessment applications.

A plant's physical protection system (PPS) includes CDAs, such as intrusion detection devices (e.g., cameras, motion detectors), radiation detectors, access control systems (e.g., hand geometry, badge readers, gate and door controllers), radios, and monitoring and alarm stations (e.g., computers, displays). Emergency preparedness (EP) applications required for communication during plant events include CDAs, such as Voice over Internet Protocol (VoIP) telephone systems, computers, displays, and emergency notification systems. The majority of digital SSCs are connected by a plant's secure network architecture, which includes typical ICT devices, such as network switches, routers, firewalls, IPSs, IDSs, and data diodes.

Many plant digital systems, such as an RPS, DCS, or PPS, are custom engineered by a vendor. Other applications may be designed and assembled in-house. Both custom engineered and in-house designed systems, however, are often implemented with commercial-off-the-shelf (COTS) components. COTS components are also commonly used in instrumentation, EP, network, and plant computer applications. Engineers, vendors, and integrators often choose to use commercially available hardware, firmware, and software due to lower cost, greater availability, better interoperability, and larger feature selection.

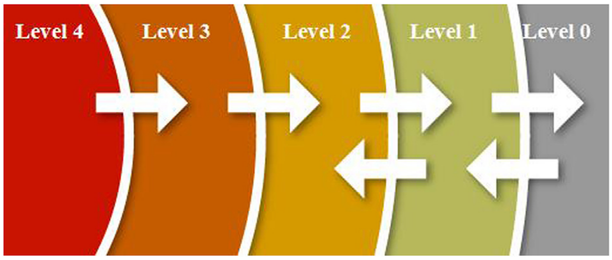

Fig. 2. Simplified cybersecurity defensive architecture illustrating data and network communication direction [5]. Level 4 is the control system network.

2.2. Cyber threat vectors and adversaries

In the U.S., an NPP is required to provide high assurance that CDAs are adequately protected against cyber-attacks, up to and including the plant's design basis threat as required by 10 CFR 73.54 [2]. Cyber-attack threat vectors in an NPP include both wired and wireless networks at the facility, portable media and mobile devices (PMMD), insiders, and supply chain. While NPP licensees implement technical, physical, and administrative controls to improve a facility's security posture by following guidance in Regulatory Guide 5.71 [5], NEI 08–09 revision 6 [8], and NEI 13–10 revision 5 [9], the supply chain for CDAs remains one of the most challenging threat vectors to secure at a nuclear facility. In addition to the acquisition guidance provided in Regulatory Guide 5.71 and NEI 08–09, subsequent publication of NEI 08-09 Addendum 3 provided further guidance on systems and services acquisition. However, while this addendum provides security controls for a licensee to use where they have responsibility for activities within the supply chain (i.e., from factory acceptance testing onward), it does not adequately address cybersecurity earlier in the lifecycle [10]. Moreover, Addendum 3 does not sufficiently address subcomponents, such as integrated circuits (ICs) or third-party software libraries or services. Although many security practitioners in industry, government, and academia are engaged in research to improve the cyber-resilience of the supply chain, it is still very difficult to secure I&C hardware, firmware, software, and system information through each stage of the supply chain, especially as components and subcomponents move from one stakeholder to another via physical and/or electronic channels [11–13].

Adversaries intent on damaging critical infrastructure are becoming increasingly more sophisticated. In fact, these attacks are often long-term offensive cyber campaigns planned and executed by nation states, such as Russia, China, North Korea, and Iran [14–19]. The goal of an OT cyber-attack is to impact the confidentiality, integrity, or availability of SSCs. The Stuxnet, BlackEnergy3, and CrashOverride malware established that highly motivated and resourced adversaries (i.e., nation states, well-funded terrorist organizations) can maliciously cause physical equipment damage or mal-action via a cyber-attack [20–22]. Furthermore, the Triton malware attacks on Schneider Electric's Triconex Safety Instrumented System controllers have demonstrated that adversaries can launch an attack against a safety control system, thereby adversely affecting safe shutdown of an industrial process [23].

3. Nuclear supply chain cyber-attack surface

3.1. Overview

Similar to traditional kinetic warfare, the increasing sophistication of cyber-attacks has led to the development of improved cyber defense controls in NPPs, including changes in plant network architectures. Malicious actors often use the least secure and easiest pathway to launch a cyber-attack. Nuclear facilities are increasingly implementing one-way deterministic data diodes to prevent data and network communication into control networks from less secure networks. Since data diodes reduce the risk of internet-based attacks, there is an increased likelihood that adversaries intent on compromising CDAs will target less protected pathways, such as the supply chain. While the Triton malware attacks on the Triconex system were launched via insecure network architecture [23], it is possible that a sophisticated adversary could develop a similar attack by infiltrating the supply chain. In fact, Symantec reported that the number of software-based supply chain attacks in 2018 increased by 78% compared to the previous year due to increases in hijacked software update processes, compromised third-party libraries and services, and stolen credentials [24].

As the ubiquitous use of COTS components in digital I&C systems increases and the supply chain becomes progressively more globalized, adversarial focus has shifted towards exploiting vulnerabilities throughout the design and acquisition process. Supply chain attacks may use the same tactics, techniques, and procedures (TTPs) as other attack methods; the difference is that supply chain exploits can be introduced early in the product lifecycle such that they remain persistent and undetected until triggered [3]. In addition, the use of commodity hardware and software lowers barriers of entry by enabling the adversary to use publicly available information to gain the knowledge necessary for successful exploits. The adversary may even have access to previously developed malware or attacks they can re-use in their campaign [25,26].

3.1.1. Supply chain vulnerabilities

I&C supply chain attacks are malicious actions or sabotage on hardware, firmware, software, or system information for the purpose of theft, counterfeiting, disruption, destruction, or compromise of the function or operation of the device. Tampering of systems can introduce malicious logic, hidden functionality, exploitable defects, or intentional backdoors for future cyber operations. In general, hardware, firmware, and system information are more susceptible to compromise during supply chain activities than during device installation and operation, while software is vulnerable throughout its entire lifecycle. Furthermore, attacks embedded into hardware and firmware are generally stealthier than software attacks, and they are often misidentified as design flaws or bugs.

While the global supply chain has shortened time-to-market, delivery speed, and component availability, this growth has resulted in expanded cyber risk from nation states. In 2019, Daniel Coats, the U.S. Director of National Intelligence, reported that China, Russia, Iran, and North Korea will increasingly use cyber espionage, attack, and influence to steal information and disrupt critical infrastructure [15]. In addition, the U.S. Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency have issued alerts warning that the Chinese government is carrying out a cyber campaign against technology service providers [18] and that the Russian government is involved in a multi-stage intrusion campaign targeting critical infrastructure sectors [19].

China is a global leader in technology and a leading provider of electronic components and electronic manufacturing. Chinese companies are not only often subsidized by the government, they are also legally required to work with them and their intelligence services. The IC market has grown dramatically with an annual 41% increase in 2017 to $699 billion [27]. During the 10-year period prior to 2017, the U.S. reduced IC imports by 35%, while China increased imports by 247%. In 2017, China led the world with $207 billion IC exports while importing $80.1 billion ICs [27].

This shift of IC production away from the U.S. has reduced prices and increased availability in the global IC market. However, due to the known ongoing cyber campaigns, it has greatly increased vulnerability within the supply chain. In 2012, a U.S. Senate Armed Services Committee investigation found over one million suspect counterfeit electronic parts from China that were bound for critical military systems [28]. As stated by Nissen et al. on the cyber vulnerabilities in the Department of Defense (DoD) supply chain, "we are in an era of adversarial asymmetric warfare for which we have no comprehensive defense" [13]. Although these reports were focused on vulnerabilities in the DoD electronics supply chain, the same concern with counterfeit and corrupted digital assets exists in all critical infrastructure sectors, including energy and nuclear power. In fact, due to findings that foreign adversaries are increasingly creating and exploiting vulnerabilities in the U.S. bulk-power system, the U.S. President signed Executive Order 13920 on May 1, 2020 to prohibit the acquisition, transfer, import, or installation onto the U.S. power grid any bulk-power system electric equipment that was designed, manufactured, or supplied by a foreign adversary that poses a risk to the bulk-power system or the security of the U.S. critical infrastructure [29,30]. The current list of foreign adversaries includes China, Russia, Iran, Korea, and Venezuela [29,30]. It is clear that the U.S.'s reliance on IC and electronics imports combined with the advancing threat of state-sponsored cyber campaigns has increased the risk of supply chain attacks in the U.S. nuclear fleet.

3.1.2. Hardware

Hardware includes microelectronic components such as ICs that are further manufactured or assembled into larger hardware devices (i.e., microprocessors, memory chips, logic chips) or other peripherals (i.e., expansion drives, communication controllers). Security breaches in the supply chain via direct access to hardware description languages, basic input/output system (BIOS) code, bitstream, logic, configuration files, or chip interfaces can enable adversaries to obtain confidential intellectual property (IP) information which can then be used to reverse engineer a device to develop hardware clones or counterfeits. A taxonomy of counterfeit parts includes recycled, remarked, overproduced, out-of-specification or defective, and cloned category types [31,32]. It is estimated that 80% of reported counterfeits are recycled ICs [32].

Reverse engineering, testing, and side-channel analysis can also reveal confidential information and stored secrets, such as cryptographic authentication or encryption data for protected IP [33]. In addition, physical access to the device could allow an adversary to tamper with hardware settings or introduce a Trojan horse or backdoor into the logic or circuitry. A hardware Trojan can impact C–I-A through functionality, specification, confidentiality, or DoS attacks [34]. Functionality attacks may tamper with the inputs and outputs of a module, modify hardware computation, bypass existing security checks, or affect a communications channel [33,34]. Specification attacks change parametric properties such as timing and power usage; confidentiality attacks occur by leaking sensitive or confidential information; and DoS attacks exhaust bandwidth, computation, or battery power to partially or permanently degrade or disable the device [34]. Referring back to the intelligent transmitter in Fig. 1, a functionality attack could potentially modify hardware computation on the electronics board resulting in an inaccurate output signal.

The design and manufacturing lifecycle of an IC typically includes specification, design, fabrication, testing, and assembly stages. All stages are vulnerable to hardware attacks due to reliance on third parties, such as tool vendors, IP vendors, designers, and foundries. Hardware Trojans can be introduced directly onto the device or by compromising the tools and software used during the IC lifecycle. Additionally, hardware Trojans typically have two parts—a trigger and a payload. The trigger monitors the signals or events in a circuit. Once the expected condition is met, the payload, or malicious behavior, is activated [35]. While there has not yet been a verified, publicly disclosed supply chain hardware Trojan attack, the large number of attacks proposed and demonstrated by the research community suggest that it is only a matter of time before adversaries adopt these TTPs.

3.1.3. Firmware

Firmware is the bridge between hardware and software; it runs higher level operations and controls basic functionality of the device, including communication, program execution, and device initialization. The firmware lifecycle typically includes design, processing, synthesis, verification, and configuration stages. The process is often iterative, interfacing with hardware fabrication to verify component operation.

By reverse engineering firmware, adversaries can learn the system, identify vulnerabilities, and corrupt code by alteration or insertion. Firmware can be reprogrammable and is, therefore, also vulnerable to supply chain attacks during routine updates or maintenance. For instance, an adversary can corrupt a firmware update package prior to installation on the device or a third-party service provider can directly add malicious code to the firmware during device maintenance. Firmware updates are often delivered as binaries without access to source code. In addition, vendors often deliberately obfuscate proprietary code to make it more difficult to compromise and steal. Both techniques make it hard for customers to verify the integrity of firmware updates.

Malicious firmware can hijack root access, steal data, affect device operation, and even disable the device similar in nature to the Shamoon cyber warfare virus, which was designed to make a device unusable by erasing its master boot record [36]. In 2019, hackers developed ShadowHammer, a Trojan version of the ASUS Live Update Utility, which was distributed to victims through the application's own update tool [37]. This utility updates the Unified Extensible Firmware Interface (UEFI) firmware, hardware drivers, and other ASUS tools. ShadowHammer targeted specific digital devices using tampered binaries signed with legitimate certificates to mask detection. A compromised UEFI provides an adversary full control over the device and can lead to propagation of additional malware, loss of sensitive information, and malfunction of the device.

Although secure architectures implemented in most nuclear facilities prevent automatic updates and reduce the risk of internet-based attacks, similar sophisticated and targeted firmware attacks are possible in air-gapped networks since testing and PMMD scanning may not detect the corrupted firmware prior to device update. For instance, an end user may download a firmware update package for the intelligent transmitter in Fig. 1 from the vendor, verify legitimacy using assumed valid certificates, and then transfer the updated, malicious firmware to the transmitter using a maintenance laptop. Once malicious code is inserted into firmware, it is often persistent and resilient—it can remain present even after the device is rebooted, software is reinstalled, or the device is rebuilt. Malicious firmware also usually remains undetected by traditional ITC tools that monitor the operating system or software.

3.1.4. Software

The software layer includes various operating systems, platforms, and packages used for I&C process control, Human-Machine Interfaces (HMIs), terminals, and application programming interfaces (APIs). Software used in I&C systems may include proprietary software, commercial software, and open-source software including third-party services or libraries. Software applications often contain numerous components. In 2019, Sonatype analyzed 500 applications and discovered that the average application contained over 450 software component releases, of which 85% were open source [38]. Sonatype also reported that repository managers are used by over 9 million developers as part of their development tool set [38].

Software is vulnerable to compromise during all phases of its lifecycle, including supply chain activities such as design, development, and maintenance, as well as during normal operational use. Software supply chain attacks take many forms: malicious code may be inserted into legitimate software, credentials may be stolen, third-party libraries may be compromised, and software updates may be hijacked. The HeartBleed Bug infected a popular version of OpenSSL, a third-party, open-source library used to protect information communicated through the Transport Layer Security (TLS) protocol (CVE-2014-0160) [39]. Although TLS is not commonly used in control system communications, secure authentication features added to other process automation communication protocols could potentially be compromised in a similar manner.

Additionally, the Stuxnet attack against the Natanz uranium enrichment facility was enabled through the supply chain—it is speculated that the private keys of two manufacturing companies were stolen to enable valid digital signatures for the maliciously modified software [40]. The subsequent introduction of the malware into the air-gapped network of the facility's control system caused destruction of centrifuges by oscillating the frequency of their operating speeds. As current NRC and NEI guidance does not adequately protect against supply chain attacks using stolen credentials, nuclear plants remain susceptible to attacks using these TTPs.

As with firmware, the software updating process can also be hijacked. In the 2014 Monju incident, an employee downloaded a software update on a computer connected to the business network in the control room of the Monju fast breeder reactor in Japan. The update package included a variant of the 'Gh0st RAT' Trojan that subsequently enabled exfiltration of corporate data to an external command and control (C2) server [41]. Technical data stolen in this attack was released online, thereby providing sensitive information that adversaries could use to develop future attacks. Similarly, in 2015, the Kingslayer malware was delivered through a popular Windows administration event log management software via a redirected download site. After the compromised update was installed, secondary malware was loaded [42]. Although Kingslayer targeted large corporations and not nuclear plants, the sophistication of this supply chain attack highlights the fact that hijacked software update channels can be used to launch attacks within the nuclear supply chain.

The Dragonfly group, also known as Energetic Bear, has launched several software-based attacks against critical infrastructure sectors, including the energy sector. At least three different attack vectors—phishing, compromised third-party software, and hijacked software updates—were used to deliver the Havex malware, a remote access tool that provided attackers with C2 capabilities on compromised computers [43]. And finally, the highly destructive NotPetya global cyber-attack on energy companies and other critical sectors that caused computers and equipment to go offline was reportedly spread by a hijacked software update of a popular Ukrainian tax software [44]. Even though internet-based attacks are unlikely in secure architectures and most reported software update hijacks are not directed against I&C systems, attacks launched via software or firmware updates remain an ongoing concern.

3.1.5. System information

System information is the complete record of information regarding a digital system or component, including system level and component level information and/or data such as requirements specifications, design documentation, fabrication, assembly or manufacturing details; validation and verification documentation; operation and maintenance manuals; credential, authentication, or cryptographic information; and product lifecycle plans. Theft, falsification, or substitution of system information may occur throughout the supply chain lifecycle. Compromise of this information could result in devices designed, manufactured, or updated with malicious or falsified data, thereby impacting operational and/or safety functions, introducing latent vulnerabilities, or providing backdoors for future adversarial use.

3.2. Digital I&C system supply chain cyber-attack surface

NIST defines attack surface as "the set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment [45].” When applied to a digital I&C component or system installed in an NPP, the attack surface includes the access points on a device as well as the system architecture. Miller applied the concept of attack surface to the DoD acquisition process by developing a supply chain attack framework based upon NIST SP 800–30 revision 1 [46], Common Attack Pattern Enumeration and Classification (CAPEC) [47], and Threat Assessment and Remediation Analysis (TARA) [48]. Miller identified points of malicious insertion attacks at six supply chain locations and two supply chain linkages to enumerate 41 supply chain attack patterns consisting of 12 different attack attributes [49]. Supply chain locations included the program office, prime contractor, subcontractor(s), hardware/software integration, primary hardware production, and primary software production. Supply chain linkages included logistics, or physical flow, as well as ICT information and data flow [49].

A novel digital I&C supply chain cyber-attack surface that extends the work of Miller [49] and other leading researchers [3,50,51] is shown in Fig. 3. This attack surface illustrates the complex network of stakeholders and activities involved in the unique flow paths of hardware, firmware, and software design and development activities as well as the flow paths for system integration, testing, installation, decommissioning, and maintenance. Each element of Fig. 3—lifecycle, stakeholders, touchpoints, supply chain attacks, and attack likelihood—is further described in the following sections.

3.2.1. Supply chain lifecycle

The supply chain lifecycle of a digital I&C component or system depends on whether the item procured is COTS, engineered, or custom in-house. In general, each hardware, firmware, and software component will have a unique lifecycle prior to integration. For instance, the supply chain lifecycle for the intelligent transmitter in Fig. 1 will include a separate path for each hardware subcomponent (i.e., microprocessor, memory module, communications module, digital display), each firmware package to control the hardware components, and for each software application required for operation, communication, and configuration tasks. Once the individual design, development, and testing activities of the hardware, firmware, and software stages are complete, the components are integrated and configured into the final specified transmitter model prior to additional testing and installation. Larger, more complex I&C systems will have multiple tiers of subcomponents and components that must be integrated according to the requirements specifications. These complex systems will also have multiple levels of testing—unit testing, system testing, factory acceptance testing, site acceptance testing—prior to commissioning and operation. Later stages of the lifecycle include maintenance, repair and return, and decommissioning.

3.2.2. Stakeholders

Fig. 3 also identifies the key stakeholders who have responsibility for the activities performed in each stage of the lifecycle. These stakeholders denote potential cyber-attack entry points where subversion of the design, integrity, or trustworthiness can occur. Adversaries can infiltrate any of the stakeholder organizations either as an insider or by using TTPs to gain a foothold through an insecure attack vector. An I&C system may have a mixture of COTS, engineered, and custom hardware components and software. Regardless, the supply chain includes multiple tiers of stakeholders. The prime contractor or integrator typically has many subcontractors, each of which may have their own designers, fabricators, and manufacturers. Every level of the supply chain, including manufacturing, production, distribution, installation,

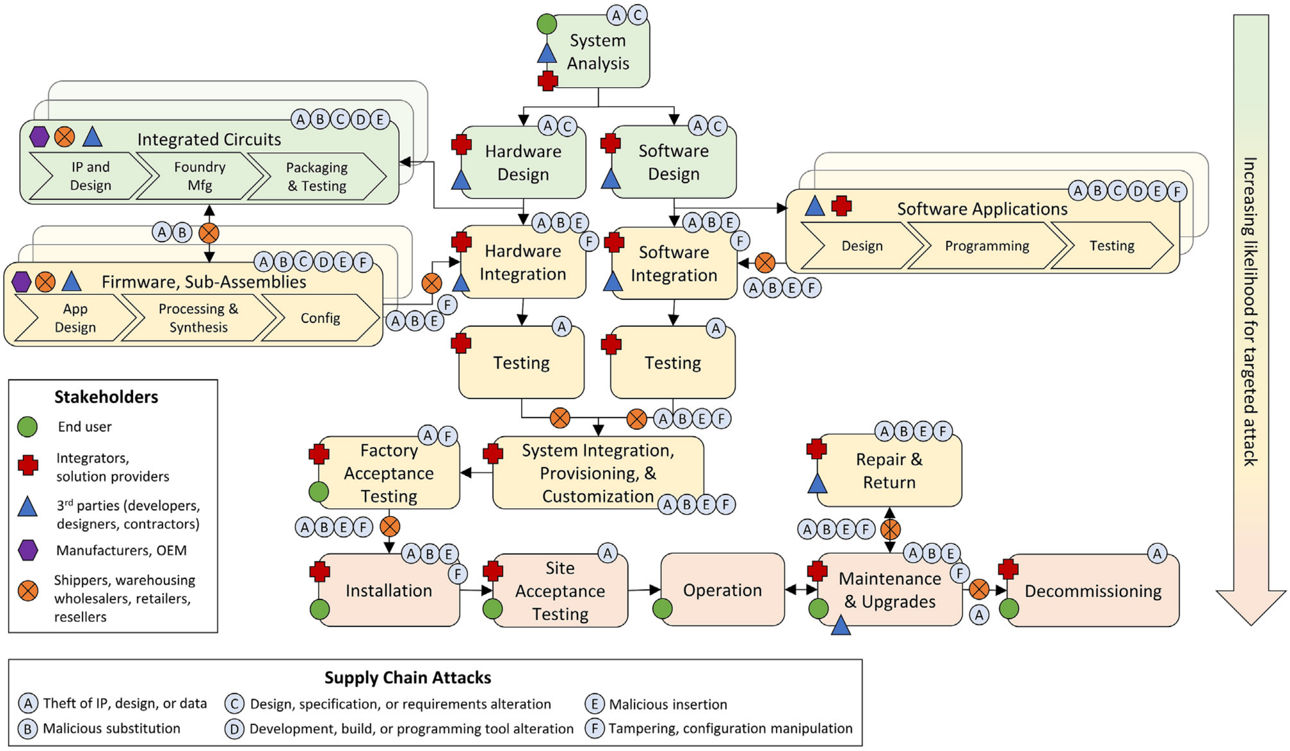

Fig. 3. The digital I&C system supply chain cyber-attack surface. A novel model illustrating the complexity of the digital I&C supply chain lifecycle overlaid with potential supply chain attacks at key stakeholder locations and touchpoints [52].

repair, and maintenance, is vulnerable to attack whether it is by theft, tampering, counterfeiting, disruption, or other compromise. And, although a prime contractor may be considered a trusted supplier, the subcontractors may have less control over design, manufacturing, and security of the hardware or software than a higher tier supplier. Adversaries are more likely to attack the least secure target with the highest success probability. Often, this target is a lower tier entity, such as a subcontractor, designer, developer, or component original equipment manufacturer, who has fewer cyber defenses implemented.

Although a stakeholder may have other roles throughout the lifecycle, only the responsible role, consistent with the RACI (Responsible, Accountable, Consulted, Informed) matrix, is identified in Fig. 3. These roles will vary depending on whether the item procured is COTS, engineered, or custom in-house. For example, an end user purchasing the intelligent transmitter in Fig. 1 will likely only have responsibility for activities from the installation stage onward while an end user requesting a custom, engineered product may have responsibilities earlier in the lifecycle, including systems analysis and factory acceptance testing. It is unlikely that an NPP end user will have responsibilities for other lifecycle stages unless they are building the solution in-house. An important insight identified through analysis of this supply chain cyber-attack surface is that end users often have limited visibility into the supply chain and often only focus on first-tier suppliers. Since the NRC and NEI service and acquisition security controls primarily address procurement and transport from the system integration stage onward, new tools and processes are needed to expand visibility into the remaining supply chain stakeholders.

3.2.3. *Touchpoints*

Touchpoints are also identified in Fig. 3. Touchpoints are the locations at which an adversary can compromise a system or component, including stakeholder locations, physical storage locations, electronic repositories, and transitions between these locations. Often, a stakeholder such as a software developer will have a secure facility and development environment, but the electronic repository and the transmission channel required to move software from one stakeholder to another is insecure. With over 9 million software developers using repository managers [38], it is important to address security controls for these digital storage locations. Hardware storage locations and distribution channels are similarly vulnerable to compromise by physical attack or theft, regardless of whether the component is located on a truck or in a warehouse, wholesaler, retailer, or reseller location. Since systems and components are most vulnerable transitioning from one trustworthy environment to another, NPPs must consider these insecure transitions when analyzing their cyber supply chain risk.

3.2.4. *Supply chain attacks*

Table 1 provides a taxonomy of supply chain cyber-attack types as developed in [10]. These supply chain attacks are defined as to “how” the attack occurs and are not specific to a lifecycle stage, stakeholder, or touchpoint. For example, a malicious insertion attack could occur in the intelligent transmitter during hardware, firmware, or software design and development; during integration, installation, maintenance, and repair; and during all the transitions in between.

Vulnerabilities and cyber risks vary throughout the supply chain lifecycle. During design phases, adversaries may steal IP, compromise design tools, alter design requirements, identify security mechanisms, or insert design vulnerabilities. Hardware components can be compromised during manufacturing and production activities via IP theft, reverse engineering, counterfeiting, overproduction, and cloning. The cyber risks associated with ICs are exacerbated due to the fact that only one of the top 10 microelectronic foundries, GlobalFoundries, is located in the U.S. (2Q19 data) [53]. The other nine foundries are located in Taiwan, South Korea, China, and Israel. In addition, while GlobalFoundries is based in the U.S., it is indirectly owned by the government of Abu Dhabi. The industry’s reliance on purchasing microelectronics from nation states known to be engaged in cyber warfare is an ongoing security concern.

Like hardware, software and firmware is vulnerable throughout the supply chain lifecycle. Software can be modified with malicious code such as logic bombs or Trojan kill switches, configured to change functionality, or altered to add backdoor capabilities for future exploitation. As noted, all software and firmware used in a systems design is vulnerable—including custom software, source code repositories or software libraries, open-source or third-party software, and COTS software.

It is important to consider the protection of system information throughout the lifecycle. As indicated in Fig. 3, system information is vulnerable to compromise or theft at all stages. Alteration of system design requirements or design data prior to manufacturing and integration enables the compromise to become part of the design record, thereby hiding its presence in plain view. Stolen design, IP, or other sensitive data provides adversaries with reconnaissance information they can use for further exploits, economic gain, or insight into methods for attacking the nation’s critical infrastructure. Theft of security credentials enables an adversary to “legitimately” sign code and appear as a trusted supply chain identity. In addition, an intelligent adversary who steals or acquires information on an NPP’s network architecture and/or I&C systems gains important building blocks they can use to further develop and launch a sophisticated, targeted attack on an NPP.

3.2.5. *Attack likelihood*

As shown in Fig. 3, attacks targeting a specific I&C installation are more likely to be launched further down the supply chain as the intended facility and final application may be unknown earlier in the lifecycle. This is especially true for applications using COTS hardware and software as these assets may be used in many different industries and control systems. For instance, ICs used in the intelligent transmitter in Fig. 1 may be common for a variety of transmitter models with the ultimate destination and configuration unknown until installed in a plant. Compromise of an IC in this instance may cause operational disturbances but would unlikely be a targeted attack intended to cause a specific outcome. However, this trend is not always the case—if an IC is designed and fabricated specifically for a unique application, an adversary may learn this information and use it to launch a targeted, advanced, and persistent attack early in the supply chain lifecycle. In fact, Stuxnet generically infected a specific PLC model but the payload was not triggered until installed in the Natanz centrifuge PLCs [20].

In addition to the potential for more targeted attacks as the device proceeds through the supply chain, the attack likelihood, including number of attacks, also increases with each new stage, stakeholder, and touchpoint. The cumulative number of potential compromises is dependent on the complexity of the device or system. Using cyber-informed engineering processes to simplify a system and reduce design complexity will inherently reduce the number of touchpoints and, therefore, reduce the overall supply chain cyber-attack surface and cumulative attack probability.

4. Discussion

The supply chain cyber-attack surface reveals that a key to reducing cyber supply chain risk is to establish accurate and complete bills of material (BOM) for CDAs that move beyond first- or

Table 1
Taxonomy of supply chain cyber-attack types in Fig. 3 [10].

Attack Type	Description
Theft of IP, design, or data	Unauthorized disclosure of information from a stakeholder who has a trust relationship with the end target, enabling future attacks and/or causing economic loss. This may include but is not limited to IP, design information, operational/configuration data, or stored secrets (i.e., private key, digital certificates).
Malicious substitution	Complete replacement of digital technology, including hardware, firmware, and/or software. Hardware clones or counterfeits may not impact all end users depending on the distribution, whereas a substituted software package may compromise all end users even if only a few were targeted.
Design, specification, or requirements alteration	Unauthorized modification of design, specifications, or requirements that compromises the design stages and results in the purposeful inclusion of latent design deficiencies (e.g., requirements that result in vulnerabilities) or built-in backdoors.
Development, build, or programming tool alteration	Unauthorized modification of the development environment, including platform, build and programming tools, with the intent to corrupt the device under development.
Malicious insertion	Addition or modification of information, code, or functionality directly into a device to cause malicious intent, such as impairing or altering device operation or function.
Tampering, configuration manipulation	Unauthorized alteration or fabrication of configuration, non-executable data, or sending of unauthorized commands with the goal of impacting device operation or function.

second-level items to include all subcomponents of hardware, firmware, and software. While proprietary obfuscation protects IP and is arguably a security control, it is also a vulnerability. Additionally, designers and vendors should focus on using cyber-informed engineering practices to simplify the design. Shrinking the BOM reduces the supply chain cyber-attack surface, thereby improving cyber supply chain exclusivity by limiting the number of stakeholders and touchpoints involved in the lifecycle.

NPPs should also focus on improving supply chain confidentiality and supplier trustworthiness by establishing and verifying capabilities for suppliers beyond the first tier of stakeholders. As shown, NPPs should not rely solely on NEI and NRC guidance to establish supply chain cybersecurity controls as this guidance does not adequately address all stages of the lifecycle, stakeholders, and touchpoints. Cybersecurity maturity models, such as the DoD Cybersecurity Maturity Model Certification [54] or Department of Energy Cybersecurity Capability Maturity Model (C2M2) [55], provide a framework NPPs can tailor to evaluate a supplier's compliance with cybersecurity best practices.

Initial steps for improving cyber supply chain integrity and authenticity include limiting purchases to components and systems that are certified to meet cybersecurity standards. While these cybersecurity product certifications are not a panacea eliminating all cyber supply chain risk, they do require suppliers and products to meet minimum cybersecurity thresholds to provide a heightened level of oversight. Finally, in addition to maintaining their Counterfeit, Fraudulent, and Suspect Items program [56] per NRC requirements, NPPs should consider joining or forming industry-wide data sharing organizations, if not already a member. These groups, such as the Government-Industry Data Exchange Program [57] and ERAI [58], share technical information on product quality, reliability, and veracity, including supply chain compromises.

5. Conclusions

As illustrated in Fig. 3, the digital I&C system supply chain cyber-attack surface is extensive and complex. Systems may contain significant numbers of digital devices and subcomponents. The hardware, firmware, software, and system information associated with these digital systems each have their own unique supply chain that may include design and development, manufacturing, assembly, integration, transportation and distribution, testing, maintenance, repair and return, and end-of-life activities. The stakeholders involved in the design of I&C systems are often organized in multi-level matrix environments that have several tiers of geographically dispersed subcontractors. Each digital asset is potentially vulnerable to compromise at any stakeholder location during any lifecycle stage. The assets are also vulnerable during transportation and storage (physical or logical) as they transition from one stakeholder and/or stage to another.

The evolution of cyber warfare and adversary sophistication will continue to change the threat landscape and impact an NPP's cyber risk. The novel supply chain cyber-attack surface described in this paper provides a dashboard for security practitioners to use in their cyber supply chain risk management process to identify unknown threats and vulnerabilities during procurement of CDAs. Using this dashboard to understand the broader cyber supply chain network, including the multiple tiers of stakeholders and touchpoints for a CDA's entire BOM, provides greater awareness of the supply chain attack surface. Practitioners can use this risk-informed knowledge to identify gaps in current processes and security controls to enable prioritization and development of improved tools and procedures.

Future work

The supply chain cyber-attack surface described in this paper will be used as a platform for continued cyber supply chain research to support the existing fleet of light water reactors as well as new advanced reactor technologies, such as SMRs and micro-reactors. Improved cyber supply chain risk analysis techniques identified through use of this platform will enable research and development of provenance-aware supply chains, enhanced security credential validation processes, improved developer and end user testing methods, and more secure tamper-proof distribution methods.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

I would like to thank Timothy McJunkin and Julio Rodriguez for their critical reviews. This research was funded by the U.S. Department of Energy Office of Nuclear Energy Cybersecurity research and development program under DOE Idaho Operations Office, Contract DE-AC07-05ID14517.

References

[1] T. Quinn, J. Mauck, K. Thomas, Digital Technology Qualification Task 2-Suitability of Digital Alternatives to Analog Sensors and Actuators, Idaho National Laboratory, 2012.

[2] 10 C.F.R. § 73.54 Protection of Digital Computer and Communication Systems and Networks, U.S. Nuclear Regulatory Commission, 2009.
[3] W.J. Heinbockel, E.R. Laderman, G.J. Serrao, Supply Chain Attacks and Resiliency Mitigations, The MITRE Corporation, 2017.
[4] M. Windelberg, Objectives for managing cyber supply chain risk, International Journal of Critical Infrastructure Protection 12 (2016) 4–11.
[5] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, January 2010.
[6] NEI 10-04, Identifying Systems and Assets Subject to the Cyber Security Rule, Revision 2, Nuclear Energy Institute, July 2012.
[7] Advisory Committee on Reactor Safeguards Digital Instrumentation and Control Systems, U.S. Nuclear Regulatory Commission, 2019.
[8] NEI 08-09, Cyber Security Plan for Nuclear Power Reactors, Revision 6, Nuclear Energy Institute, April 2010.
[9] NEI 13-10, Cyber Security Control Assessments, Revision 5, Nuclear Energy Institute, February 2017.
[10] S. Eggers, M. Rowland, Deconstructing the nuclear supply chain cyber-attack surface, in: Proceedings of the INMM 61st Annual Meeting, Online Virtual Meeting, 2020. July 12-16.
[11] S. Boyson, Cyber supply chain risk management: revolutionizing the strategic control of critical IT systems, Technovation 34 (7) (2014) 342–353.
[12] N. Bartol, Cyber supply chain security practices DNA – filling in the puzzle using a diverse set of disciplines, Technovation 34 (7) (2014) 354–361.
[13] C. Nissen, J. Gronager, R. Metzger, H. Rishikof, Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War, The MITRE Corporation, 2019.
[14] C. Anderson, K. Sadjadpour, Iran's Cyber Threat: Espionage, Sabotage, and Revenge, Carnegie Endowment for International Peace, 2018.
[15] D.R. Coats, Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community 29, Office of the Director of National Intelligence, 2019. January.
[16] Global Oil and Gas Cyber Threat Perspective: Assessing the Threats, Risks, and Activity Groups Affecting the Global Oil and Gas Industry, Dragos, August 2019.
[17] Annual report to Congress, Military and security developments involving the People's Republic of China, Office of the Secretary of Defense, 2019.
[18] US-CERT, TA17-117A: Intrusions affecting multiple victims across multiple sectors, Revised December 20 (2018).
[19] US-CERT, TA18-074A: Russian government cyber activity targeting energy and other critical infrastructure sectors, Revised March 16 (2018).
[20] R. Langner, Stuxnet: dissecting a cyberwarfare weapon, IEEE Security & Privacy 9 (3) (2011) 49–51.
[21] ICS-CERT, Ongoing Sophisticated Malware Campaign Compromising ICS, Update E, 2016.
[22] ICS-CERT, Cyber-attack against the Ukranian Critical Infrastructure, 2016.
[23] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, C. Glyer, Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure, FireEye Threat Research Blog, 2017.
[24] Symantec, Internet security threat report, February 24 (2019).
[25] https://arstechnica.com/information-technology/2019/05/stolen-nsa-hacking-tools-were-used-in-the-wild-14-months-before-shadow-brokers-leak/.
[26] https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/.
[27] Integrated circuits trade. The Obervatory of Economic Complexity (OEC). Accessed on: April 4, 2020. Available: https://oec.world/en/profile/hs92/8542/.
[28] C. Levin, J. McCain, Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts, Senate Committee On Armed Services, 2012.
[29] Executive Order 13920 of May 1, 2020, Securing the United States Bulk-Power System, The U.S. President, 2020.
[30] Securing the United States Bulk-Power System 85, Department of Energy, 2020. Federal Register, DOE-HQ-2020-0028.
[31] U. Guin, N. Asadizanjani, M. Tehranipoor, Standards for hardware security, GetMobile: Mobile Comput. Commun. 23 (1) (2019) 5–9.
[32] M. Tehranipoor, U. Guin, D. Forte, Counterfeit Integrated Circuits: Detection and Avoidance, Springer, 2015.
[33] B. Liu, R. Sandhu, Fingerprint-based detection and diagnosis of malicious programs in hardware, IEEE Trans. Reliab. 64 (3) (2015) 1068–1077.
[34] M. Beaumont, B. Hopkins, T. Newby, Hardware Trojans-Prevention, Detection, Countermeasures (A Literature Review), Australian Department of Defense, 2011.
[35] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, M. Tehranipoor, Hardware Trojans: lessons learned after one decade of research, ACM Trans. Des. Autom. Electron. Syst. 22 (1) (2016) 1–23.
[36] US-CERT, ICS joint security awareness report (JSAR-12-241-01B): Shamoon/DisTrack malware (Update B), Revised April 18 (2017).
[37] https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/.
[38] 2019 State of the Software Supply Chain: the 5th Annual Report of Global Open Source Development, Sonatype, 2019.
[39] US-CERT, TA14-098A: OpenSSL 'heartbleed' vulnerability (CVE-2014-0160), 2016. Revised October 5.
[40] N. Falliere, L.O. Murchu, E. Chien, W32.Stuxnet Dossier, Symantec, 2011, Version 1.4.
[41] M. Graham, Context threat intelligence - the Monju incident, Context Information Security (Febrary 2014).
[42] Kingslayer - A Supply Chain Attack, RSA Research, February 2017.
[43] ICS-CERT, ICS-ALERT-14-176-021: ICS focused malware (Update A), Revised August 22 (2018).
[44] US-CERT, TA17-181A, Petya ransomware, Revised Febrary 15 (2018).
[45] Attack Surface, Accessed on: July 8, National Institute of Standards and Technology, 2020. Available, https://csrc.nist.gov/glossary/term/attack_surface.
[46] NIST Special Publication 800-30, Revision 1, Guide for conducting risk assessments, 2012.
[47] CAPEC: Common Attack Pattern Enumeration and Classification. The MITRE Corporation. Accessed on: April 28, 2020. Available: https://capec.mitre.org/.
[48] J. Wynn, et al., Threat Assessment & Remediation Analysis (TARA): Methodology Description, The MITRE Corporation, 2011, Version 1.0.
[49] J.F. Miller, Supply Chain Attack Framework and Attack Patterns, The MITRE Corporation, MacLean, VA, 2013.
[50] H. Li, Q. Liu, J. Zhang, A survey of hardware Trojan threat and defense, Integration 55 (2016) 426–437.
[51] D. Shackleford, Combatting Cyber Risks in the Supply Chain, SANS Institute, 2015.
[52] S. Eggers, The nuclear digital I&C system supply chain cyber-attack surface, in: Transactions of the American Nuclear Society, Online Virtual Meeting, 122, 2020, pp. 8–11. June.
[53] https://www.trendforce.com/presscenter/news/20190613-10149.html.
[54] Cybersecurity Maturity Model Certification (CMMC), Version 1.02, Department of Defense, 2020.
[55] Cybersecurity Capability Maturity Model (C2M2) Version 1.1, Department of Energy, 2014.
[56] Guidance documents and background information for counterfeit, fraudulent, and suspect items (CFSI), Accessed on: July 21, U.S. Nuclear Regulatory Commission (2020). Available, https://www.nrc.gov/about-nrc/cfsi/guidance.html.
[57] Government-Industry Data Exchange Program. GIDEP, Accessed on: July 21 Available, www.gidep.org, 2020.
[58] ERAI, Accessed on: July 21 Available, www.erai.com, 2020.