INL/CON-20-57213-Revision-0

The Nuclear Digital I&C System Supply Chain Cyber-Attack Surface

Shannon Leigh Eggers

June 2020

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/CON-20-57213-Revision-0

The Nuclear Digital I&C System Supply Chain Cyber-Attack Surface

Shannon Leigh Eggers

June 2020

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy

Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

The Nuclear Digital I&C System Supply Chain Cyber-Attack Surface

Shannon L. Eggers

Idaho National Laboratory, Idaho Falls, ID 83415, shannon.eggers@inl.gov

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). Furthermore, new and advanced reactors, such as generation III+ reactors, small modular reactors, and microreactors, will rely on digital technology. Digital I&C provides increased functionality, better efficiency, and improved reliability within the nuclear industry; it also introduces many new cyber vulnerabilities.

Adversaries intent on malicious activity often use the easiest and most accessible attack pathway. While the U.S. nuclear fleet has made significant progress in securing NPPs against cyber-attack by implementing their Cyber Security Plans, the supply chain pathway remains a weak link. Ongoing vulnerability of the NPP supply chain is influenced by the following factors: (1) the ubiquitous nature of NPP digital assets, (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 and activities.

Cyber-attacks impact confidentiality, integrity, and availability 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 [1]. Exploits that can 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 [1]. 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. Initial steps for improving the assurance of NPP supply chain authenticity and trustworthiness are understanding the entire supply chain attack surface (as shown in Figure 1), recognizing the potential threats, and identifying the weakest links.

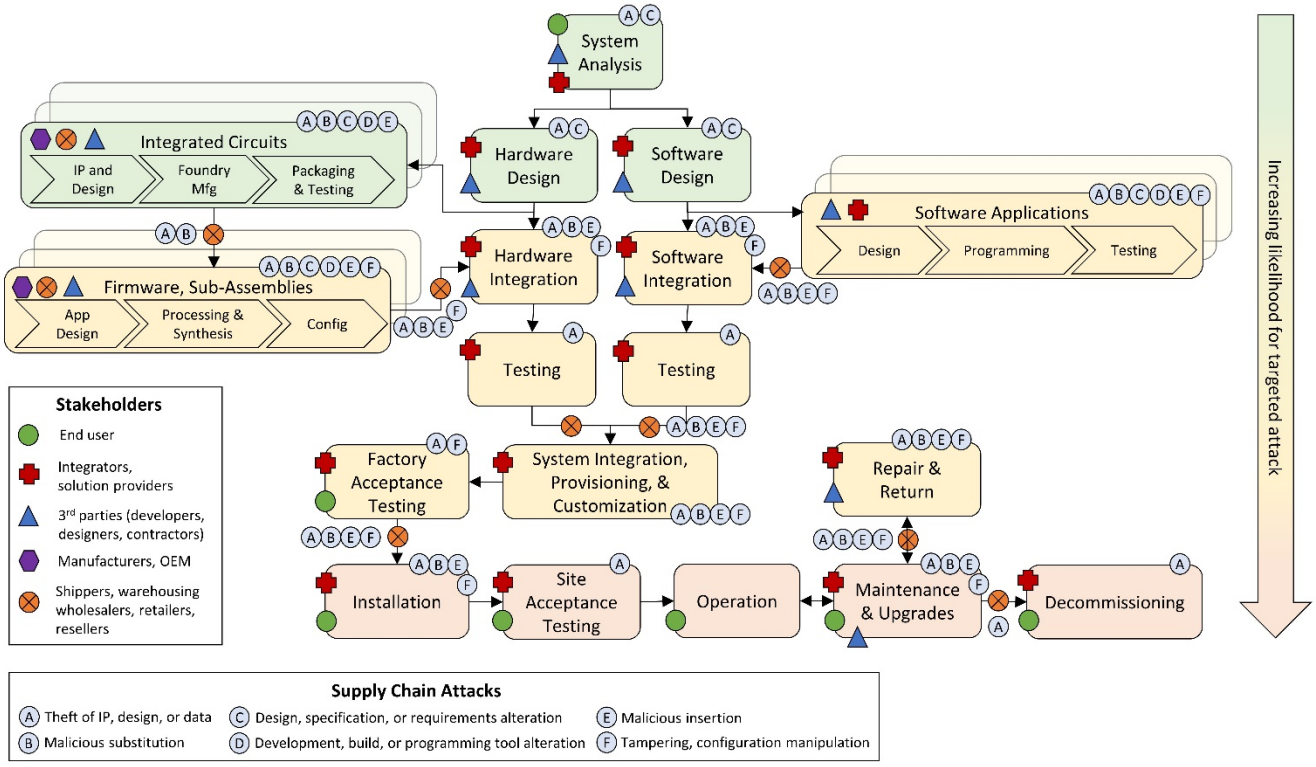

Fig. 1. The Digital I&C System Supply Chain Cyber-Attack Surface.

BACKGROUND

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 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 critical digital assets will target less protected pathways, such as the supply chain.

Adversaries are also 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 [2-7]. The Stuxnet, BlackEnergy3, CrashOverride, and Triton 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 [8-11]. While the Triton malware attacks on the Triconex system were launched via insecure network architecture [11], 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 [12].

As the ubiquitous use of commercial-off-the-shelf (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 [1]. In addition, the use of commodity hardware and software lowers barriers of entry by enabling the adversary to use publicly available information to learn the skills necessary for successful exploits. The adversary may even have access to previously developed malware or attacks they can re-use in their campaign [13, 14].

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. A taxonomy of 41 different supply chain attacks is provided by MITRE [15]. 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 [3]. 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 [6] and that the Russian government is involved in a multi-stage intrusion campaign targeting critical infrastructure sectors [7].

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 integrated circuit (IC) market has grown dramatically with an annual 41% increase in 2017 to $699 billion [16]. 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 [16].

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 [17]. 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” [18]. 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.

DIGITAL I&C SYSTEM SUPPLY CHAIN CYBER-ATTACK SURFACE

A digital I&C supply chain is primarily business-to-business and is focused on product quality instead of quantity and speed, which is typical in an ICT supply chain. The end-to-end supply chain lifecycle for an NPP digital system, such as a reactor protection system, is a complex network with

many levels of stakeholders and activities. The Digital I&C Supply Chain Cyber-Attack Surface in Figure 1 is a concise model that illustrates the complexity of the attack surface by overlaying a typical I&C supply chain lifecycle with key stakeholders at each activity. 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 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 subcontractor potentially has their own designers, fabricators, and manufacturers. Every level of the supply chain, including manufacturing, production, distribution, installation, 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, manufacture, 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 original equipment manufacturer, who has fewer cyber defenses implemented. Transitions between activities and stakeholders are also susceptible to attack. Components and software can be compromised while in transport (physical or digital distribution) or in residence (physically or digitally) at warehouse, wholesaler, retailer, or reseller locations.

As shown in Figure 1, 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 a programmable logic controller (PLC) may be common for a variety of PLC models with the ultimate destination and configuration unknown until integrated into an application at 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.

Vulnerabilities and cyber risks vary throughout the supply chain lifecycle. During design phases, adversaries may steal intellectual property (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) [19]. 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 a huge ongoing security concern.

Software and firmware are also vulnerable throughout the supply chain lifecycle, including design, testing, implementation, and maintenance phases. 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. Malicious firmware can hijack root access, steal data, affect device operation, or disable the device. 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.

Finally, the potential for system information compromise or theft is also present throughout the entire lifecycle. 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. 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 the plant.

CONCLUSIONS

As illustrated in Figure 1, the Digital I&C System Supply Chain Cyber-Attack Surface is extensive and complex. Systems may contain hundreds of digital devices that are integrated from numerous software applications and thousands of microelectronics with associated firmware. 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 move 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. Understanding the complex supply chain attack surface is necessary to persistently adapt and develop new processes, testing, and tools to improve and protect the nuclear supply chain from this evolving threat. Future research will use this knowledge as a foundation to (1) analyze the risk throughout the supply chain, (2) apply the identified supply chain risk to overall cyber risk analysis and secure architecture considerations, (3) develop new supply chain tools, methodologies, and guidelines, and (4) establish cyber-resilient supply chains.

ACKNOWLEDGEMENTS

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 under DOE Idaho Operations Office, Contract DE-AC07-05ID14517.

REFERENCES

1. W.J. HEINBOCKEL, E.R. LADERMAN, and G.J. SERRAO, "Supply chain attacks and resiliency mitigations," The MITRE Corporation (2017).
2. C. ANDERSON and K. SADJADPOUR, *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*. Carnegie Endowment for International Peace (2018).
3. D.R. COATS, "Statement for the record: Worldwide threat assessment of the US intelligence community," Office of the Director of National Intelligence, January 29, 2019.
4. "Global oil and gas cyber threat perspective: Assessing the threats, risks, and activity groups affecting the global oil and gas industry," Dragos, August 2019, Available: https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf, Accessed on: August 8, 2019.
5. "Annual report to Congress: Military and security developments involving the People's Republic of China," Office of the Secretary of Defense (2019).
6. US-CERT, "TA17-117A: Intrusions Affecting Multiple Victims Across Multiple Sectors," Revised December 20, 2018, Available: https://www.us-cert.gov/ncas/alerts/TA17-117A.
7. US-CERT, "TA18-074A: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," Revised March 16, 2018, Available: https://www.us-cert.gov/ncas/alerts/TA18-074A.
8. R. LANGNER, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49-51, 2011).
9. ICS-CERT, "Ongoing sophisticated malware campaign compromising ICS (Update E)," (2016).
10. ICS-CERT, "Cyber-attack against the Ukranian critical infrastructure," (2016).
11. B. JOHNSON, D. CABAN, M. KROTOFIL, D. SCALI, N. BRUBAKER, and C. GLYER, "Attackers deploy new ICS attack framework "TRITON" and cause operational disruption to critical infrastructure," FireEye, Ed., ed. FireEye Threat Research Blog (2017).
12. SYMANTEC, "Internet Security Threat Report," February 2019, vol. 24 Available: https://resource.elq.symantec.com/LP=6819?inid=symc_threat-report_istr_to_leadgen_form_LP-6819_ISTR-2019-report-main&cid=70138000001Qv0PAAS.
13. D. GOODIN. Stolen NSA hacking tools were used in the wild 14 months before Shadow Brokers leak. *ARS Technica*. May 7, 2019, Available: https://arstechnica.com/information-technology/2019/05/stolen-nsa-hacking-tools-were-used-in-the-wild-14-months-before-shadow-brokers-leak/
14. C. CIMPANU. Source code of Iranian cyber-espionage tools leaked on Telegram. *ZDNet*. April 17, 2019, Available: https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/
15. J.F. MILLER, "Supply chain attack framework and attack patterns," The MITRE Corporation MacLean, VA(2013).
16. "Integrated circuits trade," The Obervatory of Economic Complexity (OEC), Available: https://oec.world/en/profile/hs92/8542/, Accessed on: November 7, 2019.
17. C. LEVIN and J. MCCAIN, "Senate Armed Services Committee releases report on counterfeit electronic parts," Senate Committee On Armed Services (2012), Available: https://www.armed-services.senate.gov/imo/media/doc/SASC-Counterfeit-Electronics-Report-05-21-12.pdf.
18. C. NISSEN, J. GRONAGER, R. METZGER, and H. RISHIKOF, "Deliver uncompromised: A strategy for supply chain security and resilience in response to the changing character of war," The MITRE Corporation (2019).
19. K. CHEN, "Global Top Ten foundries for 2Q19 perform less-than-expected due to sliding demand and high inventories," TrendForce, Available: https://press.trendforce.com/node/view/3259.html.