Nuclear Power Plant Instrumentation and Control Cyber Security Common Vector Access Leading to Relational Common Cause Failures

Phillip L. Turner, F. Mitch McCrory, Lon A. Dawson[1]
Sandia National Laboratories
Albuquerque, NM USA
[1]{pturner, fmmccro, ladawso}@sandia.gov

ABSTRACT

Nuclear power plants and facilities have been implementing digital system upgrades into their previously analog systems for well over twenty years. New nuclear facilities' control, security, and emergency preparedness systems are almost exclusively built on digital architectures with a high degree of communication between the various systems that are often integrated together into a central control station to aid in operation or security of the facility. As digital systems become more widespread in nuclear facility control system architectures, cyber security related issues have become a significant concern to operators, regulators, governments, and other groups. Among the many concerns related to digital systems and cyber security is the area of common cause and common mode failures.

This paper introduces, defines, and discusses some sources of common cause failure from a cyber security perspective: *common vector access*. This refers to specific access points that an adversary can exploit through a single attack sequence that have the potential to provide relational failures through common cause on multiple components, subsystems, systems, or plants. This paper will further discuss interconnected processes where these access points may exist, the importance of limiting or controlling these pinch points, and some methods of protecting *common vector access points*.

Key Words: common vector access, nuclear, digital, instrumentation and control, cyber security

1 INTRODUCTION

Common cause or common mode failures (CCF) can occur due to a variety of factors: improper operation, poor quality control, lack of diversity in design, poor software coding practices in digital equipment, etc. Nuclear facilities are increasingly integrating digital components into their systems, with new nuclear power plants being built today being fully digital. In the past, where systems were developed specifically for use within nuclear power plants, they are now developed for larger application, of which nuclear power is a small portion. The systems being put in place are becoming increasingly complex in their hardware and software. The hardware today has added functionality that isn't necessary for the function of the plant. The size and complexity of software code in these devices is becoming so great that it is difficult to understand everything that is occurring and it creates challenges for validating the functional logic within the code. The complexity within digital control systems also provides opportunities for adversaries to attack these systems in ways that did not exist in the past.

An *interconnected process* is any process that allows data, software, or hardware to move into, out of, or make changes to the system of concern [1]. An interconnected process would provide a mechanism for a cyber upset such as malware insertion that would permeate multiple components, systems, or plants that might be connected to that process and allow for a relational CCF across multiple systems or plants. These relational failures would likely originate from the same or similar process or manufacturer. Such failures are not limited to malicious activity, for example, poor quality control at an automobile tire manufacturer led to large-scale recalls of tires due to premature failure that caused 46 deaths and hundreds of accidents [2].

Common vector access (CVA) or a *common vector access point* (CVAP) refers to a specific access point within an interconnected process that an adversary would exploit through a single attack sequence that has the potential to provide relational failures through common cause (common cause access) on multiple components, subsystems, systems, or plants. In CCF, two or more components within a system or systems fail due to a common cause such as design flaw, software error, operator error, or other root cause common to the components. This could happen within a single nuclear power plant, across multiple nuclear power plants, or even across other types of power plants and critical infrastructure where similar components or systems are used. As the failures expand beyond a single plant, there is a relationship between them that occurs across multiple plants and would generally occur within components with similar hardware and software characteristics.

Consider an interconnected process involving the installation or updating of firmware on a digital component within a plant. This process is likely similar, or the same across many different plants. The software will most likely originate at the industrial control system (ICS) manufacturer and will make its way to the plant through a series of steps and other components like a USB drive or a laptop and finally be installed on the component that is operating within the plant. If an adversary wanted to affect the largest number of components within plants at once, the access point that would provide the highest value to them would be at the manufacturer. For example, Duqu is a malware threat that focused on gathering intelligence data and assets from entities such as ICS manufacturers as reconnaissance for future attacks [3]. Attacking the manufacturer's software development network could potentially provide an access pathway into all their customers' systems and potentially allow for a coordinated cyber attack across many different systems and plants.

A single attack vector might entail compromising a single software system such as that used in a programmable logic controller (PLC) that exists in multiple systems and which, if exploited, would cause the event or series of events necessary to achieve the adversary's goals. In an example scenario, if an adversary goal is to create core damage, the adversary might need to manipulate a system into an undesired state as well as confuse the operators on the state of that system or the overall plant by providing false indications to the operators to achieve the objective. This could likely require the adversary to create multiple attacks, one to manipulate the system and another to manipulate the overall plant displays including the responses from other systems. To carry out these attacks, the adversary may need to establish multiple vectors into the plant to affect all the necessary components. Gaining access to the systems becomes much easier if the adversary can find a CVAP that provides access to all or most of the components needed to begin the attack sequence.

2 CVA AND THE ADVERSARY

As national assets, nuclear power plants in the United States (US) are among the most secure of the US critical infrastructures. This is driven by the potential adverse consequences that a successful attack on a nuclear power plant control system could have on the plant operation and the potential consequences to the public and the environment. An adversary's intent on carrying out a cyber attack against these plants may range from disruption of the plant's power production, large-scale disruption of a regional power grid [4], local or large-scale economic loss [5], or to cause physical damage to the plant with a goal of causing some form radiologic release.

2.1 Adversary

Nuclear facilities as designed in the US have robust safety themes that include redundancy and diversity of control in safety systems, defense-in-depth architectures, reliability in design, and typically use high quality components and manufacturing. These fundamental design requirements, along with limiting communication into control systems that are safety significant or safety related, do a good job of protecting nuclear facilities from less sophisticated adversaries. For example, a one-way communication device such as a data diode that is used to segment safety and control systems significantly reduces the likelihood of an adversary remotely hacking into a safety system and preventing it from performing its functions. Additionally, random malware that may find its way into a reactor system is not likely to impact plant safety. The malware might affect the system or plant, which would be a significant local event for the facility from standpoints of security, reliability, and economics; however, without being designed specifically for plant ICS components, the malware is unlikely to cause a consequential impact to the surrounding population or the environment.

Because of the aforementioned design criteria for nuclear power plants, the most important adversary of concern is an adversary with capability (knowledge and resources) [6] and intent to cause a significant radiologic release to the environment or widespread economic loss [5]. The adversary needs knowledge of plant operations and the specific systems and configurations in use. Such an adversary would need to possess highly technical capabilities to design an effective cyber attack to achieve their objective on such a complex system. Because data diodes are effective defenses against remote access to these systems and mitigate the remote access attack vector, the importance of protecting against other interconnected processes such as supply chain become a higher priority.

2.2 Information, Technology, and Access

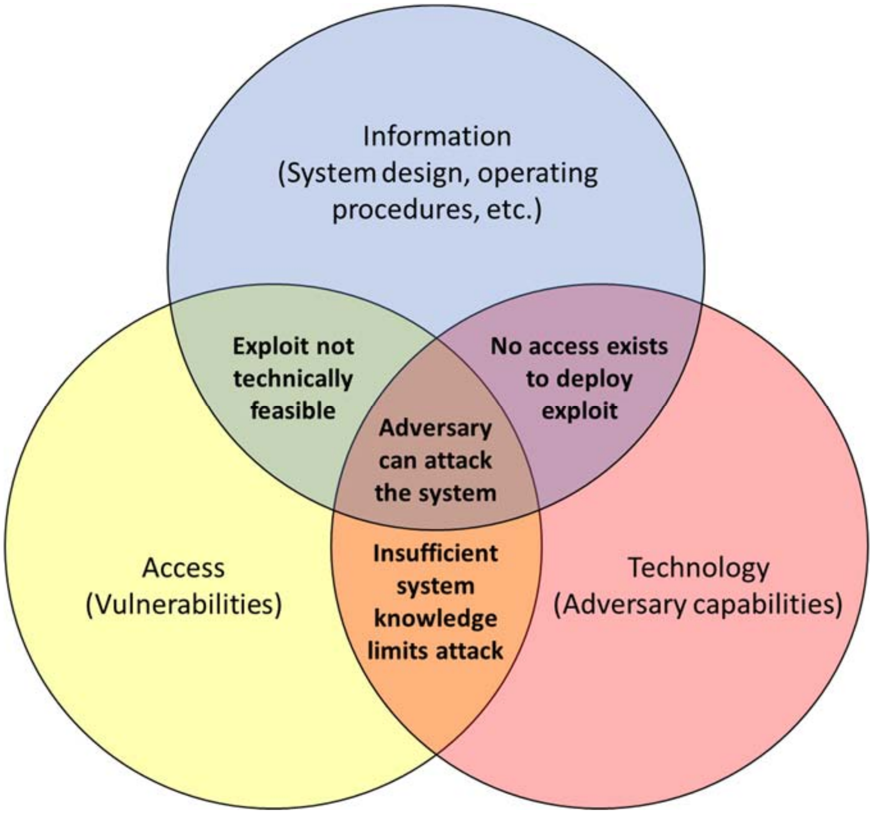
Information
(System design, operating procedures, etc.)
Exploit not technically feasible
No access exists to deploy exploit
Adversary can attack the system
Access
(Vulnerabilities)
Insufficient system knowledge limits attack
Technology
(Adversary capabilities)

Figure 1. Elements Needed for a Successful Cyber Attack

To execute a successful cyber attack, an adversary needs three things: 1) information about the plant, systems, and components, 2) technical capabilities to develop exploits needed, and 3) access that is gained through vulnerabilities within the interconnected processes. These three things are notionally represented within the Venn diagram in Figure 1. The intersection of the three circles is related to the risk to the facility from a cyber attack. Reducing the system vulnerabilities or the available information would cause Access or Information elements to get smaller, respectively, reducing risk from attack by limiting the adversary's options. If the overlapping areas are reduced such that the risk space is removed, the adversary must either expand Technology by advancing the state-of-the-art in their capabilities to overcome defenses or discover unmitigated vulnerabilities to increase Access.

2.3 Common Vector Access

CVAPs are the intersection between access and technology that allows CCFs. The significance of CVA has to do with the access an adversary needs in order to execute a successful cyber attack on a nuclear facility. Imagine an adversary wanted to attack a nuclear facility to achieve the goal of a significant radiologic release to the environment. The adversary would require an in-depth understanding of how that reactor plant worked to identify the systems necessary for exploit and attack. They would then need to craft or obtain the exploits necessary to perform the intended functions and gain access to each network segment to install the malware. That is, unless the attacker could access the systems through a single pathway. Such an access path could be through a set of common software that is used on multiple components within a system or systems and the process that provides connectivity between those components. Access could also be obtained through an interconnected process with high latency connections, e.g., electronic media like a CDROM, sent through the mail that has been compromised somewhere along that process. The significance of the CVAP is that it provides the adversary with a means of accessing the system through an interconnected process where there is perceived trust and a lack of needed mitigations.

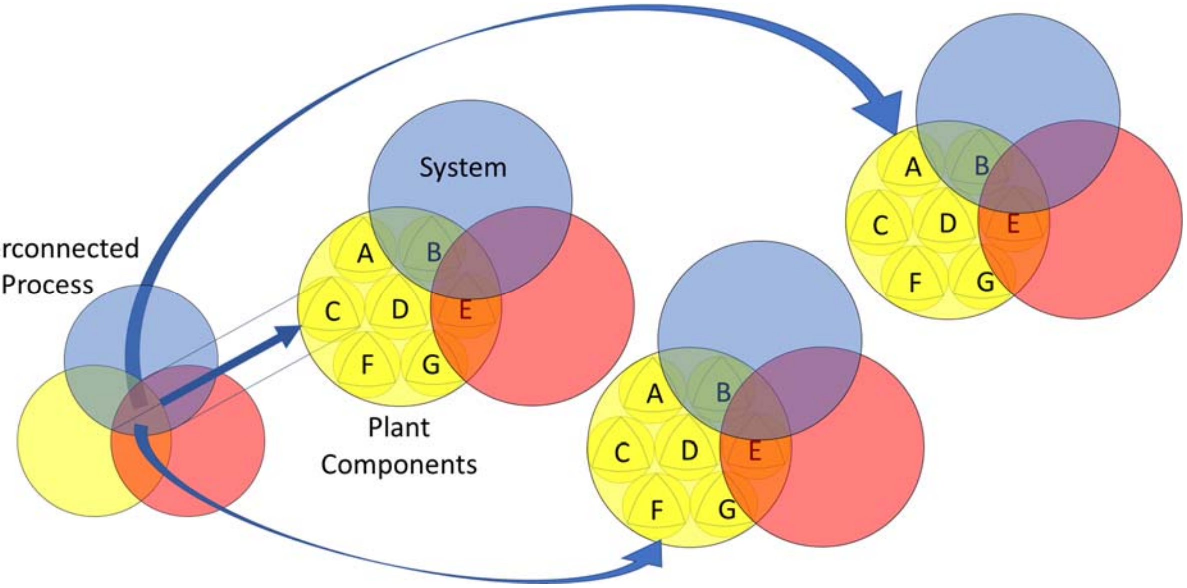

Figure 2. CVAP Compromise Leading to CCFs

Figure 2, above, illustrates how an interconnected process could be used to provide access to multiple system segments within a plant or across multiple plants. The left side of the diagram represents the first phase of the attack which is to gain control of the interconnected process. It has its own elements of Information, Technology, and Access that an adversary must exploit. Consider the attack on the Ukrainian power grid. To begin the attack on the system, the attackers started with email that contained a malicious macro. Once triggered, the malware installed a backdoor establishing the CVAP and allowing the attackers to begin their system reconnaissance. Even though the ICS portion of the grid control was firewalled off from the enterprise system, the attackers were able to steal the credentials necessary to open VPN connections to the grid control systems. When they had adequate system information, they began their attack to take the grid down and lock out the operators [4, 7]. Ultimately, the VPNs were the CVAPs that were needed to bring about the CCF across the different distribution management systems run by the different companies across the grid.

Attacks are usually multi-step or multi-phase. In the Ukrainian attack, the attackers were inside the Ukrainian networks for months before executing the attack. During this *dormant* period, they performed reconnaissance on the Ukrainian systems. They learned what systems were controlled by what and how they were controlled, what the impact of attacking different parts of the system would be in terms of their objectives, and how to keep the operators from responding to the attack by, literally, keeping them in the dark [4]. As such, even an attack that leverages a CVAP will still require at least two phases or types of attack. One attack to compromise the interconnected system that provides the CVA and the other to compromise the target system that they want to affect. Without the CVA, the number and types of attacks grows and grows, making an attack much more difficult for the adversary. Unfortunately, in today's world of increased connectivity, efficiency, and convenience, there are many CVAPs.

The following sections give examples of CVA with software and hardware:

2.3.1 Software CVA

Software CVA could be created through the firmware used in multiple devices that exist within a system such as a PLC or other programmable type of controller like an FPGA. Software development for digital control systems has been a concern for CCF for quite some time, but this paper focuses on failures resulting from malevolent actors. Current system design themes, as discussed above, use diversity in software and components as a mitigation for CCF as well as inspection of elements in the software lifecycle, where possible. With ever increasing complexity in software and exponential increases in the number of lines of code, current software analyses have limited ability to identify malicious intent. One of the biggest concerns in this area is malicious software that can be used to breakout of its component and impact other interconnected components or systems.

2.3.2 Hardware CVA

Hardware CVA can exist where the supply chain protection is not robust enough to prevent an adversary from making changes to the hardware design. These changes would then allow for insertion of malicious code that will be extremely hard to detect and remove. Kaspersky is a cyber security and anti-virus company with a reputation as one of the most advanced in detecting and fighting complex cyber attacks [8]. Recall the attack on the Kaspersky's networks via Duqu 2.0 where the malware resided in kernel memory, making detection difficult. Once the malware was finally discovered on their networks (after a significant amount of time) it was incredibly difficult to purge from their systems due to the nature of how the threat operated, residing in memory. The sophistication of Duqu 2.0 has been noted as the most advanced cyber threat ever seen [9]. An adversary with CVA into the hardware supply chain process has a very important and strategic access vector that is of high value. The adversary would easily be able to add hardware logic that provides unknown functionality or extra memory to hide malware.

3 MITIGATION

The concepts throughout this paper illustrate the importance of the CVA. In the same way that an adversary looks for and uses CVAPs, they also very important to the system owner in understanding where robust protections are needed. When a vulnerability assessment is performed, CVAPs should be identified and their cyber security controls prioritized. Any gaps or weaknesses in protection should be identified and addressed. In the world of limited resources with which to protect and defend these systems, CVAPs should be recognized for what they are and assigned a high priority for defense. The goal in applying mitigations is to increase the difficulty necessary for an adversary to be successful in their attack.

One of the most impactful security controls within the communications architecture design of the US nuclear fleet is the use of hardware based one-way communication devices (data diodes) from the reactor control and protection systems upper level networks to other or lower level networks. Incorporation of these data diodes has improved the cyber security posture of nuclear facilities' instrumentation and control systems. This single device has significantly increased the difficulty level for an outsider to significantly impact a nuclear facility. An adversary deprived of any remote access to the system would need to find another access vector into the system. This would make the risk from other access vectors such as supply chain or an insider more of a concern, should an attacker target a nuclear facility for a cyber attack. Note that the notion of an *air-gapped* system can provide a false sense of security by ignoring the high latency connections within interconnected processes. An air-gap may add a degree of difficulty for an adversary to overcome, but an interconnected process has put the air-gapped system in place with the software it is already running and is still potentially subject to CVAPs. Any process could also have the potential of being short circuited by an insider, maliciously or otherwise. The insider would then become the surrogate for remote access by adding additional connections that should not exist and the supply chain could be used to either insert a virus or provide a remote connection into the targeted control system.

With any process that touches the facility's digital components, establishing and maintaining trust is vital. When getting software from a manufacturer, secure means of delivery should be considered with an additional validation step, e.g., verifying SHA-2 hash values through an out-of-band delivery mechanism. The manufacturers also need to ensure trust within their hardware and software development systems. Robust security controls should be implemented on those networks along with a vetting process for personnel. Third party companies should be held to the same standards with an auditing program in place to verify that they are maintaining trust requirements. To ensure trusted communications within the control network, a form of authentication could be employed between devices. This would ensure the integrity of communications and help prevent attacks such as man-in-the-middle. Some form of communications monitoring could be employed to discover abnormal network behaviors and alert the operators. Implementing any of these security controls would raise the cyber security posture for a facility's control systems. They would want to analyze the relative risk from these areas and develop an effective prioritization of cyber security controls based upon their specific needs and to address any deficiencies in protection.

4 CONCLUSIONS

The significance of the CVA concept is that it helps system architects, operators, and cyber security personnel responsible for designing, operating, and defending these systems understand the importance of identifying and the need to limit or protect these access points in the system architectural designs. By doing this, the system will be more difficult to exploit and gives the system operators and defenders a better chance at identifying and mitigating an intrusion before the attacker's goals can be achieved. This concept of CVA also points to the importance of developing and implementing cyber security controls as early in the lifecycle as possible, as this is when most access points are designed into the system.

5 ACKNOWLEDGMENTS

The writing of this paper was funded by the US Department of Energy Office of Nuclear Energy.

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000, SAND2017-3160 C.

6 REFERENCES

1. Turner, P. L., Adams, S. S., Hendrickson, S. M., “Enhancing Power Plant Safety through Simulated Cyber Events”, Submitted to the *American Nuclear Society’s 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies*, San Francisco, CA (2017).

2. “Firestone Tires Recalled,” http://money.cnn.com/2000/08/09/news/firestone_recall/ (2000).

3. “The precursor to the next Stuxnet W32.Duqu Version 1.4”, *Symantec Security Response,* https://scadahacker.com/files/duqu/w32_duqu-the-next-precursor-to_the_next_stuxnet_v1.4.pdf (2011).

4. Zetter, K., “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid,” *Wired*, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (2016).

5. “Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid,” *Innovation Series*, Lloyd’s, https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf p.4 (2015).

6. McCrory, F. M., Parks, R. C., Hutchinson, R. L., “An Adversary’s View of Your Digital System,” IAEA-CN-228-54, *IAEA International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange*, Vienna, Austria (2015).

7. “Cyber-Attack Against Ukrainian Critical Infrastructure”, *Alert* (IR-ALERT-H-16-056-01), U.S. Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01, (2016).

8. “Duqu is back: Kaspersky Lab reveals cyberattack on its corporate network that also hit high profile victims in Western countries, the Middle East and Asia,” *Kaspersky Lab*, http://usa.kaspersky.com/about-us/press-center/press-releases/2015/duqu-back-kaspersky-lab-reveals-cyberattack-its-corporate-netwo, (2015).

9. Paganini, P., “Duqu 2.0 the most sophisticated threat ever seen targeted also Kaspersky,” *Security Affairs*, http://securityaffairs.co/wordpress/37714/cyber-crime/duqu-2-0-hit-kaspersky.html, (2015).