CISSM | CENTER FOR INTERNATIONAL & SECURITY STUDIES AT MARYLAND

An Effect-Centric Approach to Assessing the Risks of Cyber Attacks Against the Digital Instrumentation and Control Systems at Nuclear Power Plants

By Jor-Shan Choi, Nancy Gallagher & Charles Harry

CISSM Working Paper
February 2020

Center for International
and Security Studies at Maryland
4113 Van Munching Hall,
School of Public Policy, University of Maryland
College Park, MD 20742
(301) 405-7601

SCHOOL OF PUBLIC POLICY
CENTER FOR INTERNATIONAL & SECURITY STUDIES AT MARYLAND

Abstract

Cyberattacks against the digital instrumentation and control (DI&C) systems in nuclear power plants (NPPs) are of grave security concern. The US Nuclear Regulatory Commission (NRC) requires all NPPs to protect critical digital assets that support safety, security, and emergency preparedness functions against cyberattacks.[1] Other standards bodies like the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) have also developed standards that address cybersecurity for industrial control systems (ICS) including DI&C.[2] Due to concerns for security, relevant stakeholders such as regulators, plant operators, information technology (IT) and operation technology (OT) staff, and equipment suppliers are sometimes reluctant to reveal in technical detail about vulnerabilities posed by DI&C systems. Yet, because some types of cyberattacks against an NPP may cause core damage or significant release of radioactivity, harming the plant, the public and the industry, the safety implications of potential cyberattacks should be evaluated. This divide between security and safety is a challenge for stakeholders focused in cyber security for NPPs.

To bridge this security and safety divide, this study proposes and demonstrates a methodology for assessing and addressing the safety consequences of cyber events that disrupt one or more parts of the DI&C systems at NPPs. The methodology builds on the "effect-centric" cyber risk assessment framework developed by the Center for International and Security Studies at Maryland (CISSM). It is used to analyze two historical cyberattacks and one hypothetical attack scenario. As the focus is on plant safety, these assessment, evaluation, and analysis can be candidly and openly discussed with the goal of finding the best defense to thwart the specific cyberattack.

Introduction

Background. The instrumentation & control (I&C) systems of operating U.S. nuclear power plants (NPPs), like typical industrial control systems (ICS), were originally built with analog equipment. Such legacy systems are increasingly obsolete and costly to maintain. Upgrading to a digital-I&C (DI&C) system with microprocessors and computers helps facility operators overcome obsolescence issues, but also introduces new cybersecurity risks. (A simplified diagram of an I&C system and its components is included in the Appendix A.)

Digital replacements or upgrades in Generation II (GEN II) NPPs are often only applied to control systems that measure process parameters such as flow rates, temperature and pressures, and operational states of pumps and valves, etc. For systems with protection or safety functions, such as the reactor protection and the engineered safeguards and protection systems, the original analog devices are often being fixed, maintained, and continuously used. This hybrid (digital for control and analog for safety) I&C system is currently used in many GEN II NPPs in Japan, Europe and the United States. It avoids the costs and regulatory uncertainty if I&C systems important to safety were upgraded to digital. Gen III reactors, such as those new-builds in China, India, Finland, Russia, South Korea, United Arab Emirates and the United States, rely entirely on DI&C systems. Nevertheless, there are GEN II reactors that use digital components even for some safety-related functions, such as the Oconee NPP in the United States.

Using DI&C systems in NPPs enhances operational efficiency, availability, and performance. However, DI&C systems has made these NPPs vulnerable to cyberattack. Concern about cyber risks at NPPs has increased among various stakeholders, including license regulators, plant operators, Information Technologists (IT), the Operational Technologists (OT), and equipment suppliers. These stakeholders have their own resource constraints, protection priorities, and defense strategies. For instance, plant operators, especially of older NPPs, are very cost conscious and don't want to spend money on cybersecurity unless they can be convinced that the threat is real and the consequences could be very bad. These constraints, priorities, and strategies could impede stakeholders' collective ability to recognize and reduce the most important cyber risks.

Cyber-security regulations set by nuclear regulators are often security-centric, with an emphasis on the protection of critical digital assets (CDAs), such as the DI&C systems. IT staffs and equipment suppliers follow this security-centric approach and protect the DI&C systems using IT methods, such as anti-virus software, network segregation, intrusion detection, and security patches. This approach can reduce the likelihood of some types of cyberattacks such as spear-phishing, network scanning/probing, and abuse of authorized access, etc., but it does not prioritize protection against the types of cyber events that could cause the most damaging effects. Nor does it familiarize the IT staff with the safety functions of systems that the DI&C are protecting.

In contrast, plant operators and OT staffs often take a safety-centric approach. They are particularly concerned about cyberattacks that could directly cause core damage, a significant release of radioactivity, and/or other types of significant harm to the power

plant, the public, or the nuclear industry. They pay less attention to mundane, annoying cyber-attacks, such as spear-phishing and denial-of-services, etc. This approach is problematic because most serious cyberattacks begin with mundane intrusions that compromise key personnel's credentials, and gain access to the plants' process and DI&C systems. It also doesn't familiarize OT staffs with the cyber and digital aspects of the DI&C systems.

Study Objectives. Different stakeholders need a way to assess cyber risks at NPPs that integrates cyber security and safety concerns. The International Atomic Energy Agency (IAEA) recommends nuclear facility operators develop a computer security risk management (CSRM) process "to implement computer security to protect the functions performed by DI&C systems."[3] The guidance recommends the identification of facility functions performed by DI&C systems that could possibly compromise the safety and operations of critical systems in nuclear facilities.

While IAEA guidance spells out the need for risk assessment to prioritize security concerns among a range of possible threats, it does not describe the method to use in the assessment process. Similarly, the U.S. Nuclear Regulatory Commission (NRC) promotes a risk-based approach, and the ISA/IEC standards establish the need to conduct cybersecurity assessments, but neither specifically define nor specify a methodology. The lack of specific guidance in these international standards is not surprising. They were written by industrial groups whose expertise are in I&C equipment design, and not risk analysis.

This study proposes a risk assessment methodology to evaluate the consequences of cyberattack sequences against DI&C systems that builds on the "effect-centric" cyber-risk assessment framework developed by the Center for International and Security Studies at Maryland (CISSM).[4,5] The methodology can be applied to historical events, potential attacks involving known threat actors and vulnerabilities, or scenarios that represent how the threat landscape might evolve in the future.

This study shows how a security process hazard analysis (SPHA) can be used to identify the potential cyber-nuclear vulnerability (PCNV) scores for the targeted systems and to suggest defense strategies that could prevent or avert serious consequences in cyberattack. It applies the methodology to two historical cyberattacks against nuclear facilities. It also employs a set of hypothetical attack scenarios against the long-term cooling system in a pressurized water reactor (PWR) to illustrate how the same approach can be used for preventive cyber-nuclear vulnerability assessment and mitigation.

Cyber Incidents at Nuclear Facilities

Over twenty cyber incidents, some accidental and some deliberate, have occurred at nuclear facilities, including NPPs, around the world since 1990.[6] The most recent theft of data from an administrative network occurred in India's largest NPP in November 2019.[7] These incidents demonstrate that critical infrastructure, and even NPPs, are vulnerable to

untargeted malware and targeted cyberattack. Despite the industry's warning that cyberattacks could cause massive physical damage and loss of life, though, only two cyberattacks are known to have significantly disrupted NPP operations to date. These are the SLAMMER worm, which disabled the control room safety parameter display system (SPDS) at Davis Besse NPP in 2003 and blocked plant-operators' access to reactor core information,[8] and the STUXNET attack on Iranian uranium centrifuges around 2009, which physically destroyed about 1,000 centrifuges.[9]

The U.S. nuclear industry has experienced several cyber anomalies severe enough to cause plant emergencies and reactor shutdowns. One occurred at Browns Ferry NPP in 2006 and the other at Hatch NPP in 2008.[10,11] At Browns Ferry, both the plant's condensate demineralizers and recirculation pumps have digital equipment and embedded microprocessors that communicate data over the Ethernet Local Area Network (E-LAN). Apparently, the Browns Ferry control network produced more traffic than the digital equipment could handle (or the equipment malfunctioned and flooded the Ethernet with spurious traffic). This disabled the variable frequency drive controllers and caused the Unit 3 reactor to shut down. At Hatch NPP, an engineer updated the software for a business-network computer to synchronize diagnostic data collected from the process-control network. While rebooting the computer, the synchronization program reset the data on the process-control network, which interpreted the change as a sudden drop in the reactor's water reservoirs, and initiated a reactor shutdown.

These events are not believed to have been deliberate attacks on the digital systems supporting critical NPP operations, but they illustrate some of the different types of disruptive effects that could be deliberately engineered by a malicious actor. These events inadvertently reinforced the U.S. nuclear industry's false confidence that cyber-attacks at NPPs could disrupt power generation but not cause devastating core damage or radiological releases because safety mechanisms would shut down the reactor first. From a cyber security perspective, though, a deliberate denial-of-service attack against Browns Ferry could have had serious safety consequences if it was part of a coordinated campaign that included other attacks that prevented an automatic reactor shutdown. Similarly, malicious software deliberately embedded in network systems at Hatch could have had disastrous effects if the IT staff did not understand the interdependence of the network configurations nor recognize the safety implications of a software update to plant equipment.

In each of these cases, examining the specific IT systems involved reveals vulnerabilities created by a reliance on digital technologies without adequate safeguards. This suggests that vulnerability assessments for NPP's DI&C systems should incorporate both the percentages of analog and digital technologies used in each part of the system and what steps have been taken to make each digital component un-hackable.

Assessing Cyber-Nuclear Vulnerability and Risk

All digital and microprocessor systems are potentially vulnerable to cyber-attack. Whether or not those vulnerabilities could be leveraged to disrupt operations or steal information via a specific attack scenario depends on whether appropriate defensive measures have been taken. This section provides a general method for calculating the Potential Cyber-Nuclear Vulnerability (PCNV) of the DI&C systems at NPPs and applies it to the 2003 cyberattack at the Davis Besse NPP in Ohio and the 2009 cyberattack at the Natanz Fuel Enrichment Plant in Iran. It also indicates defensive measures that prevented, or could have prevented, the cyberattack from causing serious disruption.

The Potential Cyber-Nuclear Vulnerability (PCNV) of a NPP measures the percentage of that system (process, or a subsystem within a system) made up of microprocessors, with scores ranging 0 (no digital components) to 1 (completely digital). For a system composed of many interconnected digital subsystems, the overall PCNV would be the product of all PCNVs of the subsystems, as shown below:

Potential Cyber-Nuclear Vulnerability (PCNV) $= \prod$ (% digital)
$= \prod$ (1 – % non-digital)

After PCNVs are identified, actual cyber risks at NPPs can be mitigated in several ways, all of which should be considered. Patches for software vulnerabilities and other IT solutions might make it harder to hack a particular system. The operating systems controlled by digital mechanisms could be hardened to withstand certain types of attacks. Or, back-up systems and other safeguards could be implemented such that even if a vulnerable DI&C system were hacked and the operating system it controlled was disrupted for a significant amount of time, no serious nuclear safety event would occur. Applying one or more of these defensive mechanisms to each potential cyber-nuclear vulnerability would lower the actual cyber-nuclear vulnerability score.

Sequence of Cyberattack against Davis Besse NPP. In 2003, the SLAMMER worm infected 75,000 computer servers worldwide within 10 minutes of its release, including a computer of a consultant that worked at the Davis Besse NPP in Ohio. The IT staff at Davis Besse had not addressed the MS-SQL vulnerability that the SLAMMER worm exploited because they didn't know about the patch that Microsoft had released six months earlier.[12] The SLAMMER worm traveled from the consultant's computer to the corporate network by a privilege access that bridged the firewall. It then traveled to the plant process-control network. The traffic generated by the worm clogged the corporate and control networks and crashed a plant process computer. Plant personnel could not access the safety parameter display system (SPDS) for 4 hours and 50 minutes. Losing the SPDS could have been very serious because operators depended on it to actively adjust plant operations so that nothing bad happened. Luckily, there was an analog backup readout printer providing the safety parameters of the plant at the time.

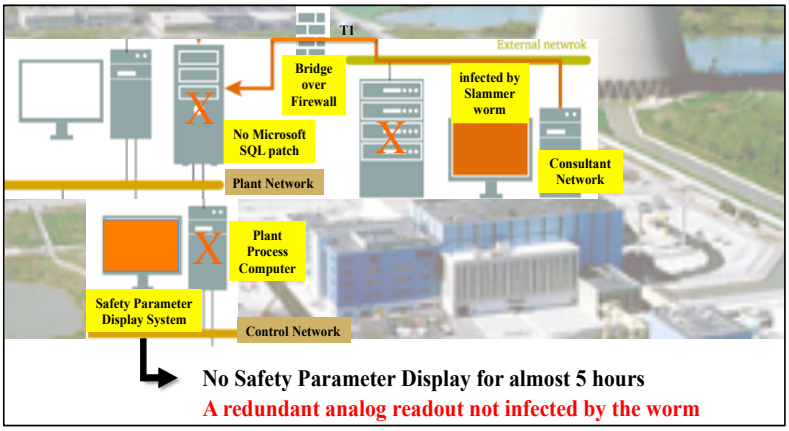

Figure 1 – Schematic of Cyber Incident at Davis Besse Nuclear Power Plant

For the cyberattack at Davis Besse NPP, Table 1 shows a PCNV of 1 during the attack phase of the sequence, because digital components were used throughout the systems, and steps had not been taken to make them un-hackable. The Defense row of Table 1 shows that the actual PCNV for that particular attack scenario was zero because the hackable digital systems were complemented by an analog readout that continued to print out reliable plant data while the SPDS was blacked-out.

Table 1 – Calculated PCNV for the Cyber-Attack at Davis-Besse NPP

Davis-Besse			Hack-able	Consequence	PCNV =∏ (1 – % non-digital)
Attack	Consultant Workstation	Digital	Y	Infected by SLAMMER worm	(1 – 0) = 1
	Fire Wall	Digital	Y	Bridged over with privileged access	1× (1 – 0) = 1
	Plant Process Computer	Digital	Y	Crashed	1×1× (1 – 0) = 1
	Safety Display	Digital	Y	Black out for ~5 hours	1×1×1× (1 – 0) = 1
Defense	Install analog readout	Analog	N	Print out reliable plant data	1×1×1×1× (1 – 1) = 0

Sequence of Cyberattack against Iran's Fuel Enrichment Plant in Natanz. In 2010, the STUXNET malware was discovered in Iran's Fuel Enrichment Plant (FEP) in Natanz. It found that STUXNET had twice attacked Siemens Step-7 Programmable Logic Controllers (PLCs), which controlled cascades of centrifuges. During the second attack in late 2009, the hackers took over the centrifuge speed controls and repeatedly ramped the speeds of some centrifuges rapidly from 0.2 percent to 130 percent of normal speed. They also altered the speed control readings in the control room display such that the attacked centrifuges' speed appeared to be normal. Over a 6-month period, STUXNET destroyed ~10 percent of 9,000 centrifuges in Natanz.[13]

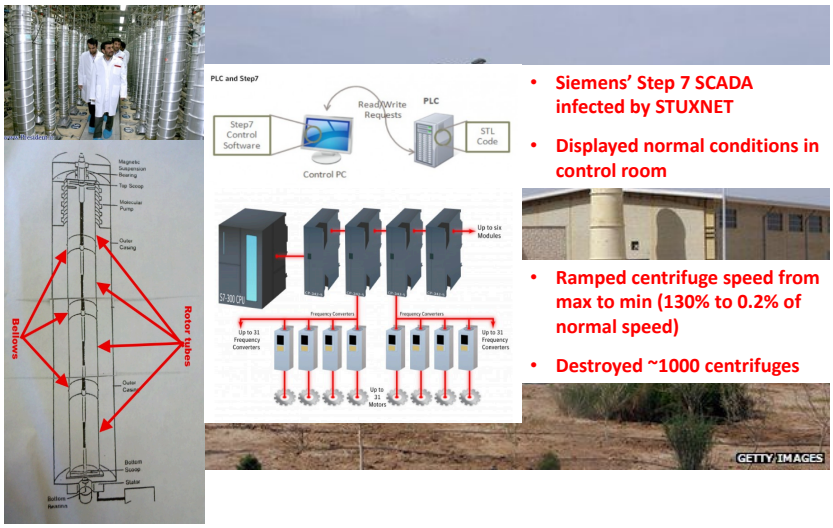

Figure 2 – Schematic of STUXNET Attack Against Iran's Fuel Enrichment Plant

Table 2 shows the series of hack-able events and the calculated PCNVs for the STUXNET campaign. It also shows that the Natanz FEP could have protected against this type of attack by installing the centrifuge rotors with a motor-over-speed-trip (MOST) or physically hardening the rotors with more advance materials.

Table 2 – Calculated PCNV for the STUXNET Attack against Natanz's FEP

Natanz			**Hack -able**	**Consequence**	**PCNV =∏ (1 – % non-digital)**
Attack	Siemens Step 7 programmable logic controllers (PLCs)	Digital	Y	Infected by STUXNET malware	(1 – 0) = 1
	Control room displays	Digital	Y	STUXNET installed pre-recorded normal data	1× (1 – 0) = 1
	Centrifuge speed controller	Digital	Y	STUXNET ramped speed from 0.2% to 130% of normal speed, and ~1000 centrifuges failed	1×1× (1 – 0) = 1
Defense Options	Install Motor-over-speed-trip (MOST)	Mechanical	N	Centrifuge motors stopped when over normal speed	1×1×1× (1 – 1) = 0
	Hardening centrifuge rotors	Physical changes	N	Centrifuge rotors withstand rapid and sporadic speed changes	1×1×1× (1 – 1) = 0

The calculated PCNV for the attack phase is 1 due to the digital components used in the rotor control system. But the centrifuge's actual PCNV could have been zero for a STUXNET-type attack scenario, if one or both suggested defenses had been implemented.

Using a Security Process Hazard Analysis (SPHA) for a Cyber-Nuclear Risk Assessment. The methodology applied to cyberattacks that disrupted operations at Davis Besse NPP and the Natanz FEP suggests that a security process hazard analysis (SPHA) could help to identify potential vulnerabilities created by DI&C systems and find un-hackable defense mechanisms to prevent different attack scenarios. A similar security process hazard analysis review (SPR) has been used in other industries such as petrochemical, oil and gas production [14].

Patches, air gaps, and other IT-based cybersecurity techniques can make it harder for an outsider to gain access to critical DI&C systems, but they cannot protect against insider threats or certain other types of attack scenarios. Therefore, all DI&C components are potentially vulnerable. At least four non-IT methods can be used to increase robustness:[15]

1. Provide robust administrative controls that protect against cyber-attacks. This may be the weakest protection because it depends on people faithfully following the administrative requirements, and people are prone to make mistakes.

2. Insert mechanical systems in place of certain digital components, or limit the range over which the DI&C system can control the problematic function.

3. Replace the problematic DI&C systems or components with analog devices, or provide a redundant analog system for the same function.

4. Design or change the process or equipment such that the system's physics prevents hazardous consequences. For example, designing or building operating systems with built-in process limitations could automatically avoid certain cyber risks.[16] This may be the strongest protection against cyber-attack, but it may also be the most difficult to implement, especially for existing plants.

CISSM's "effect-centric" cyber risk assessment framework divides the consequences of a cyber event into three aspects:[17]

1. The primary effects on organizational functions that are a direct result of interference with the IT infrastructure that supports them;

2. The secondary effects that derive from the primary effects to the network and affect the output or financial conditions to the organization as a whole, such as production losses, replacement costs, reputational damage, and stock price drops; and

3. The second-order effects on anyone outside the targeted organization, including lost access to goods or services provided by the targeted organization, reduced tax revenue, decreased confidence in important institutions and public officials, death and environmental destruction.

In the STUXNET example above, the primary effects are the false information displayed in the control room and the destruction of the centrifuges. The secondary effects would be the loss of production of low enriched uranium (LEU) from the destroyed centrifuges. If the loss of LEU production impeded the scope and schedule of Iran's enriched uranium stock, or incurred additional costs in repair or replacement of damaged centrifuges, those would be the second-order effects.

Severity Level of Cyberattack Consequence. The IAEA's computer security risk management (CSRM) process provides the following levels for cyberattacks on I&C systems, ordered from the least to the most severe consequences:

1. Normal operation: A cyberattack on DI&C systems cannot cause facility operation outside limits and conditions specified for normal operation.

2. Anticipated operational occurrence: A cyberattack on DI&C systems may cause the plant state to deviate from normal operation in a way that is anticipated to occur, but which in view of appropriate design provisions does not cause any significant damage to items important to safety or lead to accident conditions.

3. Design basis accident:[18] A cyberattack on DI&C systems may cause accident conditions that remain within the facility design basis and for which the damage to the nuclear material (or other radioactive material) and the release of radioactive material are kept within authorized limits.

4. Beyond design basis accident[18]: A cyberattack on DI&C systems may cause conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. This could include severe accidents.

Applying the Methodology to a Hypothetical Attack

To illustrate a forward-looking cybersecurity risk assessment, we analyze hypothetical attacks against the residual heat removal isolation systems (RHR-IS) of a Gen-II PWR (without a digital upgrade) and a Gen-III PWR (or a Gen-II PWR with an upgraded digital RHR-IS). A Sandia National Laboratory report described a similar scenario.[19]

Most PWR designs have piping to connect the reactor coolant systems (RCS) to the residual heat removal (RHR) pumps that circulate coolant when the reactor is shut down so that the fuel rods do not overheat. The function of the RHR system in a PWR is described more fully in Appendix B. The RCS are designed for pressures up to about 17,000 MPa, but the RHR systems are only designed for pressures about 3,000 MPa. Opening the connection between the RCS and the RHR systems when the RCS is highly pressurized could result in a loss of coolant accident (LOCA) that bypasses the containment.

Figure 3 illustrates a standard plant layout including the RHR component locations. The RHR isolation valves, which are motor-operated valves (MOVs), are located inside containment while the rest of the RHR components are not. The valves are protected against inadvertent opening by interlocks against the RCS pressure which are designed to allow the valves to open or remain open only when the RCS is at a low enough pressure to avoid damage to RHR components.

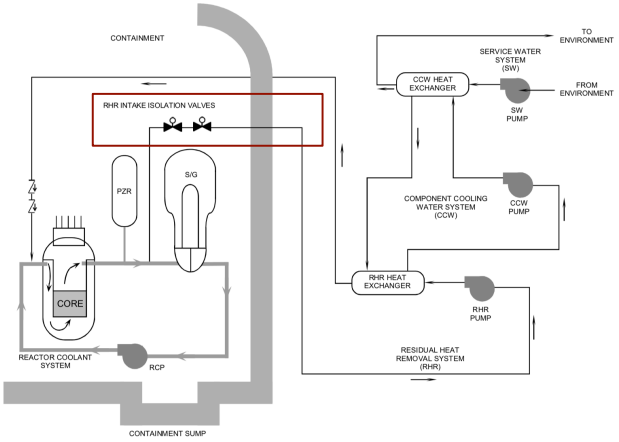

Figure 3 – PWR Plant Layout Showing the RHR Intake Isolation Valve Locations

A Gen-II PWR plant provides redundant isolation valves to separate the high-pressure systems from the RHR during normal operation, as shown in Figure 4. Each isolation valve is controlled by a pressure sensor, which would close the valve or prevent it from opening if the RCS pressure is above 3000 MPa.

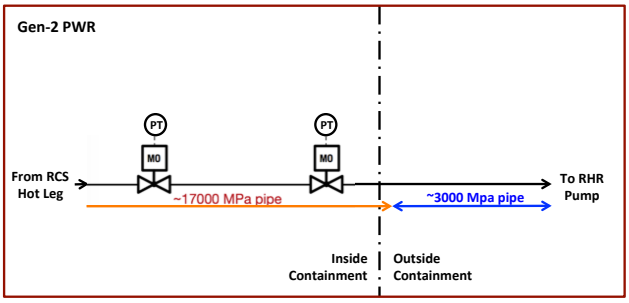

Figure 4 – A Gen-II PWR Arrangement of the RHR Intake Isolation Valves

The same arrangement is used in a Gen-III plant, except that each valve has two pressure sensors that close the valve on 1 out of 2 logic. Each valve uses a different type of pressure sensor to avoid having the same technical failure affect both of them. Figure 5 shows this arrangement.

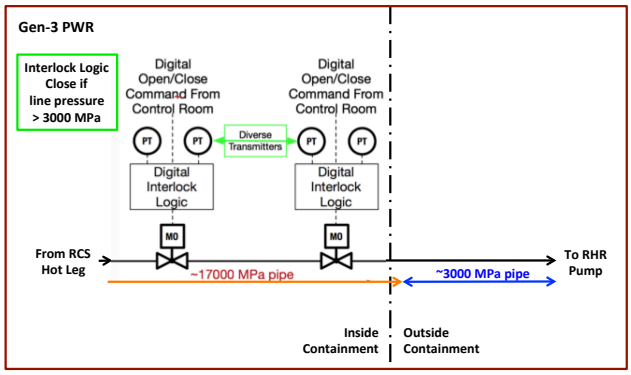

Figure 5 – A Gen-III PWR Arrangement of the RHR Intake Isolation Valves

Because the Gen-III plant valve interlock controls are digital, they are potentially vulnerable to cyberattacks. STUXNET demonstrated that hackers can attack multiple systems in the same campaign. A plausible campaign scenario could involve not only hacking the digital controls of the MOVs to open them at high RCS pressure and keep them open, but also replacing the data going to the control room displays with pre-recorded normal data to keep control room operators unaware of the attack long enough for serious damage to occur. Opening the RHR isolation MOVs at high RCS pressure would cause the pressure to propagate, damaging the RHR heat exchangers (HXs) and rupturing their tubes. An RHR HX tube rupture would not cause a leak to the auxiliary building but would over-pressurize the downstream systems such as the component cooling water (CCW) system, which operates at a significantly lower pressure than the RHR.

This attack sequence could compromise nuclear safety in several ways. A number of systems depend on cooling from CCW, including the seal cooling for the Reactor Coolant Pumps (RCPs). If the RHR tube rupture is not isolated quickly, systems that depend on CCW would soon be out of service. The loss of the CCW system would subsequently cause a RCP seal leak, reducing the coolant inventory in the reactor core and damaging the fuel. An RHR HX-tube rupture might also cause the HX shell to fail, as it is typically rated for a lower pressure than the tubes. This would cause a leak of RCS and CCW coolant into the RHR HX room outside of containment, contaminating the auxillary building and other site areas, and potentially causing a radiation release.

Potential Cyber-Nuclear Vulnerability (PCNV) and a Security Process Hazard Analysis (SPHA). Table 3 shows the PCNV calculation for an older Gen-II PWR without a digital upgrade to its RHR isolation system. In this example, the RHR system is digital, and thus potentially hackable, but the RHR isolation valves have not been put on a digital network. Because they are only opened and closed once every refueling cycle (~24 months), sending a field operator to the motor control cabinet (MCC) in the auxiliary building to manually control them is not a problem. This serves as a robust administrative control that would prevent a cyber-attack on the RHR-IS from having serious safety consequences.

Table 3 – Calculated PCNV for a Gen-II PWR without Digital Upgrade to RHR-IS.

Gen-II PWR	System	Digital	Hack-able	Consequence	PCNV =∏ (1 – % non-digital)
No digital upgrade	RHR Isolation System	Y (but no upgrade to digital network)	Y	By administrative control, a field operator controls valves in MCC during outage once every refueling cycle	(1 - 1) = 0

For a Gen-III PWR or a Gen-II PWR with digital upgrade to its RHR isolation system where the MOV controls are on the digital network, Table 4 shows the PCNV calculation for a single attack on the MOV controls and for a complex campaign that also includes a STUXNET-type attack on the control room display system.

Table 4 – Calculated PCNV of a Gen-III / a Gen-II PWR with Digital Upgrade to RHR-IS

PWR	System	Digital	Hack-able	Consequence	PCNV =∏ (1 – % non-digital)
Gen-III, or Gen-II with digital upgrade	RHR Isolation MOVs	Y	Y	MOV open when RCS is at pressure > 3000 MPa	(1 - 0) = 1
	Control Room Signal/Indicator System	Y	Y	Hackers attack display system with pre-recorded normal data showing MOVs close, and operators do not aware of cyber attack	1x(1 - 0) = 1

The consequences of the simple attack scenario are manageable, but the results of the complex campaign might not be. If the control room display system is working properly, the DI&C system would send an indication to the control room, alerting operators to issue commands to close the valves. If their commands were ignored or reversed, operators would soon send a field operator to override the digital controllers for the MOVs. That would isolate RHR from the RCS, which would probably stop the loss of RCS inventory, and arrest the LOCA phase of the transient.

If the attackers also applied the STUXNET tactic of replacing the data going to the control room displays with pre-recorded normal data, control room operators would not be aware of the first attack in time to prevent the RCP seal from leaking enough to cause a small LOCA outside of containment. Radiologically contaminated coolant would be released into less protected parts of the facility, potentially harming workers and contaminating the off-site environment. The combined campaign would yield a PCNV of 1, indicating that both the RHR isolation system and the control room display system are potentially vulnerable. Rather than risk this cyber scenario, it would be better to take the RHR-IS valves off of the digital network and send a field operator to operate the valves manually once every refueling cycle.

Conclusion

The robust cybersecurity assessment method proposed in this study demonstrates that an industrial control system (ICS), such as a DI&C system used in an NPP can be proactively evaluated from a safety perspective. The evaluation should be based on the system's potential cyber-nuclear vulnerability (PCNV), which is defined as the percentage of digital components used; and a security process hazard analysis (SPHA), which identifies options for mitigating the cyber risks. As the methodology is based on safety, the assessment, evaluation, and analysis should be candidly and openly discussed with the goal of understanding the security implication of and finding the best defense against a specific cyberattack.

The analyses of two historical cyberattacks and one hypothetical cyber scenario performed in this study (Davis Besse, Natanz's FEP, and RHR-IS) indicate that more cyber robust systems can be developed not only through standard IT practices, such as patching and air-gapping, but also through changes to operational equipment and procedures. For example:

- Installations of mechanical constraints (e.g., if the centrifuge rotors at Natanz FEP were installed with motor over-speed trip);
- Provision of redundant analog backup (e.g., the back-up system at Davis Besse);
- Changes of physical properties (e.g., if the centrifuge rotors at Natanz's FEP were hardened to withstand the rapid and sporadic speed changes); and
- Reliance on robust administrative controls (e.g., sending a field operator to the MCC to close an analog RHR-IS valve once every refueling cycle rather than using a digital RHR-IS valve.)

Some risks associated with DI&C systems can be mitigated by technical, physical, or administrative safeguards, but NPP operators would have constraints in costs, resources, and personnel to eliminate all cyber vulnerabilities. To set priorities for protection, stakeholders such as NPP operators and regulators would need a systematic way to estimate and compare the consequences of cyber disruption scenarios involving IT systems that support important organizational processes.

This approach should be systematically applied to other critical control and safety systems at NPPs to identify hack-able vulnerabilities and implement measures to reduce risk under a range of plausible attack scenarios. These critical systems include the control rod control (CRC) mechanism, the chemical and volume control system (CVCS), feed-water control system, and reactor protection and engineered safety system, etc. Particular attention should be paid to individual attack scenarios and complex cyber campaigns that could jeopardize nuclear safety rather than those which could briefly disrupt some aspect of NPP operations without causing major damage to expensive equipment, the surrounding community, or the political acceptability of nuclear power.

References

1. U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, "Cybersecurity Programs for Nuclear Facilities," January 2010.
2. ISA/IEC-62443 Series, Security for Industrial Automation and Control Systems, Research Triangle Park, NC.
3. IAEA, "Computer Security of Instrumentation and Control Systems at Nuclear Facilities, a Technical Guidance," Vienna 2018.
4. C. Harry & N. Gallagher, "An Effect-Centric Approach to Assessing Cyber-security Risk," A CISSM report, March 2019.
5. C. Harry & N. Gallagher, "Understanding Cyber Effects for Risks Assessment and Persistent Engagement," A CISSM report, July 2019.
6. A. V. Dine, M. Assante, & P. Stoutland, "Outpacing Cyber Threats – Priorities for Cybersecurity at Nuclear Facilities," Nuclear Threats Initiative, 2016.
7. J. M. Porup, "How a Nuclear Plant Got Hacked – Plugging Nuclear Plants into the Internet Makes them Vulnerable Targets for Nation-State Attacks," IT World, December 9, 2019.
8. C. Baylon, R. Brunt, & D. Livingstone, " Cyber Security at Civil Nuclear Facilities – Understanding the Risks," Chatham House, September 2015.
9. R. Langner, "To Kill a Centrifuge," 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
10. J. R. Thomson, "Nuclear Power Plant Cybersecurity Incidents," 2012. https://www.safetyinengineering.com/FileUploads/Nuclearcybersecurityincidents_1349551766_2.pdf
11. B. Krebs, "Cyber Incident Blamed for Nuclear Power Plant Shutdown," Washington Post, June 5, 2008
12. K. Poulsen, "SLAMMER worm crashed Ohio nuke plant network," Security Focus, 2003-08-19.
13. D. Albright, P. Brannan, & C. Walrond, "Stuxnet malware and Natanz: Update of ISIS December 22, 2010 report," February 2011.
14. E. Marszal and J. McGlone, "Security PHA Review – for Consequence-based Cybersecurity," International Society of Automation (ISA), 2019.
15. G. Johnson, "Cyber Robust Systems – The vulnerability of the current approach to cyber security," June 2019.
16. G. Falco and H. Lin, et. al., "Cyber Risk Research Impeded by Disciplinary Barriers," Science, Vol.366, p.1066-1069, November 29, 2019.
17. C. Harry, "A Systems Approach for Measuring the Effects of Cyber Attack," CISSM, private communication, September 2019.
18. IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection (2018 Edition), IAEA, Vienna.
19. Nuclear Power Plant Cyber Security Discrete Dynamic Event Tree Analysis (LDRD 17-0958) FY17 Report, SAND2017-10307, September 2017.

Appendix A – A Typical Industrial control System (ICS)

The I&C system, like a typical industrial control system (ICS) consists of the control center, communication protocol (e.g., radio, telephone line, cable, or satellite), and one or more geographically distributed field sites. It is the nervous system of a NPP. Figure A1 shows a simplified configuration of an ICS system.

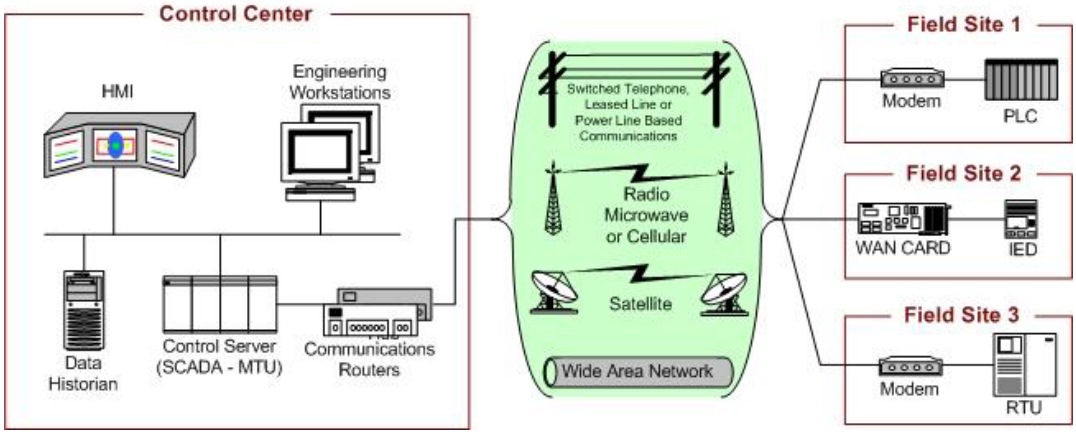

Figure A1 General Configuration and Components of an ICS System

Figure A.1 shows that the control center houses a control server (mainly the supervisory control and data acquisition (SCADA)), the communications routers, the human-machine-interface (HMI), engineering workstations, and the data historian, which are connected by a LAN. The control center collects and logs information gathered by the field sites, displays information to the HMI, and may generate actions based upon detected events. The control center is also responsible for centralized alarming, trend analyses, and reporting. The field sites consist of Remote Terminal Units (RTUs) and/or Programmable Logic Controllers (PLCs), performs local control of actuators and monitors sensors. Field sites are often equipped with an Intelligent Electronic Device (IED), such as a protective relay, which may communicate directly to the control server. Standard and proprietary communication protocols running over serial and network communications are used to transport information between the control center and field sites.

In early-day NPPs, analogue technology was used in the I&C systems for control, protection, supervision and monitoring. Progress in electronics and IT, together with the obsolescence of analog devices have created incentives to replace traditional analog I&C with digital I&C systems. Most of the replacements or modifications applied to the control systems with functions of measuring process parameters such as flow rates, temperature and pressures, and operational states of pumps and valves, etc. For systems with protection or safety functions, such as the reactor protection and the engineered safeguards and protection systems, however, the original analogue devices may continuously be fixed, maintained, and used.

The hybrid (analogue and digital) I&C system is operated today in many existing GEN II NPPs in the US, France, Japan, and Scandinavian countries. This hybrid system is used to avoid the lengthy regulatory review required for modifications or changes to I&C systems important to safety. For NPPs started or in construction in the late 90's, almost all are equipped with DI&C systems. By then, the USNRC started to review and approve DI&C systems such as Eagle Series, Teleperm XS, Common Qualified Platform (Common Q) and Triconex, for safety-related applications, clearing the way for operating GEN II NPPs to use in new or retrofitting DI&C systems at NPPs. Table A1 lists examples of NPPs with full DI&C systems.

Table A1 Examples of Nuclear Power Plants with Full DI&C Systems

Country	Plant	Commission/Modification Date
UK	Sizewell B	1995 (Eagle Series 2)
Japan	Kashiwazaki-Kariwa-6	1996 (Hitachi)
Russia	Kalinin-3	2004 (Tecnatom)
	Kola-3 Modification	2011 (Teleperm XS)
China	Tianwan 1	2006 (HolliAs/FirmSys)
	Daya Bay Modification	2006 (HolliAs/FirmSys)
ROK	Shin-Kori 1	2011 (NuTech)
	Kori 3 Modification	2015 (NICS)
US	Oconee Modification	2011 (Teleperm XS)

Appendix B – Residual Heat Removal System in a PWR

The Residual heat removal (RHR) system in pressurized water reactors (PWRs) is used to cool the core during shutdown operations, including reduced inventory and mid-loop operations.[1] High RHR system availability and reliability during shutdown conditions are important to mitigating risk and maintaining an appropriate level of safety. The RHR system is typically a low-pressure system that provides shutdown cooling when the temperature of the reactor coolant system (RCS) is reduced to about 150 ^{o}C (300 ^{o}F).

The RHR system in PWRs takes water from one or two RCS hot legs, cools it, and pumps it back to the cold legs or core flooding tank nozzles. The suction and discharge lines for the RHR pumps have isolation valves to provide reasonable assurance that the low-pressure RHR system is isolated from the RCS when the RCS pressure is greater than the RHR system design pressure. Relief valves are provided to protect the RHR system from an overpressure condition, although the relief capability is not sufficient to protect the RHR system from an overpressure condition if isolation valves are open when the RCS pressure is significantly greater than the RHR design pressure.

To accomplish RHR heat removal in a PWR, RHR heat exchangers transfer heat to the component cooling water or service water system, which then transports heat to the ultimate heat sink (UHS), such as an ocean, or a combination of a river and cooling tower or cooling pond. In PWRs, the RHR system is also used to fill, drain, and remove heat from the refueling water cavity during refueling operations, to circulate coolant through the core during plant startup before RCS pump operation, and in some to provide an auxiliary pressurizer spray.

[1] The currently-operated nuclear reactors have to be refueled periodically. During this refueling, or outage, a low water level operation, i.e., mid-loop operation, is carried out for removing the residual heat from the reactor coolant system.