Cyber Security in Nuclear Power Plants: Insights for Advanced Nuclear Technologies

Christopher Poresky
Charalampos Andreades
James Kendrick
Per Peterson

UCBTH-17-004

September 2017
Department of Nuclear Engineering
University of California, Berkeley

This research is being performed using funding received from the Center for Long-Term Cybersecurity of the University of California, Berkeley.

Abstract

This report provides a brief overview of legacy instrumentation and control in nuclear power plants, describes the state-of-the-art and currently developing technologies, and provides some insight into past, present, and future cybersecurity issues both with nuclear power plants and with critical infrastructure in general. An overview of the nuclear industry approach to cybersecurity from the guidance and design points of view is given. Then, current strategies for modern and advanced reactor designs are presented. Finally, some short concluding remarks and discussion of the lessons that can be learned and applied moving forward are provided.

1 First Instances of Digital Control in Critical Infrastructure

The digitalization of process control has led to a sharp change in the way critical infrastructure operates and performs, adding new complications that had not before been considered during the design phase of industrial control systems (ICS). There exists a rich history of process control from its early inception in ancient times, to the "classical" period, through to fully modern digital ICS [2]-[7]. The first appearance of digitalization in process control appeared in the late 1950's at the Port Arthur, Texas refinery and in 1960 at the Monsanto ammonia plant in Luling, Louisiana [4]. The widespread use of microprocessors found its way into the ICS of the electric utilities in the 1970s onwards, and the oil and gas and chemical industries in the early to mid-1980s [4], [7]. The motivation for the use and adoption of digital ICS stemmed in part from the gain in process and business efficiency, added precision in control, and in part from the physical obsolescence of old analog ICS systems and their inability to meet new regulatory requirements.

For all the benefits it bestowed, the introduction of digital ICS elements – such as external communication devices, commercial off-the-shelf components, portable field devices, etc. – has opened the door to new security issues previously not present in old "air-gapped" analog or digital systems. One of these issues, and the focus of this report, is the cybersecurity aspect of networked digital ICS in advanced nuclear power plants. The first instances of interest in the topic of cybersecurity in critical infrastructure appeared in the Presidential Decision Directive 63 of 1998, quoted at length below:

> *"Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber-attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security." [8]*

Since then, there have been several recorded and publically known cybersecurity incidents at both nuclear and non-nuclear industrial facilities, with attack vectors ranging from the benign, to disgruntled employees, to advanced persistent outsiders, to very sophisticated nation states with substantial resources. The first confirmed non-nuclear cyber-physical attack of digital ICS occurred at the Maroochyshire waste water treatment facility in Australia in 2000, where a disgruntled employee tampered with the SCADA system to release large volumes of sewage into parks and public waterways. In 2003, the Davis-Besse nuclear power plant (NPP) was infected with the Slammer worm, rendering the safety parameter display system inaccessible to operators. In 2006, the Browns Ferry NPP suffered a plant trip due to the Ethernet-based process control

system overflowing the variable frequency drives and programmable logic controllers (PLC). This demonstrates that simple incompatibility of technology can lead to cyber incidents without necessarily involving any malicious intent. Similarly, in 2008, the Hatch NPP tripped offline due to the application of a software update on a single computer. In 2014, both the Monju NPP in Japan and the Gori NPP in South Korea suffered information theft due to malware attacks. In 2014, the German Still Mill incident involved attackers disabling the shutdown systems of the plant, causing massive physical damage. In December 2015, a sophisticated attack framework known as BlackEnergy3 caused the Ukrainian grid to go offline for six hours. Although no physical damage was inflicted, it certainly was a possibility. This possibility was proven conceptually with the 2007 Aurora Generator Test at Idaho National Laboratory. In this case, a computer, taking advantage of a vulnerability in the physics of the process, remotely opened and then reclosed the substation circuit breakers out-of-phase with the grid resulting in catastrophic damage to the diesel generators.

A seminal point in ICS cybersecurity was the Stuxnet attack at the Iranian uranium enrichment facility at Natanz, which damaged nearly 1,000 centrifuges. Stuxnet was a sophisticated attack targeting specific process control system components and required extensive funding and actionable intelligence from a state sponsor. It gave instructions rather than interfere with the PLC, faking rather than disrupting sensor output, and was accomplished without any internet connection, via a supply chain attack and a thumb drive. In terms of cyber-warfare, this can be seen as analogous to the first use of nuclear weapons in the bombing at Hiroshima, where a weapon of extremely high impact was made publically known and opened the possibility for similar style attacks.

2 Cybersecurity in Nuclear Power Plants

Here we review historical lessons learned and state-of-the-art for nuclear reactor instrumentation and control (I&C) to develop cybersecurity recommendations and strategies for the design and implementation of future I&C systems in advanced nuclear power plants (NPPs) and to gain insights on cybersecurity for other critical infrastructures. The research topic of NPP cybersecurity is wide, making a focused study that results in efficient conclusions a daunting task. Cybersecurity for nuclear reactors is of paramount importance because failures of safety systems that provide heat removal from fuel – during operation and after reactor shutdown – can result in fuel damage and potentially substantial releases of radioactive materials. Here, an attempt has been made at delineating areas of interest in nuclear reactor I&C that can guide non-experts.

NPPs use multiple I&C systems that may be interconnected in various ways, including I&C for reactor safety (the Reactor Protection system), reactor control, plant control, and plant health monitoring. The design of I&C for Reactor Protection depends strongly on the physical design of reactor safety systems. Existing nuclear plants generally use “active” safety systems with multiple, active pumps, valves and electrical power supplies capable of performing heat removal under normal shutdown and accident conditions. New “passive” designs for advanced nuclear reactors

can perform these shutdown heat removal functions without external sources of power or control, and are activated to perform these functions by disconnecting external sources of power and control. However, they still require I&C to sense conditions.

This overview focuses primarily on NPP I&C for reactor safety functions. It reviews current best practices for digital control of existing plants that use active safety systems. The key question that emerges is how cybersecurity best practices for existing nuclear reactors with active safety systems are relevant to advanced passive nuclear reactor control systems.

2.1 History and Summary of Legacy Nuclear I&C

As the average age of the U.S. light water reactor (LWR) fleet exceeds 36 years [9], replacing legacy I&C is a primary effort of the industry [10]. To understand the issues faced in replacing this I&C, it is first useful to define key I&C systems used in nuclear power plants:

Reactor protection system: This system monitors reactor parameters that are important to safety and has the capability to shut down (SCRAM) the reactor and activate redundant equipment and power supplies to provide cooling and prevent damage to fuel if these parameters depart from allowable values.

Reactor control system: This part of the plant unit control system provides control of the reactor to enable it to transition from shutdown conditions to power operation, including the positioning of control rods that control the reactivity of the reactor core.

Plant control: This part of the plant unit control system controls "balance of plant" equipment, including power conversion, required to operate the reactor during normal operation and produce power.

Plant health monitoring: This system monitors plant state parameters to detect off-normal performance and materials degradation to inform operations, maintenance and replacement decisions.

While original I&C and human-machine interfaces in the nuclear power sector employed analog technologies, several issues have required the digital upgrade and/or replacement of some of these systems. Many of the original analog technologies are long obsolete and replacement equipment is no longer manufactured. Communications standards for technology have changed, rendering interfacing with some legacy systems difficult or impossible. Furthermore, the skill sets required to maintain these systems are diminishing through attrition or retirement of personnel. These problems are compounded with the need for changes to safety-related I&C systems to be approved by the Nuclear Regulatory Commission (NRC) and to be shown to meet regulatory requirements [11].

There are existing safety and security concerns with analog systems that may be overcome with a move towards digitalization, such as a lack of real-time updates for all relevant plant personnel during normal operation and transients. Moreover, the Browns Ferry fire in March 22, 1975, which

disabled cabling entering the control room, showed that plant operators may be able to manually operate equipment needed to achieve safe shutdown, and also led to plant back-fits to add redundant, remote shutdown panels in all nuclear plants. This earlier history emphasizes the importance of carrying these upgrades out with due diligence to ensure that new vulnerabilities are not created or are met with mitigating strategies. Some of these upgrades – and their implications – will be discussed.

2.2 Upgrade of I&C in Existing Nuclear Power Plants

While other power plant industries have taken advantage of advancements in I&C technologies, existing nuclear power plants have been slower to pursue adoption due to regulatory, training, and economic factors [11]. However, some upgrades have been made due to aforementioned issues, such as lack of available replacement parts and new communications standards. Integrated I&C has been widely used in fossil power plants and refineries since the 1980s but nuclear power plants have been more cautious in adoption, especially in countries with older fleets such as the United States. While Japanese plants built in the early 1970s introduced computers and microprocessors for information processing and display of results, the United States did not yet start upgrades. By the 1980s, digital technologies began being integrated into control systems for various subsystems, starting with auxiliary systems and then moving to primary systems. In the 1990s, microprocessors started being used for data logging, control, and display for most non-safety-related systems [12].

Many countries have taken unique approaches to the introduction of digital and analog hybrid I&C systems. The United Kingdom's replacement online control systems in their existing Advanced Gas-Cooled Reactors were built with a variety of microprocessor-controlled networks that are separated by function. Switzerland replaced the original Westinghouse P-250 plant computer in its Beznau Nuclear Power Plants with a modern computer network in 1989, adding, among other systems, redundant data networks and Ethernet for a robust alarm network. French N4 pressurized-water reactors (PWRs) were designed in the late 1970s and early 1980s to include a variety of modern digital features and to benefit from a set of supplementary software, including a complete offline catalog of control system architecture and characteristics. Swedish boiling-water reactors (BWRs) have been back-fit in an aggressive modernization program and use different hardware and software operating systems for safety systems and non-safety systems but program both in the same graphical programming language to facilitate ease-of-use for personnel. Temelin in the Czech Republic was also back-fit with Westinghouse I&C and has automated reactor startup with the push of a button. Korean NPPs initially built with digital I&C have elected to revert several safety-related systems in plants with analog modules to avoid common-cause failure [13]. In Finland, digital field devices in safety systems were replaced by analog field devices in order to facilitate I&C upgrade licensing. In an example of I&C upgrades in the United States, the Diablo Canyon Power Plant has employed Field Programmable Gate Array hardware logic, as opposed to microprocessors, so as to avoid a software requirement for system operation [14].

Implementation, however, has not been without challenges. In 2003, at the David-Besse NPP in Ohio, maintenance personnel bridged replacement control networks to a dial-up T1 line, transferring the Slammer worm from a private PC which was able to spread to control networks

and disabled a safety parameter display system (SPDS) for nearly five hours [15]. The SPDS does not perform control functions, but does provide post-accident monitoring capability so operators can verify that safe shutdown and been achieved and is maintained. Similar incidents during testing and maintenance have caused failure of non-safety-related reactor recirculation pumps and the condensate demineralizer controller at Browns Ferry NPP in 2006 and an automatic reactor scram at Hatch NPP in 2008 [16], as mentioned earlier. These examples highlight the potential impacts that can – and have – occurred in implementation of digital technologies, where network connectivity is a double-edged sword.

2.3 Best Practices and Strategies

Cybersecurity and controls researchers have conducted thorough studies into mitigation strategies for NPP I&C issues such as common-cause failure, monoculture, and other common pitfalls resulting from heavy reliance on new technologies. A variety of organizations have developed guidance and best practices for NPP digital I&C, such as the Electric Power Research Institute, the Institute of Nuclear Power Operations, the Nuclear Energy Institute, and the Nuclear Information Technology Strategic Leadership group [10]. One practice of high importance and pervasive in the nuclear industry is the division of NPP systems and networks into a level structure [13], [16]-[18].

An example control room architecture is shown in Figure 2-1 to illustrate this level structure [19]. Here, we see the component (device) control level, the system (group) control level and the plant control level. Some of the systems depicted conduct fault detection so action can be taken to mitigate the consequences of system faults. The Protection System is the primary fault detection system for safety I&C containing self-diagnostics functions and alerting operators to unusual conditions or internal failures, and generating control signals to shut down (trip) the reactor and initiate heat removal if operating parameters depart from acceptable limits. The signal conditioning system can take input signals including status and health monitors for the actuators it controls to inform prioritization of which signals to trust. For the operations I&C, the limitation system detects deviations from desired operational values and takes effect to reduce reactor trips and actions by the protection system [20]. Clear cybersecurity and diversity implications exist because, for example, the reactor protection system uses signals from sensors that are also used for plant unit control functions.

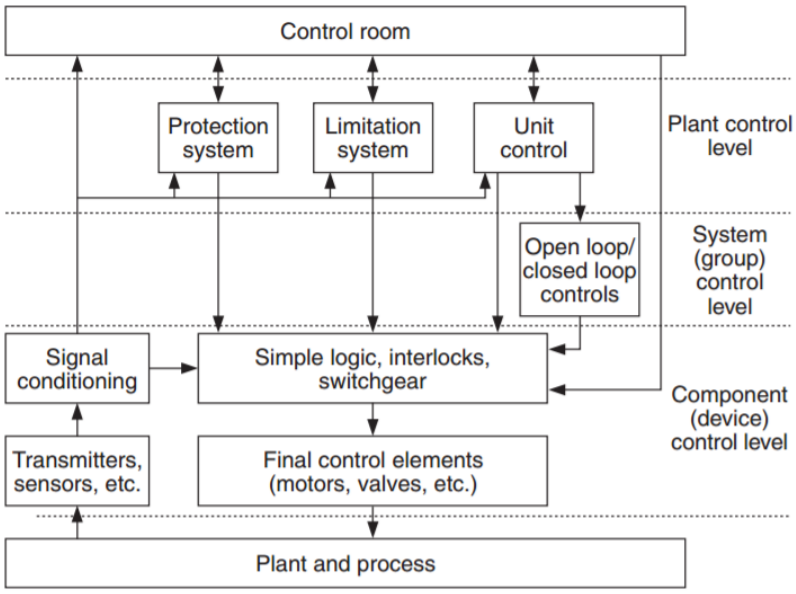

Figure 2-1. Example modern nuclear reactor instrumentation and controls architecture.

Separating, to the degree possible, safety-related and non-safety-related systems from one another helps to balance the leveraging of efficiency and ease-of-use with added vulnerability from connectivity. Divisions can, and should be, more detailed by isolating certain systems from two-way communication so that the spread of cyber-threats can be stopped with physical barriers [16]. Data diodes, for example, are often used to allow data transfer from the plant control network to the corporate network while preventing data transfer in the opposite direction [21]. These theoretically enable significant value extraction from process data and operations research and replace "air gaps" in which a system is truly isolated from external communication. Redundancy, diversity, and defense-in-depth are all principles which are central to all NPP safety design, and therefore extend naturally to digital I&C. In fact, GE-Hitachi adopts the practice of ensuring that all digital I&C meets the original design bases and standards of the system that the legacy analog I&C met [11].

In designing a control system, the NRC's Regulatory Guide (RG) 5.71 gives a comprehensive set of requirements for NPP I&C. In order to develop a sophisticated understanding of potential attack vectors and known vulnerabilities, an NPP I&C system will require maintenance and test activities as well as a thorough search into the NPP network, operating systems, and applications [18]. The difficulty of instituting these activities, regulatory burden, cost, and potential for malfunction can be alleviated with computerized system testing [13], a practice which would enable an iterative approach to system upgrade and development. Attack vectors are not restricted to an individual system, but can be exposed through a combination of physical and cyber-based means [16]. This means that analog backup systems cannot be the only mitigation strategy for cybersecurity concerns. One trend across many industries that may also be very useful in NPPs is that of fault-tolerant control systems [22]. These systems seek to handle off-normal conditions regardless of whether faults are instigated by physical or cyber-phenomena. They address vulnerabilities of

conventional feedback control in terms of performance and stability through "self-repairing" design, but they must also be able to offer non-optimal solutions by strictly-imposed deadlines in order to secure acceptable plant operation, or, if necessary, graceful failure.

While advancements in digital I&C and sophisticated strategies for implementation can mitigate many cybersecurity concerns, current systems are limited primarily by communication technologies as opposed to actual computational or processor technologies [13]. Data transfer rates may not be able to accommodate newly-developed control systems, while an incremental upgrade approach may leave gaps and inconsistencies in data synchronization across plant networks. For this reason, the trend in digital I&C development is toward fewer networks and reduced complexity, which may also exacerbate the potential for common-cause failure. A balance needs to be struck with software integration optimization, hardware diagnostics in software design, techniques for establishing and confirming time coherency of data, and automated system testing.

2.4 Challenges Unique to Advanced Nuclear Systems

1996 saw the first fully digital I&C system integrated into the newly-built Japanese Kashiwazaki-Kariwa Advanced Boiling Water Reactor (ABWR), the world's first operational Generation III reactor [23]. However, the ABWR design continued the use of active safety systems. New passively safe reactor designs provide new opportunities that remain to be fully explored, as compared to existing and evolutionary LWR designs. For example, the I&C systems used in the passively safe AP1000 reactor, now being constructed in China and U.S., has very similar architecture to earlier digital I&C developed for active LWR design. In the near-term, the first new passive NPP designs that will have substantial I&C changes will be light-water small modular reactors (SMRs) like the NuScale plant design, which are smaller both in size and power output than the NPPs in commercial operation today. Their comparatively smaller size imposes new spatial constraints, while a tendency towards more integration and less exposed piping also adds to this difficulty. Suggested strategies for meeting these challenges require more pervasive data collection and sharing as well as cutting-edge instrumentation technology, which may increase dependency on digital I&C in some respects and reduce it in others [24]. While communication has already been established as a limiting factor in digital I&C development, software itself poses important maintenance and cyber-issues that will become more important as its importance to critical plant operation increases. These issues include memory management, data corruption, system interactions, and the accumulation of digital round-off errors [25].

One strategy for improving advanced NPP economics and construction times is modular construction, especially in SMRs like the NuScale plant. If coherency is desired among all of the units for a multi-unit NPP while many modules are controlled using some dedicated I&C, that I&C must be complete and uninterrupted within one module while it must also be seamlessly adaptable to the introduction of new modules [13]. Finally, physical degradation will require new conditions to be met for advanced NPP I&C so that they are qualified for use. This is due both to miniaturization of technology that elevates new degradation mechanisms to primary concerns and diverse environments presented by advanced NPP designs with different coolants, operation temperatures, and structural materials.

The nuclear energy industry was not explicitly required to address cybersecurity until after the terrorist attacks of Sept. 11, 2001 [26]. Now, every company operating nuclear power plants has an NRC-approved cybersecurity program. This means that, unlike all commercially operating reactors in the United States, every new reactor company that will be licensed must design its plant to satisfy existing cybersecurity requirements. However, in contrast to "safety", a "cybersecurity" tab is difficult to find on virtually every new reactor company's website. While the concept of cybersecurity may not have existed during the design of most operating plants, designers risk leaving significant cybersecurity vulnerabilities in their plant designs if they do not consider this growing threat, especially if they wish to innovate by leveraging modern I&C technologies. A brief survey of websites and available documents reveals a wide range in the degree of consideration already given to control strategies by new plant designers, with some of the most interesting findings summarized in Table .

Table 2-1. Selected cybersecurity-related strategies of new reactor companies.

Company Name	Reactor Type	Cybersecurity Mentioned?	Other Relevant Considerations
Advanced Reactor Concepts	Sodium-cooled fast reactor	No	Control approach for control rods attempts to avoid problems due to sensor, control logic, or actuator malfunction [27]
NuScale Power	Small modular light water reactor	Yes	Extensive review of regulations from NRC and other, non-nuclear regulatory groups, incorporation of cybersecurity threat mitigation strategies in control room and I&C integration [28]
TerraPower	Sodium-cooled fast reactor	No	First phase control room simulator built to study reactor operation, reactor does not require prompt operator actions to put reactor in safe shutdown conditions [29]
ThorCon Power	Molten salt reactor	No	No requirement for operator (or control system) intervention during accidents, no safety-critical I&C, electronic systems for operational control only, multiple control rooms and external control room with continuous transmission of operational data to engineers and regulatory agency [30]

One common feature of new and advanced reactor designs is passive safety – the capability of the plant to shut down (trip) and activate heat removal without requiring any external source of electrical power or active control. Reactor designs that leverage passive safety may inherently reduce the concern from cybersecurity threats, at least from a public health standpoint. However, cybersecurity considerations are seen from NuScale's plans as it incorporates modern digital I&C into a new control room design. ThorCon plans to completely avoid electronics in its safety systems but also plans to supply operational data continuously to external control rooms and external parties. TerraPower and Advanced Reactor Concepts also plan to avoid the need for operator actions using passive systems. While all of these represent strategies that can potentially support robust cybersecurity defense, previous incidents outlined in earlier sections can still cause equipment failure or reactor shutdown. Bill Gross, Nuclear Energy Institute Senior Project Manager of Cybersecurity, has stated that "cybersecurity is handled" [31]. However, this is not an accurate statement. Cybersecurity threats are ever-evolving and meeting regulations as they are amended may not be enough to protect our nation from large-scale power failures. For this reason, the level of need and unique challenges for new and advanced nuclear reactor designs will need to be further explored.

3 Relevance to Design Strategies and Discussion

Upon reviewing NPP I&C and current ideas about the role of digital I&C in the nuclear power industry, some prominent issues and strategies have become clear. Issues with NPP I&C include availability of control hardware and expertise, need for pervasive data collection and communication with need to identify and mitigate common-cause failure and implement physical barriers to cyber-threats, and changing requirements based on changing and diverse plant technologies. Of course, these issues exist even before regulatory challenges are brought into the mix. One strategy for solving these issues is a division and categorization of systems for a hybrid analog-digital I&C system. Fault detection and plant health monitoring functions should be provided for both safety and operational systems to mitigate consequences of digital system compromises or failures. Software integration can be optimized for managing communications constraints and cybersecurity vulnerabilities while automated and standardized computer-based I&C testing can ensure system compliance throughout an integrated design process. Additionally, the design and cybersecurity for other technologies, such as commercial aviation (with insights recorded in [1]), autonomous vehicles, and lithium-ion battery packs, can be studied to identify examples of better – and worse – practice.

This list of activities reveals an inherent need that pervades all strategies for implementing digital I&C in advanced NPPs: tradeoff analysis. In order to effectively leverage digital I&C technology to maximize NPP safety, economic performance, and efficiency, the system needs to be divided into levels and categorized by *risk-importance* so that optimal solutions can be found across all fronts.

Acronyms and Abbreviations

ICS – Industrial control system(s)
NPP – Nuclear power plant
PLC – Programmable logic controller
I&C – Instrumentation and control
LWR – Light water reactor
SCRAM – Shut down (a nuclear reactor)
NRC – Nuclear Regulatory Commission
PWR – Pressurized-water reactor
BWR – Boiling-water reactor
SPDS – Safety parameter display system
RG – Regulatory Guide
ABWR – Advanced boiling-water reactor
SMR – Small modular reactor

4 References

[1] C. Andreades, C. Poresky, J. Kendrick and P. Peterson, "Cyber Security in Civilian Aviation: Insights for Advanced Nuclear Technologies," UCBTH-17-001, Berkeley, CA, 2017.

[2] S. Bennett, *A History of Control Engineering, 1930-1955*, First. London, UK: Peter Peregrinus Ltd., 1993.

[3] S. Bennett, "A brief history of automatic control," *IEEE Control Syst. Mag.*, vol. 16, no. 3, pp. 17–25, Jun. 1996.

[4] E. Hayden, "An Abbreviated History of Automation & Industrial Controls System and Cybersecurity," 2015.

[5] H. L. Hazen, "Theory of servo-mechanisms," *J. Franklin Inst.*, vol. 218, no. 3, pp. 279–331, Sep. 1934.

[6] S. Bennett, "Control and the Digital Computer: The Early Years," *IFAC Proc. Vol.*, vol. 35, no. 1, pp. 237–242, 2002.

[7] H. Smith, "A brief history of electric utility automation systems," *Electr. Energy T&D Mag.*, 2010.

[8] The White House, "PRESIDENTIAL DECISION DIRECTIVE/NSC-63," Washington, D.C., 1998.

[9] U.S. Energy Information Administration, "Energy Information Administration Frequently Asked Questions," 3 March 2017. [Online]. Available: https://www.eia.gov/tools/faqs/faq.php?id=228&t=21. [Accessed 4 April 2017].

[10] B. P. Hallbert and K. Thomas, "Advanced Instrumentation, Information, and Control Systems Technologies Research in Support of Light Water Reactors," in *ISOFIC/ISSNP*, Jeju, Korea, August 24-28, 2014.

[11] L. Chi and B. Zhang, "Managing I&C Obsolescence for Nuclear Power Plant Life Extension," IAEA INIS, Washington, DC, 2012.

[12] Nuclear Regulatory Commission, "History of Digital Instrumentation and Controls," Nuclear Regulatory Commission, 31 December 2015. [Online]. Available: https://www.nrc.gov/about-nrc/regulatory/research/digital/history.html. [Accessed 6 April 2017].

[13] Oak Ridge National Laboratory Preferred Licensing Services Logenecker & Associates, "Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC, April 2004.

[14] S. B. Patterson, J. W. Hefler and E. L. Quinn, "Diablo Canyon Power Plant Digital Process Protection System Replacement Diversity and Defense-in-Depth," Nuclear Regulatory Commission, Washington, DC, 2012.

[15] B. Kesler, "The Vulnerabilities of Nuclear Facilities to Cyber Attack," *Strategic Insights*, vol. 10, no. 1, 2011.

[16] C.-S. Cho, W.-H. Chung and S.-Y. Kuo, "Cyberphysical Security and Dependability Analysis of Digital Control Systems in Nuclear Power Plants," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 3, pp. 356-369, 30 June March 2016.

[17] Y. Sun, "Digital Instrumentation and Control System for Unit 5 & 6 of YangJiang NPP," *Journal of Energy and Power Engineering*, vol. 8, pp. 1777-1782, 8 April 2014.

[18] J.-G. Song, J.-W. Lee, G.-Y. Park, K.-C. Kwon, D.-Y. Lee and C.-K. Lee, "An Analysis of Technical Security Control Requirements for Digital I&C Systems in Nuclear Power Plants," *Nuclear Engineering and Technology*, vol. 45, no. 5, pp. 637-650, 21 April 2013.

[19] International Atomic Energy Agency, "Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook," International Atomic Energy Agency, Vienna, Austria, 1999.

[20] U.S. Nuclear Regulatory Commission, "Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update (NUREG/CR-6992)," Office of Nuclear Regulatory Research, Oak Ridge, TN, 2008.

[21] A. Scott, "Tactical Data Diodes in Industrial Automation and Control Systems," SANS Institute InfoSec Reading Room, 2015.

[22] J. J. Youmin Zhang, "Bibliographical review on reconfigurable fault-tolerant control systems," *Annual Reviews in Control*, vol. 32, pp. 229-252, 3 May 2008.

[23] GE Hitachi, "ABWR Nuclear Power Plant," GE Hitachi, 2017. [Online]. Available: https://nuclear.gepower.com/build-a-plant/products/nuclear-power-plants-overview/abwr.html. [Accessed 6 April 2017].

[24] B. R. Upadhyaya, M. R. Lish, J. W. Hines and R. A. Tarver, "Instrumentation and Control Strategies for an Integral Pressurized Water Reactor," *Nuclear Engineering Technology*, vol. 47, pp. 148-156, 13 July 2015.

[25] H. Liang, P. Gu, J. Tang, W. Chen and F. Gao, "Discussion on software aging management of nuclear power plant safety digital control system," SpringerPlus, 2016.

[26] Nuclear Energy Institute, "Cyber Security for Nuclear Power Plants," Nuclear Energy Institute, July 2016. [Online]. Available: https://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants. [Accessed 9 April 2017].

[27] D. C. Wade and L. Waters, "ARC-100: A Modular Nuclear Plant for Emerging Markets: Safety Strategy," in PHYTRA 2 - *The Second International Conference on Physics and Technology of Reactors and Applications*, Rabat, Morocco, 2011.

[28] B. Arnholt, "Multinational Design Evaluation Program Digital I&C Working Group Common Position Evaluations for NuScale Digital I&C Design, Presentation to NRC, PM-0815-16440, Revision 0," Nuscale I&C Engineering, 2015.

[29] TerraPower, LLC, "Safety," TerraPower, LLC, 2017. [Online]. Available: http://terrapower.com/pages/safety. [Accessed 9 April 2017].

[30] J. D. Devanney, L. Jorgenson, C. Uhlik and Martingale, "IAEA Advanced Reactor Information Service Status Report - ThorCon Molten Salt Reactor," International Atomic Energy Agency, Vienna, Austria, 2016.

[31] Nuclear Energy Institute, "Digital: The New Word in Nuclear Power Plant Control Rooms," Nuclear Energy Institute, 2 June 2016. [Online]. Available: https://www.nei.org/News-Media/News/News-Archives/Digital-The-New-Word-in-Nuclear-Power-Plant-Contro. [Accessed 6 April 2017].