Cyber security for microreactors in advanced energy systems

Received (in revised form): 18th November, 2020

Piyush Sabharwall

Senior Staff Nuclear Research Scientist, Idaho National Laboratory, USA

Piyush Sabharwall PhD is a Senior Staff Nuclear Research Scientist working in the Nuclear System Design and Analysis Division at Idaho National Laboratory (INL). Piyush has more than 14 years' research and development experience in nuclear/thermal engineering. He serves as the technical lead on DOE Office of Nuclear Energy's Microreactor R&D Program and leads the development of gas-cooled cartridge loop for the Versatile Test Reactor. He has helped position INL as an intellectual leader in areas such as verification and validation, development of experimental programmes, small modular reactors, molten salt reactor technology and integrated energy systems. Piyush has authored two books, contributed chapters to technical books on advanced reactors and thermal systems, process heat transfer and published over 120 peer-reviewed publications. He holds an adjunct associate professor appointment in the Department of Mechanical Engineering at Texas A&M University and serves on the ASME Heat Transfer Division (K-9 and K-13 committees). He is a member of the advanced (Gen IV) reactor technical advisory group at EPRI. Piyush has consulted for industries both nationally and internationally, building technical expertise while focusing on market studies and economic viability to rebuild the US nuclear industrial infrastructure and position US industry to continue to be a leader in the global energy market.

Nuclear System Design and Analysis Division, Idaho National Laboratory, PO Box 1625, MS 3760, Idaho Falls,
ID 83415, USA
Tel: +1 208-526-6494; E-mail: Piyush.Sabharwall@inl.gov

James Gibb

Senior Critical Infrastructure Cybersecurity Analyst, Idaho National Laboratory, USA

James Gibb is a Senior Critical Infrastructure Cybersecurity Analyst at Idaho National Laboratory and conducts Industrial Control System (ICS) cyber security assessments for critical infrastructure entities throughout the USA. James' experience includes supporting the spectrum of cyber operations to include capability development, network defence, incident investigation and cyber intelligence threat analysis. He has experience in software engineering, advanced forensics analysis, network architecture analysis and adversary-based threat modelling. James holds a Bachelor's degree in computer engineering from North Carolina State University, and a Master's in national security and strategic studies from the Naval War College in Newport, RI. His work experience includes six years at Idaho National Laboratory and 22 years' service in the US Navy.

Idaho National Laboratory, PO Box 1625 MS 3510, Idaho Falls, ID 83415, USA
Tel: +1 208-526-4597; Mob: +1 208-409-1793; E-mail: james.gibb@inl.gov

Christopher Ritter

Group Lead, Idaho National Laboratory, USA

Christopher S. Ritter is the Group Lead with the Digital and Software Engineering group at Idaho National Laboratory. Ritter's expertise is in software engineering, software development, leading software teams, systems engineering software integration and database management. Before coming to INL, he was Director of Software Development at SPEC Innovations in Manassas, VA. He served as the chief architect of Innoslate, a popular system engineering tool that leverages elastic cloud technologies and AI/NLP for high scalability and advanced analytics. He also architected the software system and consulted on the data ontology for a centralised mission risk management system for the joint staff at the Pentagon and supported Marine Corps business process reengineering for its capability portfolio management processes. He holds a Bachelor's degree in computer science from Virginia Polytechnic Institute and State University.

Digital and Software Engineering Group, Idaho National Laboratory, PO Box 1625, MS 1334, Idaho Falls,
ID 83415, USA
Tel: +1 208-526-2657; E-mail: Christopher.Ritter@inl.gov

Kathleen Araújo

Director of the CAES Energy Policy Institute, Boise State University, USA

Kathleen Araújo is the Director of the CAES Energy Policy Institute and Associate Professor of Energy Systems, Innovation and Policy at Boise State University. She advises, teaches and conducts research on better practices and policy relating to disruptive change. Specific areas of focus include international regulation of cyber/nuclear risk, disaster readiness and pivot points in decarbonisation, such as those evaluated in her book *Low Carbon Energy Transitions: Turning Points in National Policy and Innovation* (Oxford University Press). Kathleen is the book series editor for Routledge's Studies in Energy Transitions. She also consults for inter-governmental organisations and industry.

CAES Energy Policy Institute, Boise State University, Boise, Idaho, 83706-1014, USA
Tel: +1 208-426-4845; E-mail: Kathleenaraujo@boisestate.edu

Abhinav Gupta

Director of the Center for Nuclear Energy Facilities and Structures, NC State University, USA

Abhinav Gupta is Director of the Center for Nuclear Energy Facilities and Structures (CNEFS) at North Carolina State University. Presently, he also serves as the President of International Association SMiRT. Abhinav's research has focused on uncertainty quantification and probabilistic methodologies for risk assessment. He has worked on developing new computational and probabilistic models needed for decision support and strategy development in reducing operation, maintenance and construction costs. He received the Outstanding Paper Award at the 2005 ASME-Pressure Vessel and Piping Conference and chaired the highly successful SMiRT 25 conference in 2019. He has served as the chair of ASCE's Committee on Emerging Computing Technologies, as Associate Editor for the *Journal of Structural Engineering*, and as a visiting faculty at the US Nuclear Regulatory Commission. In 2010, Abhinav was inducted into the Academy of Outstanding Teachers at NC State University. Presently, he is working on ARPA-E sponsored projects for data-driven, AI-enabled strategies needed in the development of digital twins for advanced reactors.

Center for Nuclear Energy Facilities and Structures, NC State University, Campus Box 7908, Raleigh,
NC 27695-7908, USA
Tel: +1 919-515-1385, E-mail: agupta1@ncsu.edu

Ian Ferguson

Idaho National Laboratory, USA

Ian Ferguson completed an internship through the US Department of Energy's Science Undergraduate Laboratory Internships programme at Idaho National Laboratory. Ian holds a BS in nuclear engineering from Oregon State University.

Idaho National Laboratory, PO Box 1625, MS 3860, Idaho Falls, ID 83415, USA. Tel: +1 503-888-7756
E-mail: ian.ferguson97@gmail.com

Bri Rolston

Critical Infrastructure Security Researcher, Idaho National Laboratory, USA

Bri Rolston is a Critical Infrastructure Security Researcher at Idaho National Laboratory specialising in defensive security engineering research and threat response. Bri has more than 20 years' experience in telecommunications, information technology (IT), industrial automation and control systems (IACS)/operational technology (OT) security research. She periodically switches from research to operations work to stay abreast of security trends and has a wide range of operational security experience, including incident response, threat management, risk analysis and remediation, vulnerability management, secure code development, cloud security and ICS security operations. She has trained several ICS incident response teams including DHS CIRT in 2005, contributed to IACS and OT security standards development for DHS, DOE, NIST, and ISA/IEC, and has a patent for efficient attack path selection and

risk analysis. Bri has been extensively involved in the security research community since 2000 and helps organise security conferences such as BSides IF. Her personal research areas of expertise are threat research, attack path prediction, halo effects in exploit development and second-payload detection in IACS/OT attacks.

Idaho National Laboratory, PO Box 1625, MS 3545, Idaho Falls, ID 83415, USA
Tel: +1 208-526-1460; E-mail: Bri.Rolston@inl.gov

Ron Fisher
Director of Infrastructure Assurance & Analysis Division, Idaho National Laboratory, USA

Ron Fisher PhD is the Director of the Infrastructure Assurance & Analysis Division at Idaho National Laboratory. Ron provides over 20 years' critical infrastructure protection and resilience experience including serving on President Clinton's Presidential Commission on Critical Infrastructure Protection. His research activities include developing vulnerability assessment methodology, risk and resiliency analyses and infrastructure interdependencies. The methodologies he helped to develop have been conducted at thousands of critical infrastructure facilities throughout the USA. He has been the Programme Manager for critical infrastructure protection activities for the Departments of Energy, Defence, and Homeland Security. Ron has over 300 classified publications and over 150 unclassified publications including contributions to multiple books, as well as a copyright and trademark in geospatial information technology. Ron received a doctorate degree in organisational development from Benedictine University and has a BS in finance and an MBA.

Infrastructure Assurance & Analysis Division, Idaho National Laboratory, PO Box 1625, MS 3650, Idaho Falls,
ID 83415, USA
Tel: +1 208-526-5630; E-mail: Ron.Fisher@inl.gov

Jess Gehin
Chief Scientist of Nuclear Science and Technology and Acting Director, Idaho National Laboratory, USA

Jess Gehin joined INL in 2018 as the Chief Scientist for Nuclear Science and Technology and is the acting Director of the Advanced Scientific Computing Division at Idaho National Laboratory. He also serves as the Technical Director of DOE Office of Nuclear Energy's Microreactor R&D Program. Jess worked at ORNL from 1992 to 2018 where he held several positions including director of the Consortium for Advanced Simulation of Light Water Reactors (CASL), a DOE Energy Innovation Hub, at Oak Ridge National Laboratory (ORNL) and leadership responsibilities for reactor technology integration, nuclear energy programmes and reactor analysis. Jess is a fellow of the American Nuclear Society.

Advanced Scientific Computing Division, Idaho National Laboratory, PO Box 1625, MS 3860, Idaho Falls,
ID 83415, USA
Tel: +1 208-526-3486; E-mail: Jess.Gehin@inl.gov

Youssef Ballout
Division Director, Idaho National Laboratory, USA

Youssef Ballout is the Division Director of INL's Reactor Systems Design & Analysis. Youssef Joined INL in December 2018 as the manager of the Fuel Design and Development department. Prior to INL he was the President of Elysium Industries Limited, where he was engaged in leading the design and development of a chloride molten salt fast reactor. Youssef also spent 26 years at the Naval Nuclear Laboratory (NNL)/ Knolls Atomic Power Laboratory where he worked on nuclear reactor design, reactor materials, reactor thermal hydraulics and reactor structural performance.

Reactor Systems Design & Analysis, Idaho National Laboratory, PO Box 1625, MS 3860, Idaho Falls, ID 83415, USA
Tel: +1 208-526-1293; E-mail: Youssef.Ballout@inl.gov

Abstract Demand for clean and resilient energy has led to new and advancing frontiers of energy development in nuclear technology, specifically in the development of microreactors. These miniaturised modular reactors are generally <20 megawatts thermal (MWt) or 10 megawatts electric (MWe) and offer new opportunities to meet energy needs in remote locations and mobile operations. As with the slightly larger small modular reactors (<300 MWe), microreactor development must demonstrate security and safety, as well as economic competitiveness, to be seen as potential opportunities for new applications. Current research focuses on passive safety features, capital costs, reliability, semi-autonomous or autonomous control, cyber informed design, digital twins and non-proliferation. This paper focuses specifically on microreactor cyber informed design and cyber risk. An overview of microreactor technology provides a basis for examining the cyber nuclear playing field, with an emphasis on the USA. Frameworks for evaluating cyber security threats, and thereby designing for them, are reviewed. Recommendations follow with ideas for future research.

KEYWORDS: microreactors, cyber digital twins, cyber informed design, cyber risk, nuclear power

INTRODUCTION

For more than half a century, nuclear energy has been a source of low carbon electricity in the global supply. Along with renewables, energy efficiency and other innovative technologies, nuclear technology can make a significant contribution to achieving sustainable, low carbon development. An emergent area of nuclear energy with disruptive potential is the microreactor. Such miniaturised modular reactors are generally <20 MWt or 10 MWe, offering new opportunities to meet energy needs in remote and mobile operations, as shown in Figure 1.

Microreactor technology is being developed so that the reactors can provide decentralised power and heat to remote communities, military bases, industrial users and mobile operators. Unlike diesel generation, which can involve expensive delivery of fuel, microreactors could address these needs with added benefits of low carbon fuel.

Technology designs for microreactors emphasise factory fabrication and transport of self-contained reactors[1] via lorry, rail, water or aircraft for a 'plug-and-play' approach. Lower upfront capital costs, compactness, semi-autonomous control and use of low enriched uranium fuel up to 20 per cent enrichment are other features that are expected to distinguish the miniaturised reactors from the larger counterparts.

As research and development continues on microreactor technology, new regulatory approaches will be needed to account for the distinct technological attributes and potential uses for the reactors. The remote siting of microreactors, their smaller size, fully assembled condition at transport and fuel enrichment levels translate to different oversight needs compared to larger plants. Microreactor designs are also expected to use fewer components and may rely more fully on self-contained systems. Such systems could include automated controls to perform certain tasks, with the end result being maintenance and stability of the reactor system based on pre-programmed algorithms and logic responses. Designs are also factoring for diagnostic capabilities to identify aging instrumentation and properly compensate over time.

Microreactor technology designs anticipate the use of semi-autonomous or highly automated control systems composed of digital components such as wireless monitoring, digital communications, remote or shared data processing and modern control-system components.[2] These

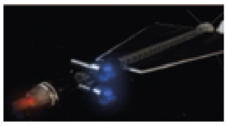
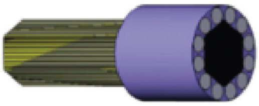
	Electric Power	Type	Application(s)	Power (kW)
	500 W - 10 kW	Non-Light Water Reator (LWR)	Deep Space Power	10^0 10^1
	10 kW - 1 MW	Non-LWR	Space propulsion Planetary surface power Military applications	10^2 10^3
	1 MW - 10 MW	Non-LWR	Military bases Remote locations Disaster relief	10^4
	10 MW - 50 MW	Non-LWR	Power to grid Military bases Process heat	
	50 MW - 300 MW	LWR & Non-LWR	Power to grid Small cities Burning of actinides	10^5
	1000 MW	Mostly LWR	Power to grid	10^6

Figure 1: Electric power production of microreactors and other reactor types

technologies have been well-integrated into industries such as aerospace, yet are relatively new to the nuclear industry, so design-based system hardening and risk management have added significance for emerging nuclear reactors.

This paper focuses specifically on design aspects for cyber nuclear risks. Public safety, socio-economic and related security trade-offs of semi-autonomous or automated use of microreactors are an important subject for fuller additional inquiries. The remainder of the paper examines cyber informed design and cyber risks for microreactors, beginning with an overview of microreactor technology. The paper then discusses the cyber nuclear field, with a focus on the USA. General frameworks for evaluating cyber security threats and designing against them are then reviewed and recommendations follow.

This paper concludes with ideas for future research.

CYBER NUCLEAR BASIS IN THE USA

The US nuclear fleet of commercial power plants has historically relied on analogue systems and simple programmable logic controllers. Today, nuclear plants in the USA use digital and analogue systems to monitor, operate, control and protect plants.[3] Digital assets that are deemed critical for the safety and security of plant operations, however, are air-gapped or isolated from external networks, including the Internet. Even though these systems are air-gapped, it is important to recognise that an air gap will not stop all malicious attacks, but they do introduce additional complexity into the attack path planning process.

Currently, cyber security rules for commercial nuclear plants are based on Regulatory Guide (RG) 5.71,[4] Title 10 of the Code of Federal Regulations (CFR), Section 10 CFR 73.54, and Nuclear Energy Institute guidance NEI 08/09.[5,6] In line with these rules and guidance, all nuclear power reactor licensees in the USA must submit a cyber security plan for approval by the U.S. Nuclear Regulatory Commission (NRC), and adhere to NRC regulation which includes inspections. Additional standard requirements pertaining to supply chain risk mitigation were approved through Order No. 850 by the NRC, effective 1st July, 2020.[7] These mitigations require operators to develop, implement and review supply chain plans that account for vendors' remote access, verify software integrity and authenticate code to ensure the code is not counterfeit or modified without knowledge of the software supplier.[8]

With new microreactor designs anticipating a potential for remote use, portability of the systems, and critical digital process control of microreactors, the existing design-basis threat analysis for nuclear plants must be adapted to account for disruptive failures of automated technology and malicious threats, such as targeted cyberattack. A brief review of planned microreactor features will highlight this point.

Digital control is expected to be essential for a significant number of devices in a microreactor. Wireless instrumentation (if used in microreactors) transmits data input to the control system from a variety of sources, including flow meters, pressure and strain gauges, filtration systems, thermocouples, resistance temperature detectors (RTDs) and turbine-speed monitors. Even the control system, whether it is semi or fully autonomous, is a digital system. Digital systems and wireless devices, including the remote systems for autonomous control and monitoring, will be vulnerable to cyber exploitation in ways that their analogue counterparts are not. Because they are highly interconnected systems, there exists the potential for malware or malicious activity to move laterally through the network from one component to the next.

THE CYBER PLAYING FIELD AND FRAMEWORKS FOR ANALYSIS

Cyberattacks are not a new threat for many industries. As early as 2003, companies began to report cyberattacks and events as a risk in their Securities and Exchange Commission (SEC) 10-K filings.[9] In 2009, 33 per cent of all reported cyberattacks or intrusions of industrial control systems (ICSs) occurred within the energy industry. By 2011, these cyber events grew to 44 per cent and by 2013, to 59 per cent.[10,11] Even though these types of threat are not new, all industries are still struggling to adapt to cyber threats.[12] Each year the attack sophistication increases while knowledge of what the malicious threat actor needs in order to initiate an attack decreases dramatically, as shown in Figure 2.[13]

This phenomenon is directly related to the integration of uniform digital systems that operate on a software platform that will be used for reactor control systems. Previously, a cyber threat actor would need to spend an extensive period of time learning how the software environment they wished to infiltrate functions. These environments were largely proprietary and custom-configured

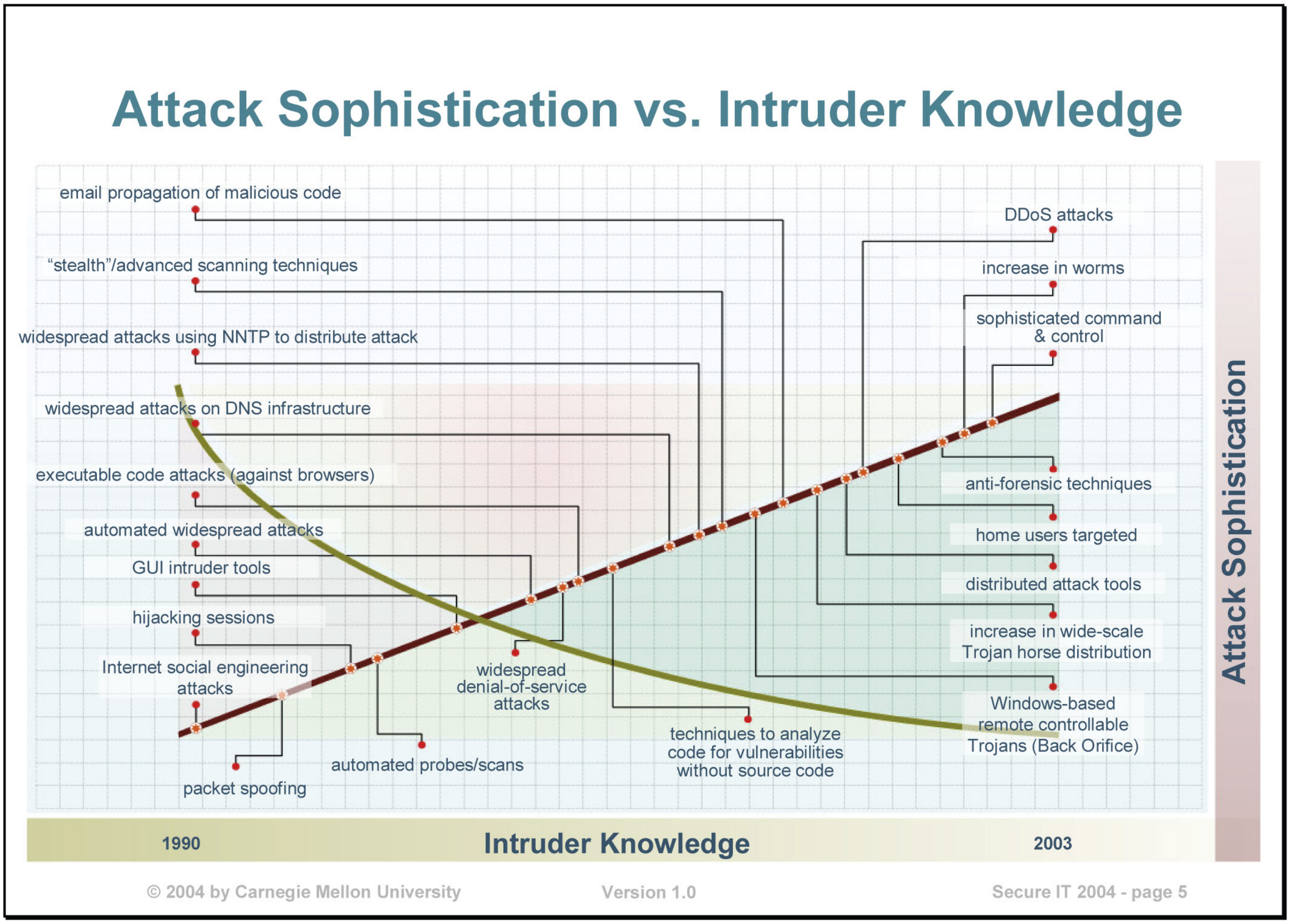


Figure 2: Progression of cyberattack sophistication in relation to the intruder knowledge required to execute the kind of attack[14]

for a specific system's operational environment. With uniform digital systems, the operating system is standardised, requiring less knowledge gathering for the adversary to effectively enter the system and access the areas and information needed to conduct an attack. The heavy use of digital networks and systems increases the need for a cyber security defensive architecture. The complexity of modern digital systems and their related operating system and software components entail unavoidable errors and programming flaws that can be discovered and exploited by an adversary across like brands of computers and systems. As a result, cybersecurity efforts among many industries have become largely reactive, requiring that defenders respond to attacks after they have already occurred because the attack vectors are unknown until the moment of attack, and attacks happen rapidly.

A framework for thinking about cyber security in microreactor plants must be factored for the technology to be robust, diverse and proactive, rather than reactive. A hierarchical approach to cyber security is an effective way to organise all the necessary instrumentation and control information required to create an effective security system. The National Institute of Standards and Technology (NIST), widely considered one of the most authoritative sources for cyber security references and standards, published a systems security engineering reference on architecture in November 2016. The Systems Security Engineering Framework[15] (see Figure 3) contains a comprehensive and concise outline of how to incorporate cyber security into new or existing systems. Application of this framework is complex and less direct than the design workflow for either the industrial engineering or the process–control design example for microreactors. Integration of cyber security protection into the nuclear engineering design process, based on the NIST reference, requires a great deal of customisation and security expertise. Even then, implementation will also need to be highly customised in line with the

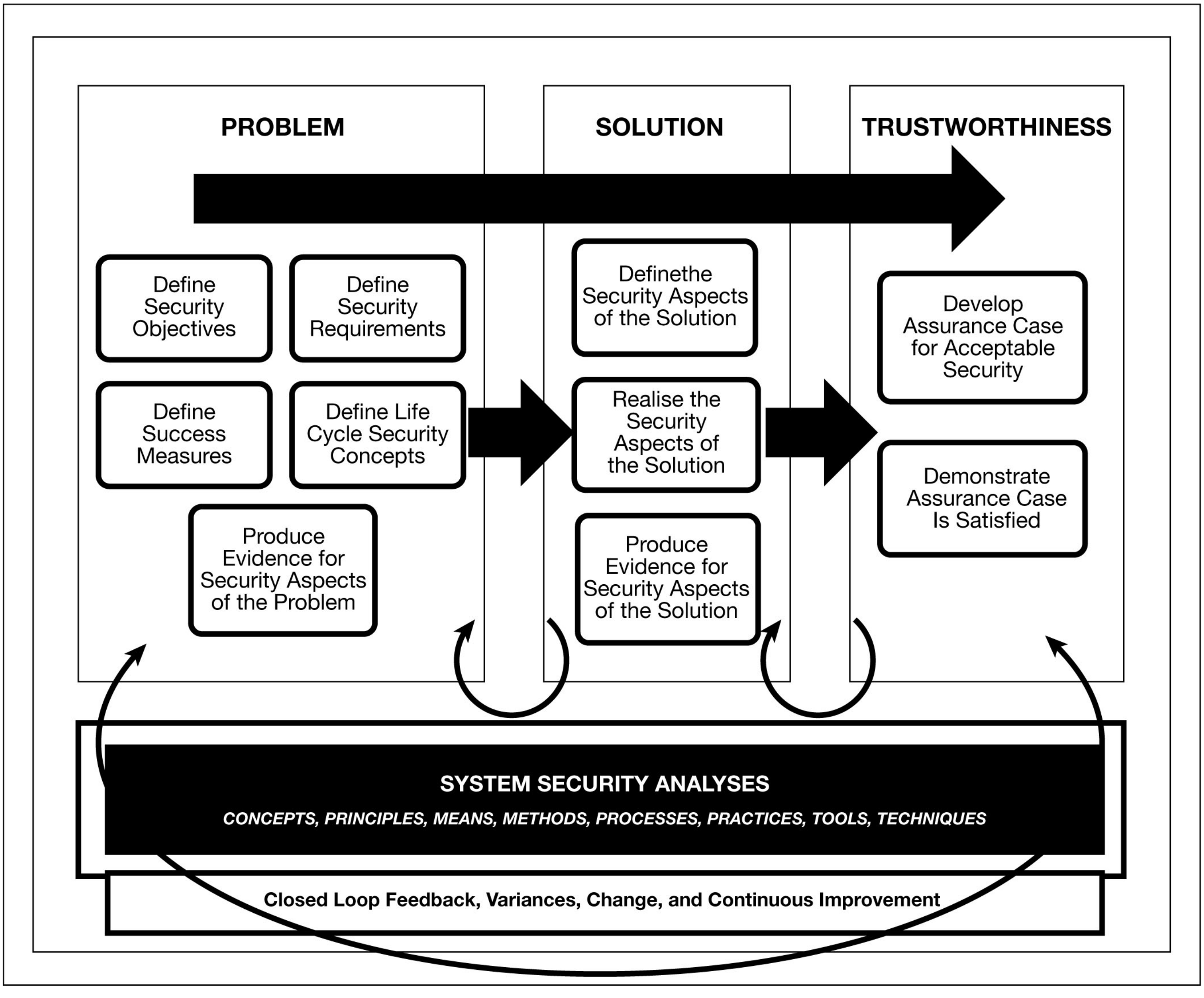

PROBLEM
SOLUTION
TRUSTWORTHINESS
Define Security Objectives
Define Security Requirements
Define Success Measures
Define Life Cycle Security Concepts
Produce Evidence for Security Aspects of the Problem
Definethe Security Aspects of the Solution
Realise the Security Aspects of the Solution
Produce Evidence for Security Aspects of the Solution
Develop Assurance Case for Acceptable Security
Demonstrate Assurance Case Is Satisfied
SYSTEM SECURITY ANALYSES
CONCEPTS, PRINCIPLES, MEANS, METHODS, PROCESSES, PRACTICES, TOOLS, TECHNIQUES
Closed Loop Feedback, Variances, Change, and Continuous Improvement

Figure 3: NIST 800-160 systems security engineering framework

maturity of an organisation's cyber security programme, resources and support, along with the availability of an ICS cyber security expert within the organisation, its ICS vendors or ICS service providers.

Figure 4 illustrates a microreactor's general system categories, organised by sophistication, that are involved in controlling and operating the microreactor. At the highest level are the reactor–operator human–system interfaces and manual controls. Below that level is the autonomous or semi-autonomous control system. At the lowest level are sensors, actuators and data transmitters. Such a hierarchical architecture blends well with a multilayer segmentation of networks to enhance safety through defence-in-depth. A segmented network can also allow implementation of single-directional communication between networks to isolate critical aspects of control and data acquisition systems from cyberattacks.

A functional view of a system can be assessed for vulnerability to cyberattack. Cyber threats originate from two general threat areas: external and internal environments. External threats emerge from a source outside of the physical area of the nuclear power plant, usually involving a remote attack from an online source to an online component of the plant. These include embedded malware in a supply chain component or may be introduced into a plant system on-site by an external service provider.

Internal threats emerge from inside the nuclear power plant and can be accidental or intentional. Accidental internal attacks are often caused by a piece of malware inadvertently being introduced from a device (eg a thumb drive) by an employee, as files on the device contain hidden malware. Intentional internal attacks originate from an employee choosing to introduce malicious code into the nuclear power plant. When examining a functional view of the reactor system's cyber security relevant components, each component should be evaluated for the types of threat to which it is vulnerable.

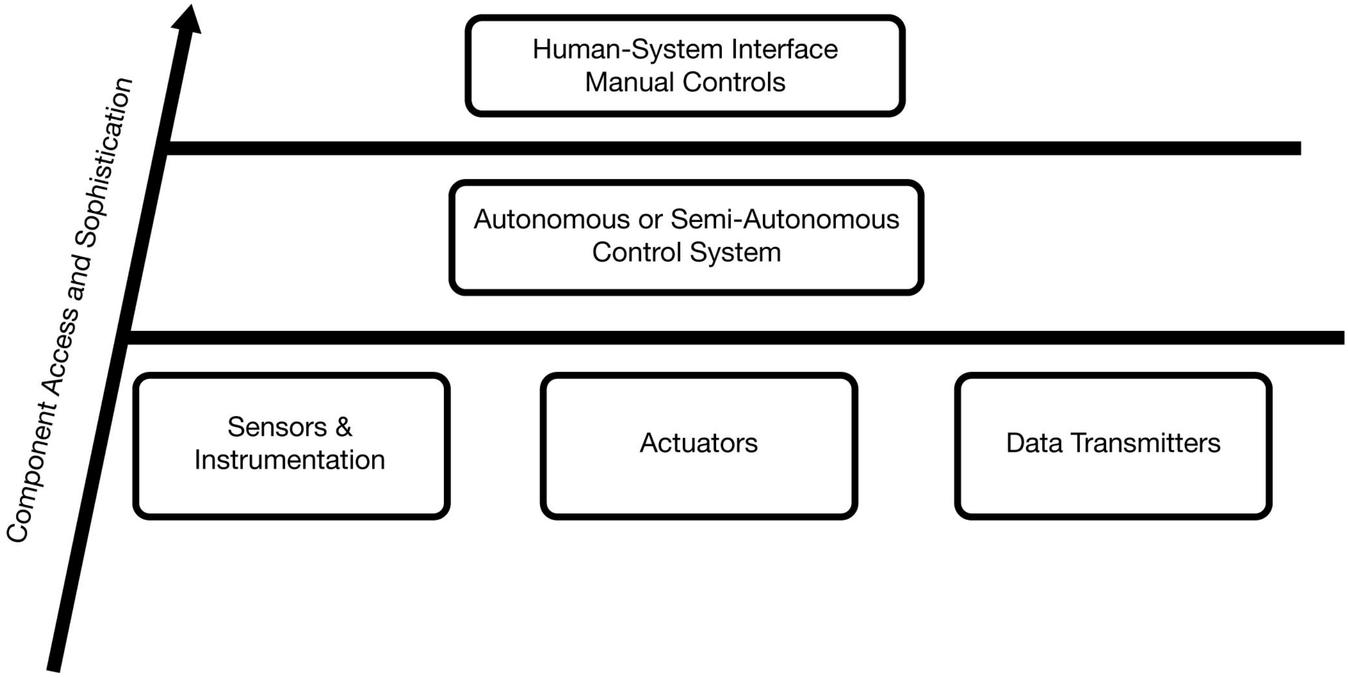


Figure 4: Hierarchical framework of the general system categories involved in controlling and operating a microreactor, organised by their sophistication into hierarchical levels

The supply chain for system components, including computers and cyber physical systems, must also be examined. For example, the incorporation of a variable frequency drive pump in the design requires complex investigation and research. Components that should be evaluated range from the design schematics and circuitry to any built-in programming. Even the hardware components on any circuit board could have been manipulated during the manufacturing process to include additional unwanted communications paths or control instructions that could enable a cyberattack at a future date. Software must also be developed in a secure fashion to protect from external manipulation.

After identifying threat types for each component in the reactor control environment, the means and exploitation path of cyber vulnerabilities of each component must be determined. To ascertain this, the communication and connection pathways outlined in the hierarchical framework can be examined. This map of devices and software assists in determining how an attack could propagate, based on whether and how the compromised device or software communicates with other components. This analytic approach, termed 'attack path analysis', will enable cyber security experts to examine the eventualities of a compromise at the top of the hierarchy that attempts to spread downward or, if the compromise occurred at another location, how it might propagate throughout the system. Based on this analysis, cyber security experts may plan preliminary defences that can be integrated into both the reactor and system designs that will help mitigate damage from a cyberattack.

This hierarchical framework and assessment method should be part of microreactor design *ab intitio* to assist in identifying system vulnerabilities and potential vectors for cyberattack. These vulnerabilities and vectors can be further compared to the cyber defences of other industries that have similar vulnerabilities and vectors. These could potentially assist with mitigation strategies. System designers then may be able to integrate similar solutions into microreactor design. Because microreactor designs are still evolving, incorporating a cyber informed approach at the design stage would add robustness and help prevent major changes at a later stage that could lead to more capital expenditure in order to address a vulnerability concern or challenge. Thus, consideration of cyber threats and cyber informed engineering and design approaches are of utmost importance as is the involvement of cyber security experts at the initial design stage and throughout the entire microreactor lifecycle. Future challenges and potential threats are discussed in the following sections, together with lessons learned from other industries.

IDENTIFYING THE THREATS

To properly assess which existing cyber threats could have an impact on microreactor design, examples from related industries were examined. Two primary industries were used for comparison: the chemical and aerospace industries. Both have heavy regulation and low general tolerance for security breaches, like the nuclear energy sector.

The most well-known cyber threats come in the form of malware. Relevant types of malware include viruses, worms, trojans and rootkits.[16,17] These are invasive files or code that can infiltrate a digital system and perform a variety of malicious functions. Viruses commonly enter a digital system through a file or piece of software to which the virus is attached. When the infected software or file is shared to another location, the virus copies itself into that location and attempts to attach itself to other files or pieces of software. Worms infiltrate a drive, replicate themselves and destroy data and files until there is nothing left to destroy on the drive.

The most dangerous and malicious kind of malware is a trojan. Trojans pose as files or software that seem to be legitimate (and are often distributed in the form of a spear phishing e-mail, which is an e-mail sent from a fake address that seems to originate from an authentic authority, such as a government agency or trusted commercial entity). Trojan malware then makes changes to the system's files and operating system, to facilitate infection by additional malware components (multi-stage or modular malware frameworks), or conducts destructive or disruptive actions, such as deletion or ransomware encryption.

The last category of malware considered is a rootkit, which is a type of system attack that leverages a vulnerability in the firmware (the basic input output system or BIOS programming that allows an operating system to function) of a system component. The rootkit establishes a foothold at the very centre of a system or device and can then push changes or modular malware components into the operating system. When a system administrator eradicates malware such as a virus, worm or trojan from the operating system, the rootkit would be able to reinfect the system and maintain the desired presence in a network, which is discussed next.

A common goal of malware is to facilitate interaction by the threat actor of the targeted system. While the initial attack sequence may be automated via a spear phishing e-mail with an attached trojan (for example), advanced cyberattacks targeting critical infrastructure such as the electric grid or nuclear reactors generally have a more established sequence, as shown in Figure 5. The SANS[18] ICS Kill Chain[19] describes the multi-step process advanced threat actors would typically follow in order to achieve their goals within the targeted system. One strategy that these threat actors establish beyond the automated malware infection point is to create an interactive control capability with the targeted system (in cyber security parlance, a remote shell). This remote shell might be created targeting a control station computer, known as a human–machine interface (HMI), or other plant systems. The HMI enables a control room operator to interact with the controlled equipment in a structured manner (whether that be a chemical, electrical or nuclear process). You can imagine what effects an advanced adversary might be able to enact if they were to establish a remote shell to the HMI for a SMR or micro-reactor.

All types of malware present real threats to microreactors, so determining the malware's vector, severity and extent will be essential to constructing a cyber security system that can respond properly to them. Additional social/ethical/economic considerations of ransomware raise important questions for additional study.

Perhaps less obvious than malware or remote access cyber threats is the threat that originates from people who interact with any software, instrumentation or hardware connected to the reactor system. This is why robust address by policy or programming is needed that addresses cyber security aspects, including threat analysis, asset inventory, risk management, vulnerability assessments, patch management, incident response, cyber hygiene, network monitoring, access control, training, etc. An uninformed user may make a system that is theoretically well defended vulnerable to attack. Threats from an uninformed user include failure to ensure network segmentation, failure to patch any or all software with the latest anti-malware protections, inability to recognise phishing attempts and failure to properly install new systems in a way that ensures the best possible security of the whole system.

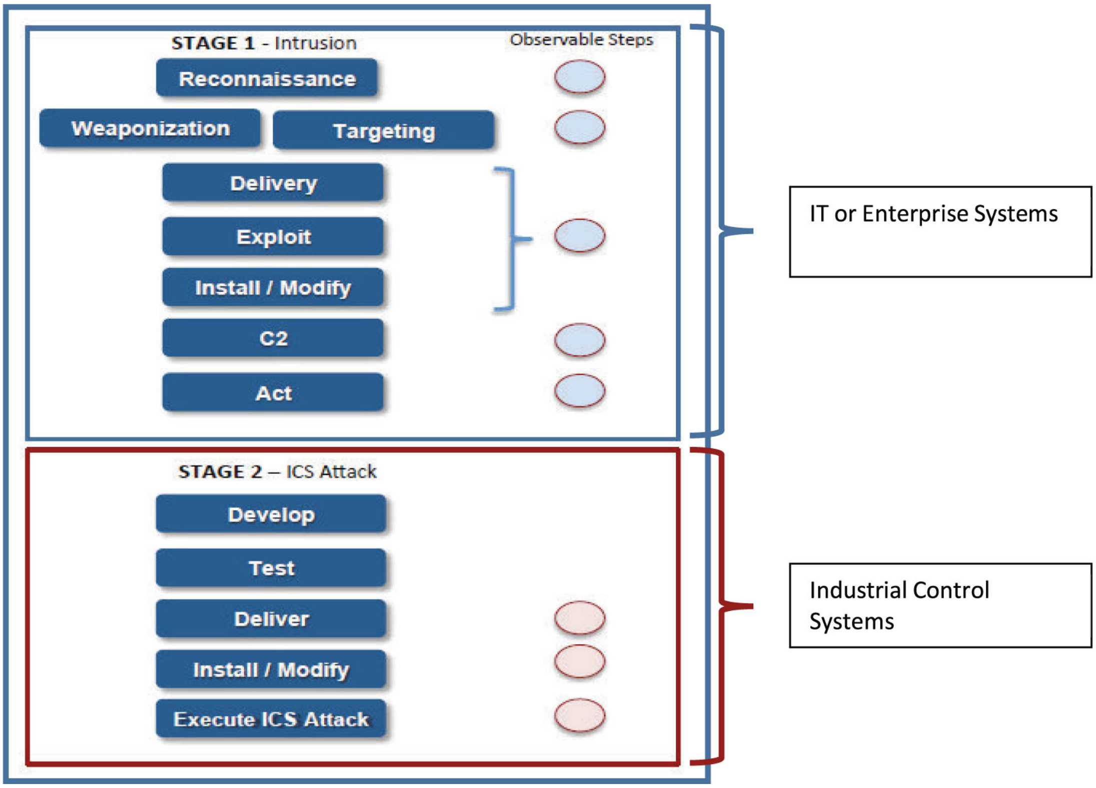


Figure 5: SANS ICS Kill Chain. The stage 1 intrusion phase establishes a foothold in the targeted network, and then, over an extensive period of time, the adversary is able to discover the necessary information to develop and deliver the stage 2 attack

An example of this kind of vector for cyberattack occurred in the chemical industry in 2011. A chemical production company was given a request to produce a chemical batch. The batch turned out poorly, losing the company both its customer and its good reputation. Upon investigation of the equipment used, malware was discovered on one of the actuators controlling the temperature of the batch. This malware interacted with the equipment, causing the system to fail to raise the process temperature to the level required and then failing to alert operators that this was occurring within the control system. The malware infiltrated the system through a cyber security expert who patched the antivirus software for the ICS because the expert's laptop was itself infected with the malware.[20] This is a human originating failure to maintain cyber security, because ensuring any outside systems were not infected with malware prior to allowing those systems to connect to the ICS is a human responsibility.

The above threat is applicable to a microreactor system. A microreactor's primary output (thermal energy) is essential and must meet certain requirements as imposed by the system (the turbine for power production or the needs of an industrial user) in terms of flow rate, temperature and pressure. In some cogeneration cases, the distribution of thermal energy is managed and controlled with distributed self-actuated valves. These controls would typically be autonomous in nature and dependent upon the load. Such systems, remotely operated, present a vulnerability challenge. The valve controls could be compromised in a manner similar to the previously cited example.

THREAT CLASSIFICATION AND TYPES OF THREAT

Cyber threats will be classified as external or internal — or both. Such categories assist in creating the functional framework for cyber security, as discussed in the previous section. Understanding the origination points for threats is essential to maintaining effective cyber security. Organising the threats by vector and then addressing them will allow cyber security experts to determine the necessary protections that should inoculate the nuclear power plant system and anticipate any challenges that may be presented by threats that have multiple vectors of attack.

It is important to note that these threats often work in tandem with another, particularly malware and remote access threats. After 2015, the threat landscape for ICS moved away from the exclusive use of novel hacking tools and codes, such as malware. Instead, cyber threat actors utilise a technique called 'living off the land'. Initially, the attacker enters the system by fraudulent means that seem legitimate to the system, much like a remote access threat. Then, the attacker spends an extended period (sometimes months or years) gathering information and the required credentials to gain access to the areas of the ICS that are critical to their attack plan. Finally, when the attacker is ready, they would insert the custom-designed malware that is equipped with tools to execute a very fast set of commands to disrupt, destroy or harm the ICS. This attack technique is very hard to detect initially, and the attack itself is nearly impossible to stop once it is executed. An example of this attack is the CRASHOVERRIDE attack.[21]

CRASHOVERRIDE (also known as Industroyer) is particularly relevant as it was a cyberattack on a regional electric power transmission substation in December 2016. The attack infiltrated the network of the substation and caused the grid to crash and remain down for several minutes. The potential consequences of this kind of attack for the nuclear industry have already been observed. On 14th August, 2003, a software bug in conjunction with power lines touching tree branches caused a regional blackout resulting in 55m customers losing power and seven nuclear reactors tripping because of the power transient.[22]

ASSESSING VULNERABILITIES: DEFINING THE SYSTEM, ASSUMPTIONS AND METHODOLOGY

Microreactor designs include a variety of different reactor types, with similar desired electrical power and thermal outputs. Design types include heat-pipe, gas-cooled, pressurised water, molten salt and liquid metal-cooled reactors. With this variety comes a diverse set of required instrumentation and control systems that must be compatible with each system but will likely not be universal to every design. A simplified diagram of this is shown in Figure 6.

The framework established in the diagram will be the basis for the vulnerability assessment.

Assumptions about the system are:

- The control system is autonomous or semi-autonomous;
- All wireless connections use Wi-Fi and are connected to the Internet;
- The reactor has some human–system interface (HSI) through which the reactor operator may patch the system, manually control the reactor and view reactor performance data;
- The use of data transmitters is implied to send information between connections.

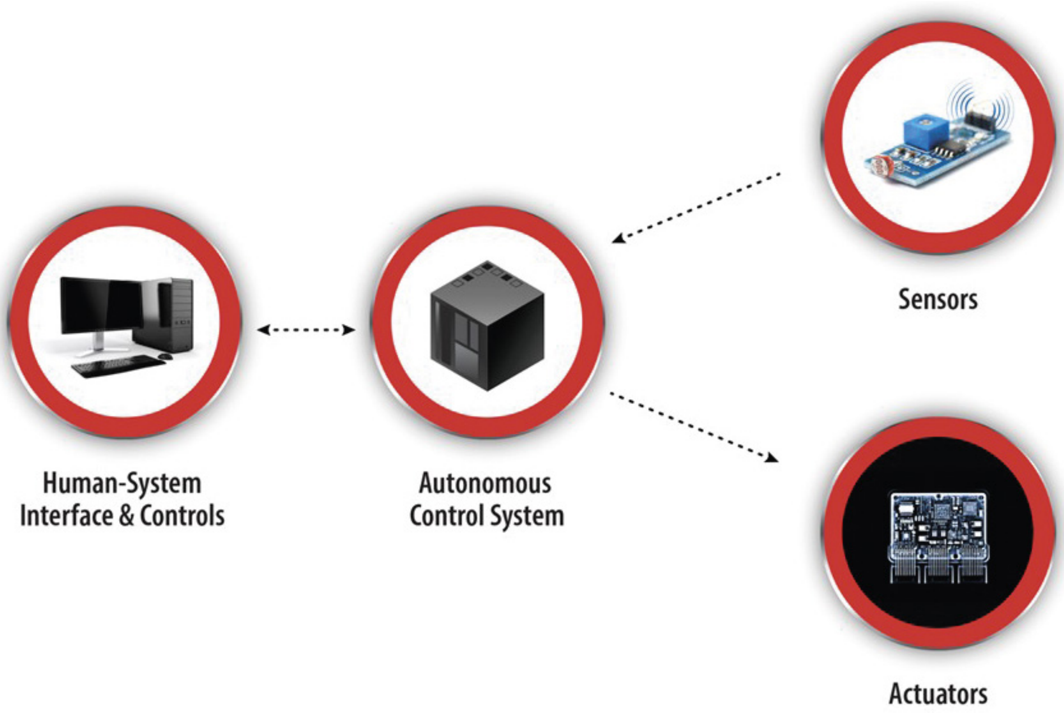


Figure 6: Schematic visualising the instrumentation and control system. The dotted lines represent wireless connections between the components. The arrows denote communication pathways

The methodology to be applied is a static one. Static methodologies identify individual components of the system, detail the vectors through which a cyberattack may invade that component, and design protections based on that analysis. The HSI, for example, is vulnerable to all five vectors of attack, namely wired, wireless, removable media, physical and supply chain. The interface is designed specifically to allow humans to interact directly with the system through this component and includes patching. Any sort of error characterised as a human error threat is possible, leaving the interface vulnerable to the other two vectors of attack. Beyond this, the system may suffer an internal attack should a device with malware be connected to it.

Semi- and autonomous control systems (ACSs) are vulnerable to human error, malware infiltration and remote access. Any failure of the human support to adhere to proper cyber security hygiene (ie best practices to improve cyber security) may result in some flaw that malware can exploit. Even without human error, an ACS that is wirelessly connected to most components in the system will be vulnerable to remote access or backdoor threats. Malware infection in a component either above or below the ACS may result in the infection spreading to the ACS due to its high level of interconnectivity.

Another consideration includes the actuator elements that would be most vulnerable to malware infections. Because the sole function of these components is to receive commands from the control system and make appropriate changes to components in the reactor system, they represent a single avenue to propagate a downward-moving connection. An actuator would suffer significantly from malware interference with its ability to properly receive and issue commands. In addition, sensors may be vulnerable to remote access and malware attacks. These components are well connected, and the information that they provide to the control system is essential to safe operations. Remotely accessing and monitoring that information would be of critical interest to a threat actor. Actuator motors are simple machines that receive a given command input and execute it. The primary threat to this component is malware infecting software in the machine and causing it to behave improperly — for example, the temperature control actuators in the chemical industry case study prevented proper heating of a chemical batch.[23]

Once the microreactor's instrumentation and control system cyber vulnerabilities have been assessed, it is also important to analyse the defence by which similar industries prevent cyber security problems within their ICS to further add defence-in-depth mitigation strategies, resilience and robustness for microreactor control infrastructure.

POTENTIAL CYBER SECURITY SOLUTIONS

Wireless connections that use the Internet and digital systems to communicate are the primary means by which a cyber oriented adversary would move through a system. The nuclear industry already has made provisions for this vulnerability and provided some solutions for it.[24] To secure wireless connections and prevent remote access and backdoor threats, a commercial grade or stronger encryption scheme can be placed on the wireless network. The use of wireless signal shielding and highly directional signals are also proposed. These protective methods control the spread of the wireless signal, preventing or mitigating how much attack surface is exposed for exploitation beyond physical boundaries.

Another method suggested by the International Atomic Energy Agency (IAEA) is segmenting these connections.[25] Segmented wireless connections between two components allow communication only between those two components. Should a cyber threat enter the system in any location, it can only spread to those unsegmented components, instead of having access to a variety of interconnected components. The National Aeronautics and Space Administration's (NASA) inspector general recommended the use of this technique at the Jet Propulsion Laboratory to protect against future cyberattacks.[26]

Integrating one-way connections would ensure higher security for components that have control functions, such as the automated control system.[27] If the system were only allowed to issue commands, but not receive signals, it would not be vulnerable to upward threat movement. It is likely, however, that for any control system, there will need to be exceptions to one-way connections. For example, the system relies on readings from instruments in the reactor to make informed decisions that allow the control system to maintain reactor health and safety and enable online monitoring of the reactor. Thus, it needs some way to receive information from those instruments. In these situations, IAEA proposes to use controlled signal messages that are highly encrypted and only meant to communicate between the two devices of interest.

Automated intrusion-detection systems generally require manual human monitoring to ensure against exploitation. Advanced malware is equipped with tools to hide from automated intrusion-detection systems more effectively, but the presence of that malware or unauthorised external access may still be detectible by human observation. This also applies to checking system logs for unusual behaviours, particularly ICS commands issued that are not part of standard operating procedures.[28] Establishing a formal, documented threat-hunting process is an effective way to integrate human involvement in detecting malware and other intrusions in the system.[29]

Anti-malware software must be updated regularly, and software patches must be investigated after installation to make sure that they were installed properly. This cyber security measure is good for protecting against general threats, but additional measures are needed to engineer a system resilient to cyberattack. Running routine tests for updates and using a digital twin framework to perform these checks could further enhance system cyber-readiness before the updates are seen by the main control framework.

Establishing a robust and diverse network of security checks and gates that allow only authorised users to enter the system will assist in preventing malware intrusions and mitigating damage, should one occur, by containing it. This method is particularly applicable to securing any human control commands to the system. The operator can authorise commands using forms of multifactor authentication that make it more challenging for malware to issue fraudulent commands without the physical component required for authorisation.[30] While this method is generally effective, in the case of an advanced persistent threat attack, it is possible for the attacker to spend time obtaining the credentials required to infiltrate the system remotely, regardless of advanced authentication measures.

Ultimately, humans are accountable for ensuring the cyber security of the system, and their ability to observe proper protocols and good cyber security habits affects how secure the system is. Human error is the most addressed cyber-related threat in incident reports from both the chemical and aerospace industries. To combat the vulnerabilities presented by human error, it is best to create a culture of cyber security and mindfulness. NASA is doing this at its Jet Propulsion Laboratory by creating a plan for institutional IT knowledge and requiring dissemination of lessons learned from cyberattacks.[31] A human who is informed about the safest ways to perform duties pertaining to digital systems is less likely to make a costly mistake.

UNADDRESSED THREATS

Many actions taken within the critical infrastructure sector and industry to respond to the current cyber threat landscape only partially address the problems presented by state-of-the-art cyberattacks perpetrated by advanced persistent threats (APT).[32] They are primarily concerned with reacting to ICS attacks after they have occurred. The problem with this is that some cyberattack strategies are slowly implemented and carefully planned, so there will be very little or no time for an effective defence response once the attack is launched. This is all possible because of a lack of visibility in and supervision over digital IT systems and ICSs. This is true for many industries. Living-off-the-land threats can only be effectively detected through careful, sustained monitoring of the native processes and techniques used by digital systems. The key to noticing a threat like this is examining digital systems for behaviours that are out of the ordinary despite their authenticated appearance. Detecting this behaviour may stop a cyberattack in its early stages, before it can be executed in a fashion that is difficult to stop and compromises the safety of the reactor. It is important to note, however, that placing all focus on IT components is not sufficient; attackers may still be able to bypass this system into ICS controls before being detected.[33]

The most challenging aspect of anticipating future threats is that the framework for thinking about how threats operate can only be based on what is known. Cyber threats are ever evolving, and the methods that are most effective today for addressing them may be irrelevant tomorrow. A new method for keeping pace with the changing threat would help greatly with the effort to maintain a capable cyber security framework for microreactors.

RECOMMENDATIONS AND POTENTIAL SOLUTIONS

To develop effective cyber security strategies for an evolving threat, advances in technology may work to the advantage of cyber security efforts. One prospective solution is the concept of an autonomous cyber defence system that works to seek out vulnerabilities in an IT component or ICS, essentially hacking them and exploring any vulnerabilities it can exploit.[34] In essence, the autonomous system works to beat prospective hackers at finding weaknesses in a system and creating a proactive form of defence. The system would then report the weaknesses and start finding ways to patch out vulnerabilities. There will be challenges in developing an autonomous system that is sophisticated enough to do this, and it may require specialised programming to work with novel ICS; however, it is not out of the realm of possibility. The Defense Advanced Research Projects Agency hosted the Cyber Grand Challenge on 4th August, 2016, in which teams competed to develop just such an autonomous cyber defence system.[35]

While the above technology does not yet exist in useable form; nonetheless, the same concept of proactive defence is possible now. Instead of using autonomous machine learning (ML) to perform the task, a team of hacking and cyber security experts can be tasked to analyse systems in a similar way. If microreactor plant owners desire, these teams could be maintained for the lifetime of the reactor to continue to test current patches for the information technology and ICS and provide feedback. By testing the threat in a digital twin framework and observing the vulnerabilities and consequences, proper mitigation steps and strategies could be implemented.

The use of digital twins in industry is relatively new; however, some techniques have been developed to help protect digital twins from cyber intrusion. One such technique is called data and software transformation. It simultaneously merges functions to break up modular codes and then entangles the transformed data with the altered control flow of the software. This approach would significantly increase the complexity of the processed software programming (or binary) and would make any attempts at reverse engineering the programme difficult, if not impossible.[36] In essence, data and software transformation scrambles all communications to and from the digital twin. This defends the system in two ways: 1) it makes it significantly harder for attackers to understand how the system functions because they cannot understand how it communicates; and 2) it makes modified commands issued from an external source stand out because they are incompatible with the system's communication protocol.

If autonomously controlled microreactors are dependent on digital twins, it will be important to properly protect any of the implementing software from being infiltrated. Should the software become compromised by hackers, a cyber criminal's plan of attack on a microreactor would accelerate. Protecting the digital twin and microreactor IT and ICS will be made easier if the software and systems are designed to allow the most visibility and clarity to all processes that occur within them. It is not always viable for every component in an ICS to be easily visible; however, the more components that can be easily observed in the software system, the less likely it is that a cyberattack will be able to remain hidden within it. Another tool that may be useful for protecting digital twins is Whitebox cryptography and the use of hardened application programming interfaces. These tools lock the use and access of the digital twin and give access only to specified devices. Should the digital twinning software or its data be accessed from an unauthorised device, the device will not be able to do anything with the twin or the data it generates because the device does not have the required permissions.

It is important to note that much of the recent development in the artificial intelligence (AI)/ML driven autonomous control systems or digital twin technologies is based on using existing off-the-shelf algorithms developed for non-nuclear applications. Vulnerability of such solutions to infiltrations is relatively much higher compared to a scenario in which such technologies are researched, modified to be more secure, developed and implemented as a completely independent solution for each reactor design. Any approach, however, will have potential vulnerabilities that need to be evaluated in a risk framework. Significant progress has been made and research is underway to secure the online monitoring systems that are part of ICSs from cyber threats. Some of the potential solutions that are being explored in this field focus on setting up alerting mechanisms for manipulation of electromechanical devices.

Other options include multilayer network segmentation, using one-way communication devices such as diodes wherever possible, separation of physical and logical networks, etc. The use of fit-for-purpose isolated subnets and egress packet inspection is already being applied in the development of digital twins for reactor design. Another option that is increasingly being considered focuses on integrating plant-specific information on reactor design into any control system architecture to minimise portability of malware and bots. Integration of reactor design-specific knowledge into such autonomous systems and digital twins will reduce the portability of malware and bots. It would require cybersecurity experts to work very closely with reactor designers and vice versa.

Still another aspect that is critical to the development of resilient digital twins and autonomous control systems is the concept of modularisation. A modular design and implementation would bring the transparency and clarity needed to improve cyber resiliency. For example, modularisation would lead to a digital twin hub instead of a single digital twin because of the nature of the technology profile. The hub would consist of separate digital twins for diagnosis, prognosis and strategy assessment (see Figure 6). In fact, it might be more appropriate to implement the initial development and implementations of automated control systems to be semi-autonomous (see Figure 7). The system would help in autonomous control during normal operation but would require operator intervention for actions in an emergency or accident conditions. Such a system can provide the operator with a ranked list of potential options, but let the operator select the final action. A greater degree of modularisation would include many different potential algorithms for ML-based assessments wherein different approaches are used to address different scenarios of operations and emergencies.

Another key element that has received relatively little attention relates to the concept of 'discrepancy assessment'. Autonomous systems can exhibit discrepancy in their predictions during two stages: 1) training of the AI/ML solutions using knowledge base, simulation data and monitored data; and 2) actual operation. It is extremely important to develop a strong concept of discrepancy assessment at both stages by using a multi-attribute, multiparameter model, thereby eliminating the dependence on a single or a few corrupted streams of information. The concept would need to be integrated at the design stage of the plant so that one would

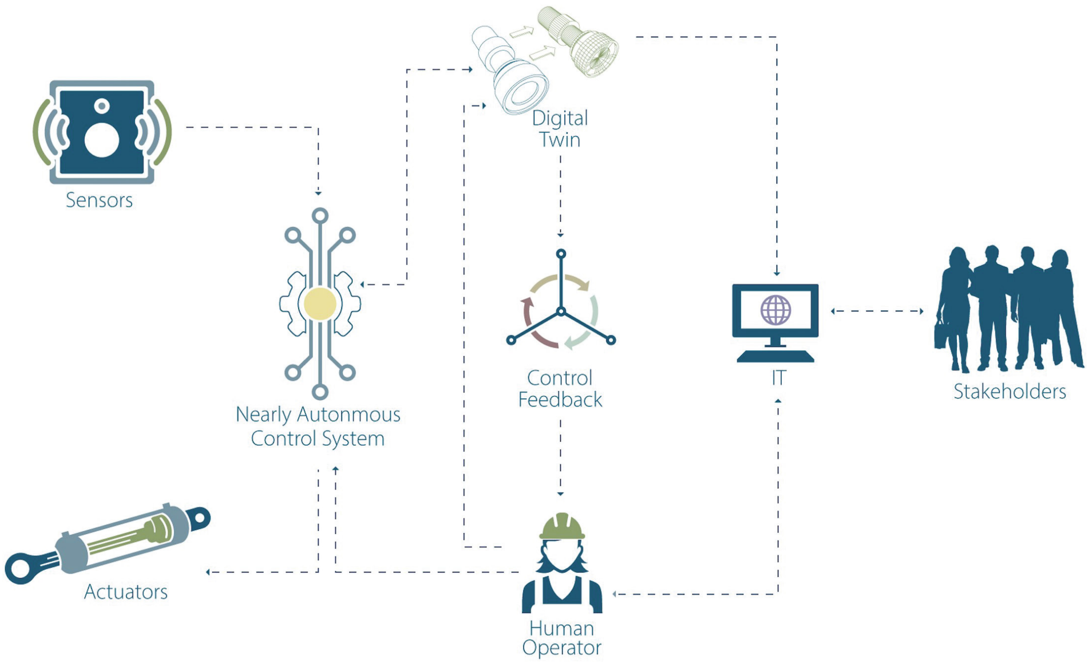


Figure 7: Semi-/nearly autonomous assessment hub

be able to assess the degree of discrepancy in data or predictions that are consistent with various scenarios of operating and emergency conditions. Such a knowledge base would be able to provide additional barriers on any potential deviation of data and predicted control actions beyond what is estimated from the knowledge base.

The concept of discrepancy assessment would need to be integrated into real-time management of emergency scenarios. Once a control action is undertaken by an operator or an autonomous control system, the state of the plant could be tracked at a regular time interval (for example, every few seconds) to determine whether the plant is following the response as was predicted by the autonomous system following the safety action taken by the operator and control system. As the discrepancy between the actual versus predicted states increases, the operators would be able to undertake corrective actions or even scram the plant. For digital twins, the concept of 'as-built' instead of 'as-designed' models for training the ML algorithms can provide added security, ensuring data integrity. Modular architecture for the digital twins that is implemented as a digital hub with independent digital twins for diagnosis, prognosis and strategy planning can allow the necessary heterogeneity needed to provide defence in depth (see Figure 8).

DOMAINS FOR COOPERATIVE ENGAGEMENT

Microreactor designs are unique to their manufacturers; therefore, the vulnerability of a microreactor plant to cyberattack depends on the specific design of the reactor being attacked. Factors that play a role in this are physical design and organisation of the plant, the computer systems used, the means of communication among internal systems and with outside sources, and the efficacy of the safety-based design features' response to successful cyber incidents.

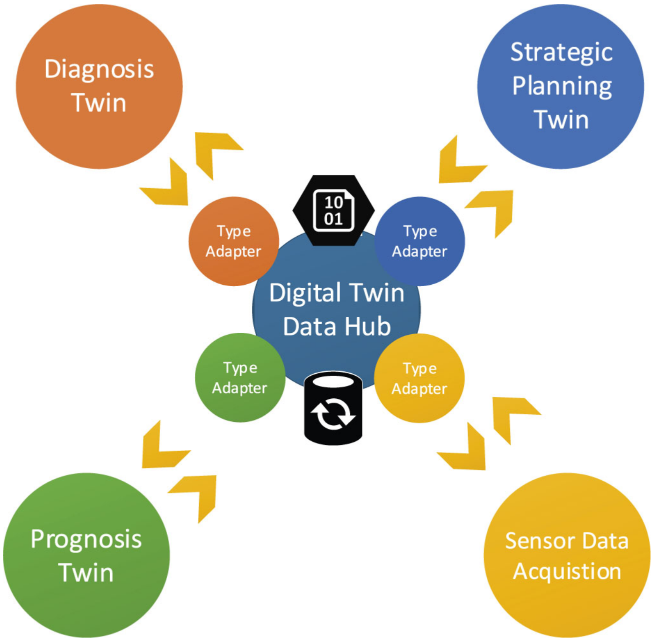


Figure 8: Modular digital twin architecture

Microreactor power plant systems must carefully account for an inventory of the potential vectors for cyberattack and the consequence of a successful attack through each of these vectors. Developing models and decision-making processes that can assess consequences — considering design, monitors and safety aspects — is critical.[37] The framework established in this paper is a step. The relevant plants should then implement cyber security measures based on the framework. Several ways to do this include increasing the visibility of ICS and IT systems, restricting network access to only those authorised to engage with it in specific locations, maintaining high levels of information security and monitoring the ICS and IT systems for abnormal behaviours so that the microreactor stays within its operating envelope.[38]

Industries, both nationally and internationally, may collaborate with one another and their government authorities to seek out and share information on the changes in the cyber threat landscape. This exchange of information will help microreactor plants adapt to the new threats and assess the impact of a successful attack of the newly discovered threat. For cooperation between industry and government authorities, procedures should be established to share information safely and reliably and a framework should also be developed for the time and means to do so.[39] This can be of value as microreactor development focuses on international markets.

CONCLUSIONS

Microreactors have potential to support energy systems due to reactor design characteristics: small, mobile, capable of being placed in remote locations and semi-autonomously/autonomously controlled. Automated control systems that use the Internet and digital components to communicate between reactor instrumentation and the control system create a potential for new threats to nuclear systems through cyberattacks. Cyber security measures need to be developed for microreactor systems. The current threat profile and methodology is already challenging to address, with stealth techniques such as living off the land being used for related autonomous or highly automated ICS.

There is not a single facile method for creating effective cybersecurity for a microreactor; however, the framework discussed and potential solutions provide a basis for refinement and future work. Possessing a detailed understanding of every component and connection type in the instrumentation and control system will make it easier to identify the locus of vulnerabilities in the system and how an attack may spread. Cyber security measures can then be developed around those weaknesses and known pathways.

Using a cyber informed design approach for microreactors is a path that is strongly encouraged for future deployment to make sure these reactors are robust and resilient to cyberattacks. The concept of semi- autonomous control systems, instead of a fully autonomous control system, appears to be quite a powerful concept. It could entail human intervention for any occurrences that fall under abnormal operating conditions but allow autonomous operation during normal conditions. Semi-autonomous use can also provide added safety by allowing only one-way communication between the external world and the digital twin. For digital twins, the concept of as-built, instead of as-designed, models for training the ML algorithms can provide added security, ensuring data integrity. Heterogeneous architecture is a power concept that has been used to provide added security. This can be achieved by implementing digital twins as a 'hub' with different twins for diagnosis, prognosis and strategy planning, each with an independent architecture.

While inbuilt cyber security is important, it is more important that those who are responsible for checking and monitoring information technologies and ICS are up to date on state-of-the-art cyberattack techniques and are vigilant in observing good cyber security habits and hygiene. Ultimately, a cyberattack on a microreactor may succeed by finding a way around inbuilt security measures. It is up to the cyber security defenders to detect anomalous behaviour in IT and ICSs and effectively address any successful intrusions. Integrating high levels of monitoring for every part of these systems will be essential for defenders performing this task. This monitoring must be able to expand to encompass new technologies such as digital twinning. Through integrating visibility and maintaining awareness of the nature of existing cyber threats, cyber security experts will establish security for microreactors that is robust, diverse and proactive.

A successful cyberattack against any kind of nuclear facility would have substantial consequences (societal and economic impacts) and would undermine a community's confidence in the owner and operator's ability to run the plant in a safe and secure manner. This would also hamper any potential growth nationwide or globally. With international collaboration, the US nuclear industry can maintain the peaceful use of nuclear energy and bolster trust and relations with those collaborators. In the execution of this effort, a framework for preventing cyberattacks on nuclear facilities should be created and innovated based on a methodical review and analysis of lessons learned from attacks on other industries. Learning about the mitigation and execution strategies used by other industries will enable a more robust platform for cyber security moving forward.

References

1. A mobile reactor is generally intended to be moved with some regularity between operational periods, whereas a 'transportable' reactor is intended to be moved to its intended site generally for its operational life and then is removed once operation is completed.
2. Ramuhalli, P. and Cetiner, S. (2019), 'Concepts for Autonomous Operation of Microreactors', Oakridge National Laboratory, pp. 1–21.
3. United States Nuclear Regulatory Commission (2019), 'Backgrounder on Cyber Security', available at https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cybersecurity-bg.html (accessed 10th July, 2020).
4. United States Nuclear Regulatory Commission (January 2010), 'Cyber Security Programs for Nuclear Facilities', Regulation Guide 5.71, available at https://www.nrc.gov/docs/ML0903/ML090340159.pdf (accessed 10th July, 2020).
5. *Ibid.*, note 5.
6. Department of Homeland Security (DHS) (2015), 'Nuclear Sector Cyber Security Framework Implementation Guidance for U.S. Nuclear Power Reactors', available at https://www.cisa.gov/sites/default/files/publications/nuclear-cybersecurity-framework-implementation-guide-2015-508.pdf (accessed 10th July, 2020).
7. Eke, P. (September 2019), 'Cybersecurity Updates

and Audits, Lessons Learned Report', FERC, Washington DC, available at https://www.nrc.gov/docs/ML1927/ML19270D583.pdf (accessed 10th July, 2020).

8. *Ibid*., note 7.
9. Fisher, R., Wood. J., Porod, C. and Greco, L. (2020), 'Evaluating cyber risk reporting in US financial reports', *Cyber Security: A Peer-Reviewed Journal*, Vol. 3, No. 3, pp. 1–12.
10. Cyber Emergency Response Team (December 2013), 'ICS-CERT Monitor Incident Response Activity', ICS-CERT Monitor, Department of Homeland Security, available at https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf (accessed 10th July, 2020).
11. International Atomic Energy Agency (2011), 'Computer Security at Nuclear Facilities', *Computer Security at Nuclear Facilities*, available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf (accessed 10th July, 2020).
12. Cyber Emergency Response Team (2011), 'ICS-CERT Incident Response Summary Report', Department of Homeland Security, pp. 1–17.
13. Allen, J. H. (204), 'Building a Practical Framework for Enterprise-Wide Security Management', Carnegie Mellon Software Engineering Institute, p. 5, available at https://resources.sei.cmu.edu/asset_files/Presentation/2004_017_001_51841.pdf (accessed 10th July, 2020).
14. *Ibid*., note 13.
15. Ross, R., McEvilley, M. and Carrier Oren, J. (November 2016), 'Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems', NIST Special Publication 800-160, Vol. 1, p. 21, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf (accessed 10th July, 2020).
16. National Aeronautics and Space Administration, Office of the Inspector General, Office of Audits (2019), 'Cybersecurity Management and Oversight at The Jet Propulsion Laboratory', available at https://oig.nasa.gov/docs/IG-19-022.pdf (accessed 10th July, 2020).
17. Malwaretruth (2020), 'A List of Malware Types', available at https://www.malwaretruth.com/the-list-of-malware-types/ (accessed 10th July, 2020).
18. Note that the Stage 1 Cyber Kill Chain was developed by Lockheed Martin and enhanced by SANS ICS researchers to enumerate Stage 2 actions.
19. Assante, M. and Lee, R. M. (October 2015), 'The Industrial Control System Cyber Kill Chain', p. 16, available at https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297, (accessed 10th July, 2020).
20. Chemical Sector Coordinating Council (CSCC) and Department of Homeland Security (November 2020), 'Securing Industrial Control Systems Roadmap Awareness Initiative—Making the Business Case, Department of Homeland Security', available at https://www.cisa.gov/sites/default/files/publications/Business-Case-Testimonial-Nov-2012-508_0.pdf (accessed 10th July, 2020).
21. Slowick, J. (2019), 'Evolution of ICS Attacks and Prospects for Future Disruptive Events', Dragos Inc., available at https://www.dragos.com/wp-content/uploads/Evolution-of-ICS-Attacks-and-the-Prospects-for-Future-Disruptive-Events-Joseph-Slowik-1.pdf (accessed 10th July, 2020).
22. History (November 2009), 'Blackout Hits Northeast United States', available at https://www.history.com/this-day-in-history/blackout-hits-northeast-united-states (accessed 10th July, 2020).
23. *Ibid*., note 18.
24. Korsah, K., Holocomb, D. E., Muhlheim, M. D., Mullens, J. A., Loebl, A., Bobrek, M., Howlader, M. K., Killough, S, M., Moore, M. R., Ewing, P. D., Sharpe, M., Shourbaji, A. A., Cetiner, S. M., Wilson Jr., T. L. and Kisner, R. A. (October 2009), 'Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update', Nuclear Regulatory Commission, available at https://www.nrc.gov/docs/ML0929/ML092950511.pdf (accessed 10th July, 2020).
25. *Ibid*., note 10.
26. *Ibid*., note 15.
27. Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A. P., Watkins, L., Robinson, W. H. and Alexis, W. (December 2016), 'Securing Commercial WiFi Based UAVs from Common Security Attacks', Securing Commercial WiFi-Based UAVs from Common Security Attacks—IEEE Conference Publication, IEEE, available at https://ieeexplore.ieee.org/abstract/document/7795496/authors#authors (accessed 10th July, 2020).
28. *Ibid*., note 19.
29. *Ibid*., note 19.
30. *Ibid*., note 10.
31. *Ibid*., note 15.
32. Advanced persistent threat: An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (eg cyber, physical and deception).
33. *Ibid*., note 21.
34. McDonald, S. (October 2016), 'What Could Possibly Save Us from Cyber Attacks? Autonomous Computers', NASA, available at https://www.nasa.gov/feature/langley/what-could-possibly-save-us-from-cyberattacks-better-computers-of-course (accessed 10th July, 2020).
35. Fraze, D. (n.d.), 'Cyber Grand Challenge(CGC) (Archived)', Defense Advanced Research Projects Agency, available at https://www.darpa.mil/program/cyber-grand-challenge (accessed 26th January, 2021).
36. Hearn, M. and Rix, S. (November 2019), 'Cybersecurity Considerations for Digital Twin Implementations', *Industrial Internet Consortium Journal of Innovation*, available at https://www.iiconsortium.org/news/joi-articles/2019-November-JoI-Cybersecurity-

Considerations-for-Digital-Twin-Implementations.pdf (accessed 10th July, 2020).

37. Shea, T., Gaycken, S. and Martellini, M. (October 2013), 'Cybersecurity for Nuclear Power Plants', *Cyber Security*, SpringerBriefs in Computer Science, pp. 25–35.

38. *Ibid*., note 37.

39. *Ibid*., note 25.