Cyber Security
and Privacy
Research Institute

THE GEORGE WASHINGTON UNIVERSITY

Assessment of Cyber Security Challenges in Nuclear Power Plants
Security Incidents, Threats, and Initiatives

Rahat Masood*

August 15, 2016
Report GW-CSPRI-2016-03

*Current Affiliation: National University of Sciences & Technology (NUST),
School of Electrical Engineering &Computer Sciences (SEECS),
H-12 Islamabad, Pakistan.
Email: rahat.masood@seecs.edu.pk

Support for this work was provided by the Civilian Research & Development Foundation (CRDF) Global under the Nonproliferation studies scholarship program, and the Cyber Security and Privacy Research Institute (CSPRI) of the George Washington University (GWU). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the CRDF, GWU, or CSPRI.

Assessment of Cyber Security Challenges in Nuclear Power Plants
Security Incidents, Threats, and Initiatives

Rahat Masood

Abstract

Nuclear power plants play an important role in electricity production for many countries. They supply power to industries, centers, government facilities, and residential areas. Yet, upon review, several cases reveal that even a small-scale attack on a nuclear power plant could lead to catastrophic consequences for a country's citizens, economy, infrastructure, and security. In recent years, there has been increased attention to the area of nuclear cybersecurity due to attacks or incidents designed to disrupt NPP operations. In spite of this rise of nuclear-related cyber attacks, the security for NPPs has not been holistically addressed. Literature review reveals the lack of a comprehensive information security framework to secure nuclear power plants from internal and external threats.

This research highlights the significance of performing security assessments within NPPs as it relates to cyber defense. The contribution of this paper is twofold. First, it presents a detailed review of cyber challenges and security incidents that have occurred within NPPs, followed by a discussion on the initiatives taken by governments and regulatory bodies in mitigating such security challenges. Contextual background information on Critical Infrastructure Protection, nuclear power plants and information security risk management has been supplied to aid reader understanding. Additionally, this research posits that any kind of cyber incident on nuclear infrastructure may lead to catastrophic results, from which recovery may be impossible. Therefore, there is a significant need to perform detailed threat and vulnerability assessments that address either stand-alone attacks or coordinated attacks against the use of computer systems on NPPs.

Following this discussion, a threat modelling is presented using an established methodology, which identifies possible threats to, vulnerabilities in, and adversaries of a generic Instrumentation and Control (I&C) system of a NPP by considering its characteristics and architecture. The analysis reveals that NPPs are not fully armed against cyber attacks and identifies a significant need to conduct security assessments such as the Information Security Risk Assessment, which would provide comprehensive and reliable risk analysis functionality to NPPs.

Table of Contents

1. Introduction

Nuclear power plants (NPPs) are considered to be the major sources of electricity and power for many countries [1]. However, though nuclear energy provides countless benefits, NPPs pose the risk of potential disaster if left unattended or unguarded. The United States (U.S.), Russia, United Kingdom (UK), South Korea, and China have raised concerns about securing their facilities from catastrophic incidents. The Chernobyl incident of 1986 [2] and Fukushima Daiichi nuclear disaster of 2011 [3, 46] have also shown that a disastrous situation can occur when the proper safety and security protocols are not followed. These events are indications of weak security and safety controls, resulting in reputation damage, loss of trust, reduction in shareholder value, financial fallout, and loss of human lives.

The security of the digital systems used in NPPs has been studied in recent years. A surge in the increased use of information and communication devices, integration of digital control system devices, and interconnectedness among systems in NPPs has made cyber threats of increased interest to the nuclear and cybersecurity community. A recent analysis by Chatham House on the security of civil nuclear facilities revealed that the nuclear industry is still struggling to overcome cyber threats [4]. This is partly due to the nuclear sector's late adoption of digital systems compared to other sectors. There have been a number of cyber attacks and incidents that indicate the possibility of severe risks associated with NPPs [9]. One such example is the Stuxnet worm. This malicious program makes it possible to interfere with software and physical equipment deployed in nuclear facilities [5].

One practice that might be hurting the nuclear industry is its increased use of commercial "off-the-shelf" software. This type of software does not provide an adequate level of protection from external threats and is often viewed as a direct way of penetrating a facility network. The use of subpar software, combined with executive-level unawareness of security risks, creates an easy route for an attacker to exploit assets. Management often refers to nuclear facilities as being "air-gapped" – completely isolated from the Internet – meaning that the industry is safe from cyber attacks. This is a misrepresentation. Much commercial software provides internet connectivity via virtual private networks (VPNs) or Intranet. These connections often go unreported and remain neglected while deploying software or setting up temporary internet connections for a project. In addition, nuclear industry regulations previously focused more on physical safety and protection rather than on cybersecurity controls. Therefore, very few developments have been made to reduce cyber risks through standardized control and measures [4]. Hence, all of these factors demand steps to secure a nuclear facility through proper prevention and detection mechanisms.

The looming threats of ionized radiation release, espionage, and sabotage have triggered the development of a vast array of security measures and guidelines designed to prevent catastrophic effects. Specifically, those measures are intended to combat loss of lives, health effects, infrastructure collapse, sensitive information exposure, and economic instability. The Chatham House report strongly suggests going further through the establishment of security frameworks to maintain the momentum of nuclear plants and to prepare for possible upcoming security attacks [4]. The report also recommends the enforcement of standards and best practices to measure the security risks in the nuclear industry, which will eventually help improve not only security, but also understanding of risks at the executive management level.

Industry has proposed various solutions and risk analysis methods to improve the security of NPPs. However, cyber security of NPPs is still considered to be in an early phase of development. While contemporary research has identified the need to protect NPPs from cyber attacks, this information is very limited. It does not provide a comprehensive view on managing security threats. The key problem seems to be the lack of methods and frameworks for identifying threats and incorporating the latest security trends, which can holistically combat the cyber attacks that targets NPPs.

The existing literature on the security of NPPs is very limited. It is largely unstructured, and abstractly covers the security issues of SCADA (supervisory control and data acquisition) systems and critical infrastructures (railway, supply-chain, and transportation) -- with only a few covering nuclear facilities. Moreover, the existing literature focuses on very few security features, such as confidentiality and authorization, and does not holistically cover all security mechanisms and requirements of the nuclear industry.

This work focuses on the development of strong security measures for NPPs by exploring the current challenges, assessing state-of-the-art initiatives, and conducting threat assessments on power plants. The contribution of the paper is twofold: i) a holistic review of the fundamental aspects of nuclear security alongside historical security incidents within NPPs, and ii) threat modelling of a NPP through attack trees to identify security vulnerabilities. Amenaza SecurITree [91] was used for the creation of attack paths and attack trees. The STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) threat model was also used to formally categorize the possible attacks identified using attack trees. The security requirements and threat modelling serve as a motivation for an improved security framework for NPPs.

The remaining sections cover the following: Section 2 provides the background of NPPs. Section 3 discusses cybersecurity in relation to NPPs and offers a historical perspective on cyber incidents. The recorded efforts of industry and governments to improve NPP cybersecurity are discussed in section 4. Section 5 covers threat modelling. The paper concludes in Section 6 with a summary of the main contributions and an outlook on the future of security in NPPs.

2. Relevant Concepts/Background

This section presents contextual information about Critical Infrastructure Protection (CIP) and NPPs to assist the reader’s understanding.

2.1 Critical Infrastructures Protection

Critical infrastructure protection (CIP) is of great concern to developed and developing countries alike. Countries have deployed a number of critical systems for infrastructure sectors including, but not limited to oil and gas, transportation, water treatment and distribution, emergency services, dams, electric power generation, and nuclear power plants [6]. These critical infrastructures perform core operational functions from decision-making and planning, through monitoring and controlling, to information management. An appropriately designed infrastructure should be adaptable, autonomous, efficient, reliable, safe, and usable.

Industrial Control Systems (ICSs) are considered to be the most critical components of any infrastructure as they are responsible for most of the core functionality and they provide support to other components. Typically, these systems collect information from sensors and field devices, process and display the information, transmit it over the network, and send control commands to remote equipment [7]. In the electric power generation industry, an ICS manages, transmits, and distributes the electricity. This process is implemented in the actions of opening and closing circuit breakers and setting threshold values. Similarly, in the oil and gas industry, an ICS performs refinement operations and can remotely monitor the pressure and flow of gas pipelines. In water management, an ICS remotely monitors the well levels, water flow, and chemical composition. Thus, an ICS performs from simple to complex operations, such as being used to monitor the temperature of a building or to manage the critical functions of NPPs.

ICSs are divided into two main types: i) Distributed Control Systems (DCS), which are used within a single plant or a small geographic area and ii) SCADA (supervisory control and data acquisition) systems, which are used in large facilities and are geographically dispersed [8, 13]. The components and architecture of an ICS vary with each sector. In some cases, the components of the ICS include a central repository, supervisory control station (SCADA), monitoring station, sensors, and field devices. In order to receive information, sensors take readings from equipment. These readings include water level, heating temperature, voltage and current values, etc. The SCADA system issues commands or instructions to field devices, e.g. turn on the switch, increase the temperature, turn off the valve, or dispense the chemical, etc. They may also be programmed to generate alarms when a certain level is crossed. The monitoring station consists of two or more human machine interfaces (HMI), which are used by an operator to remotely view, update, or manage the other parts. In order to exchange information and configure commands, the station is connected to other application servers and engineering workstations via a communication network (internet, wireless, or a public switched telephone network).

A number of industrial sectors such as NPPs use additional components that communicate with the monitoring station. In those sectors, SCADA systems also include control servers, long and short range communication devices, Remote Terminal Units (RTUs), and/or Programmable Logic Controllers (PLCs) [10]. The RTUs and PLCs control the field devices and send data to control servers. The control server gathers and processes data from the RTUs and PLCs, and transmits it to central site for monitoring and controlling purposes. The collected data is viewed on computers at a central site by operators or automated supervisory tools, which issue commands to field devices. The communication devices, such as switches and routers, allow the information transfer between the control servers and RTUs/PLCs. Figure 1 shows the general architecture of an ICS. The control center consists of the control server and the communication devices. Other components may include a HMI, engineering workstations, and the database system, all connected through a local area network (LAN) [10]. The control center collects data from the field devices, displays it to the HMI, and generates further actions via the control server. The field devices perform core functionalities. They may sense sensors' values (such as temperature, humidity, speed, etc.), run equipment, and are often connected remotely to the LAN. The ICS supports common protocols such as TCP/IP and industry-specific protocols such as Modbus and radio networks.

Despite the numerous advantages offered by the infrastructure, its amalgamation with computers and networks has introduced vulnerabilities and cyber threats to critical assets [11]. Critical infrastructures are tempting targets for enemies such as nation-states, activists, terrorists, and cyber criminals; these enemies can plan strategic attacks on infrastructures without being physically present. This disruption in security to critical infrastructures may lead to significant socio-economic crises, thereby causing negative political, geographical, and security consequences. The U.S. President's Commission on Critical Infrastructure Protection states that "the widespread and increasing use of SCADA systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means" [7]. Hundreds of cyber incidents have been reported over the last few years, resulting in economy costs, deaths, and the complete destruction of infrastructures [4, 14].

In order to confront such attacks, a number of methodologies and tools on deterrence, prevention, detection, response, and damage control have been introduced [11]. These tools and technologies can exist at both technological and nationally strategic levels. The technical level focuses on solutions to prevent and detect cyber attacks, using tools such as firewalls, intrusion detection systems, anti-virus programs, back-ups, authentication, and encryption. It also includes ways to identify vulnerabilities in a system, then seeks secure solutions to eliminate those vulnerabilities.

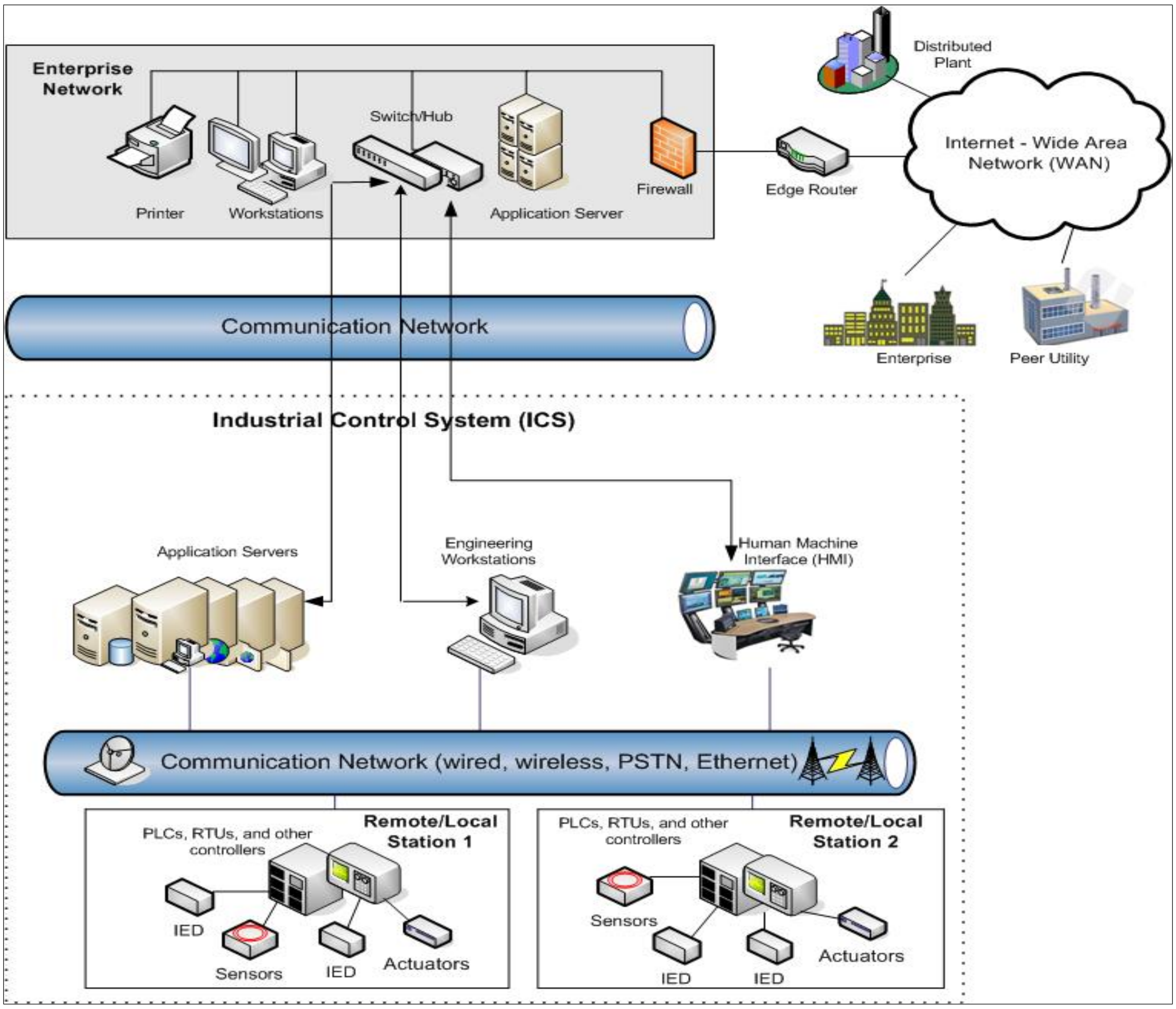

Figure 1: Architecture of ICS

However, organizations cannot completely protect their infrastructures without the enforcement of sound security policies developed by policy makers. At that point, the strategic level comes into play with the development of comprehensive policies on protecting critical infrastructures by taking into account social, economic, organizational, and political aspects. This development requires joint discussions between representatives from all concerned departments, mainly those responsible for ensuring security in the critical infrastructure industry[1]. A report by McAfee [12] shows that countries such as the U.S., Russia, China, UK, and France have established various cybersecurity departments with the purpose of protecting their national infrastructure and developing domestic cyber capabilities.

2.2 Nuclear Power Plants (NPPs)

Though NPPs are used to produce electricity, there exist significant differences between nuclear and other electrical generating plants. The most common method to produce and distribute electricity is through an "electrical generator" [14]. It uses different types of mechanical forces such as wind and water, or mechanical devices such as steam turbines, diesel engines, etc. In order to produce electricity, a turbine and a generator are attached to each other; the kinetic energy of the wind, falling water, or steam is pushed against the fan-type blades of the turbine, which causes the turbine and rotor of the electrical generator to spin and produce electricity.

Another type of plant is a hydroelectric plant in which water travels from higher elevations to lower levels through the metal blades of a water turbine [14]. As a result, the rotor of an electrical generator spins to produce electricity. Fossil fuelled power plants use heat from burning coal, oil, and natural gas to convert water into steam, which is then piped into a turbine. The steam in a turbine passes through the blades and spins the electrical generator, which results in a flow of electricity. This type of plant also follows the reconversion process where steam is converted back into water in the condenser and pumped back to the boiler to be reheated and converted back to steam [14].

The components of a NPP are similar to those in fossil fuelled plants, except that the steam boiler is replaced by a Nuclear Steam Supply System (NSSS) [14]. The NSSS consists of a nuclear reactor and the equipment used to produce high pressured steam. The steam then turns turbines for generating electricity. A nuclear reactor has four main parts: the uranium fuel assemblies, the control rods, the coolant/moderator, and the pressure vessel. The fuel assemblies, control rods, and coolant/moderator make up what is known as the reactor core. The core is surrounded by the pressure vessel [14].

The energy in NPPs comes from the fission (splitting) of fuel atoms, i.e. U-235 (uranium). Most of the reactors use U-235 for fuel because it can be more easily split during a fission process than other forms of uranium. The fuel cycle for power reactors begins with the mining of the uranium and ends with the disposal of the nuclear waste, going through three main phases. In the first phase, the fuel is prepared; the second phase is the service period in which fuel is used to generate electricity; and in the final phase, fuel is either disposed of or reprocessed [15].

[1] These representatives should belong to government, major governing bodies, information technology and information security sectors.

The raw uranium, mined from ore deposits, cannot be used in power reactors; it has 99.3% of U-238 and 0.7% of U-235. However, the fission process requires U-235 enriched to a level of 3–5% [15]. Therefore, the raw uranium must be processed through a series of steps to produce usable fuel. The concentration of U-235 is increased through the enrichment process, in which uranium gas is introduced into fast-spinning cylinders and heavier isotopes are pushed to the cylinder. Once the fuel is enriched with U-235, it is fabricated into ceramic pellets. The pellets are slender metal tubes, typically 8-15 mm (0.314 -0.59 inches) in diameter and 3.65 meters (12 feet) long.

The pellets are then pressurized with helium gas, after which they are packed in long metal tubes to form fuel rods and are bundled together into “fuel assemblies”. The assemblies are then shipped to the power plant for introduction to the reactor vessel where the controlled fission process occurs. Fission splits the U-235 atoms and releases heat energy, which is eventually used to heat water and produce high pressure steam. The fuel in the reactor is used for 3 to 5 years, and then the reactor is loaded with fresh fuel. Because the spent fuel is very hot and radioactive, it is stored in water pools to provide cooling and shielding from radioactivity [15]. After a few years, the fuel is sent to interim storage facilities, which have either wet storage, where spent fuel is kept in water pools, or dry storage, where it is kept in casks. If spent fuel needs to be reprocessed, it is sent back to a conversion facility and the process is repeated. The spent fuel contains 1% plutonium, 96% uranium and 3% waste material. After the conversion and enrichment process, the spent uranium can be reused in reactors.

2.2.1 Architecture of NPPs

It is important to give a description of the typical NPP Instrumentation and Control (I&C) systems and to characterize the various modules. In digital NPPs, I&C systems, together with the operations personnel, serve as the central nervous system. The purpose of an I&C system is to support reliable power generation. Ideally, a NPP should keep plant parameters such as power, power-density, temperature, pressure, and flow rate below a design limit, which is accomplished through thousands of electromechanical components like motors, pumps, or valves. The coordination between these components is controlled by the different elements of I&C systems; they sense process parameters, calculate deviations/abruptions, monitor performance, integrate information, issue corrective actions to field devices, and make automatic adjustments to plant operations as necessary [87]. They also send alerts and responses to abnormal events or failures, thus ensuring goals of efficient power production and safety are met. Moreover, an I&C system sends and receives responses from a HMI about the status of plant parameters and their deviations. In short, an I&C system senses, communicates, monitors, displays, controls, and issues commands between the plant components and plant personnel. For this research, we have used the Evolutionary Pressurized Reactor (EPR) architecture (the U.S. version is called the Evolutionary Pressurized Reactor or US-EPR) [87]. However, due to space limitations, we have discussed the architecture at an abstract level. The EPR is divided into three main levels: i) Level 0, process interface level; ii) Level 1, system automation level; and iii) Level 2, unit supervision and control level. Figure 2 displays the simplified architecture of a generic NPP I&C system.

Level 0 – Process Interface Level provides measurement and sensory capabilities to support functions, such as monitoring or controlling devices to enable plant personnel to assess status. This level consists of field devices, such as sensors and detectors, which are deployed at the plant, and send signals through a communication system to the operators or to the decision-making applications (analog or computer-based). These devices help make automatic and manual decisions, both for control systems and operators, during normal and irregular situations. The parameters measured include plant temperature, pressure, flow rate, level, etc. The measurements are then sent to *Level 1 systems* (discussed below), which compare them with defined values and take corrective actions, if required.

Level 1 – System Automation Level is made up of systems related to the processing and controlling of parameters and to the safety of the plant. These systems automatically control the devices of the main plant and ancillary systems, based on the inputs received from sensors and detectors. The automation of power plant control reduces the workload of operations staff, thus allowing them more time to monitor plant behaviour and evolving conditions. This level consists of the protection system (PS), safety automation system (SAS), process automation system (PAS), priority actuation and control system (PACS), and reactor control, surveillance, and limitation (RCSL) system.

Level 2 – Unit Supervision and Control Level bears responsibility for forming interactions between operators and the rest of the plant systems at levels 1 and 0. It consists of the HMIs and panels of the main control room (MCR), remote shutdown station (RSS), technical support center (TSC), process information and control system (PICS), and safety information and control system (SICS). HMIs allocate and distribute tasks among workstations; select and prioritize alarms and their integration with other components; display plant statuses, measurements and values; etc.

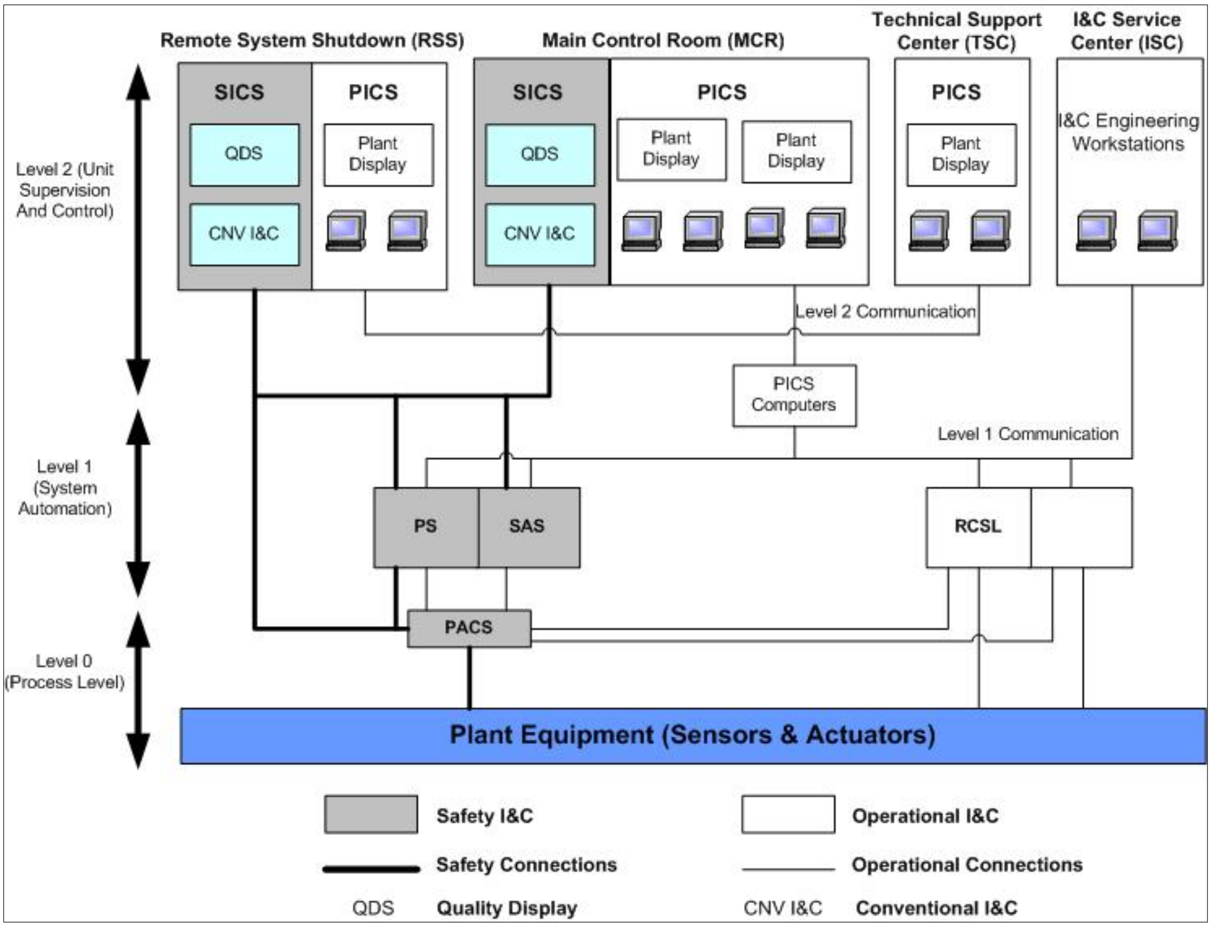

Figure 2: U.S. Evolutionary Pressurized Reactor instrumentation and controls architecture [87]

Moreover, the International Atomic Energy Agency (IAEA) has divided I&C systems into three main classes: safety, safety-related, and not-safety systems [88]. Each level, discussed above, may contain both safety-related and non-safety-related systems. The purpose of ***safety systems*** is to protect the plant and environment from natural hazardous or disastrous consequences that result from the malfunction of plant components. These systems perform automatic actions under abnormal conditions. It consists of PACS, PS, SAS, and SICS, which further include plant components such as reactor trip, emergency core cooling, decay heat removal, containment fission product removal, emergency power supply etc. ***Safety related systems*** do not directly protect the plant, but are otherwise important for the safe execution of plant operations that control reactor power, control pressure and temperature for heat removal, monitor radiation levels, measure and display plant status, etc. These systems consist of PAS, RCSL system, and PICS. ***Not-Safety systems*** are not necessary to maintain the plant within a safe environment. They are not covered in detail in this paper.

3. Cyber Security and Cyber Warfare in the Nuclear Industry

Concern surrounding cyber warfare has gained attention in the international community, and now it has become a matter of concern for the nuclear industry as well. The consequences of a cyber war are no less than those of a traditional war with the loss of money, lives, infrastructure, and national stability. The war between Russia and Georgia demonstrated that cyber warfare mechanisms are modern war mechanisms [26]. Similarly, the Estonian attack of 2009 proved that unpreparedness for cyber incidents may lead to catastrophic situations for government, businesses, and media [27]. In 2009, another large attack, "GhostNet", was launched and able to steal confidential information from more than a hundred governments and private organizations from various countries [28]. It was also reported that a botnet named "Patriot" was created by Israeli hacktivists and launched on the computers of non-technical activists, running as a background process and awaiting orders from the hacktivists' leaders [29].

In the same vein, this section focuses on cyber challenges and security incidents that occurred within NPPs, supporting the assertion that any kind of cyber incident on a nuclear infrastructure may lead to catastrophic results and from which recovery will not be possible. However, it is necessary to understand three basic cyber risk scenarios before going into the depth of security events and challenges.

3.1 Cyber Risk Scenarios

IAEA has clearly identified three possible risk scenarios involving nuclear facilities: i) "cyber attacks", which corrupt nuclear command and control systems and remove radioactive material; ii) "cyber sabotage", which affects the normal operations of a nuclear facility and causes serious damage to nuclear equipment; and iii) "cyber espionage", the collection of confidential information from a nuclear facility and its usage for malicious purposes [16].

Cyber Attacks: It is difficult to successfully execute a "cyber attack" because of the involvement of physical as well as cyber actions. Such attacks can be executed if the facility has weak security controls and policies, and with the involvement of an insider. The sophistication of these attacks demands identification of vulnerabilities, expertise in ICS, and the creation of malicious programs.

Terrorist groups are unlikely to have access to such expertise or resources, but military nation states might have such capabilities to execute attacks against another country.

Cyber Sabotage: Cyber sabotage is another threat which NPPs have faced. Sabotage can come in many forms: it could cause physical disruption to nuclear equipment, introduce viruses or malware into a system, or even plant malware that could result in nuclear explosion. The supply chain management cycle and procurement of third party software are also seriously threatened. History has witnessed a number of incidents, in which intentional or unintentional acts of deploying malicious software resulted in unrecoverable damage to a nation's infrastructure [23]. Incidents which modified the Iranian vacuum pumps in 1990, planted explosive material in Iran's nuclear equipment in 2012, and altered cooling components in Iran's nuclear power reactor in 2014 are a few examples of cyber sabotage [24,26]. Stuxnet [5,34] is another example of cyber sabotage, which caused significant damage to Iranian centrifuges and SCADA control systems.

Cyber Espionage: Recent years have seen a substantial increase in cyber espionage attacks. Cyber espionage is more common than sabotage since this type of attack does not require as much technical expertise. There are many tools, such as key loggers and spyware, freely available on the internet, which could be remotely installed on a victim's computer to penetrate a trusted network and access sensitive information. The nuclear industry has been a target of cyber espionage since 1986; however, a new series of attacks began in 2005, when Chinese hackers penetrated U.S. military systems for nuclear secrets [17]. In 2006, Israelis planted a Trojan Horse on Syrian computer systems and gained access to their secret nuclear program [18]. Similarly, in 2008, Russian forces created a malware named agent.btz to hack the U.S. classified network [21]. A number of attacks were launched from 2011 to 2013 on U.S. and IAEA sensitive facilities. Duqu [21], Flame [21], Zeus [20], Shady RAT [20] and malwares by Deep Panda [22] are examples of cyber espionage attacks, which have been designed to gain intelligence from critical infrastructures.

3.2 History of Nuclear Cybersecurity Incidents

Literature reports very few cybersecurity incidents in the nuclear industry. The reason is quite obvious: governments do not want to publish the weaknesses of their critical infrastructures or even make the general public aware that such vulnerabilities exist. However, in order to better protect systems from future attacks, one needs to analyse previous cyber incidents on nuclear or any other critical infrastructure. There have been incidents which are not the result of cyber attacks on NPPs, but those incidents demonstrate similar impacts compared to those of a cyber attack on a critical infrastructure.

A number of power outages occurred during August and September 2003 in major countries like the U.S., Canada, England, Denmark, Sweden, and Italy [37]. "The North East Blackout" power outage in the U.S. and Canada affected around 55 million people and resulted in 11 deaths [38]. The notable Chernobyl SCADA incident caused a catastrophic amount of damage [30]. This incident led to 56 deaths and an estimated 4000 cancer cases. The recovery process was estimated at $1.2 billion and the site will remain radioactive for an estimated 100,000 years. The 2011 incident of Fukushima Daiichi NPP, which occurred due to the preceding earthquake and tsunami, is another major event which resulted in disastrous consequences. Around 100,000 people were asked to evacuate their homes, and a large agricultural area was declared to be uninhabitable for thousands of years. The Japanese government is still coping with the effects of the released radiation [40]. A similar incident was reported in July 1999 when a pipeline ruptured in Whatcom Creek, Washington, spilling 237,000 gallons of gasoline. This ignited gasoline resulted in three deaths and damage worth approximately $45 million. Analysis of this event shows that the pipeline company was not adequately managing the protection of its SCADA system [41].

In 2003, the SQLSlammer worm breached Ohio's Davis-Besse NPP through a contractor's system. The worm crashed the safety parameter display system (SPDS) and monitoring systems of the nuclear plant [42]. SQLSlammer exploits a vulnerability in Microsoft SQL Server 2000 database software. The worm scans a system, and if it finds SQL Server 2000 running, then it infects the system and propagates to the next random IP address. The worm generated a large volume of network traffic. Fortunately, Ohio's Davis-Besse plant was not in use at the time and damage was not serious. Similarly, a computer virus called "Sobig" shut down a train signalling system in Florida, U.S., in 2003 [43]. It shut down the signalling and dispatching of the systems deployed at CSX corporation, which caused train delays. In August 2006, the Browns Ferry nuclear plant in Alabama, U.S., was manually shut down because of an overload of network traffic, which resulted in the failure of reactor recirculation pumps and the condensate demineralizer controller [44]. Both of these devices transmitted data over an Ethernet network, which contained network vulnerabilities allowing irrelevant traffic to pass through the plant. This incident reveals the impact of the failure of one or more devices in a plant.

The Hatch NPP was shut down in March 2008, when an engineer's computer connected to the plant's business network. The computer was connected to the ICS and its system update was designed to synchronize the data between two devices. However, when the computer was restarted after the update, it reset all the data of the control system to zero. The plant personnel incorrectly interpreted the zero value and thought that there was an inadequate level of water in the reactor [45]. This shows that nuclear personnel had insufficient training and knowledge of the incident, and that their unawareness caused more problems than the original one. Industrial espionage was also reported in 2009, when Chinese and Russian spies penetrated the U.S. electrical power grid and installed malicious software programs [46].

In 1992, a technician at Ignalina NPP intentionally injected a virus into the control system. Though his purpose was to highlight the vulnerabilities in a plant, it demonstrated the dangers of the insider threat [47, 48]. In 2000, a disgruntled employee gained unauthorized access to the computerized management system of his company, and caused millions of litres of raw sewage to spill out into local parks and rivers [49]. The attacker installed the company's software on his laptop and infiltrated the company's network to control waste management. Another insider attack occurred in 2007 in California when a former electrical supervisor installed unauthorized software on a SCADA system, causing damage to the company's assets [50].

A major cybersecurity incident occurred in 2010, when Iran's NPP was hit with the Stuxnet computer worm. Cybersecurity experts claim that this worm is the first cyber weapon that was targeted to exploit SCADA systems, damaging 1,000 centrifuges in the process [5]. Stuxnet targeted the Siemens control systems and had the ability to reprogram the PLC. The worm was highly sophisticated, as it exploited five zero-day vulnerabilities and was initially spread from infected USB flash drives. This renders the claim of NPPs "being air gapped" as an ineffective security method. Stuxnet demonstrates the effects of maintaining unpatched systems and allowing vulnerabilities to enter the facility. This malware extracted the hard coded password from the Siemens database (CVE-2010-2772) and acquired access to the SCADA system files. It then manipulated the frequency of the frequency drivers, which in turn, damaged the centrifuges. The virus installation was made hidden through the use of driver signing keys, which had been stolen from RealTek and JMicron [51]. The attack was launched by a nation-state targeting Iran's nuclear technologies. The Stuxnet incident made nations realize that cyber warfare is a serious concern and that proper security is needed to protect their critical infrastructures. Iran reported the replacement of 1,000-2,000 centrifuges in a few months [52]. According to several published reports, Stuxnet also infected a Russian nuclear power plant around 2010. The incident was revealed by Eugene Kaspersky, founder and CEO of Kaspersky Lab. Though Stuxnet was a very targeted attack, its unprecedented capabilities showed that this worm could also be used for more destructive purposes.

In 2011, McAfee reported the attack named "Night Dragon", launched on five global energy and oil firms which were compromised using mechanisms such as phishing, Trojan Horses, Windows exploits and social engineering [53]. There are many attacks which targeted the corporate companies attached to the SCADA infrastructures. An incident was reported on South Korea's state-run operator, Korea Hydro and Nuclear Power Co., in December 2014. The attackers gained access to the system by sending phishing emails to the employees. An employee's accidental click on the malicious link given in the email allowed malware to download, infecting the company network. The attack specifically targeted the blueprints and electrical flow charts of nuclear reactors [54].

A number of attacks have been reported on SCADA systems. It is difficult to identify whether these attacks are because of IT network or SCADA software vulnerabilities. According to Eric Byres, from 1982 to 2000, 70% of SCADA attacks were internal, i.e. due to disgruntled employees and their mistakes, while 30% were external attacks from hackers and cyber terrorists [55]. Byres then explained that a survey for the years 2001 to 2003 showed that 70% of attacks were external and 30% were internal. The complete reversal of statistics shows that industry is neither using standardized networking protocols, nor verifying the security of third-party software. This change did not occur because there are fewer internal attacks, rather, the number of external attacks has risen so much it caused the reversal of these figures.

3.3 Nuclear Cybersecurity Challenges

The abovementioned incidents have made cybersecurity an ever increasing concern for nuclear facilities, including power plants and weapons facilities. This evolution in technology has also introduced vulnerabilities in and hacking attempts on nuclear systems. Software vulnerabilities have made it easy for hackers to steal sensitive information, spoof systems, or potentially damage critical nuclear facilities and processes. Such vulnerabilities could be introduced through bugs in software programs or zero day exploits.

The research performed by the Chatham House project identified major challenges in civil nuclear facilities [4]. The report highlighted that infrequent disclosure of incidents at nuclear facilities has made it difficult for security analysts to analyse the extent of the problem in order to implement security controls. Governments and nuclear authorities do not disclose nuclear security incidents out of concern for reputation and trust among other countries, which leads to the erroneous belief that it is nearly impossible to attack a nuclear facility. Nuclear personnel often interpret security incidents as malfunctioning of hardware because there is a lack of nuclear forensics and logging techniques that can determine the cause of incidents.

In addition, there is currently no mechanism in place to facilitate the exchange of information and to enhance collaboration with other industries that are making progress in this field [4]. The nuclear industry is reluctant to share its information and collaborate with other industries to learn from their experiences. The lack of sharing means that the nuclear industry cannot identify the attack patterns discovered by other sectors nor can it apply fool-proof security controls. There are also insufficient cybersecurity regulatory guidelines and standards which nuclear facilities can follow for compliance. A few regulators have issued best practices guidelines; however, their guidelines do not cover enforcing security controls and managing cyber risks [4].

It has also been observed that nuclear plant personnel and cybersecurity professionals have a difficult time communicating security requirements and suggestions to each other [4]. The reasons seem to be the off-site location of cyber professionals and lack of information security awareness among nuclear personnel. Nuclear plant personnel are not trained through cyber drills and they lack preparedness for large-scale cybersecurity incidents. Their level of technical training is insufficient, in addition to it consisting of training material that is poorly written and leads to procedural misunderstanding. Many employees leave their personal computers unattended with their emails, simulation software, and sensitive documents running. Many times the employees are working with around 60-70 other employees, and any mistake could lead to an incident, which might be unrecoverable [4].

In traditional attacks, the attacker is known to everyone, however cyber attacks change the dimensions of attacks, making it now possible to disrupt, paralyze, or even physically destroy critical systems through sophisticated computer tools and technology [4]. It is now easy for an attacker to find Internet-connected SCADA systems using specialized search engines such as Shodan [30]. Once a system is identified, the attacker can scan the network for vulnerabilities and open ports or analyse traffic to intercept passwords. Many software programs use default passwords such as “Admin”, “12345”, “Test” etc., which if left unchanged, may enable attackers to easily penetrate the network and systems.

The problem also stems from the myth that nuclear facilities are “air gapped” – or completely isolated from the public internet – and that this protects them from cyber attack [4]. Many nuclear facilities now have internet connectivity primarily because legitimate third parties, such as the vendors, owner-operators, and head officers are located off-site and need access to the data generated at the plant. The data is required to update the deployed software, check the status of the plant functions, and rapidly diagnose plant malfunctions. Internet connectivity thus allows corporate business networks to create a direct link with the industrial control system network [4]. The DragonFly cyber espionage campaign provides an example of how malware, particularly a Trojan Horse, can infect NPP facilities via a software update [35]. Facilities may be using basic rules in their firewalls and intrusion detection systems (IDS), yet it is relatively easy to bypass these mechanisms by resetting them or disguising the malware as legitimate traffic. Sometimes plants are protected through VPNs; however, if they are inadequately configured, there can still be attacks, as in the case of the Davis-Besse power plant [31]. Often, these nuclear facilities have undocumented internet connections, which are not known to plant managers; these, too, can provide a route for malware to infect the facility.

Moreover, nuclear facilities lack strong security controls such as authentication, authorization, and encryption services in their digital systems. Their software is ‘‘insecure by design’’ and does not integrate strong security features as defensive measures [4]. Additionally, vulnerabilities in typical IT systems extend to SCADA software. For instance, SCADA systems use TCP/IP protocols[2] to perform certain functions [32]. However, these protocols have some known vulnerabilities such as IP spoofing, man in the middle attacks, SQL injection, etc., which may result in severe consequences if left unattended. [33].

The existence of Stuxnet has enabled less-skilled hackers to copy the technique and develop malware on their own for destructive purposes. These malwares could be used for attacking nuclear facilities since the Stuxnet attacking logic is publically available now [4]. On the other hand, the increasing use of penetration testing and exploitation tools such as the metasploit framework [19] allows an attacker to execute a payload to exploit a system vulnerability. The framework was originally designed for penetration testing, but hackers are also using it to fulfil their malicious intentions. The problem becomes more serious when companies in grey markets try to sell zero-day vulnerabilities to nation-states or non-state hackers with the purpose of obtaining money [4].

Bring Your Own Device (BYOD) is another challenge which is an emerging focus, not only for nuclear facilities, but also for other sectors [4]. People (employees, contactors, and vendors) often bring their personal devices (mobile phones or laptops) into sensitive areas and connect to the network. If their devices are already infected with some worm or malware, then it is pretty easy to infect the facility network and resources. Similarly, a few vendors and employees deploy temporary connections within a facility in order to perform their work, but then forget to remove the connections. If they remain unattended, these connections can be utilized by an attacker to gain illegitimate access.

NPPs also sometimes do not follow the ‘‘fail-safe’’ principle[3], and there seems to be a reduction in creating backups of systems [4]. This practice has made NPPs a single point of failure. Moreover, NPPs approach security using the ‘‘Security through Obscurity’’ principle, which does not remain effective today [4]. Much of the documentation on nuclear architecture, software, and protocols used within nuclear facilities is available online. For example, documentation of NPP protocols, Distributed Component Object Models (DCOM), and Remote Procedure Calls (RPC), is available on the internet, which makes it easy for an attacker to understand the overall working mechanism, and then to find (un)known vulnerabilities in these protocols [36].

“Off the shelf” software is often not up to date, and it is not feasible for nuclear personnel to take down systems regularly to apply patches. This is because components of NPPs need to be functional 24 hours per day, seven days per week. The same applies to software and operating systems (OS) hosting nuclear plants. Therefore, an attack on unpatched software could bring down or give access

[2] TCP/IP protocols are used to transfer information over the network.

[3] A fail-safe is a practice that, in the event of a specific type of failure, responds or results in a way that will cause no harm, or at least minimize harm, to other devices or to personnel [98].

to a network of NPPs. On the other hand, patching software can also introduce unknown vulnerabilities into the system since testing is usually not performed before patching [4].

Thusly, the nuclear past is littered with examples of near misses and accidents – many of which can be either directly or indirectly launched through computers and software – and the ratio of such attacks may increase with the introduction of more sophisticated systems into the nuclear industry. While the probability of a catastrophic event such as the release of radioactive material is relatively low, the consequences could be severe. Furthermore, all of these factors indicate the lack of a well-defined cybersecurity risk management strategy for nuclear facilities. The nuclear industry is not investing as much as they should be in cybersecurity. Additionally, developing countries are at more risk, since they have lower budgets for security enforcement. States are implementing strategies and policies to prevent large scale cyber attacks, but it is too early to tell how impactful these will be.

4. Industry and Government Responses on NPP Cybersecurity

The above section has highlighted vulnerabilities and security challenges in NPPs that pose significant risks to the economy and to national security. There have been a number of attempts made by international organizations, regulatory and research institutes, and governments to establish cybersecurity guidelines, standards, and frameworks for the security of NPPs.

A number of international regulatory bodies such as IAEA, National Institute of Standards and Technology (NIST), World Institute for Nuclear Security (WINS), and the Institute of Electronics and Electronics Engineers (IEEE) have published documents [56 – 59] on securing nuclear facilities. These documents focus on ICS and SCADA systems. NIST has published a well-established risk management framework in NIST Special Publications (SP) 800-30[60], 800-37 [61], and 800-39 [62], which analyse different threat scenarios and evaluate the possibilities of attacks that can exploit system vulnerabilities. However, the NIST risk assessment framework does not define specific procedures on how a company should assess the quantification of risks, i.e. how and to what extent an attack can affect system confidentiality, integrity, or availability. In 2008, NIST released a guideline on securing Industrial Control Systems (ICS) [63]. This special publication comprehensively discussed the security of ICS systems, mainly covering SCADA architecture, distributed control systems (DCS), secure software development, and deployment of controls to secure networks. NIST also worked with the Industrial Automation and Control Systems Security ISA99 Committee to formulate a guideline on the Security for Industrial Automation and Control Systems [64].

The IAEA and WINS are playing the major roles in the nuclear cyber domain. They have begun to address cybersecurity concerns on a global scale. Currently, they are: i) publishing a number of cybersecurity documents on nuclear facilities protection, ii) offering technical and strategic security training to nuclear concerned officials of member countries, and iii) providing expert advice and capacity building to officials and representatives. The IAEA has published NSS-17 [65] as technical guidance for ensuring computer security at nuclear facilities. Likewise, the IAEA NSS-13 [66] recommends that all computer-based systems in nuclear facilities must be protected against compromise and that a proper threat assessment must be carried out to prevent attacks. The series has identified threats from different adversaries' perspectives and has also addressed detection and prevention mechanisms for compromises of NPP information systems.

A number of other organizations have also established sets of best practices or guidelines to address nuclear-related cyber issues. The IEEE produced the SCADA cryptography standard in 2008, which provides a detailed explanation on how to establish secure communication between SCADA servers and workstations. Organizations can also achieve certification under this IEEE standard if they comply with the requirements [67]. The International Organization for Standardization (ISO) has also developed a standard, ISO/IEC 27002:2013, which provides guidelines for initiating, implementing, maintaining, and improving information security management in organizations [68]. All of these guides and standards offer security best practices and provide generic guidelines on performing security assessments within NPPs.

While there are a number of guidelines for protecting industrial systems, there are fewer standards that define compliance. Compliance is important since it provides a security baseline to industries and ensures continuous protection of systems. Efforts put forward by NIST in 2004 helped develop the System Protection Profile (SPP). This profile was designed to cover SCADA systems [69] and briefly discussed cyber risks. There are a number of proprietary companies, which also offer certifications such as the Achilles certification program from Wurldtech Security Technologies and the "Music" certification from Mu Dynamics [70]. These certifications involve auditing by an outside company to ensure that I&C systems are meeting security requirements.

At the same time, government organizations also play a vital role in improving the security of critical infrastructures. The U.S. Department of Homeland Security (DHS) [71], Nuclear Regulatory Commission (NRC) [72], Federal Energy Regulatory Commission (FERC) [73], and North American Electric Reliability Corporation (NERC) [74] offer public-private partnerships to protect critical infrastructure and to provide cross-sector strategic coordination and information sharing. The U.S. issued the Presidential Decision Directive (PDD) in 1998, which highlighted risks to national critical systems and solutions to secure them [75].

In 2007, the NRC included cybersecurity as part of Design Basis Threat[4], defined in 10 CFR, Section 73.1. Subsequently, in 2009, the NRC issued 10 CFR Section 73.54, titled "Protection of Digital Computer and Communication Systems and Networks," which required all licensed[5] NPPs to provide high assurance that their computers and communication systems are protected against cyber attacks [76]. The protection must be assured for the following functions: i) safety-related and important-to-safety functions; ii) security functions; iii) emergency preparedness functions, including offsite communications; and iv) support systems and equipment. In Nov 2009, 10 CFR 73.54 required NPP authorities to submit their cybersecurity implementation plans to the NRC, describing how the NPPs would comply with the above requirements. In order to assist the licensees, the NRC issued formal cybersecurity regulatory guide (RG) 1.152 [78] in 2010. The NRC has also issued RG 5.71 [77] for enforcement of cybersecurity measures at NPPs. These regulations address security vulnerabilities in each of the following phases of the digital safety system lifecycle: i) Concepts; ii) Requirements; iii) Design; iv) Implementation; v) Test; vi) Installation, Checkout, and Acceptance

[4] DBT is a description of the attributes and characteristics of potential insiders and/or external adversaries, who might attempt sabotage or unauthorized removal of nuclear material, against which a physical protection system is designed and evaluated [66].

[5] The "licensees" referred to in the CFR are the people who have licenses to operate the NPPs, and that requires them to provide assurance that their plant has a cybersecurity plan.

Testing; vii) Operation; viii) Maintenance; and ix) Retirement. At the 2014 Nuclear Security Summit, the U.S. announced its plans to monitor the activities of NPP operators, and to check if cybersecurity principles are properly followed.

Besides the U.S., other countries such as the UK, Germany, Australia, Netherlands, China, Belgium, France, South Korea, Hungary, Canada, and the Czech Republic have also implemented cybersecurity strategies for protecting NPPs from cyber attacks [80-82]. The UK established the National Infrastructure Security Coordination Centre (NISCC) in 1999, the role of which was to minimise the risk to critical infrastructure from cyber attacks [79]. In 2007, the Centre for the Protection of National Infrastructure (CPNI) was established by the UK to guide companies and individuals on how to secure SCADA systems [83]. The CNPI published nine best practice documents, which cover a diverse range of security issues - from third-party risks to firewall deployment.

Moreover, there have been a number of agreements between countries to establish confidence building measures in cyberspace. Nation-states are often reluctant to share their cyber expertise and skills with other countries. This leads to mistrust among countries and haste to improve one's own cyber capabilities. In an effort to address this problem, the U.S. and Russia made an agreement in 2013 [96]. This treaty involved information sharing between the U.S. computer emergency response team (CERT) and its Russian counterpart, creation of working groups, and the use of the dedicated nuclear hotline to communicate cyber crises. Similarly, a bilateral agreement was signed between the U.S. and China in 2013, however, the agreement did not last and ended in May 2014 [85]. The European Union (EU) is also doing notable work in preventing and responding to nuclear attacks at a global level. EU-CERT and the European Network and Information Security Agency provide support to governments during crisis management and also provide training to operators [86].

Nevertheless, all of these efforts are ongoing and require indefinite time to mature. The guidelines, standards, and recommendations offered by governments and regulatory authorities require comprehensive review to ensure that they cover the latest risk assessment developments – for example, cyber threat information sharing, risk assessment of tacit knowledge, dissemination of risk assessment results, etc. These features are required to keep NPP risk assessment up-to-date on advanced cyber threats and to manage cyber incidents in an appropriate way. However, at present, the abovementioned guidelines do not provide enough detail on enforcing security controls and preventing cyber risks. Our findings have also revealed that none of the proposed guidelines have holistically provided detailed security procedures specific to the architecture and working of NPPs. Threat and risk assessment of NPPs is necessary since it provides realistic insights into systems security and helps in implementing appropriate defense-in-depth measures.

5. Threat Modelling for NPPs

In the previous section, we have highlighted a number of standards and guidance documents that have been published to evaluate the security risks of IT or Instrumentation and Control (I&C) systems. However, these documents do not describe threat and vulnerability assessment of I&C systems of NPPs. Design basis threat (DBT) profiles determine threat levels, develop security postures, and provide statements about the attributes of potential adversaries of NPPs [89]; nevertheless, they focus more on physical safety of the plant than they do on cyber protection. There is a significant need to perform detailed threat and vulnerability assessments of NPPs that consider both stand-alone attacks and coordinated attacks against the use of computer systems. A coordinated attack is a carefully planned and executed offensive action in which the various elements, such as systems and personnel are involved in a manner to utilize their skills as a whole; whereas a standalone attack is an individual effort to launch an offensive action.

This section presents the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges) threat model of a generic NPP's I&C system by considering its characteristics and architecture. First, security requirements for a NPP are identified, followed by the analyses of security vulnerabilities in I&C systems. The identification of requirements and vulnerabilities further led us to the discovery of threats that adversaries pose on the I&C system of a NPP. As a next step, adversaries are classified based on attacker profiles given in the IAEA NSS-17 series [65] and IAEA-CN-228-54 [90] conference publication. Finally, STRIDE methodology is used to develop threat models, followed by the formulation of attack trees using Amenaza SecurITree [91].

Scope of Threat Modelling: The scope of our threat modelling is limited to *Level 2* of I&C system architecture, which is common to all types of NPPs. There are a number of reasons that limit the development of a complete threat model for the ICSs of NPPs. It is difficult to address the ICSs of NPPs as a whole because of the depth and breadth of the nuclear power plant discipline. Firstly, every type of NPP has a different ICS architecture that varies significantly with the purpose and scope of the plant. Secondly, an ICS system of a NPP is composed of a variety of technological elements, such as modules, elements, components, sub-component systems, and sub-systems, that are connected to each other through a number of possible ways (data link, LAN, WAN, Intranet etc.), depending on the architecture of the ICS and the functions of these elements. Finally, an ICS system also relies on other influencing factors, such as human actions, information management, simulation, software engineering, system integration, prognostics, and cyber security. Therefore, it is difficult to completely characterize a NPP and perform a threat modelling. The related government departments and nuclear authorities are ultimately responsible for performing a complete threat modelling on every nuclear facility (real world) and using the results to mitigate high-level attacks.

We have chosen *Level 2* because it has the most interaction with the outside world and the plant. External and internal threats begin propagating from this level since it is connected to the Internet as well as to the internal network. Humans, the weakest link of the security chain, also interact from this level. The systems at *Level 2* are the safety information and control system (SICS) and the process information and control system (PICS). The SICS plays its part when the PICS is unavailable: it monitors and controls certain safety-related systems, such as the component cooling water system (CCWS) and ventilation, for a short interval under certain conditions. It consists of human machine interfaces (HMIs) and qualified display systems (QDSs). The PICS monitors and controls the plant under every condition. It consists of i) computers (HMIs) – for monitoring and control at the operator workstations in the main control room (MCR) and technical support center (TSC), ii) Visual Display Units (VDUs) – for displaying the plant overview in the MCR on large screens, and iii) soft controls. Both of these systems have access to Level 1 and 2 systems. Moreover, PICS also displays alarms and provides guidance to the operators for corrective actions. Other details, including the communication procedure[6], are available in IAEA and U.S. Nuclear Regulatory Commission publications [87, 88].

5.1 Security Requirements of a NPP

In order to identify threats, it is first necessary to discuss the security requirements of NPPs. These requirements are generic such that any NPP can implement security measures based on them.

1. **Mutual Authentication:** The various components, systems, and sub-systems of a NPP must be mutually authenticated with each other during their interactions. This is required to ensure that only authenticated entities can interact with and access critical or sensitive information from the relevant components. For example, remote shutdown stations (RSS) or workstations at the MCR must authenticate systems at Level 2 before exchanging information, and vice versa. Also, the operator sending control commands or requesting data for display must be authenticated using two-factor authentication at every workstation. In return, the workstation must be authenticated by the controller from which it is fetching data. This mutual authentication will help in preventing spoofing and masquerading attacks on NPP components as well as personnel.

2. **Confidentiality** involves securing data at rest as well as the data being shared during communications. The data being exchanged among the systems of layers 0, 1, and 2, as well as between the plant personnel and layer 2 systems, must be secured and disclosed only to the systems that have to perform certain functions on the data. If systems at different layers are hosted on different networks, then the data exchange between them should be secure. For example, safety automation systems (SAS) and protection systems (PS) at layer 1 must send encrypted messages to workstations at MCR and RSS. Secure data communication ensures protection against external attempts to leak data and to expose critical information regarding plant status and its parameters. The data at rest, such as that stored in databases and on workstations, also needs to be secured using encryption mechanisms for preventing unauthorized or illegal access to critical resources.

3. **Authorization:** Physical access control has already been implemented at NPPs. However, software based access control is another major security process which must be validated. It is necessary that only authorized employees and systems are able to access relevant information about plant equipment and their parameters. “Least Privilege Principle” and “Separation of Duties Principle” must be present in access controls to ensure that an operator/employee will only get data on a need-to-know basis. For example, the data display at VDUs and workstations of operators must be filtered as per the access control policy and then presented.

4. **Data Integrity:** The data received from Level 0 (i.e. sensors, actuators), Level 1 (PS, SAS), and Level 2 (Workstations) must be accurate. The readings of temperature, pressure, etc.,

[6] The communication system provides information and data exchange among various components of the ICS and plant. It uses a number of protocols and mediums to perform its functions. The mediums could be wires, fibre optics, PROFIBUS, fieldbus, wireless or wired network, etc., while protocols depend on the requirements of a plant but mainly include TCP/IP, MODBUS, etc. Most digital power plants around the world are limited to LAN or intranet.

received from sensors must be correct; similarly, commands received from the controller must be verified as being the same commands the operator issued. This requirement is ensured through data integrity, using either encryption or hashing techniques, such as SHA or MD5, to verify data was not corrupted in transit. Misleading or erroneous data could result in disastrous effects for the plant and the environment.

5. **Non-repudiation** is an important requirement for every system within the plant architecture in order to ensure that the data or command received is actually from the authorized system or person it claims. For example, the command issued by an operator to increase the speed of centrifuges or to send information about water level must be sent with the digital signature of that operator. Similarly, the commands issued by controllers at Level 2 need to be tracked for auditing purposes to track failures or malfunctioning of specific components.

6. **Systems Security Capability Monitoring:** The components and systems at every layer should be certified by a trusted third party to ensure reliable and secure behaviour. In the case of replacement for any system or component, the system must be recertified to guarantee robustness.

7. **Auditing:** All operations (such as modify temperature, increase speed, display data, etc.) being performed by the systems and components must be logged for future reference. This requirement will also help forensics investigations by providing evidence of any malicious attempt by an adversary. For example, if any system or component is compromised or spoofed, leading to some malicious activity within a plant, then auditing will help trace the malicious component that breaches security and violates rules. If properly logged, activities and tasks can help gather evidence against the enemy, as well as keep a check on system activities in real-time, preventing serious damage to the plant.

8. **Availability:** This is the most important requirement for an NPP. The I&C system of an NPP has a dependent architecture, where components require inputs from other components deployed at different layers. The unavailability of one component without a backup could result in disastrous effects. Components such as sensors, detectors, PS, SAS, etc., should be available as per their requirements.

5.2 Security Vulnerabilities of a NPP

Having identified the security requirements for a NPP, we now thoroughly analyse the security vulnerabilities of the I&C system components which may result in system breakdowns or plant shutdown. This further helps us to identify threats that result from the exploitation of one or more vulnerabilities. Table 1 displays the categories of vulnerabilities that could occur in the I&C systems of a NPP, along with the lists of threats and vulnerable components. These vulnerability categories are based on a U.S. ICS-CERT document for Industrial Control Systems [92]. In this sub-section, only major vulnerabilities of a NPP are explained.

Table 1: Vulnerability Categories and Associated Threats in NPPs

Vulnerability Category	Attacks	Vulnerable Modules
No or Incorrect Input Validation	Buffer over flow; cross-site scripting; SQL injection; command injection.	Workstations at MCR, RSS; PICS; SICS; HMIs.
Improper Authorization	Data tampering; Escalation of privileges.	Workstations at MCR, RSS; PICS; SICS; HMIs, SAS, PS, PAS.
Improper Authentication	Network eavesdropping; Brute force attacks; Dictionary attacks; Credential theft; Cookie replay; Identity Spoofing.	All I&C systems, sub-systems and components
Unencrypted Sensitive Data	Data exposure; Data tampering; Network Eavesdropping; Credential theft; Man-in-the-Middle.	All I&C systems, sub-systems and components
Improper Software Configurations and Management	Access to default accounts; Exploit unpatched flaws, unprotected files and directories, etc.; Install Malware/Botnets	Workstations at MCR, RSS; PICS; SICS; HMIs, SAS, PS, PAS.
Lack of Backup Facilities	Interrupt plant operations; Shutdown plant; destroy plant equipment.	SAS, PS, PAS, Sensors, Actuators, PICS, SICS.
Lack of Audit and Accountability	Repudiation; No traces of network attack patterns; No traces of installation of malicious software.	All I&C systems, sub-systems and components

1. **No or Incorrect Input Validation:** Services and scripts written by I&C vendors often suffer from bad coding practices that allow attackers to send malicious requests and thusly modify program execution. Similarly, the use of insecure protocols for networking is also vulnerable to malformed packets. Vulnerabilities in these protocols and services make an attacker capable of manipulating plant components, i.e. viewing and modifying values, using well-known attacks. In the architecture discussed above, sensors receive all requests from SAS and PS, which in turn receive requests from workstations at the MCR, which might be victim to such attempts by an attacker. The attacks that could occur through this vulnerability are buffer overflows, command injections, SQL injections, cross site scripting, etc.

2. **Improper Authorization:** Access control mechanisms are implemented in the system or within a number of integrated systems to allow only authorized entities to access resources and data. Lack of or weak mechanisms can be exploited by attackers to gain illegal access and to tamper with I&C system components. If software installed at operator workstations, PAS, SAS, sensors, etc., does not perform or incorrectly performs access control checks, then attackers are able to perform unauthorized actions. Every component of an I&C system must first check whether the requesting module is authorized to access the resource. Escalation of privilege is one of the attacks that could be executed using authorization vulnerabilities.

3. **Improper Authentication:** Improper authentication creates vulnerabilities in I&C protocols, network packets, products, and databases. The network protocols deployed within the I&C system architecture for communication often have weak authentication to verify the identity of the packet as well as the user. The weak authentication security enables attackers to eavesdrop on network communications and capture the identity credentials of legal users, resulting in unauthorized privilege. The components of I&C also do not perform mutual authentication before sending or receiving data. If I&C protocols and software do not verify the origin or authenticity of data, it may result in the allowing of malicious data into components, credential theft, authentication bypass, etc. Moreover, the credentials stored in databases can also be exploited if not properly protected using an encryption mechanism[7]. Many times, I&C vendors forget to remove authentication details from their product code or documentation, which can be easily accessed. Weak passwords are another important vulnerability for which to monitor.

4. **Unencrypted Sensitive Data:** Data at rest and in transit is often unencrypted, which makes this sensitive information vulnerable to disclosure. In addition, network packets exchanged between various components of I&C are in plaintext form, which can also lead to exposure of product source code, topology, legitimate user credentials, etc.

5. **Improper Software Configurations and Management:** Misconfigurations or vulnerabilities in I&C software lead to security breaches and exploitations of plant operations. These vulnerabilities occur because of poor patch management, poor maintenance, and built-in flaws in I&C products. Moreover, incorrect installations of applications also provide attackers a door of opportunity. Administrators often overlook available security features and use the default security options throughout the I&C system architecture.

6. **Lack of Backup Facilities:** A number of NPP I&C systems do not have backup and restore facilities for databases and software. The NPPs that have backup facilities store them offsite, and they are rarely exercised and tested. A NPP needs to be operated 24/7; therefore, in the event of an incident, the lack of a backup feature can result in disastrous effects.

7. **Lack of Audit and Accountability:** Most attacks are launched in a stealthy manner and thus are difficult to detect. The absence of auditing and logging features enables attackers to cover their tracks after attacks. It is very necessary to store activity logs of I&C components and operator actions to trace attack patterns and also to prevent repudiation threats from plant personnel as well as I&C components and systems.

5.3 Classification of Adversaries

The IAEA NSS-17 series has categorized adversaries into eight classes that can pose serious threat to NPPs. The categories are as follows: covert agents, disgruntled current employees, disgruntled ex-

[7] Here, we assume that every user is properly authenticated before accessing the HMI.

employees, recreational hackers/hobbyists/script kiddies, militant opponents to nuclear power, non-state hackers (cyber criminals/organized crime), nation-state hackers (governments & militaries), and terrorists (non-state armed groups). An attacker profile matrix has already been provided in the NSS-17 series; therefore, this sub-section briefly presents motivations and potential objectives of the attackers. The description could then help identify threats from each attacker (threat modelling).

a. Covert Agent

A covert agent is an individual who is either retired from or a present employee of an intelligence agency, and whose identity is hidden from rest of the world. The purpose of the agent's hiring is to steal sensitive business information, nuclear secrets, and personal information of opponents. At a personal level, a covert agent can blackmail nuclear and government agencies for money or any other incentive. In order to gain information, a covert agent may need system access and documentation, or use a social engineering technique. Moreover, a covert agent must have a knowledge of programming and system architecture, for example, insertion of backdoors/Trojans, password extraction, etc. The time to compromise a target varies depending on the type of motivation, but it could take only hours.

b. Disgruntled Current Employees

A disgruntled employee is one who is not satisfied with his or her job and wants to compromise a big target through illegal methods. The reasons for being disgruntled vary, but the most common motivations are to take revenge, create chaos, embarrass one's employer, degrade nuclear security's image, or steal information for economic gain. This type of attacker needs medium to high level resources to execute an attack (e.g. systems access, documentation access, expertise of specific operations). In addition, an employee must have some level of privileges on processes and systems, knowledge of programming and system architecture, possible knowledge of existing passwords, and an ability to insert "kiddie" tools or scripts. The time to perform an attack varies depending on the target to achieve.

c. Disgruntled Ex-Employee

The motivation for this type of attacker is the same as that of a disgruntled employee still at his or her job. He or she may want to take revenge on the employer, sell sensitive nuclear information to enemies for economic gain, or disclose confidential information to the public to embarrass the employer or to degrade its public image. This type of attacker is sometimes associated with large group of people attempting to get resources. Being a former employee, he or she may still possess sensitive documentation, access to facility resources, and possible ties to working employees. The time to prepare and launch an attack depends on the associated group of people. In order to launch an effective attack, a disgruntled employee should have information about systems passwords, access to systems, and backdoors created through social engineering techniques.

d. Recreational Hackers/Hobbyists/Script Kiddies

Hobbyists or script kiddies often hack systems for fun or for a challenge. They want to learn about new vulnerabilities and exploits by trying them hands-on in the real world. These attackers often download and use free scripts and tools from the Internet. Their intentions are harmless; however, their mechanisms to learn things are dangerous. Their inquisitive natures could prove to be destructive to NPPs if deployed safeguards are not sufficient. Frameworks such as Metasploit offer SCADA-specific exploits, which could be used by script kiddies to launch an attack without having advanced knowledge and hacking skills. However, hobbyists do not have the funding to buy expensive tools and exploitation codes that are sold underground. They also have limited knowledge of computing and programming. Such attackers could easily be blocked by enforcing best practices such as patch management, policy enforcement, and adequate use of antivirus, intrusion detection systems (IDS), and firewalls within the organization.

e. Militant Opponent to Nuclear Power

This type of attacker considers himself a saviour of the world. He has strong public opinions on specific nuclear issues, and often impedes nuclear business operations. These attackers are financially supported through secret channels or agencies [65]. However, they have little knowledge of the system outside of public information. They are patient, but determined in achieving their aims. Moreover, they have plenty of time to launch an attack and usually target during certain known events such as elections. Militant opponents may or may not have computer skills; however, they can get support from the hacker community to launch a cyber attack.

f. Non-State Hackers (Cyber Criminals/Organized Crime)

Non-state hackers are groups or individuals with the main intention of obtaining money by stealing nuclear material or confidential information belonging to a nuclear facility and then blackmailing the facility into paying a ransom. They hold a facility or government hostage by threatening to exploit vulnerabilities in their SCADA systems. Therefore, their main purpose is financial gain. These criminals do have funds and can hire skilled hackers or purchase hacking tools to attack systems. There are a number of SCADA-targeted automated attack tools in the form of Metasploit add-ons that can help launch attacks on industrial control systems. Sometimes, these actors also hire former/current employees of a facility or perform social engineering to extract information. The time to prepare an attack varies, but is usually short-term.

g. Nation-State Hackers (Governments & Militaries)

Nation-state hackers are individuals hired by a government to perform cyber operations (inter)nationally. Currently, the frequency of state attacks is low, but if properly planned and conducted on SCADA systems, an attack's impact would be disastrous. State hackers deface and block websites, and perform industrial espionage to steal a country's sensitive information. Furthermore, state hackers are the most dangerous threats to SCADA systems, as these hackers get all of their resources and funds from the government. The government can hire the best hackers and provide them the money, infrastructure, and facilities to create zero-day exploits, which can be used against an enemy country for theft of nuclear technology, intelligence collection, etc. Though zero-day attacks are single-use weapons, they can cause terrible damage to a country's infrastructure, economy, and systems, even when used singly.

h. Terrorist (Non-state Armed Groups)

A terrorist is a widely-known type of attacker. Looking into the history of cyber attacks, no evidence can be found of a terrorist attack on SCADA systems; however, the situation will not remain so in future. According to former U.S. President George W. Bush, terrorists can get into a network with the intent to attack a nuclear facility, and the consequences of getting into the network could be unbearable [97]. The motivations of terrorists vary: sometimes they want to collect intelligence, build access points in facility for later use, spread fear among the public, or take revenge on the government. They may use scripts and home-grown tools to execute an attack, and may employ former/current employees to get inside information. Moreover, some terrorist groups have acquired significant capabilities to use social media as a means of hiring people for hacking.

5.4 STRIDE Threat Modelling

This sub-section performs threat modelling on the I&C systems of a NPP based on the vulnerabilities discussed above. Microsoft's STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) methodology, which describes an adversary's objectives, is used for threat modelling [93]. Table 2 explains threat categories, along with the corresponding vulnerabilities and the types of adversaries that can transform the particular threat into an attack.

Table 2: Threat categories with corresponding attacker types and vulnerability categories

Threat Category	Definition	Attacker Type	Vulnerability Category
Spoofing	The attacker gets illegal access to the I&C systems or any specific module, with the purpose to misuse or disrupt them, either by spoofing identity or authentication information of the operators or the systems. If spoofed, the systems performing critical functions, such as SAS, PACS, and PS, which control the plant equipment, can cause the worst damage.	• Covert Agent • Disgruntled Ex-Employee • Non-State Hacker • Terrorist	• No or Incorrect Input validation • Improper Authentication • Improper Authorization
Tampering (Integrity threat)	This refers to the unauthorized modification of data, i.e. data being exchanged (authentication credentials, status or parameter values, issued commands, sensor values, etc.), data stored in databases (operator information, plant equipment status, operation status, etc.), or data being processed or generated at various points by the equipment (temperature, feedback, water level, speed, etc.)	• Militant Opponent • Recreational Hacker • Terrorist	• Improper Authentication • Improper Authorization • Improper Software Configuration & Management
Repudiation	An operator or a spoofed system may deny performing certain actions or operations on plant systems, e.g. a plant operator changes the values of temperature and water level of a plant but later denies it.	• Disgruntled Current Employee	• Auditing and logging
Information Disclosure	Critical plant information may be maliciously released, such as system login details and plant workflow or documentation, through the exploitation of certain vulnerabilities.	• Covert Agent • Disgruntled Current Employee • Non-State Hacker • Disgruntled Ex-Employee	• Sensitive Data • Improper Authentication • Improper Authorization • Improper Software Configuration &

		• Militant Opponent	Management
Denial of Service (DoS)	The attacker may overwhelm I&C systems with repetitive similar requests, resulting in a DoS attack due to the unavailability of required components, e.g. target sensors or actuators at Level 0, by sending them many requests to provide sensed data. The request can be sent by maliciously installed malware or by a system connected through a hidden internet connection. This could result in service unavailability.	• Recreational Hacker • Terrorist	• Improper Software Configuration & Management • No or Incorrect Input Validation • Lack of Backup Facilities
Elevation of Privilege	A malicious insider (disgruntled employee) obtains illegal access to operations that control core plant equipment by exploiting vulnerabilities that exist in the plant systems. An attacker may stop core functions or delete or modify parameter values using the elevated privileges of a higher security level user account.	• Disgruntled Current Employee	• Improper Authentication • Improper Authorization

Figure 4 shows the hierarchy of threats that exists in I&C systems, and that could be transformed into attacks if vulnerabilities are exploited. NPP threats are broken down into the following categories using STRIDE methodology:

- *'Spoofing'* is a threat in which an attacker or a malicious program disguises itself as a legitimate entity, thereby gaining an illegitimate advantage. In the case of a NPP, this illegal access can result in disruption or misuse of I&C systems. Spoofing is further sub-categorized into *'system'* and *'personnel'* spoofing. While the former focuses on spoofing the credentials of an I&C system, the latter is concerned with gaining access to personnel credentials such as passwords and tokens, and then masquerading as a known person. There are a number of ways to achieve these types of spoofing. Session hijacking is common for personnel spoofing, where an attacker intercepts an on-going session and tries to connect to the receiver as a legitimate entity. Injecting malicious code in the form of scripts into a web browser is a well-known method of system spoofing. Other ways to spoof credentials include social engineering (observing and/or manipulating user or system behaviour and activities) and incorrect input (SQL injection).
- *'Tampering'* involves changing legitimate data, thus compromising the integrity of the system. The data can be tampered with online (in transit) or offline (at rest). An attacker can easily compromise data integrity if he finds any improper configuration together with a lack of integrity checking within a system.
- *'Repudiation'* is caused when a system lacks proper auditing and logging mechanisms. An attacker can bypass logging mechanisms, steal keys via social

engineering, or create fake digital signatures to deny the illegitimate actions. As an example, an operator or a spoofed system at a NPP can deny performing certain actions or operations on plant systems, e.g. a plant operator changes the values of temperature and water level of a plant, but later denies doing so.

- *'Information disclosure'* occurs when information is not properly protected. The information can be of any form – for example, system/user credentials, network packets, source code, files, or a database. Through this threat, critical plant information can be maliciously released through the exploitation of vulnerabilities such as improper software configurations, authorization mechanisms, or authentication mechanisms.
- In a *'Denial of Service (DoS)'*, an attacker can overwhelm I&C systems with thousands of repetitive requests, resulting in the unavailability of required components. The requests can be sent by maliciously installed malware or by a system connected through a hidden internet connection. DoS commonly occurs when a system lacks a backup facility and has no input validation methods.
- An *'elevation of privileges'* is a threat which could result in the abuse of legitimate access. A malicious insider (disgruntled employee) having legitimate access to resources or operations may modify his account permissions to allow him additional accesses to systems to which he might not normally have access. He could then abuse his privileges by stopping core functions or deleting or modifying parameter values. The hierarchy is further explained via attack trees mentioned below.

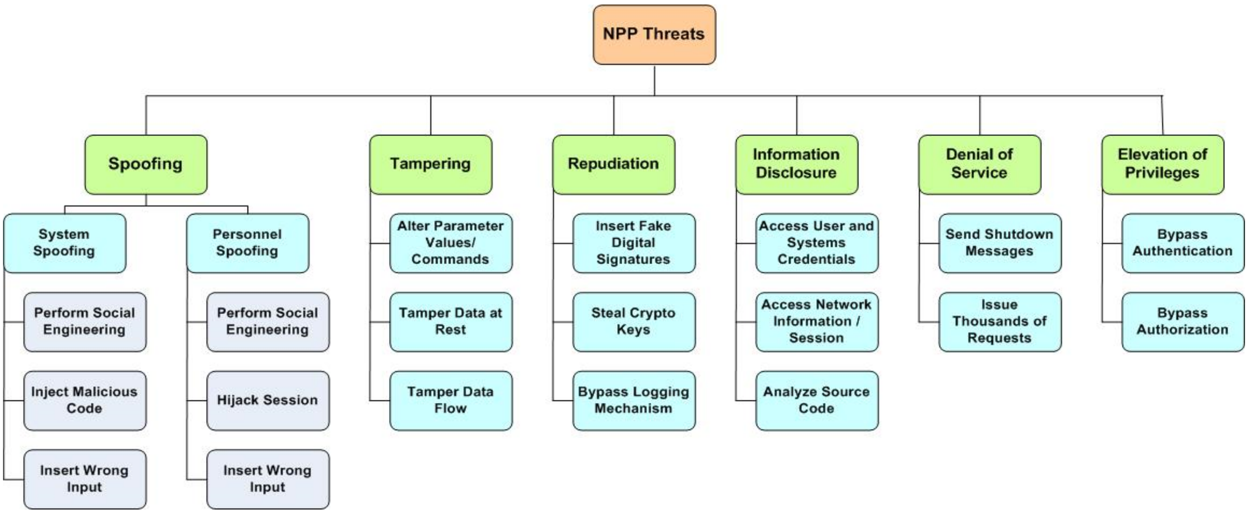

Figure 3: NPP I&C Systems Threats Hierarchy

5.4.1 Attack Trees

There are a number of attack graphing tools that can be used to model attacks [94-96]. Attack trees are suitable for several reasons: i) they describe the steps of a successful attack in a more structured way than natural language; ii) the model of an attack tree is easy to understand, even for beginners; and iii) attack trees follow a hierarchical representation, in which higher-level attack goals are broken down into sub-goals, until the desired refinement level is achieved.

In order to perform a threat modelling on I&C systems of a NPP, Amenaza SecurITree [91] is used for creating attack paths and trees, using STRIDE. The SecurITree application provides a tool to assess threats from an adversary's perspective. It uses an attack tree method for assessing how an asset can be attacked by an attacker, what harm he or she does with an attack, and what measures need to be taken to become immune to that attack. The attack trees (Figures 5-10) given below, illustrate how an attack can possibly be launched through a series of steps, beginning with a small attack goal or vulnerability. Thusly, each category of threats identified in the above section can be executed as attacks through a number of steps, i.e. exploiting a number of possible vulnerabilities. In Figures 5-10, the green shape (wide curve) represents “OR”, blue (flat-bottomed curve) represents “AND”, and grey (rectangular) represents the leaf nodes.

1. **Spoofing:** Figure 5 shows the ways an attacker can spoof a NPP personnel identity to perform malicious activities, such as issuing commands to decrease the water level or temperature, to increase the speed of centrifuges, to shut down the plant, to turn off the protection and alarm systems, etc. Similarly, sensors or actuators could also be spoofed to send incorrect parameter values to PACS and RCSL about temperature, water level, and speed of the plant. The spoofing could be performed by stealing personnel credentials. In addition, an attacker can exploit the vulnerability of incorrect input validation to steal the unique request IDs assigned to operators and I&C systems, using brute force or network eavesdropping techniques and then reusing the eavesdropped parameters to issue fake requests.

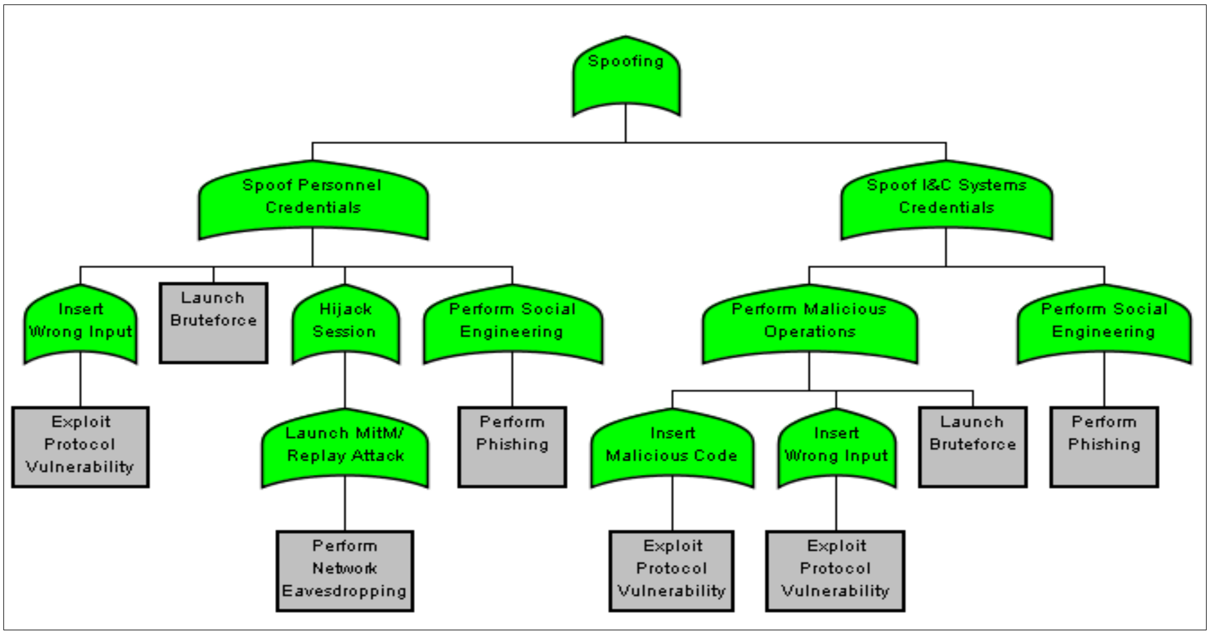
Spoofing
Spoof Personnel Credentials
Spoof I&C Systems Credentials
Insert Wrong Input
Launch Bruteforce
Hijack Session
Perform Social Engineering
Perform Malicious Operations
Perform Social Engineering
Exploit Protocol Vulnerability
Launch MitM/ Replay Attack
Perform Phishing
Insert Malicious Code
Insert Wrong Input
Launch Bruteforce
Perform Phishing
Perform Network Eavesdropping
Exploit Protocol Vulnerability
Exploit Protocol Vulnerability

Figure 4: Attack Tree of Spoofing Threat in NPP I&C Systems

2. **Tampering:** Tampering is the unauthorized modification of data, which could be done by altering data flow, parameters, data sent and received from operators or systems, or data at rest. Data flowing between different I&C systems is vulnerable to manipulation by adversaries. The adversaries could capture the parameters being exchanged between various I&C systems, which are critical for plant operations. These parameters, such as speed, water level, and temperature, are provided by sensors or actuators to the PACS,

which in turn sends them to the HMIs where they could be modified by the attacker when in transit. Similarly, commands issued by controllers or operators could be tampered with by inserting incorrect values into the network packet. These actions could be done if the HMIs, PACS, or sensors have misconfigured software installations or improper authentication or authorization. An attacker can perform man-in-the-middle attacks to exploit these vulnerabilities. The data stored in the system database could also be modified through the same vulnerabilities, or additionally, by inserting malware to corrupt the data. The attack tree is illustrated in Figure 6.

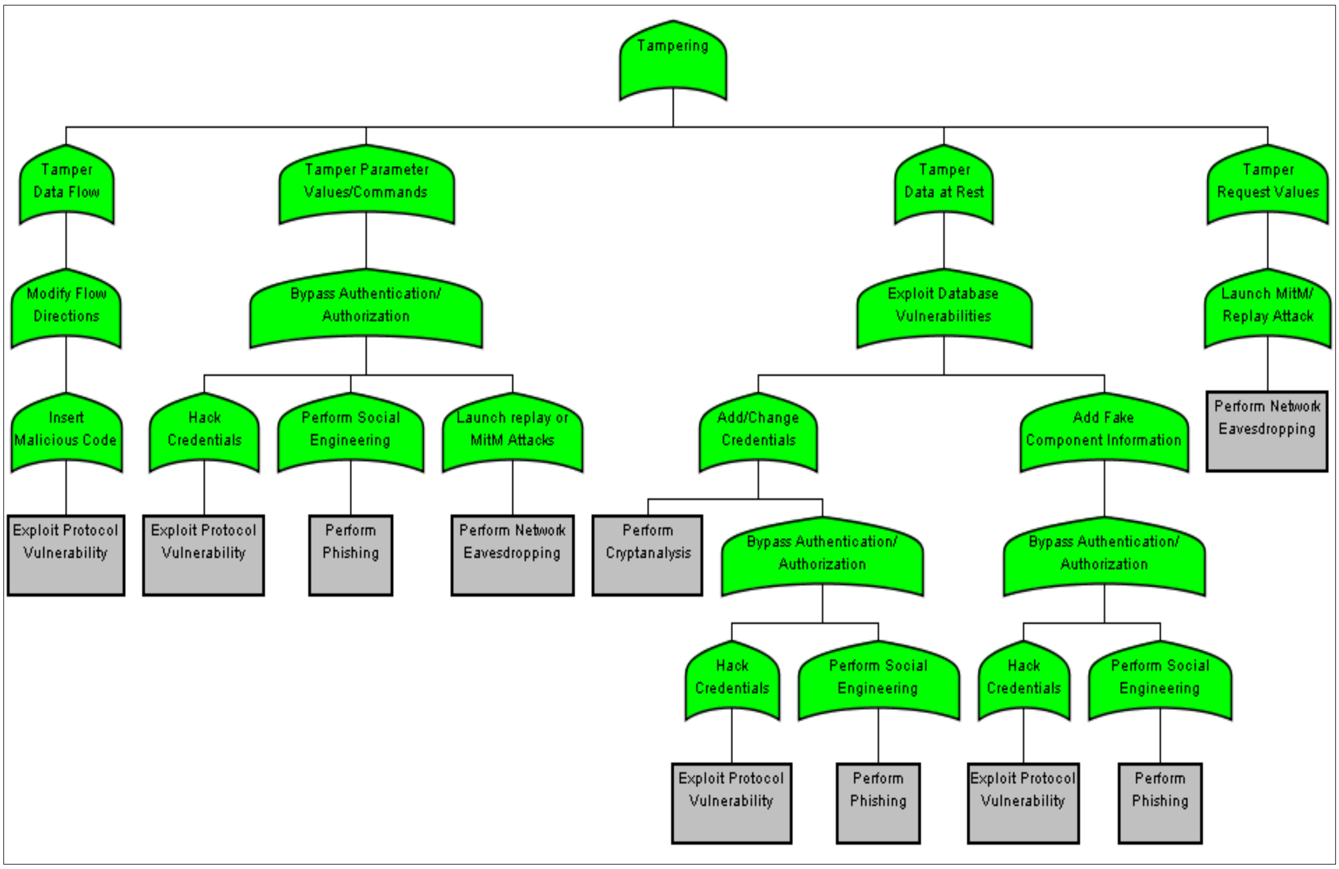
Tampering
Tamper Data Flow
Tamper Parameter Values/Commands
Tamper Data at Rest
Tamper Request Values
Modify Flow Directions
Bypass Authentication/ Authorization
Exploit Database Vulnerabilities
Launch MitM/ Replay Attack
Insert Malicious Code
Hack Credentials
Perform Social Engineering
Launch replay or MitM Attacks
Add/Change Credentials
Add Fake Component Information
Perform Network Eavesdropping
Exploit Protocol Vulnerability
Exploit Protocol Vulnerability
Perform Phishing
Perform Network Eavesdropping
Perform Cryptanalysis
Bypass Authentication/ Authorization
Bypass Authentication/ Authorization
Hack Credentials
Perform Social Engineering
Hack Credentials
Perform Social Engineering
Exploit Protocol Vulnerability
Perform Phishing
Exploit Protocol Vulnerability
Perform Phishing

Figure 5: Attack Tree of Tampering Threat in NPP I&C Systems

3. **Repudiation:** As already mentioned, repudiation refers to the ability of users, legitimate or otherwise, to deny that they performed specific actions. An adversary can easily deny performing malicious actions on a NPP due to the absence of audit information and digital signatures. Thus, it becomes difficult to counter the repudiation attack. As a result, an attacker could insert false information into a network packet, such as an incorrect parameter value, or send a fake command to start or cancel a specific plant service. An attack tree is given in Figure 7. Vulnerabilities in internet protocols such as HTTP or TCP/IP might allow an attacker to inject a malicious script within I&C system module or components. The vulnerability could be lack of input validation, which an attacker could exploit with a SQL injection attack. Successful execution of this attack will allow an attacker to hijack sensitive system credentials such as passwords or tokens. Once an attacker has access to these credentials, he or she can easily bypass deployed authentication and authorization

mechanisms[8]. Illegitimate access to I&C systems via legitimate credentials means that an attacker can send any kind or type of commands to NPP components such as sensors or temperature modules at Level 0. There is no way to check if the command or data is really sent by a spoofed or a real person. Similarly, there is no method to detect repudiation when a disgruntled employee sends a request to change the values of NPP equipment.

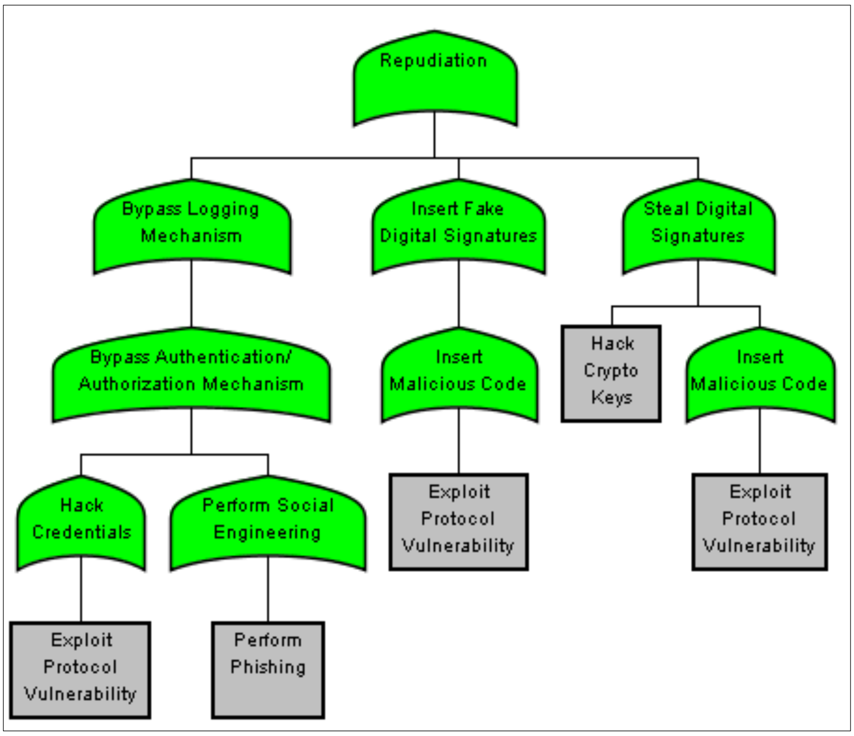
Repudiation
Bypass Logging Mechanism
Insert Fake Digital Signatures
Steal Digital Signatures
Bypass Authentication/ Authorization Mechanism
Insert Malicious Code
Hack Crypto Keys
Insert Malicious Code
Hack Credentials
Perform Social Engineering
Exploit Protocol Vulnerability
Exploit Protocol Vulnerability
Exploit Protocol Vulnerability
Perform Phishing

Figure 6: Attack Tree of Repudiation Threat in NPP I&C Systems

4. **Information Disclosure:** Information disclosure is the undesired exposure of the sensitive data of any application, service, or software. A person with no or low privileges can view the sensitive information or analyse the data flowing over the network. Figure 8 shows the attack tree for information disclosure. Information within the system is generally exposed through various ways; for example, the data is usually added by programmers in hidden fields of forms, which can easily be viewed and manipulated by an attacker. Comments are usually added within the web page code, which reveal information about the system and the functions it is performing. These comments could lead to the revealing of critical information regarding modules, system exception handling mechanisms, etc., which could be very useful for the attacker. Moreover, cookies could also be accessed through the inspection of URLs as well as monitoring of data flow between web pages through network eavesdropping. Hidden parameters in web pages could be viewed by inspecting the web page code. Also, user credentials could be accessed by eavesdropping. Similarly, data request or command parameters could be viewed as well, since URLs as proper filtering mechanisms are not

[8] The most deployed authentication and authorization methods such as role-based access controls, attribute-based access controls (ABAC), password-based authentication, etc., have no way of detecting the spoofed credentials.

implemented in I&C systems. The software used by I&C systems has no such mechanism that could guarantee the prevention of such an involuntary exposure of information.

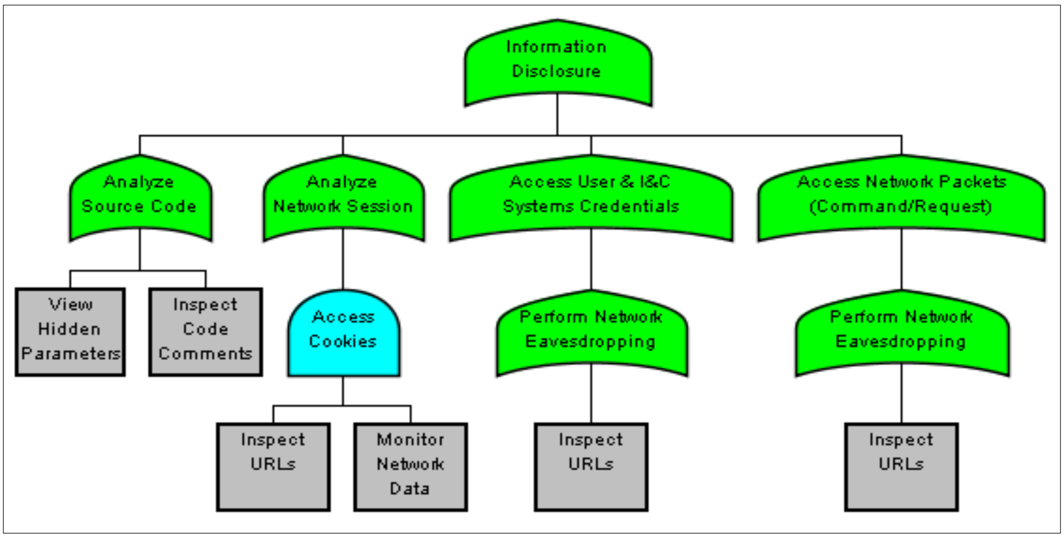

Figure 7: Attack Tree of Information Disclosure Threat in NPP I&C Systems

5. **Denial of Service (DoS):** The most important security feature for a NPP is constant availability of all services running within and between systems. This feature helps the core operations of a NPP to smoothly produce electricity. Therefore, DoS attacks can have a disastrous effect on NPP operations as well as the NPP surroundings. Figure 9 illustrates the attack tree for a DoS attack. Such attacks could be launched on a NPP by flooding I&C systems with requests using bots that generate automated requests. An attacker may also insert malicious code that takes control of all systems. Similarly, PS or SAS could be spoofed to send a large number of requests, which would overwhelm the sensors and actuators. This could again be accomplished by installing bots within the network. The DoS attack could also be done by tampering with parameters, such as increasing the water level, temperature, or speed of the centrifuges. This tampering might exhaust the equipment and eventually shutdown the plant. An attacker could also perform SQL injection attacks and cross site scripting attacks to insert malicious data and disrupt the plant’s operation.

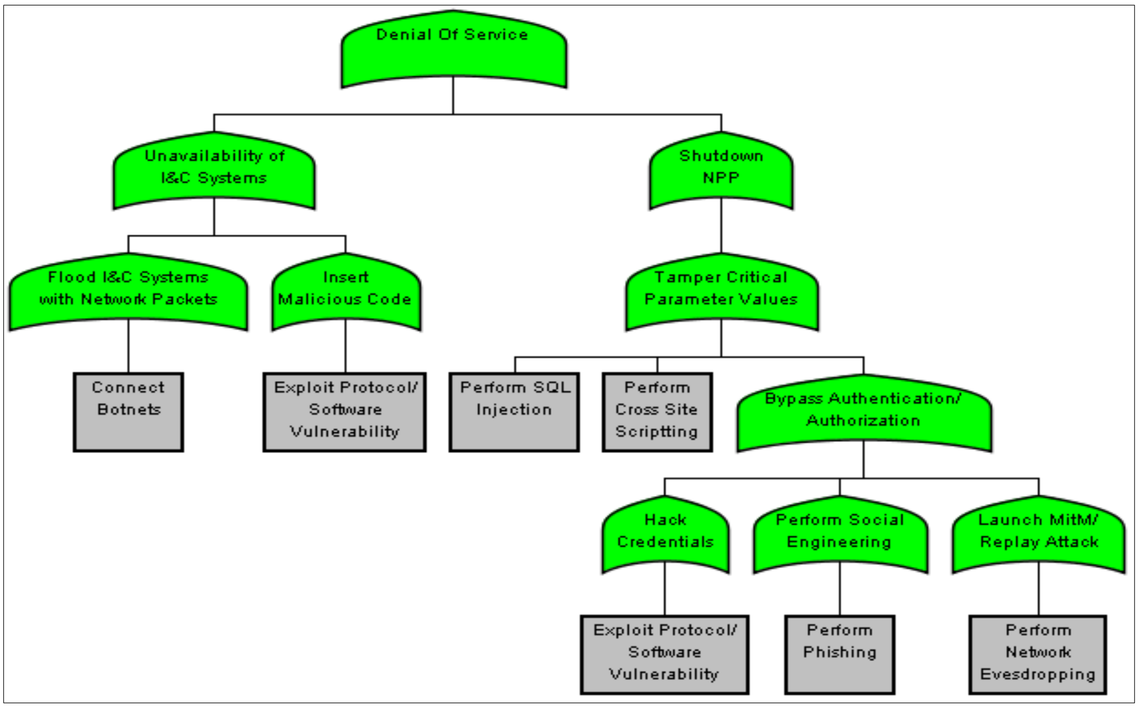
Denial Of Service
Unavailability of I&C Systems
Shutdown NPP
Flood I&C Systems with Network Packets
Insert Malicious Code
Tamper Critical Parameter Values
Connect Botnets
Exploit Protocol/ Software Vulnerability
Perform SQL Injection
Perform Cross Site Scriptting
Bypass Authentication/ Authorization
Hack Credentials
Perform Social Engineering
Launch MitM/ Replay Attack
Exploit Protocol/ Software Vulnerability
Perform Phishing
Perform Network Evesdropping

Figure 8: Attack Tree of Denial of Service Threat in NPP I&C Systems

6. **Elevation of Privileges:** Elevation of privilege occurs when a user with limited privileges gains unauthorized access to a system or resources via illegal methods. An attack tree is shown in Figure 10, which illustrates that an attacker can maliciously access higher privileges to take control of a highly sensitive component or a module by inserting a malicious script or by spoofing the system already deployed. Brute-force is a well-known attack where a powerful software could be used to generate a large number of consecutive guesses to gain access to the system or to the system credentials. Man-in-the-Middle (MitM) is another type of attack which can intercept network traffic to steal sensitive information, for use later in bypassing authentication and authorization mechanisms. The success chances of this type of attack are good when traffic is not encrypted and is sent in plaintext form.

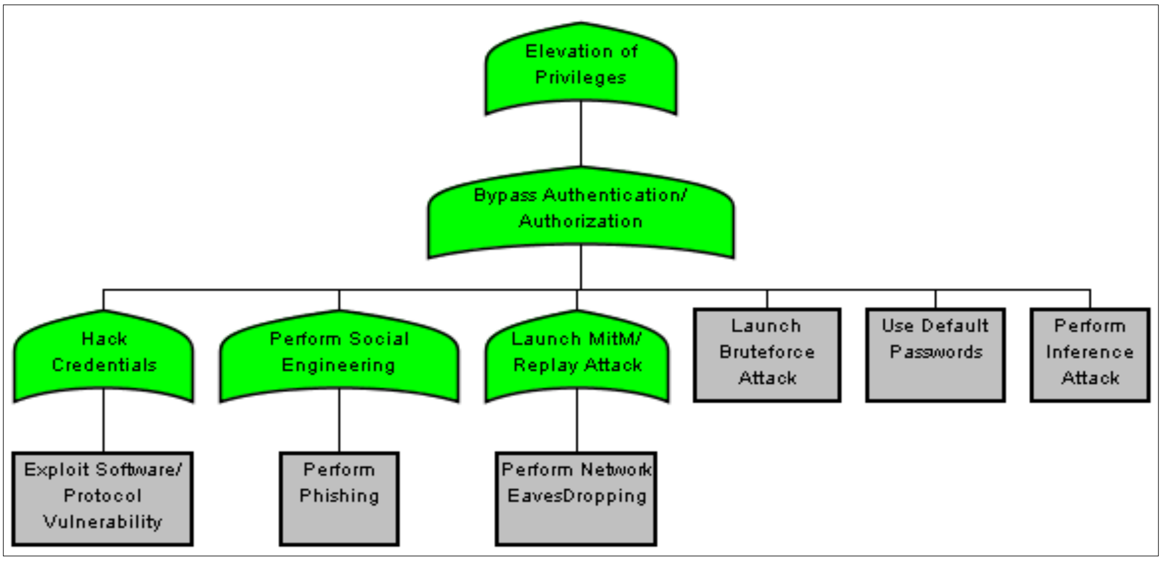
Elevation of Privileges
Bypass Authentication/ Authorization
Hack Credentials
Perform Social Engineering
Launch MitM/ Replay Attack
Launch Bruteforce Attack
Use Default Passwords
Perform Inference Attack
Exploit Software/ Protocol Vulnerability
Perform Phishing
Perform Network EavesDropping

Figure 9: Attack Tree of Elevation of Privilege Threat in NPP I&C Systems

6. Conclusion

Nuclear regulatory authorities are still trying to understand cyber risks and are looking for mechanisms to adequately prevent attacks on security. This research work has initially explored many unanswered questions while demystifying cybersecurity challenges for NPPs, i.e. how cyber evolution has created vulnerabilities in nuclear facilities, which have been a subject of cyber-nuclear sabotage. Following this, threat modelling was performed on a generic I&C architecture of a NPP using STRIDE methodology to analyse possible threats and vulnerabilities from the adversary's perspective. The presented threat methodology is also enhanced through the identification of NPP security requirements and vulnerabilities, along with the discussion on NPP attackers' profiles.

The work presented in this paper can go in various future research directions. The threat model discussed in section 5 does not reflect a real NPP scenario. Therefore, there is a need to formulate threat models through STRIDE or a related threat methodology in a real NPP scenario. Moreover, we plan to propose a holistic Information Security Risk Management (ISRM) taxonomy for NPPs and then to evaluate existing NPP ISRM methods using that taxonomy. The purpose of focusing on ISRM is to help the NPP industry select the most suitable ISRM method for their security requirements, and also to identify areas that have not been addressed but may still be important for NPPs. Therefore, ISRM is one of the ways through which NPPs can detect and fix security loopholes prior to any cyber attacks on a facility.

7. Acknowledgments

I am incredibly grateful for all the funding and financial assistance provided by Civilian Research & Development Foundation (CRDF) Global under the Nonproliferation Studies Scholarship Program. A special thanks to my supervisor at The George Washington University, Professor Lance Hoffman, for his continuous support in the research work. Dr. Hoffman was always there to listen and to give advice. He taught me how to express my ideas and also showed me different ways to approach a research problem. I also thank my other two supervisors from Sandia National Laboratories (SNL), Eric Andrew Wallace and Adriane C. Littlefield with whom I explored the ideas, requirements, and development of threat models. I would also like to pay my gratitude to National University of Sciences & Technology (NUST) and NUST School of Electrical Engineering & Computer Science (SEECS) to grant five months leave and allow me to work with GWU and SNL as a visiting scholar.

I thank George Washington University (GWU) and its School of Engineering and Applied Science (SEAS) for hosting and facilitating me in the administration process. My special thanks is extended to GWU's Cyber Security Policy and Research Institute (CSPRI) for providing technical guidance, valuable feedback, and constant encouragement during the course of this research. Last but not the least, I would like to thank Ms. Janice Rosado for her invaluable suggestions on paper structuring and also proofreading the paper in every iteration.

8. References

[1] Holt, Mark, and Anthony Andrews. *Nuclear Power Plant Security and Vulnerabilities (CRS Report No. RL34331)*. Washington, DC: Congressional Research Service, 2014. Last accessed July 31, 2016. https://www.fas.org/sgp/crs/homesec/RL34331.pdf

[2] Berger, Eva M. "The Chernobyl Disaster, Concern about the Environment, and Life Satisfaction." *Kyklos* 63, no. 1 (February 2010): 1-8. doi: 10.1111/j.1467-6435.2010.00457.x.

[3] Ohnishi, Takeo. "The Disaster at Japan's Fukushima-Daiichi Nuclear Power Plant after the March 11, 2011 Earthquake and Tsunami, and the Resulting Spread of Radioisotope Contamination." *Radiation Research* 177, no. 1 (January 2012): 1-14. doi: 10.1667/RR2830.1

[4] Baylon, Caroline, Roger Brunt, and David Livingstone. *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*. London: The Royal Institute of International Affairs, Chatham House, 2015. Last accessed July 31, 2016. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf

[5] Falliere, Nicolas, Liam O Murchu, and Eric Chien. "W32. stuxnet dossier." Symantec Corp. February 11, 2011. Last accessed July 31, 2016. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[6] Ellefsen, Ian, and Sebastiaan Von Solms. "Critical Information Infrastructure Protection in the Developing World." In *Critical Infrastructure Protection IV*, edited by Tyler Moore and Sujeet Shenoi, 29-40. Berlin, Germany: Springer Berlin Heidelberg, 2010. doi: 10.1007/978-3-642-16806-2_3.

[7] Dacey, Robert F. *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*. (GAO-04-628T). Washington, DC: U.S. Government Accountability Office, 2004. Last accessed July 31, 2016. http://www.gao.gov/products/GAO-04-628T

[8] Control Systems Security Program, National Cyber Security Division. *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*. Washington, DC: Department of Homeland Security, 2009. Last accessed July 31, 2016. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

[9] Miller, Bill and Dale Rowe. "A survey SCADA of and critical infrastructure incidents." In *RIIT '12 Proceedings of the 1st Annual conference on Research in information technology*, 51-56. New York: ACM, 2012. doi: 10.1145/2380790.2380805.

[10] Nicholson, Andrew, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke. " SCADA security in the light of Cyber-Warfare." *Computers & Security* 31, no. 4 (June 2012): 418-436. doi: 10.1016/j.cose.2012.02.009.

[11] Tabansky, Lior. "Critical Infrastructure Protection against Cyber Threats." *Military and Strategic Affairs* 3, no. 2 (November 2011): 61-78. Last accessed January 3, 2016. http://www.inss.org.il/uploadimages/Import/(FILE)1326273687.pdf

[12] Baker, Stewart, Shaun Waterman, and George Ivanov. "In the Crossfire: Critical Infrastructure in the Age of Cyber War." McAfee. 2010. Last accessed January 3, 2016. https://resources2.secureforms.mcafee.com/LP=2733

[13] Stouffer, Keith, Joe Falco, and Karen Scarfone. *Guide to Industrial Control Systems (ICS) Security* (NIST 800-82). Washington, DC: National Institute of Standards and Technology, 2011. Last accessed January 3, 2016. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[14] USNRC Technical Training Center. "Nuclear Power for Electrical Generation." *Reactor Concepts Manual*. Washington, DC: U.S. Nuclear Regulatory Commission, 2012. Last accessed January 3, 2016. http://www.nrc.gov/reading-rm/basic-ref/students/for-educators/01.pdf

[15] *Nuclear Fuel Cycle Information System: A Directory of Nuclear Fuel Cycle Facilities* (IAEA-TECDOC-1613). Vienna, Austria: International Atomic Energy Agency, 2009. Last accessed January 3, 2016. http://www-pub.iaea.org/mtcd/publications/pdf/te_1613_web.pdf

[16] Dudenhoeffer, Donald. "IAEA Information and Computer Security." Office of Nuclear Cyber Security Programme, International Atomic Energy Agency. May 21, 2013. Last accessed January 3, 2016. https://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-22-05-24-TWG-NPE/day-2/4.cyber_security_introduction.pdf

[17] Hagestad II, William. *21st Century Chinese Cyberwarfare*. Cambridgeshire, United Kingdom: IT Governance Ltd. 2012. Last accessed January 25, 2016. http://www.itgovernance.co.uk/shop/p-319-21st-century-chinese-cyberwarfare.aspx

[18] Follarth, Erich and Holger Stark. "The Story of Operation Orchard: How Israel Destroyed Syria's Al Kibar Nuclear Reactor." *Spiegel Online 11*, November 2, 2009. Last accessed January 3, 2016. http://www.spiegel.de/international/world/the-storyof-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html

[19] O'Gorman, Jim, Devon Kearns, and Mati Aharoni. *Metasploit: The Penetration Tester's Guide.* San Francisco, USA: No Starch Press. pp. 328 July 25, 2011. https://www.nostarch.com/metasploit

[20] Nortan-Taylor, Richard and Julian Borger. "Chinese Cyber-Spies Penetrate Foreign Office Computers." *The Guardian* 4, February 5, 2011. Last accessed January 3, 2016. http://www.theguardian.com/world/2011/feb/04/chinese-super-spies-foreign-officecomputers

[21] Morton, Chris. "Stuxnet, Flame and Duqu – the Olympic Games." *A Fierce Domain: Conflict in Cyberspace 1986 to 2012.* Edited by Jason Healey, 219-221. Arlington, VA: Cyber Conflict Studies Association, 2013.

[22] Russia Today. "U.S. Nuclear Weapons Researchers Targeted with Internet Explorer Virus." May 7, 2013. Last accessed January 3, 2016. http://rt.com/usa/attack-department-nuclear-internet-955/

[23] Farnsworth, Timothy. "Study sees cyber risk for U.S. arsenal." Arms Control Association, April 2, 2013. Last accessed January 3, 2016. http://www.armscontrol.org/act/2013_04/Study-Sees-Cyber-Risk-for-US-Arsenal

[24] Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power.* Random House, New York: Broadway Books, 2013.

[25] The Associated Press. "Iran says nuclear equipment was sabotaged." *New York Times,* September 22, 2012, Last accessed January 3, 2016.

http://www.nytimes.com/2012/09/23/world/middleeast/iran-says-siemens-tried-to-sabotage-its-nuclear-program.html?_r=0

[26] Futter, Andrew. "Hacking the Bomb: Nuclear Weapons in the Cyber Age." In *International Studies Annual Conference*, New Orleans: ISA February 2015. Last accessed January 3, 2016. http://www2.le.ac.uk/departments/politics/people/afutter/copy_of_AFutterHackingtheBombISAPaper2015.pdf

[27] Virtual Criminology Report 2009. *Virtually Here: The Age of Cyber Warfare.* Santa Carla, United States of America: McAfee. 2009. Last accessed January 3, 2016. http://img.en25.com/Web/McAfee/VCR_2009_EN_VIRTUAL_CRIMINOLOGY_RPT_NOREG.pdf

[28] BBC News. "Major Cyber Spy Network Uncovered." March 29, 2009. Last accessed January 3, 2016. http://news.bbc.co.uk/1/hi/7970471.stm

[29] Barlow, Jeffery. *Inside Cyber Warfare: Mapping the Cyber Underworld*. United States of America: O'Reilly Media, 2nd Edition, 2011. http://shop.oreilly.com/product/0636920021490.do

[30] Shodan. Last accessed Jan 4, 2016. https://www.shodan.io/

[31] Kesler, Bent. "The Vulnerability of Nuclear Facilities to Cyber Attack." *Strategic Insights* 10, no. 1, (2011), 15–25. http://calhoun.nps.edu/handle/10945/25465

[32] Motta Pires, Paulo S and Luiz Affonso H.G. Oliveira. "Security Aspects of SCADA and Corporate Network Interconnection: An Overview." In: *International Conference on Dependability of Computer Systems*, Szklarska Poreba : IEEE, May 2006. p. 127-134. doi: 10.1109/DEPCOS-RELCOMEX.2006.46

[33] Myers, Robbie. "Attacks on TCP/IP Protocols." Last accessed Jan 4, 2016. http://www.utc.edu/center-information-security-assurance/pdfs/course-paper-5620-attacktcpip.pdf

[34] Shubert, Atika. "Cyberwarfare: A Different Way to Attack Iran's Reactors." CNN, November 8, 2011. Last accessed July 30, 2016. http://edition.cnn.com/2011/11/08/tech/iran-stuxnet/

[35] Symantec. "Dragonfly: Cyber Espionage Attacks Against Energy Suppliers." Symantec Corp. version 1.21. Mountain View, California. July 7, 2014. Last accessed July 31, 2016. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf

[36] O'Shea, Kevin. "Examining the RPC DCOM Vulnerability: Developing a Vulnerability-Exploit Cycle." SANS Institute. September 3, 2003. https://www.sans.org/reading-room/whitepapers/threats/examining-rpc-dcom-vulnerability-developing-vulnerability-exploit-cycle-1220

[37] Fernandez, John D. and Andres E. Fernandez. "SCADA Systems: Vulnerabilities and Remediation." *Journal of Computing Sciences* 20, no. 4 (April 2005): 160-168. http://dl.acm.org/citation.cfm?id=1047872

[38] Abraham. "Final report on the August 14th blackout in the United States and Canada." 2003. Last accessed July 30, 2016. https://reports.energy.gov/BlackoutFinalWeb.pdf

[39] The Hitchhiker's Guide to the Galaxy. “The Chernobyl Disaster.” January 25, 2006. Last accessed July 30, 2016. http://h2g2.com/edited_entry/A2922103

[40] Breidthardt, Annika, Andreas Rinke and Hans-Edzard Busemann. “German Government wants Nuclear Exit by 2022 at latest.” Reuters, May 29, 2011. Last accessed July 30, 2016. http://www.reuters.com/article/germany-nuclear-idUSLDE74T00A20110530

[41] National Transportation Safety Board. *Pipeline Rupture and Subsequent Fire in Bellingham, Washington (*NTSB/PAR-02/02). Washington DC: Pipeline Incident Report. 1999. Last accessed July 30, 2016. http://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf

[42] Poulsen, Kevin. “Slammer Worm Crashed Ohio Nuke Plant Net.” The Register, August 20, 2003. Last accessed July 30, 2016. http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke

[43] Niland, M. “Computer Virus brings down Train Signals.” InformationWeek, August 20, 2003. Last accessed July 30, 2016. http://www.informationweek.com/computer-virus-brings-down-train-signals/d/d-id/1020446?

[44] Nuclear Regulatory Commission. *NRC Information Notice: 2007e15: Effects of Ethernet-based, Non-Safety related Controls on the Safe and Continued Operation of Nuclear Power Stations.* Washington DC: Office of Nuclear Reactor Regulation, 2007. Last accessed July 30, 2016. http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf

[45] Krebs, Brian. “Cyber Incident Blamed for Nuclear Power Plant Shutdown.” The Washington Post, June 5, 2008. Last accessed July 30, 2016. http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html

[46] Gorman, Siobhan. “Electricity Grid in U.S. Penetrated by Spies.” The Wall Street Journal, April 8, 2009. Last accessed July 30, 2016. http://online.wsj.com/article/SB123914805204099085.html

[47] Bukharin, Oleg. “Upgrading Security at Nuclear Power Plants in the Newly Independent States.” *The Nonproliferation Review* 4*,* no.2, (1997): Taylor & Francis, 28-39. doi: 10.1080/10736709708436663

[48] Nuclear Threat Initiative. “Russian Warns of Cyber Terror Against Nuclear Sites.” November 9, 2006. Last accessed July 30, 2016. http://www.nti.org/gsn/article/russian-warns-of-cyber-terror-against-nuclear-sites/

[49] Smith, Tony. “Hacker Jailed for Revenge Sewage Attacks.” The Register, October 21, 2001. Last accessed July 30, 2016. http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

[50] Goodin, Dan. “Elecrical Supe Charged with Damaging California Canal System.” The Register, November 30, 2007. Last accessed July 30, 2016. http://www.theregister.co.uk/2007/11/30/canal_system_hack/

[51] Matrosov, Aleksandr, Eugene Rodionov, David Harley, and Juraj Malcho. “Stuxnet under the Microscope.” ESET LLC. September 2010. Last accessed July 30, 2016. http://www.welivesecurity.com/media_files/white-papers/Stuxnet_Under_the_Microscope.pdf

[52] Zetter, Kim. “How Digital Detectives Deciphered Stuxnet, The Most Menacing Malware in History.” WIRED, November 7, 2011. Last accessed July 30, 2016. http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1

[53] Leyden, John. “Chinese Cyberspies’ Target Energy Giants.” The Register, February 10, 2011. Last accessed July 30, 2016. http://www.theregister.co.uk/2011/02/10/night_dragon_cyberespionage/

[54] Kim, Sohee and Meeyoung Cho. “South Korea Prosecutors Investigate Data Leak at Nuclear Power Plants.” Reuters, December 21, 2014. Last accessed July 30, 2016. http://www.reuters.com/article/us-southkorea-nuclear-idUSKBN0JZ05120141221

[55] Iversen, Wes. “Hackers Step Up Scada Attacks.” Automation World. October 12, 2004. Last accessed July 30, 2016. http://www.automationworld.com/webonly-898

[56] International Atomic Energy Agency (IAEA). Last accessed July 30, 2016. https://www.iaea.org/

[57] National Institute of Standards and Technology (NIST). Last accessed July 30, 2016. www.nist.gov

[58] World Institute for Nuclear Security (WINS). Last accessed July 30, 2016. https://www.wins.org/

[59] “Radiation Effects.” IEEE Nuclear & Plasma Sciences Society. Last accessed July 30, 2016. http://ieee-npss.org/technical-committees/radiation-effects/

[60] Stoneburner, Gary., Alice Y. Goguen, and Alexis Feringa. *SP 800-30. Risk Management Guide for Information Technology Systems*. Technical Report. Gaithersburg, MD, United States: National Institute of Standards & Technology. 2002. http://dl.acm.org/citation.cfm?id=2206240

[61] Ross, Ron. *Guide for the Security Certification and Accreditation of Federal Information Systems.* Diane Pub Co, 2004. http://dl.acm.org/citation.cfm?id=1204602

[62] Aroms, Emmanuel. *NIST Special Publication 800-39 Managing Information Security Risk.* Paramount, California: National Institute of Standards and Technology (NIST), 2012. http://dl.acm.org/citation.cfm?id=2331278

[63] Stouffer, Keith, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams, and Adam Hahn. “Guide to Industrial Control Systems (ICS) Security.” *NIST Special Publication* 800, no. 82, Revision 2 Draft (May 2014). http://www.gocs.com.de/pages/fachberichte/archiv/164-sp800_82_r2_draft.pdf

[64] *NIST Cybersecurity Framework: ISA99 Response to Request for Information.* North Carolina: International Society of Automation (ISA), April 5, 2013. Last accessed July 30, 2016. http://csrc.nist.gov/cyberframework/rfi_comments/040513_international_society_automation.pdf

[65] IAEA Nuclear Security Series No. 17. *Computer Security at Nuclear Facilities.* Vienna, Austria: International Atomic Energy Agency (IAEA). 2011. Last accessed July 30, 2016. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf

[66] IAEA Nuclear Security Series No. 13. *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Revision 5). Vienna, Austria: International Atomic Energy Agency (IAEA), 2011. Last accessed July 30, 2016. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf

[67] “IEEE Trial Use Standard for Scada Serial Link Cryptographic Modules and Protocol.” IEEE. March 21, 2011. Last accessed July 30, 2016. http://grouper.ieee.org/groups/sub/wgc6/documents/drafts/P1711%20Draft%203%202008-08-16.pdf

[68] ISO/IEC 27002:2013. *Information Technology - Security Techniques - Code of Practice for Information Security Controls.* International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). Last accessed July 30, 2016. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

[69] Melton, Ron, Terry Fletcher, and Matt Earley. *System Protection Profile: Industrial Control Systems* (NISTIR 7176). Gaithersburg, MD: U.S. Department of Commerce. October 2004. https://scadahacker.com/library/Documents/Standards/NIST%20-%20System%20Protection%20Profile%20Industrial%20Control%20Systems.pdf

[70] Gold, S. “Look after your SCADA Heart.” January 1, 2009. Last accessed July 30, 2016. http://www.infosecurity-us.com/view/659/look-after-yourscada-heart/

[71] U.S. Department of Homeland Security (DHS). Last accessed July 30, 2016. www.dhs.gov

[72] Nuclear Regulatory Commission (NRC). Last accessed July 30, 2016. www.nrc.gov

[73] Federal Energy Regulatory Commission (FERC). Last accessed July 30, 2016. www.ferc.gov

[74] North American Electric Reliability Corporation (NERC). Last accessed July 30, 2016. www.nerc.com

[75] “Critical Infrastructure Protection.” The White House. Washington: May 22, 1998. Last accessed July 30, 2016. http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

[76] United States Nuclear Regulatory Commission (NRC). *73.54 Protection of Digital Computer and Communication Systems and Networks.* Office of Nuclear Regulatory Research. December 02, 2015. Last accessed July 30, 2016. http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html

[77] United States Nuclear Regulatory Commission (NRC). *Cyber Security Programs for Nuclear Facilities.* Regulatory Guide 5.71. Office of Nuclear Regulatory Research. January 2010. Last accessed July 30, 2016. http://www.nrc.gov/docs/ML0903/ML090340159.pdf

[78] United States Nuclear Regulatory Commission (NRC). *Criteria for Use of Digital Computers in Safety Systems of Nuclear Power Plants.* Regulatory Guide 1.152. Office of Nuclear Regulatory Research. July 2011. Last accessed July 30, 2016. http://www.nrc.gov/docs/ML0903/ML090340159.pdf

[79] “Supervisory Control and Data Acquisition (SCADA).” Centre for the Protection of National Infrastructure (CNPI). 2008. Last accessed July 30, 2016. https://www.cpni.gov.uk/scada/

[80] Cann, Michelle, Kelsey Davenport and Sarah Williams. “An Arms Control Association and Partnership for Global Security Report.” The Nuclear Security Summit: Assessment of Joint Statements. March 2015. Last accessed July 30, 2016.

http://www.fmwg.org/acapgs/ACA_NSS_Report_2015.pdf

[81] Abreu, David and David Slungaard. “Highlights from National Progress Reports.” 2014 Nuclear Security Summit. Partnership for Global Security. March 24, 2015. Last accessed July 30, 2016. https://pgstest.files.wordpress.com/2015/03/2014-progress-reports-highlights.pdf

[82] Ogilvie-White, Tanya and David Santoro. *Preventing Nuclear Terrorism: Australia’s Leadership Role.* Special Report. Canberra: Australian Strategic Policy Institute, January 2014. Last accessed July 30, 2016. https://www.aspi.org.au/publications/preventing-nuclear-terrorism-australias-leadership-role/SR63_prevent_nuclear_terrorism.pdf

[83] *Process Control and SCADA Security: A Good Practice Guide.* Centre for Protection of National Infrastructure (CNPI), 2008. Last accessed July 30, 2016. http://www.cpni.gov.uk/Documents/Publications/2008/2008031-GPG_SCADA_Security_Good_Practice.pdf

[84] Nakashima, Ellen. “U.S. and Russia Sign Pact to Create Communication Link on Cyber Security.” The Washington Post. June 17, 2013. Last accessed July 30, 2016. https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html

[85] Pennington, Matthew. “U.S. Seeks Resumption of Cyber Security Group Suspended by China.” Washington: The Associated Press, June 27, 2014. Last accessed July 30, 2016. http://www.theglobeandmail.com/news/world/us-seeks-resumption-of-cyber-working-group-suspended-by-china/article19357546/

[86] Abousahl, S., S. Klement, W. Rudischhauser, S. Tsalas, and E. Maier. EU Efforts to Strengthen Nuclear Security. In *International Conference on Nuclear Security: Enhancing Global Efforts. Proceedings of the Interational Conference.* Vienna, Austria: International Atomic Energy Agency (IAEA). 2014. Reference No. IAEA-CN--203/149

[87] Korsah, K. et al. *Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update (*NUREG/CR-6992). Washington DC: U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research. October 2009. Last accessed July 30, 2016. http://www.nrc.gov/docs/ML0929/ML092950511.pdf

[88] IAEA Nuclear Energy Series No. NP-T-3.12. *Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants. Technical Report.* Vienna, Austria: International Atomic Energy Agency (IAEA). 2011. Last accessed July 30, 2016. http://www.pub.iaea.org/mtcd/publications/pdf/pub1495_web.pdf

[89] IAEA Nuclear Security Series No. 10. *Development, Use and Maintenance of the Design Basis Threat.* Implementing Guide. Vienna, Austria: International Atomic Energy Agency (IAEA). 2009. Last accessed July 30, 2016. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf

[90] McCrory, Mitch F, Raymond C. Parks, and Robert L. Hutchinson. “An Adversary’s View of Your Digital System (IAEA-CN-228-54)”, In *IAEA International Conference on Computer Security in a*

Nuclear World: Expert Discussion and Exchange. Vienna, Austria: International Atomic Energy Agency (IAEA). June 2015. Last accessed July 30, 2016. https://conferences.iaea.org/indico/event/65/session/6/contribution/54/material/paper/0.pdf

[91] "SecurITree - Attack Tree-based Threat Modeling Software", Amenaza Technologies Limited, Last accessed July 30, 2016. http://www.amenaza.com/

[92] Nelso, Trent and M Chaffin. "Common Cybersecurity Vulnerabilities in Industrial Control Systems." Control Systems Security Program. Washington DC: Department of Homeland Security (DHS), National Cyber Security Division. May 2011. Last accessed July 30, 2016. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

[93] "The STRIDE Threat Model." Microsoft Developer Network. Last accessed July 30, 2016. http://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[94] Ou, Xinming, Sudhakar Govindavajhala, and Andrew W. Appel. "MulVAL: A Logic-based, Data-Driven Enterprise Security Analyser." In *14th UNSENIX Security Symposium*. Baltimore, Maryland, U.S.A: August 2005. http://people.cs.ksu.edu/~xou/publications/mulval_sec05.pdf

[95] WinGraphviz. Last accessed January 4, 2016. http://wingraphviz.sourceforge.net/wingraphviz/ .

[96] "TANAT - Threat And Attack Tree Modeling plus Simulation." Last accessed January 4, 2016. http://www13.informatik.tu-muenchen.de:8080/tanat/

[97] CFR.org Editorial Staff. "Targets for Terrorism: Nuclear Facilities." Council on Foreign Relations. January 1, 2006. Last accessed January 4, 2016. http://www.cfr.org/homeland-security/targets-terrorism-nuclear-facilities/p10213

[98] Gilb, Tom, and Susannah Finzi. *Principles of Software Engineering Management.* Vol. 11. Reading, MA: Addison-Wesley, 1988.