Safety, Cybersecurity and Interoperability aspects in Modern Nuclear Power Plants

Asmaa Tellabi[1, 4], Ines Ben Zid[2, 4], Edita Bajramovic[3, 4], Karl Waedt[4]
[1]University of Siegen, Siegen, Germany
[2]University of Bielefeld, Bielefeld, Germany
[3]Friedrich-Alexander-University Erlangen-Nuremberg, Erlangen, Germany
[4]Framatome GmbH, Erlangen, Germany

E-mail:{firstname.lastname}@framatome.com

Abstract—**The integration of digital equipment and diverse automation platforms in modern nuclear plants, including Nuclear Power Plants is due to the gradually increasing use of digital technologies. This digitalization either comes gradually based on a succession of refurbishment projects of Instrumentation & Control and Electrical Power Systems or as comprehensive architectures with new-built power plants. Therefore, similar to any critical infrastructure facing a growing risk of cyber-attacks, cybersecurity for Nuclear Power Plants has become a subject of rising concern. We envision that the findings in this paper provide a relevant understanding of the threat landscape facing digital systems in nuclear power plants. The knowledge can be used for an improved understanding and a better identification of security risks during the analysis and design of supporting systems. This paper gives an overview of the security issues and vulnerabilities, helping to better understand the big picture of cybersecurity issues and vulnerabilities in Nuclear Power Plants. Identifying these vulnerabilities and issues helps to establish new security countermeasures. A new draft standard IEC 63096 is presented in this paper as well.**

Keywords-nuclear power plants; cybersecurity interoperability.

I. INTRODUCTION

Digital Instrumentation and Control (I&C) systems are defined as computer-based devices that monitor and control nuclear power plants (NPP). Electrical Power Systems (EPS) provide the redundant power supply for different plant operation scenarios, which have to be fully supported. The EPS may include the connection to external highest voltage (e.g., 400 kW) or high voltage (e.g., 110 kV) grid connections, Emergency Diesel Generators, Station Blackout Diesel Generators, different Uninterruptable Power Supplies (UPS), e.g., for 2 hours and 12 hours [1][2].

Furthermore, different inverters and rectifiers are responsible of controlling and monitoring the entire aspects of the plant's health, all plant states and helping to respond with the care and adjustments as needed. They are seen as the nervous system of NPP. Generation III+ and IV reactors are equipped with digital I&C systems, while analog systems in older reactors are being replaced with digital systems [2]. The high level communication between NPP control networks is done by Supervisory Control and Data Acquisition systems (SCADA) in order to coordinate power production with transmission and distribution demands. Integration of digital I&C systems and the connectivity between NPP control networks and external networks represent a threat for NPP, making them a target to cyber-attacks which can include physical damage to reactors. With possibilities of cyber-attacks targeting NPP increasingly, cybersecurity has aroused as a significant problem [3].

The remainder of this paper is organized as follow. Section II gives background information on typical system architecture in NPP. Section III outlines some of the notorious publically known cyber-attacks against NPP. In Section IV , a new IEC 63096 standard [4] is described. We conclude the paper in Section V.

II. NUCLEAR POWER PLANTS

A. NPP architecture

The general digital systems configuration of NPP is almost similar to that of Industrial Control Systems (ICS) SCADA systems. The general architecture can be separated into two distinct domains: I&C systems, EPS and plant-local or corporate IT systems. The restriction on these networks is not similar, but also the nature of the traffic.

According to Fig. 1, operations, such as office automation, document management, and email, which consist of conventional IT systems, such as PCs and enterprise workstations use the corporate network of the Utility. As an illustration, Internet access, FTP, email, and remote access will normally be allowed on the enterprise network level but should not be permitted on the ICS network level.

Nuclear safety is the accomplishment of correct operating conditions, prevention of accidents or alleviation of accident consequences, ending up with the protection of workers, the public and the environment from extreme radiation hazards. On the other hand, nuclear security is the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.

Safety is expected to prevent accidents, while security is implemented to stop intended acts that might harm the NPP or lead to the theft of nuclear materials. Safety evaluations focus on risks arising from accidental events occurrences

originated from nature (such as earthquakes, tornadoes, or flooding), hardware failures, supplementary internal events or interruptions (such as fire, pipe breakage, or loss of electric power supply), or human mistakes (such as the incorrect application of procedures, or incorrect alignment of circuits). For security, risks, or events, worried about result from malicious acts accomplished with the objective to steal material or to cause damage. Therefore, security events are based on 'intelligent' or 'deliberate' actions achieved intentionally for theft or sabotage and with the purpose to avoid protective measures [1] [3].

Safety and security have various elements in common and both focus on protecting the plant with the eventual purpose of protecting people, society, and the environment. As stated above, the essential objective of each is identical — the protection of people, society and the environment. Whether it was a safety or a security event causing harm, the acceptable risk is likely the same, usually they both adopt the strategy of defense in depth, which is defined as the usage of layers of protection.

First concern is given to prevention. Second, abnormal situations need to be identified early and take action promptly to avoid resulting damage. Mitigation comes in the third place of an operative strategy. Finally, considerable emergency planning should be implemented in case of the failure of prevention, protection and mitigation systems [5].

I&C are censorious in NPP. They are responsible of monitoring the operational state of the nuclear reactors through interaction with physical equipment, but also in charge of process control. With the introduction of digital technologies in the 2000s, I&C systems shifted from analog technologies to digital technologies. The usage of digital technologies has been steadily increasing. NPP I&C systems engage in environments that are different than those of typical IT systems.

In a typical NPP, I&C architecture contains two types of systems: Non-safety and Safety systems. The Non-safety system is defined as a distributed computer system containing a number of remote control nodes spread across the NPP, which uses redundant real time data network to communicate with each other and with the Human Machine Interface (HMI) [6].

Communication with third party systems and Operation Maintenance Corporate Systems (OMS) are also supported through open protocols like Object Embedding Linking Process Control, fieldbuses and Modbus-TCP [7].

Additionally, monitoring and manual control of the NPP processes is done by the use of HMI consoles connected in the non-safety system. In order to display critical information related to safety on the non-safety HMI, the safety system will communicate with the non-safety system through Interface gateways.

On the contrary, a safety system is regularly based on a channelized Programmable Logic Controllers (PLC) that holds a number of PLC nodes distributed across the NPP. These PLC and its cabinets are designed to resist seismic events, environmental events and cybersecurity attacks. Furthermore, they can still be able to operate safely.

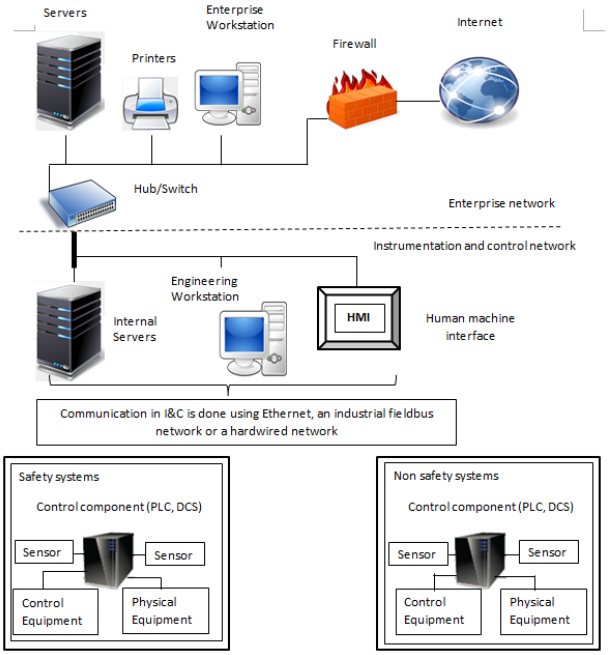

Figure 1. General architecture in nuclear power plants [2].

The purpose of this distribution is to coordinate with safety components in the process system, and also to ensure a safe communication in a safety channel using the redundant real time data safety network or through dedicated high speed links in between safety channels. Distributed control systems (DCSs) or PLC are common control components in I&C systems, they interact with physical equipment directly and industrial PCs or engineering workstations that are employed to configure control components and their related works [1].

B. ICS vs. IT systems

I&C systems are used to control the physical world, while IT systems´ purpose is to manage data. Requirements for performance and reliability, operating systems used and applications employed for I&C systems may be considered uncommon in a typical IT network environment [5].

At first, Industrial control systems (ICS) were similar to IT systems to some extent, in a way where ICS were inaccessible systems running on proprietary control protocols, and applying special hardware and software. Easily accessible, low-cost Ethernet and Internet Protocol (IP) devices are now taking the place of the majority of proprietary technologies; as a result cybersecurity vulnerabilities and incidents are increasing. Nowadays, the deployment of IT solutions in ICS is made to validate the use of business connectivity and remote access abilities, created and implemented to control typical industry computers, operating systems (OS) and network protocols. This combination of distinct IT capabilities provides considerably less separation for ICS from the outside world than previous systems, making security an essential requirement for these systems. These security solutions´ objectives were to handle security concerns in traditional IT systems; considerable

safety measures must be taken when introducing these same solutions to ICS environments. Environments in which ICS and IT systems operate are constantly changing, operation environments comprise, but are not limited to [5]:

- The threat space; vulnerabilities; missions/business activities; mission/business processes; enterprise and information security architectures; information technologies; personnel; facilities; supply chain relationships; organizational governance/culture; procurement/acquisition processes; organizational policies/procedures; organizational assumptions, constraints, risk tolerance, and priorities/trade-offs).

The following lists some special considerations when addressing security for ICS [5][6]:

1) Timeliness and Performance Requirements

Usually, ICS are considered time-critical, with a tolerable margin of delay and jitter, which depends on the application. Deterministic and reliable response are mandatory for some systems, e.g., for closed loop control. For IT systems, high throughput is necessary, while this it is not considered critical for ICS. In some cases, e.g., a reactor protection I&C system, automated system response in real time and timely response to human interaction is seen critical, e.g., for display systems in a main control room. Real-time operating systems (RTOS) or embedded real-time micro-kernels are implemented in ICS, where real-time responses are required.

2) Availability Requirements

In general, ICS processes are continuous, meaning that sudden interruptions of systems that control industrial processes are not allowed. An advanced schedule of these interrupts must be done. Sometimes, the production is considered more vital than the information, which can be undesirably affected by stopping and/or restarting ICS. In case traditional IT strategies are used, e.g., rebooting a module, they will have a negative effect on high availability requirements, reliability and maintainability of the ICS. In some industries, redundant components running in parallel are deployed to provide continuity when some components are unreachable.

3) Risk Management Requirements

Confidentiality and integrity are normally the principal concerns for IT systems. On the other hand, for ICS systems the main concerns are: availability, integrity, human safety and fault tolerance, regulatory compliance, destruction of equipment, loss of intellectual property, theft or damaged products. Safety and security concepts are paired; staffs in charge of the operation, security, and maintenance of ICS must understand those essential concepts. Security measures that jeopardy safeties are not allowed.

4) Physical Effects

ICS field devices, e.g., PLC, control physical processes. Interactions between ICS and physical processes can be very difficult, and can lead to severe consequences that can be noticeable in physical events.

5) System Operation

Generally ICS environments, counting operating systems (OS) and control networks, are completely different from IT systems, necessitating specific skill sets, experience, and levels of expertise. Usually, industrial control networks are managed by control engineers, and not by IT personnel.

6) Communications

In ICS environments, communication protocols and media needed by field device control and intra-processor communication are very different from nearly every IT environment.

7) *Patch Management*

Preserving the integrity of both IT and control systems is required. For IT systems software updates as well as security patches, are normally executed in a specific time based on appropriate security policy and procedures. On the other hand, software updates on ICS cannot always be forced on a timely basis without negatively affecting the system. Moreover, these procedures are usually automated via server-based tools. Before their implementation, these updates need to be tested by both the vendor and the end user. Also, a schedule of days/weeks must be planned by the ICS owner in advance. Patch management is also associated to hardware and firmware, the process demands careful assessment by ICS experts, e.g., control engineers, working in partnership with security and IT personnel.

8) Component Lifetime

IT components´ lifetime is in the order of 3 to 5 years, with briefness due to the fast progress of technology. For ICS, the implemented technology has been designed for precise use cases and implementation; the lifetime of the proposed solution is often in the order of 10 to 25 years and sometimes longer.

9) Component Location

Some IT modules are physically reachable by local transportation, also placed in corporate and commercial facilities. Remote locations may be used for backup services. Contrariwise, distributed ICS components must be isolated, remote services should not be allowed or used when required only by approved persons. Also, modules´ location necessitates important physical and environmental security measures.

III. CYBERSECURITY AND CYBER WARFARE RELATED TO NUCLEAR POWER PLANTS

Advancement in electronics and IT was the main motivation behind the replacement of traditional analog I&C systems in NPP with I&C systems, e.g., systems based on computers and microprocessors. Also, digital systems allow superior reliability, improved plant performance and supplementary diagnostic aptitudes. The systems used today were designed to satisfy performance, reliability, safety, and flexibility requirements, most of them were created a long time ago before new technologies became a crucial part of business operations.

In most typical implementations, these systems are physically isolated from outside networks and are based on

proprietary hardware and software. Communication protocols include basic error detection and correction capabilities but lack secure systems [7]. Accordingly, it is crucial not to connect such systems to an Intranet or the Internet.

A. History of Selected Attacks in NPP

First, in this Section we present some of the notorious attacks against NPP. In [8], attack taxonomy is defined by 5 dimensions: precondition, vulnerability, target, attack method, effect of the attack. It was combined with a new dimension target—the effect it has on the confidentiality, availability, integrity (CIA) of a system.

1) Ignalina NPP (1992)

At the Ignalina NPP in Lithuania, a technician intentionally introduced a virus into the industrial control system.

- **Precondition:** Direct access to the system.
- **Attack method:** Insider attack.
- **Target:** Availability and integrity.
- **Effect of the attack:** In this case, little harm was caused, but someone with malicious intent could have provoked a serious incident [9][10].

2) Davis-Besse NPP (2003)

This plant located in Ohio was infected by the Slammer worm (also called W32/SQLSlam-A or Sapphire).

- **Precondition:** Unpatched system.
- **Attack method:** At first, the worm scans and sends itself to random IP addresses; if worm reaches a machine that is running Microsoft SQL 2000, it infects that machine and begins scanning and sending itself to another machine.
- **Target:** Availability.
- **Effect of the attack:** The safety parameter display system (SPDS), responsible of collecting and displaying data regarding the reactor core from the coolant systems, temperature sensors and radiation detectors, was unavailable for nearly five hours [9][10].

3) Browns Ferry NPP (2006)

This NPP located in Alabama experienced a malfunction of both reactor recirculation pumps (which use variable-frequency drives to control motor speed and are needed to cool the reactor) and the condensate demineralizer controller (a type of PLC).

- **Precondition:** Device failure, attack method. Both of these devices contain microprocessors that communicate by sending and receiving data over an Ethernet network.
- **Attack method:** Ethernet operates by first sending data to every device on the network; then they have to inspect each packet to define if the packet is intended for them or if they can ignore it, making them vulnerable to failure if they accept enormous traffic.
- **Target:** Availability.
- **Effect of the attack:** The excess traffic produced by network broke down the reactor recirculation pumps and condensate demineralizer controller. As a consequence, the plant's Unit 3 had to be manually shut down in order to prevent a meltdown [9][10].

4) Hatch NPP (2008)

Hatch NPP located in Georgia experienced a shutdown as an unintended consequence of an update performed by contractor. An engineer contractor that manages the plant's technology operations installed an update to a computer on the plant's business network.

- **Precondition:** Human error.
- **Attack method:** The update was intended to synchronize data. The updated computer was connected to one of the plant's industrial control system networks, consequently when the engineer restarted the updated computer; the synchronization changed the control system's data to zero for a short moment.
- **Target:** Availability and integrity.
- **Effect of the attack:** The interpretation of the temporary changed values by the plant's safety system was incorrect. The updated value to zero of the water level signified that there was not enough water to cool the reactor core, which conducted to automatic shutdown for 48 hours of the plant's Unit 2 [9][10].

5) Natanz Nuclear Facility and Bushehr NPP – Stuxnet (2010)

First exposed to public in June 2010, the Stuxnet computer worm infected both the Natanz nuclear facility and the Bushehr NPP in Iran, partially destroying around 1,000 centrifuges at Natanz.

- **Precondition:** Use of commercial-off-the-shelf (COTS) Operating System (OS), Stuxnet infects computers using the Microsoft Windows OS, exploiting vulnerabilities in the system that allows it to obtain system-level access.
- **Attack method:** The worm uses forged certificates as a result the installed files look to come from an authentic source, misleading antivirus. Iranian nuclear facilities work with Siemens Step 7 SCADA system. Once the machine is infected, Stuxnet inspects the network to find computers attached to a similar system. Stuxnet duplicates itself on other computers by exploiting another set of vulnerabilities found in print spoolers and also through USB flash drives, so it spreads to networks using shared printers. Stuxnet's payload is activated only if the computer is connected to a similar Siemens system. It reprograms the system's PLC, in charge of controlling centrifuges applied in enriching nuclear fuel, so that they spin rapidly and eventually finish by break down.
- **Target:** Availability and integrity.
- **Effect of the attack:** As a result, Stuxnet destroyed over 1000 centrifuges at Natanz [9][10].

6) Korea Hydro and Nuclear Power Co. Commercial Network (2014)

Hackers infiltrated and stole data from the commercial network of Korea Hydro and Nuclear Power Co., which operates 23 of South Korea's nuclear reactors.

- **Precondition:** Human error: Access to the confidential data was obtained by hackers through phishing emails to the owner-operator's employees. Some of them finished by clicked on the links and downloaded the malware.
- **Attack method:** Sending phishing emails to employees.
- **Target:** Confidentiality.
- **Effect of the attack:** The hackers acquired the blueprints and manuals of two reactors, electricity flow charts, personal data that belongs to approximately 10000 of the company's employees, also radiation exposure estimates for nearby residents [9][10].

B. Security Vulnerabilities

In general, I&C in NPP are physically isolated from external networks and have a different operational environment from that of conventional IT systems. As a result, NPP were regarded as being safe from external cyber-attacks. However, continuous cyber-attacks against NPP signified that NPP are as susceptible to cyberattacks as other critical infrastructures [11] and conventional IT systems.

ICS, usually control the physical world and IT systems manage data. ICS are different from traditional IT systems, including dissimilar risks and priorities. Some of the different characteristics include important risk to the health and safety of human lives, severe destruction of the environment, and financial problems such as production deficit, and undesirable effect to a nation's economy. Performance and reliability requirements for ICS are distinct, by using operating systems and applications that may be seen unusual in a classic IT network environment. At first, ICS had slight similarities to IT systems in that ICS were inaccessible systems implementing proprietary control protocols with specific hardware and software. Commonly accessible, low-cost Ethernet and Internet Protocol (IP) devices are now substituting the older proprietary technologies, which raises the likelihood of cybersecurity vulnerabilities and events. Currently, ICS are embracing IT solutions to endorse corporate connectivity and remote access abilities, and are being created and employed via industry standard computers, operating systems (OS) and network protocols, where the resemblance to IT systems comes from. This novel integration deploys IT capabilities, but it meaningfully offers less separation for ICS from the outside world than antecedent systems, increasing the necessity to secure these systems. Despite the fact that security solutions have been designed to deal with these security matters in characteristic IT systems, particular precautions must be engaged when presenting these similar solutions to ICS environments [1].

1) Lack or Improper Input Validation

Attackers exploit vulnerabilities in services and scripts written by I&C vendors, resulting from the non-secure coding practices, allowing attackers to send forged request in order to modify the program execution. In the same way, using vulnerable protocols with for networking will be exploited to create malformed packets. Vulnerabilities found in these protocols and services make an attacker able to manipulate plant component, via well-known attacks. Vulnerable modules that might be concerned include Workstations at Main Control Room (MCR), Remote Shutdown Station (RSS); Process Information and Control System (PICS); Safety Information and Control System (SICS) and HMI. The attacks that could take place by exploiting this vulnerability are buffer overflow, command injection, and SQL injection.

2) Inappropriate Authorization

Authorization guarantees access to resources only by authorized entities. Access control mechanisms are implemented to ensure appropriate authorization. Absence of or weak authorization mechanisms can be exploited by attackers to gain illegal access to resources and tamper I&C system components. Software installed at operator workstations side must perform access control checks, or it will open a new door for attackers to perform unauthorized actions. Vulnerable modules include Workstations at MCR, RSS, PICS, SICS, HMI, Safety Automation System (SAS), Protection System (PS), Process Automation System (PAS). Existing module in I&C system must first verify whether the requesting module is allowed to access the resource. Escalation of privilege is one of the attacks that could be performed with authorization vulnerability.

3) Improper Authentication

Network protocols used within I&C system architecture during communication, frequently suffer from weak authentication mechanisms to verify the identity of the packet and also the user. Weak authentication vulnerabilities permit attackers to eavesdrop on network communications and capture the identity credentials of legal users, ending with an unauthorized privilege. Mutual authentication before sending or receiving data is not performed by the components of I&C. Not verifying the origin or authenticity of data, permits malicious data into components, credential theft, authentication bypass, etc. Furthermore, non-properly protected confidential data stored in databases can also be exploited. Vulnerable modules that might be touched by this are almost all I&C systems, sub-systems and components [10]. Often, I&C vendors leave behind authentication information from their product code or documentation, which can be definitely accessed and exploited by attackers. Weak passwords or using default passwords are another significant vulnerability to consider. There are numerous possible aspects that can be used to authenticate a person, device, or system, together with something the user knows, something the user has or something the user is. For instance, authentication could be founded on something known (e.g., PIN number or password), something possessed (e.g., key, dongle, smart card), something the user is like a biological characteristic (e.g., fingerprint, retinal signature), a location

(e.g., Global Positioning System (GPS), location access), the time a request is made, or a mixture of these attributes. Normally, the more authentication process includes more factors, the more strong the process will be. Multi-factor authentication refers to the process when two or more factors are used [5].

4) Unencrypted Sensitive Data

Frequently data at rest and in transit is unencrypted, making them vulnerable to disclosure. Moreover, network packets exchanged between several components of I&C are not encrypted but in plaintext form. Vulnerable modules that might be touched by this are almost all I&C systems, sub-systems and components [10]. Exposure of product source code, topology, legitimate user credentials, might result as a consequence.

5) Incorrect Software Configurations and Management

Security breaches and exploitations of plant operations are a result of misconfigurations or vulnerabilities found in I&C software. Modules that are seen vulnerable to this are Workstations at MCR, RSS, PICS, SICS, HMI, SAS, PS, and PAS. The existence of these vulnerabilities is caused by poor patch management, poor maintenance, and built-in flaws in I&C products. Additionally, improper installations of applications also offer an opportunity to attackers to tamper the system.

6) Lack of Backup Facilities

Some of I&C systems in NPP do not own backup and restore facilities dedicated to databases and software. NPP that possess backup facilities often store them offsite, and they are not often exercised and tested. Vulnerable modules that might be concerned by lack of backup facilities are SAS, PS, PAS, Sensors, Actuators, PICS, and SICS [10]. NPP must be operated 24/7 and the absence of a backup feature can result in catastrophic effects if an incident occurs.

7) Absence of Audit and Accountability

Some attacks are hard to detect since they are launched in a cautious manner like insider attacks. The nonexistence of auditing and logging mechanisms assists attackers into covering their tracks after attacks. Vulnerable modules that might be touched by this are almost all I&C systems, sub-systems and components. Storing activity logs of I&C components and operator actions is vital in order to trace attack patterns, but also to avoid repudiation threats from insiders as well as actions in I&C components and systems.

8) Absence of Security Awareness

Technology advancements and the people using these technologies present multiple risks to information security. The human factor is considered as one of the major sources of information security risk, also one of the most difficult to control. According to a Deloitte's Technology, Media, and Telecommunications (TMT) Global Security Study [12], 70% of the TMT organizations surveyed rate their employees' lack of security awareness as an "average" or "high" vulnerability, which was the case for Korea Hydro and nuclear Power Co. Security controls that are conform to the NIST SP 800-53 Awareness and Training (AT) family offer policy and procedures for guaranteeing that each user of an information system is equipped with elementary information system security awareness and training materials before authorization to access the system is granted. Security awareness is a crucial part of ICS incident prevention, mainly when it comes to social engineering threats. Social engineering is seen as a method used to influence individuals into revealing private information, such as passwords. This information can then be exploited to endanger otherwise secure systems. Employing an ICS security program may bring changes to the means used by personnel to access computer programs, applications, and the computer desktop itself [9].

C. Classification of adversaries

In [13] adversaries are categorized into eight classes that can endanger safety and security of NPP. The categories are as follows: covert agents, disgruntled current employees, disgruntled ex- employees or insider attackers, recreational hackers/ hobbyists/ script kiddies, militant opponents to nuclear power, non-state hackers (e.g., cyber criminals/organized crime), nation-state hackers (e.g., governments and militaries), and terrorists (e.g., non-state armed groups).

1) Covert Agent

A retired or a present employee of an intelligence agency, and whose identity is unknown to others. The agent is hired to steal secret information and personal information about adversaries. In order to get information, this agent must have access to the system and documentation, or apply a social engineering method.

2) Disgruntled Current Employees or insider attackers

Someone who is not satisfied with his/her job, and wants to compromise the system by using illegal approaches. Reasons behind dissatisfaction vary, but the usual motivations are to take revenge, create chaos, damage nuclear security's image, or steal information for economic gain. To perform such attack, the attacker needs medium to high level resources to execute an attack, e.g., systems access. Moreover, an employee must own some higher privileges on processes and systems, programming skills and information about the system´s architecture, information about possible existing passwords, and the capability of installing "kiddie" tools or scripts.

3) Disgruntled Ex-Employee

This person has similar motivations as the ones of a disgruntled employee. Their purpose is to take revenge on the employer, sell confidential information to adversaries for economic gain, or disclose confidential information to the public in order to damage employer´s public image. As an ex-employee, she/he may still own confidential documentation, access to facility resources, and potential connections to other employees. To execute such an active attack, an attacker should have knowledge about systems´ passwords, access to systems, and backdoors made by social engineering techniques.

4) Recreational Hackers/Hobbyists/Script Kiddies

Their motivations behind the intrusion to systems are for fun or to win a challenge. These attackers are interested into learning about new vulnerabilities and exploiting by performing them on real systems. They often download and use free scripts and tools available on Internet. Their intentions might be harmless; yet, mechanisms used to learn about these vulnerabilities and the way to exploit them is risky. In case cybersecurity mechanisms are not well deployed inside NPP, this might be destructive. Without owning an advanced level of expertise, frameworks such as Metasploit provide SCADA-specific exploits, which script kiddies can use to execute an attack easily. Such attackers could certainly be blocked by imposing best practices such as patch management, policy enforcement, and suitable use of antivirus, intrusion detection systems (IDS), and firewalls inside the organization.

5) Militant Opponent to Nuclear Power

She/he has strong public thoughts on precise nuclear issues, and often slows down nuclear business operations. These attackers are financially supported through secret channels or agencies [10]. However, they only know the public information available on systems. Moreover, they have sufficient time to perform such attacks and mainly aim defined public events such as elections. They may or may not have computer skills; still, they get help from the hacker community to execute a cyber-attack.

6) Non-State Hackers

Groups or individuals with the main objective are financial gain by stealing nuclear sensitive data belonging and then blackmailing the facility to which data belong to into paying a ransom. Usually, they threaten to exploit vulnerabilities in SCADA systems. These attackers do have funds and can hire expert hackers or buy hacking tools in order to attack systems. A set of SCADA-targeted automated attack tools, in the form of Metasploit add-ons that can help in executing attacks on ICS, exist. Every so often, these attackers employ former/current employees of a facility to perform social engineering to extract information.

7) Nation-State Hackers

Governments hire specific individuals to perform cyber operations, internationally or nationally. State hackers vandalize and block access to websites, and perform industrial espionage to steal a country's confidential data. Additionally, state hackers constitute the most harmful threat to SCADA systems, as long as these hackers get all of their owned information and funds from the government. The government has resources to hire the best hackers and offer those funds, infrastructure, and facilities to create zero-day exploits, to use them against an enemy country in order to steal a nuclear technology, intelligence collection, etc. Although zero day attacks are single-use weapons, they are capable of causing a huge damage to a country's infrastructure, economy, and systems.

8) Terrorist

Throughout the history of cyber-attacks on SCADA systems, no evidence can be found of a terrorist attack; still, the situation will not stay like this in the future. According to former U.S. President George W. Bush, terrorists can get into the network with the intention to attack a nuclear facility, and consequences of such intrusion could be intolerable [10]. Objectives of such terrorists differ: sometimes they want to accumulate intelligence, create backdoors for later use, spread fear and panic among the public, or take revenge on the government. Furthermore, some terrorist groups have developed important skills to use social media as a way to hire hackers.

D. Cybersecurity requirements

Cyber security features that provide confidentiality, integrity, and availability must be integrated in the design of safety systems. Cybersecurity controls should not have an opposite effect on the plant´s safety objectives and should not intervene with their operations. Concerns have been raised regarding possible effects that such features can have on safety functions´ performances. Also, it shall not jeopardize diversity and safety Defense in Depth (DiD) features effectiveness implemented in I&C architecture [14].

- **Confidentiality**

Imposing this feature inside a safety system restricts actions an attacker can make on information transferred between safety systems, or between safety and non-safety systems. In general, to ensure confidentiality cryptographic techniques must be deployed, in order to avoid any illegal disclosure of information during transmission and reception [15]. To make sure that these added cryptographic features do not degrade safety functions, these cryptographic mechanisms are employed for communication between safety and non-safety systems. In case an unpredictable overhead is introduced to data communications because of added cryptographic approaches, other possibilities exist. These supplementary implementations may implicate physical and logical access controls on the system, monitoring dynamically and tracking all accesses to the system to detect and respond to intrusions in a convenient way, by enforcing auditing and/or validation mechanisms to identify unauthorized access and alterations to the system. For authorized individuals´ a background check should be accomplished with regards to their experiences and trustworthiness.

- **Integrity**

The purpose of protecting safety systems´ integrity is to restrict malicious actions attackers can perform on safety systems so that they cannot negatively impact safety functions [15]. Protecting integrity can be accomplished by restricting unauthorized alterations of software and hardware in safety system. Limiting access to these systems might be a possibility, since access is made via direct interfaces, e.g., ports on the hardware, or using indirect interfaces like data links. An access control list including

authorized actions should be implemented so that illegal system modification via direct interfaces is forbidden [15].

- **Availability**

Affecting negatively safety systems´ availability must not be permitted [15]. Safety systems´ operations can be compromised directly or indirectly by refusing access to the system to authorized users. Methods for restricting an attacker´s ability of performing such attacks or controlling the attack´s effect on a system, should not interfere with safety function, as enforced e.g., by IEC 62859 [14]. These approaches consist of installing mechanisms at the system's external interface to prevent and limit denial of service attacks´ effects. While configuring these systems, restrictions on users´ actions should be considered to prevent them from executing such attacks against other systems, by controlling capacity surplus and/or bandwidth to stop information-flooding and attacks´ effects. Some cryptographic mechanisms are capable to comply with these requirements, e.g., by limiting the attacker´s actions, to possibly make modifications that may negatively affect the availability.

E. STRIDE threat modelling

This Section presents the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges) threat model of a typical NPP' I&C system by taking into consideration its characteristics and architecture. STRIDE is a method developed by Microsoft, which describes an adversary's objectives, is used for threat modelling [10]. Tab 1. shows a summary of the STRIDE analysis.

- **Spoofing**

Spoofing is a scam category where an intruder tries to gain unauthorized access to a user's system or information by pretending to be the legitimate user [10]. For NPP, this unauthorized access can cause I&C systems´ disruption or lead to the system´s misuse. Spoofing can be divided into two categories, it can be related to the system or linked to the personnel. The first type focuses on spoofing I&C system´s credentials, the second type concentrates on unauthorized access gained after stealing personnel credentials, e.g., Passwords and tokens, and then pretending to be the real authorized user. Session hijacking is a typical attack for personnel spoofing; the attacker captures a current session and attempts to connect to the receiver as an authentic user. In the case of a system spoofing, malicious code injection in the form of scripts into a web browser is a common strategy. Other techniques exist in order to spoof credentials; it includes social engineering, e.g., watching and/or manipulating user or system behavior and activities, and incorrect input, e.g., SQL injection.

- **Tampering**

Consists of altering legitimate data, and as a consequence the system´s integrity is compromised. The data can be tampered whether it is in transit or at rest. An attacker can exploit any misconfiguration or if there is no presence of integrity checking procedure in the system to compromise the system´s integrity.

- **Repudiation**

It is caused by the lack of appropriate auditing and logging mechanisms. An attacker can exploit vulnerabilities in the logging mechanism, steal keys, or even produce fake digital signatures to allow unauthorized actions. As an illustration, an operator or a compromised system at a NPP can deny executing some actions or operations on plant systems, e.g., a plant operator alters temperature´s values and water level of a plant, but later denies performing such an action.

- **Information disclosure**

This threat is a result of improper protection of information. There are many forms of information – for example, user credentials, network packets, source code, files, or a database. Sensitive plant´s information can be illegally released by exploiting vulnerabilities like software misconfigurations, improper authorization or authentication mechanisms.

TABLE 1 STRIDE ANALYSIS.

Threat category	Attacker type	Vulnerability category
Spoofing	Covert Agent Disgruntled Ex-Employee Non-State Hacker Terrorist	No or Incorrect Input validation. Improper Authentication Improper Authorization
Tampering	Militant Opponent Recreational Hacker Terrorist	Improper Authentication Improper Authorization Improper Software Configuration & Management
Repudiation	Disgruntled Current Employee	Auditing and logging
Information Disclosure	Covert Agent Disgruntled Current Employee Non-State Hacker Disgruntled Ex-Employee	Improper Authentication Improper Authorization Improper Software Configuration & Management
Denial of Service	Recreational Hacker Terrorist	Improper Software Configuration & Management No or Incorrect Input Validation Lack of Backup Facilities
Elevation of Privilege	Disgruntled Current Employee	Improper Authentication Improper Authorization

- **Denial of service (DoS)**

By overwhelming I&C systems with a large number of repetitive requests, required components become unavailable. These requests can be sent by installing a malware or in case the system is connected to internet with a hidden connection. DoS attacks generally take place when backup facilities are unavailable and inexistence of input validation methods.

- **Elevation of Privilege**

Leading to an abuse of legitimate access, malicious insiders having access to resources or operations may alter

their account permissions to permit supplementary accesses to systems to which they do not have access to. They can then abuse their privileges by performing malicious actions, e.g., stopping core functions or altering parameter values.

F. Industry and Government Responses to NPP Cybersecurity

In the previous Section, known attacks and vulnerabilities in NPP were underlined. Since they pose important risks to the economy and to national security, numerous attempts were made by international organizations, regulatory and research institutes, and governments to set up cybersecurity guidelines, standards, and frameworks dedicated to security of NPP.

For industry adoption and regulatory approval, three features of digital I&C systems are distinguishing.

First, a digital I&C system is more complicated than its analog predecessor because of the number of connections it has among its many components. Second, the digital system rely more on software. Usually, a unit has around 10000 sensors and detectors and 5000 km of I&C cables. The total mass components connected to I&C, is close to 1000 tones. Making I&C system one of the heaviest and most extensive non-building structures in any NPP. Third, the complete reliance on computers increases the importance of cybersecurity. The first two of these features, complexity and software-dependence, introduce new possibilities for common cause failures.

The increased use of commercial "off-the shelf" software is considered as one practice hurting the nuclear industry. This type of software does not deliver a suitable level of protection from external threats and is often seen as a direct approach to penetrate a facility network. The use of insufficient software, mixed with executive-level ignorance of security risks, builds an easy way for an attacker to misuse assets. There is a common misrepresentation which refers to nuclear facilities as being "air-gapped" – totally inaccessible from the Internet – signifying that the industry is safe from cyber-attacks. Considerable commercial software offers Internet connectivity through virtual private networks (VPN) or else Intranet. These connections often go unlisted and keep on being ignored while implementing software or deploying momentary Internet connections for a project. Furthermore, the focus has been given more to physical safety and protection instead of cybersecurity controls. Therefore, very few developments have been made to reduce cyber risks through standardized control and measures [11].

NPP are securely maintained and considered as the most protected and secure facilities in the world. However, accidents can happen, undesirably affecting environment and people. Vulnerabilities threatening the physical security of a NPP and their ability to launch acts of terrorism were elevated to a national security issue following the attacks of 9/11, 2001. Consequently, the American congress endorsed new nuclear plant security requirements and has frequently devoted attention on regulation and enforcement by the Nuclear Regulatory Commission (NRC). Years passed after the 9/11 attacks, but security at NPP persists as a vital matter. To decrease the likelihood of an accident, the International Atomic Energy Agency (IAEA) supports Member States in applying international safety standards to reinforce safety in NPP [10]. NIST has published a well-established risk management framework in NIST Special Publications (SP) 800-30 [16], 800-37 [17], and 800-39 [18], which analyzes distinct threat scenarios and evaluates the various attack possibilities that can exploit system vulnerabilities. On the other hand, the NIST risk assessment framework, mentioned above, does not describe precise procedures on the approach a company should assess the quantification of risks, i.e., how and to what degree an attack can endanger system confidentiality, integrity, or availability. In 2008, NIST issued a guideline on securing ICS [5]. It systematically explained the security of ICS systems, mostly containing SCADA architecture, distributed control systems (DCS), secure software development, and deployment of controls in order to secure networks. NIST also came up with a guideline on the Security for Industrial Automation and Control Systems while working with the Industrial Automation and Control Systems Security ISA99 Committee.

The IEEE produced the SCADA cryptography standard in 2008 [19], which offers a comprehensive explanation on the way to found secure communication between SCADA servers and workstations. Organizations can also attain certification under this IEEE standard if they fulfill with the requirement. The International Organization for Standardization (ISO) has also issued a standard, ISO/IEC 27002:2013 [20], which gives guidelines for initiating, implementing, maintaining, and improving information security management in organizations [10]. NRC's cybersecurity regulations necessitate each NPP to present a cybersecurity plan and implementation schedule. The plan must deliver "high assurance" that the digital computer and communications systems implemented in order to perform the next functions will deliver sufficient protection against design basis attacks:

- Safety-related Functions or vital to safety.
- Security functions.
- Emergency mobility functions, as well as offsite communications.
- Support systems plus equipment that, if compromised, would undesirably jeopardize safety, security, or emergency mobility functions [4].

As a result, cybersecurity has been adopted as NPP regulation requirement under the US code of federal regulation (CFR) [3]. Also, regulatory agencies like the US NRC and IAEA created and distributed regulatory guidelines, considering construction of cybersecurity plans and programs for NPP. The IAEA and World Institute for Nuclear Security (WINS) are multiplying their efforts in order to protect NPP by addressing cybersecurity issues and challenges on a global scale. Currently, some of issues include:

- Issuing multiple documents addressing cybersecurity on nuclear facilities.

- Providing technical and strategic security training to involved officials of member countries.
- Offering expert guidance and capacity building to officials and representatives.

NSS-17 [13] was issued by IAEA as a technical guidance for guaranteeing computer security at nuclear facilities. Similarly, the IAEA NSS-13 [21] recommends that the available computer-based systems included in nuclear facilities must be protected against compromise, and also an appropriate threat assessment must be realized in order to prevent attacks.

Threats were classified from various adversaries' perspectives, detection and prevention mechanisms for compromises of NPP information systems were also addressed [22]. Additionally, nothing like usual ICS and SCADA systems, governments, and NPP regulatory agencies specify that NPP I&C systems must comply with the following firm safety requirements [5][23]:

- Requirements for annual maintenance, best availability and functionality levels, and environment tests.
- Nuclear reactor safety and also physical protection of nuclear material must be taking in consideration.
- Defining system security levels by bearing in mind safety level ranking, and evaluating safety risks in relation to security threats.
- Verification that security functions do not have opposing effects on the safety and functionality of facilities.
- Management and maintenance must consider the safety and reliability of systems, examination and also qualification by regulatory agencies.
- Redundancy and diversity must be taken in consideration in the design.

However, all of these efforts are continuing and necessitate indefinite time to mature.

The guidelines, standards, and recommendations provided by governments and regulatory authorities necessitate complete review to make sure that they describe and include the newest risk assessment developments, for example, cyber threat information sharing, risk assessment of tacit knowledge, dissemination of risk assessment results, etc. These features are obligatory in order to keep NPP risk assessment up-to-the-minute on progressive cyber threats and to be able to manage cyber incidents in a proper manner.

On the other hand, at present, the abovementioned guidelines do not provide a detailed approach on imposing security controls and avoiding cyber risks.

IV. SECURITY CONTROLS FOR NPP

Standards are endorsing the improvement of cybersecurity in NPP. Fig. 2 shows the standardizing processes and procedures, which are important to accomplish an international rewarding collaboration. Abundant standards addressing information security were established in recent years. Still, not all of them are practical to apply in NPP.

Designed for I&C systems in NPP, the new draft IEC 63096 is expected to be published in 2019. The standard aims its attention specifically on the selection and application of cybersecurity controls from the contained security controls within the catalogue. Preventing, detecting, also reacting to digital attacks against computer-based I&C systems are the major functions of the selected and applied cybersecurity controls. Based on IEC 62645 [24], IAEA, in addition to country precise guidance in the technical and security application area. Designers and operators of NPP (utilities), systems evaluators, vendors and subcontractors, and by licensors can use this standard. For that reason, the goal of this standard is to enlarge the SC45A series of documents focusing on cybersecurity with IEC 62645 [24] as its high-level document, by classifying nuclear I&C precise cybersecurity controls for I&C systems into Safety Classes 1, 2, 3 and non-classified (NC) I&C systems. A major difference between this standard and usual IT systems or industrial automation systems standard is the safety classification of I&C nuclear systems and related safety requirements. IEC 62645 [24] was issued in August 2014, and IEC 62859 [14] was published in 2016, along with this new standard related to cybersecurity controls, are planned to be used for I&C systems and NPP. The new standard is structured as follow.

The first main Section designates the intended audience, which is distinguished by parties that are in charge of:

- I&C platform development.
- Project Engineering for I&C system, including installation and commissioning.
- Operation and maintenance of I&C system.

In the second main Section, a detailed description of each security control is explained. Inside this structured representation, the purposes of Security Degrees along with the specific control are defined either highly recommended or optional. As well, additional description specifies whether the control conserves the confidentiality, integrity or availability. Each Section related to a security control provides specific implementation guidance on how to implement the control; it also differentiates between I&C platform development, project engineering or operation and maintenance.

Based on IEC 62645 [24], the third main Section is dedicated to the process of selecting the available security controls. Controls are allocated depending on the security degree of the particular I&C system. Tools and Legacy systems are also considered in this standard. After selecting the security controls, a threat and risk assessment is required in order to detect a residual risk that necessitates the implementation of supplementary security controls.

Concerning controls three cases are distinguished, using the guidance provided by the Draft ISO/IEC 27009 [25] on sector specific security controls. The following three cases on the refinement of ISO/IEC 27002 security controls are examined [20]:

- Security controls are adopted from ISO/IEC 27002 [20] without any adjustment. If needed, the obligatory details are added by the standardized structure.

- To meet requirements from the nuclear I&C domain, Security controls from ISO/IEC 27002 [20] were modified and described in details to better.

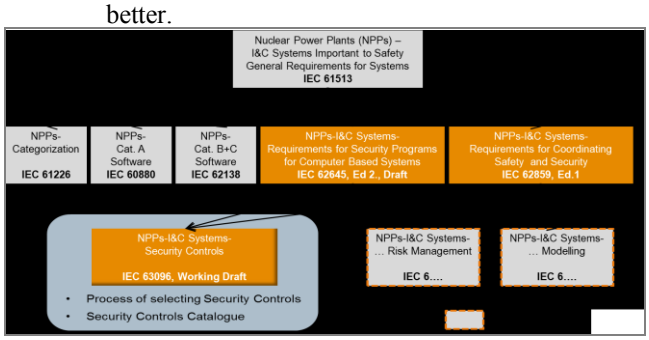

Figure 2. New IEC 63096 Security Controls standard in the SC45A standards hierarchy [4].

- In order to meet the particular requirements from the nuclear I&C domain, a new security control has been added and inserted into ISO/IEC 27002 [20] clause (5 through 18. This is the case where the ISO/IEC 27002 [20] does not define specific security controls needed in nuclear I&C.

IEC 62541 [26] defines the open platform communication Unified Architecture (OPC UA), it is an automation middleware or machine-to-machine (M2M) protocol. The standard features an object-oriented meta-model to characterize data structures and remote procedure calls, which can be dynamically explored and modified through IP communication, along with security mechanisms such as authentication and encryption. OPC UA is adaptable to manufacturing software, it defines [26]:

- An information model for structure, behavior and semantics description.
- A message model for interactions between applications.
- A communication model to carry data between end points.
- And a conformance model to guarantee interoperability between systems.

The communication services of OPC UA are mainly used in the following domains: Process automation, power plants with, traditional and renewable Building automation, and Factory automation (in particular robotics).

The OPC UA specifications are made up by 13 parts, the first seven parts are related to the core specifications e.g., the concept, security model, address space model, services, information model, service mappings and profiles. The parts eight to thirteen are related to access type specifications like data access, alarms and conditions, programs, historical access, discovery and aggregates. Interoperability is achievable by using a communication standard that is platform and vendor independent, such as IEC 62451 [26] (OPC UA) and IEC 61850 [27] (Communication Networks and Systems in Substations). OPC UA is a platform-independent standard that helps into reaching interoperability between devices with dissimilar manufacturers and communication protocols. OPC UA simplifies communication by sending messages between OPC UA Clients and Servers. For example, its applicability to the nuclear context is demonstrated by Framatome. Recognizing the potential of OPC-UA in sensors, Framatome started incorporating them into monitoring instruments (SIPLUG®) for mountings and their related electric drives. The solution is employed in the nuclear Industry for monitoring critical systems in remote environments, without undesirably affecting the availability of the system [28].

V. CONCLUSION

This paper gave an overview of security vulnerabilities in I&C systems and EPS inside NPP, by going through notorious attacks across history and listing some of the vulnerabilities that can be exploitable by malicious attackers. An introduction to a new draft standard, IEC 63096 [4] had being given. The improved performance digital technology has offered a significant influence on I&C systems design in NPP. The nuclear industry has a conservative methodology in approaching safety, and a considerable effort is obligatory in order to provide the essential evidence and analysis to guarantee that digital I&C systems can be employed in safety-critical and safety-related applications. In general, I&C systems are inaccessible from outside communication systems. Still, this is not sufficient for secure operation inside NPP, as in the case of Stuxnet. Interoperability has to be addressed from I&C architecture design phase, as the systems have to interact. The threat from cyber-attacks is more and more seen as a problem of national and international security as cyber-attacks evolve, become more advanced and as actors behind them are no longer limited to private hackers or organized criminals, but also nation states and insiders.

In future work, we intend to focus more on the listed vulnerabilities, and introducing security in hardware by using a trusted platform module instead of only focusing on securing software, also some best practices to widen the protection area.

ACKNOWLEDGMENT

Some of the addressed cybersecurity related topics are being elaborated as part of Framatome GmbH's participation in the "SMARTEST" R&D (2015-2018) with German University partners, partially funded by German Ministry BMWi.

REFERENCES

[1] A. Tellabi, I. Ben Zid, E. Bajramovic, and K. Waedt, "Safety, Cybersecurity and Interoperability of Modern Nuclear Power Plants," IARIA 8th International Conference on Performance, Safety and Robustness in Complex Systems and Applications, 2017.

[2] J. Rrushi, R. Campbel, "Detecting cyber attacks on nuclear power plants," The International Federation for Information Processing (ICCIP 2008), Springer, Boston, vol. 290, 2008, ISBN: 978-0-387-88522-3.

[3] INSAG-24, International Nuclear Safety Group, "The interface between safety and security at nuclear power plants," IAEA, 2010.

[4] J. Bochtler, E. Quinn, and E. Bajramovic, "Development of a new IEC standard on cybersecurity controls for I&C in Nuclear Power Plants – IEC 63096," NPIC & HMIT 2017, San Francisco, 2017.

[5] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security,", NIST, 2011.

[6] A. Tellabi, Y. Sassmanhausen, E. Bajramovic, and C. Ruland, "Overview of Authentication and Access Controls for I&C systems ," IEEE 16th international conference on industrial informatics, 2018.

[7] M. Holt, A. Andrews, "Nuclear Power Plant security and vulnerabilities," Congressional Research Service, January 2014.

[8] D. Papp, Z. Ma, and L. Buttyan "Embedded systems security: threats, vulnerabilities, and attack taxonomy," 13th Annual Conference on Privacy, Security and Trust (PST), IEEE, 2015, doi:10.1109/PST.2015.7232966.

[9] C. Baylon, R. Brunt, and D. Livingstone, "Cybersecurity at civil nuclear facilities understanding the risks," Chatham House Report, September 2015.

[10] R. Masood, "Assessment of cybersecurity challenges in nuclear power plants security incidents, threats, and initiatives," Cybersecurity and Privacy Research Institute the George Washington University, 2016.

[11] B. Kesler, "The vulnerability of nuclear facilities to cyber-attack," Defense and Diplomacy Journal, vol. 5, No. 3, 2016.

[12] Deloitte, "Security Awareness: People and Technology," [Online]. Available from: http://www2.deloitte.com/, 2017.12.19.

[13] IAEA Nuclear Security Series No. 17, "Computer Security at Nuclear Facilities," IAEA, 2011.

[14] IEC 62859:2016, Nuclear Power Plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity, IEC.

[15] Regulatory Guide 5.71, Revision 0, "Cyber Security Programs for Nuclear Facilities," U.S. Nuclear Regulatory Commission, January 2010.

[16] G. Stoneburner, A.Y. Goguen, and A. Feringa, "NIST Special 800-30: Risk Management Guide for Information Technology Systems,", NIST, 2002.

[17] Joint Task Force Transformation Initiative, "NIST Special Publication 800-37 Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach," NIST, 2014.

[18] E. Aroms, "NIST Special Publication 800-39: Managing Information Security Risk," NIST, 2012.

[19] "IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links," in IEEE Std 1711-2010, vol., no., pp.1-49, 2011.

[20] ISO/IEC 27002:2013, Information Technology - Security Techniques - Code of Practice for Information Security Controls, ISO/IEC.

[21] IAEA Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities," IAEA, 2011.

[22] W. Ahn, M. Chung, B. Min, and J. Seo, "Development of cyber-attack scenarios for Nuclear Power Plants using scenario graphs," International Journal of Distributed Sensor Networks, vol. 11, April 2015, doi: 10.1155/2015/836258.A

[23] ISO/IEC 27001:2005, Information Technology –information security management systems –requirement, ISO/IEC.

[24] IEC 62645:2014, Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Security Programs for Computer-Based Systems, IEC.

[25] ISO/IEC 20009-1:2013, Information technology – Security techniques – Anonymous entity authentication, ISO/IEC.

[26] IEC 62451-1:2016, OPC Unified Architecture – Part 1: Overview and Concepts, IEC.

[27] IEC 61850:2013, Communication networks and systems for power utility automation, IEC.

[28] V. Watson, A. Tellabi, J. Sassmannshausen, and X. Lou, "Interoperability and security challenges of Industrie 4.0," 2017, doi:10.18420/in2017_100.