Safety, Cybersecurity and Interoperability of 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.

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 a nuclear power plants (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 [1]. The high level communication between NPPs 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 NPPs control networks and external networks represent a threat for NPPs, making them a target to cyber-attacks which can include physical damage to reactors. With possibilities of cyber-attacks targeting NPPs increasingly, cybersecurity has aroused as a significant problem [2].

The remainder of this paper is organized as follows. Section II gives background information on typical system architecture in NPPs. Section III outlines some of the notorious publically known cyber-attacks against NPPs. In section IV, a new IEC 63096 standard [3] is described. We conclude the paper in Section V.

II. NUCLEAR POWER PLANTS

The general digital systems configuration of NPPs 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

ISBN: 978-1-61208-628-6

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, the 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 [2].

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 [2].

I&C are censorious in NPPs. 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 [4]. NPPs I&C systems engage in environments dissimilar from 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 NPPs, which uses redundant real time data network to communicate with each other and with the Human Machine Interface (HMI).

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 [5].

Additionally, monitoring and manual control of the NPPs 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 NPPs. These PLCs and its cabinets are designed to resist seismic events, environmental events and cybersecurity attacks. Furthermore, they can still be able to operate safely.

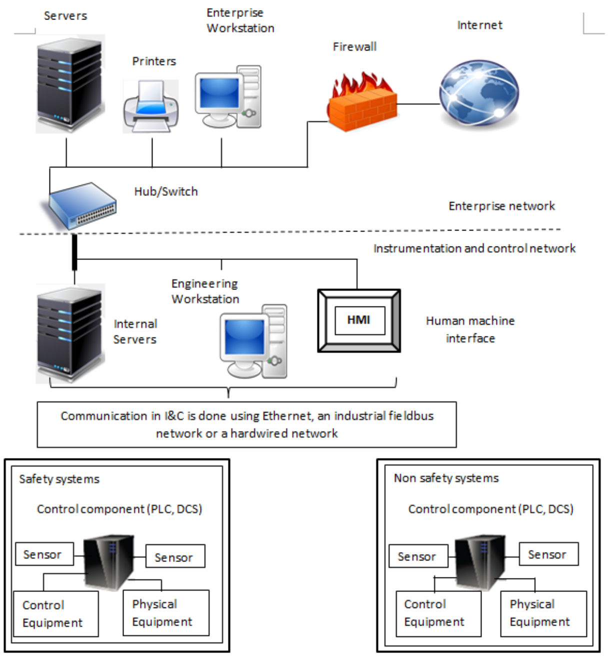

Figure 1. General architecture in nuclear power plants [6].

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 PLCs 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.

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 NPPs 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. The communication protocols include basic error detection and correction capabilities but lack the secure systems [5]. Accordingly, it is crucial not to connect such systems to an Intranet or the Internet.

A. History of Selected Attacks in NPPs

First, in this section we present some of the notorious attacks against NPPs. In [7], 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 [8][9].

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 [8][9].

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 [8][9].

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 [8][9].

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 operating system, 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 duplicate 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 PLCs, 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 1,000 centrifuges at Natanz [8][9].

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 10,000 of the company’s employees, also radiation exposure estimates for nearby residents [8][9].

B. Security Vulnerabilities

In general, I&C in NPPs are physically isolated from external networks and have a different operational environment from that of conventional IT systems. As a result, NPPs were regarded as being safe from external cyber-attacks. However, continuous cyber-attacks against NPPs signified that NPPs are as susceptible to cyberattacks as other critical infrastructures [10] 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. ICS and IT systems operate in continuously changing environments. The environments of operation comprise, but are not limited to the threat space, vulnerabilities, missions/business purposes, mission/business procedures, 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) [4].

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); Human Machine Interface (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, HMIs, 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

The 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 [9]. 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 [4].

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 [9]. 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, HMIs, 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 NPPs do not own backup and restore facilities dedicated to databases and software. NPPs 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 [9]. NPPs 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 [11], 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. The security controls that 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 [8].

C. *Industry and Government Responses to NPPs Cybersecurity*

In the previous section, known attacks and vulnerabilities in NPPs 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 NPPs.

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 (VPNs) 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 [10].

NPPs 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 NPPs 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 NPPs 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 NPPs [9]. NIST has published a well-established risk management framework in NIST Special Publications (SP) 800-30 [12], 800-37 [13], and 800-39 [14], 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 [4]. 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 [15], 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 [16], which gives guidelines for initiating, implementing, maintaining, and improving information security management in organizations [9]. NRC's cybersecurity regulations necessitate each NPPs 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 [3].

As a result, cybersecurity has been adopted as NPPs regulation requirement under the US code of federal regulation (CFR) [2]. Also, regulatory agencies like the US NRC and IAEA created and distributed regulatory guidelines, considering construction of cybersecurity plans and programs for NPPs. The IAEA and World Institute for Nuclear Security (WINS) are multiplying their efforts in order to protect NPPs 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 [17] was issued by IAEA as a technical guidance for guaranteeing computer security at nuclear facilities. Similarly, the IAEA NSS-13 [18] 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 NPPs information systems were also addressed. Additionally, nothing like usual ICS and SCADA systems, governments, and NPPs regulatory agencies specify that NPPs I&C systems must comply with the following firm safety requirements [4][19]:

- 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 NPPs 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 NUCLEAR POWER PLANTS

Standards are endorsing the improvement of cybersecurity in NPPs. 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 NPPs.

Designed for I&C systems in NPPs, 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 [20], IAEA, in addition to country precise guidance in the technical and security application area. Designers and operators of NPPs (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 [20] 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. The major differences between this standard and usual IT systems or industrial automation systems standard are the safety classification of I&C nuclear systems and related safety requirements. IEC 62645 [20] was issued in August 2014, and IEC 62859 [21] was published in 2016, along with this new standard related to cybersecurity controls, are planned to be used for I&C systems and NPPs. 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 [20], 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.

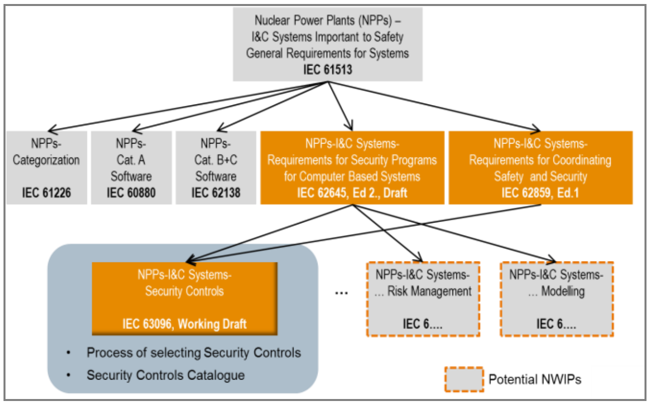

Figure 2. New IEC 63096 Security Controls standard in the SC45A standards hierarchy [3].

Concerning controls three cases are distinguished, using the guidance provided by the Draft ISO/IEC 27009 [22] on sector specific security controls. The following three cases on the refinement of ISO/IEC 27002 security controls are examined [16]:

- Security controls are adopted from ISO/IEC 27002 [16] 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 [16] were modified and described in details to better.
- 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 [16] clause (5 through 18. This is the case where the ISO/IEC 27002 [16] does not define specific security controls needed in nuclear I&C.

IEC 62541 [23] 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 [23]:

- 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 [23] (OPC UA) and IEC 61850 [24] (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 [25].

V. Conclusion

This paper gave an overview of security vulnerabilities in I&C systems and EPS inside NPPs, 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 [3] had being given. The improved performance digital technology has offered a significant influence on I&C systems design in NPPs. 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 NPPs, 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] 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.

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

[3] 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.

[4] 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.

[5] Andrews, M. Holt, “Nuclear Power Plant security and vulnerabilities,” Congressional Research Service, January 2014.

[6] 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.

[7] 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.

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

[9] 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.

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

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

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

[13] 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.

[14] E. Aroms, “NIST Special Publication 800-39: Managing Information Security Risk,” NIST, 2012.

[15] “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.

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

[17] IAEA Nuclear Security Series No. 17, “Computer Security at Nuclear Facilities,” IAEA, 2011.

[18] IAEA Nuclear Security Series No. 13, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities,” IAEA, 2011.

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

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

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

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

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

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

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