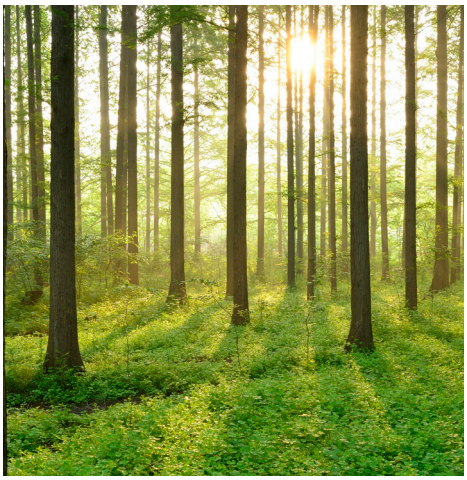
INDUSTRIAL INTERNET OF THINGS IN NUCLEAR

REPORT 2021:726



NUCLEAR

DIGITALIZATION IN
NUCLEAR APPLICATIONS

Energiforsk

Industrial Internet of Things in Nuclear

Feasibility study

ARTO LAIKARI & JERE BACKMAN

ISBN 978-91-7673-726-2 | © Energiforsk January 2021 |Cover illustration modified from Pixabay
Energiforsk AB | Phone: 08-677 25 30 | E-mail: kontakt@energiforsk.se | www.energiforsk.se

Foreword

Industrial Internet of Things (IIoT) is a rising technology, which is predicted to have an enormous impact also in the nuclear power plant context in the close future.

Curently, IIoT is not implemented at the Nordic nuclear power plants (NPPS) to a large extent, but projects to build wireless networks are currently either ongoing or planned. When wireless networks become available at the Nordic NPPs, IIoT applications could be feasible for some functions.

To be prepared for this development and avoid mistakes when building IIoT infrastructure, the Energiforsk Digitalization in nuclear applications program has commissioned senior researchers Arto Laikari and Jere Backman at VTT to gather information on IIoT in a nuclear perspective.

The Energiforsk Digitalization in nuclear program is financed by Vattenfall, Uniper/Sydkraft Nuclear, Fortum, TVO, Skellefteå Kraft and Karlstads Energi.

Sammanfattning

Målsättningen med denna studie var att identifiera och sammanställa information om existerande industriella ”internet of things” (IIoT) lösningar som används i kärnkraftsindustrin samt i andra industrier som kan tillämpas i den nordiska kärnkraftsindustrin.

Under de senaste åren har digitaliseringen varit ett av de huvudsakliga teman i utvecklingen av olika industrier och samhällen. Den snabba utvecklingen inom trådlös kommunikation och IIoT relaterad teknologi har öppnat nya affärsmöjligheter och skapat nya serviceformer och lösningar som tagits i bruk av olika intressenter. Industriell IIoT används som term då IIoT principer tillämpas i industriella faciliteter och processer.

Nordiska kärnkraftverk har designats och byggts före digitaliseringens tids era. Det innebär att dessa kärnkraftverk saknar IIoT lösningar i själva kraftverken. Saknaden av IIoT lösningar gäller även för många internationella kraftverk som byggts före digitaliseringens tids era.

Digitaliseringen har gått framåt stort i samhället och positive erfarenheter uppmuntrar kärnkraftsindustrin att också följa I dessa fotspår. Trots att det förekommer tvivel och motgångar som hindar adapteringen av IIoT inom kärnkraftverken, görs det mycket satsningar på att överkomma hindren och restriktionerna som är specifika för kärnkraftsindustrin. Olika intressenter inom industrin samt forskare jobbar tillsammans med industrin på detta.

Ett huvudsakligt mål med denna studie var att erbjuda stöd åt de nordiska kärnkraftverken att börja planera och ta i bruk IIoT.

Denna studie baserar sig på en on-line förfrågan som gjordes åt utvalda experter från de nordiska kärnkraftverken samt på en litteratur undersökning från olika källor, erfarenheter från relevanta forskningsprojekt och egen praktisk erfarenhet.

Summary

The aim of this study was to identify and compile information of existing industrial Internet of things (IIoT) solutions used both in nuclear industry and other industries, which could be applicable to the Nordic nuclear industry.

In recent years, digitalization has been one of the mainstream driving themes across industries and society. Rapid advancements in wireless communication and Internet of things (IoT) related technologies have opened new business opportunities and created new services and solutions, which various stakeholders take into use. Industrial IoT (IIoT) is used as a term, when IoT principles are applied in industrial plants and processes.

Nordic nuclear plants (NPPs) have been designed and constructed before the digitalization age has started. This results to the fact that these NPPs are lacking the IIoT solutions in the actual nuclear plants. Missing IIoT solutions applies also many international NPPs, which have been built before the digitalization era.

Digitalization is advancing in the society and positive experiences encourage also the nuclear industry to follow these steps. Although there exist also doubts and obstacles hindering the IIoT adoption in NPPs, various nuclear field stakeholders and research communities together with the nuclear industry are studying opportunities to overcome the additional obstacles and restrictions specific to the nuclear industry.

One main target of this study has been to offer support for the Nordic nuclear plants to start planning and adopting the IIoT into use.

This study is based on on-line surveys with selected experts from the Nordic nuclear power plants as well as on literature reviews from various sources, experience gained from relevant research projects and own practical experience.

Abbreviations

2G - 2nd generation mobile networks / 2nd generation wireless systems

3G - 3th generation mobile networks / 3th generation wireless systems

4G - 4th generation mobile networks / 4th generation wireless systems

5G - 5th generation mobile networks / 5th generation wireless systems

AAKR - Auto Associative Kernel Regression

AI - Artificial Intelligence

AR - Augmented Reality

ATEX - Appareils destinés à être utilisés en ATmosphères EXplosibles

CBM - Condition-Based Maintenance

CIs - Critical Infrastructures

CM - Condition Monitoring

COTS - Commercial Off-The-Shelf

CRP - Coordinated Research Project

DAS - Distributed Antenna Systems

DLT - Distributed Ledger Technologies

DOE - U.S. Department of Energy

EMC - ElectroMagnetic Compatibility

EMI - ElectroMagnetic Interference

EPRI - Electric Power Research Institute

ERS - Emergency Response System

ETSI - European Telecommunications Standards Institute

FoF - Factory of the Future

GPS - Global Positioning System

IaaS - Infrastructure as a Service

IAEA - International Atomic Energy Agency

I&C - Instrumentation and Control

ICT - Information and Communication Technology

IEC - International Electrotechnical Commission

IEEE - Institute of Electrical and Electronics Engineers

IIC - Industrial Internet Consortium

IIoT - Industrial Internet of Things

IIRA - Industrial Internet Reference Architecture

IISF - Industrial Internet Security Framework

IoT - Internet of Things

IP - Internet Protocol

IPSec - Internet Protocol Security Architecture

IPv4 - Internet Protocol version 4

IPv6 - Internet Protocol version 6

IWLAN - Industrial Wireless Local Area Network

LPWA - Low Power Wide Area

LTE - Long Term Evolution

LTE-M - Long Term Evolution for Machines

LTO - Long Term Operation

MEC - Mobile Edge Computing

M2M - Machine to Machine

NB-IoT - Narrowband Internet of Things

NEA - Nuclear Energy Agency

NFC - Near-Field Communication

NPP - Nuclear Power Plant

NRC - U.S. Nuclear Regulatory Commission

OECD - Organization for Economic Co-operation and Development

PaaS - Platform as a Service

pLTE - Private Long Term Evolution

PRIS - Power Reactor Information System

RFID- Radio Frequency Identification

SaaS - Software as a Service

SCADA - Supervisory Control And Data Acquisition

SKB - Svensk Kärnbränslehantering AB

SSM - Swedish Radiation Safety Authority

SSO - Single Sign-on

STUK - Radiation and Nuclear Safety Authority of Finland

TCP/IP - Transmission Control Protocol / Internet Protocol

TETRA - Terrestrial Trunked Radio

UHF - Ultra high frequency

UWB - Ultra-WideBand

URL - Underground Research Laboratory

VoIP - Voice over Internet Protocol

VR - Virtual Reality

WLAN - Wireless Local Area Network

WMAN - Wireless Metropolitan Area Network

WPAN - Wireless Personal Area Network

WSN - Wireless Sensor Network

List of content

1 Introduction

Figure 1 Smart city illustration (source Pixabay.com).

Even though the Internet of Things (IoT) has not yet revolutionized our lives, the number of devices connected to the web is constantly increasing and the business potential of IoT solutions is growing. Many people associate the Internet of Things with home appliances or smart lighting, but the most common IoT devices are, for example, remotely read electricity meters. Many other IoT devices in use today are also various measuring instruments that can be used to save energy or improve the efficiency of operations. An IoT device installed on site can, for example, monitor the condition of a machine and indicate need for maintenance. Collecting data and thereby understanding the operation of the target is the most significant benefit of IoT.

Industrial IoT (IIoT) is the application of the same "consumer" IoT principles to industrial plants and processes. For example, gathering process data, temperatures, flow rates, vibration, and other measures to enable IIoT system to make plants more efficient, safer, reliable, etc. Industrial technology providers have IIoT offerings, products devices, and services. IBM's Watson, GE's Predix. Schneider's EcoStruxure, Honeywell's Sentience. [23]

Industrial Internet of Things (IIoT) is a rising technology, which is predicted to have an enormous impact also in the nuclear power plant context in the close future. At the moment, IIoT is not implemented at the Nordic nuclear power plants (NPPs) to a large extent, but projects to build wireless networks are currently either ongoing or planned. When wireless networks [1] become available at the Nordic NPPs, IIoT applications could be feasible for some functions. To be prepared for this development and avoid mistakes when building IIoT infrastructure, it has been seen feasible to gather information on IIoT in a nuclear perspective.

It should be noted that IoT can be considered as an umbrella definition and lot of technologies are needed in order to build a complete working IIoT system. Depending also on the source, concepts and definitions are also overlapping. Example wireless issues are often an integral part of an IIoT system. These technologies are discussed in the following chapter 2.

1.1 OBJECTIVE

The aim of this study is to identify and compile information regarding existing Industrial Internet of Things (IIoT) solutions used by the nuclear industry and in other demanding environments, which could be applicable in the nuclear industry. The study depicts and takes into account reasons why and how to use IIoT solutions in the nuclear field and what pitfalls should be taken into account in order to achieve a successful IIoT solution. The specialty of the nuclear field is accounted for in the work and the constraints presented by specific regulations, restrictions and higher security and reliability requirements will be addressed, including cyber security aspects.

1.2 BACKGROUND

This study is based on a survey with selected experts from Nordic utilities, utility owners and regulators and on literature reviews. Experience and knowledge gained from previous and on-going research projects have been utilized, as well as established networks with relevant regulators, research organizations and industry bodies both domestically and internationally.

1.3 STRUCTURE OF THE REPORT

This report is divided into five main sections. The first section is the introduction where the scope and the background of this study is defined.

In the second section we present main definitions in IIoT and related key technologies and issues, like wireless technologies, data storage, data management and cyber security.

The third section presents the IIoT applications in the nuclear field. First part of this section is dedicated to the regulatory requirements and restrictions, which is followed by the discussion of standardization issues. Next, we present a brief summary of the IIoT applications used in the Nordic nuclear power plants, as well as the future plans and wishes of the IIoT usage in them. Information in this part is collected from the surveys with the representatives of the Nordic NPPs. End part of the section picks up some examples of the IIoT usage in the international NPPs. Information in this latter part is based on the literature survey.

The fourth section presents wireless technology examples from other industries to encourage the nuclear industry to consider the possibilities of the IIoT technology usage in the NPPs.

The last section summarizes the findings from the previous sections. Opportunities and challenges using the IIoT applications in nuclear power plants are presented

and some proposals for IIoT application business models and strategies. This final section contains also guidelines for making the first steps to start defining the adoption the IIoT technologies into use in the nuclear power plants.

Keywords

Nuclear, nuclear plant, I&C, Internet of Things, IoT, Industrial Internet of Things, IIoT, digitalization, wireless, cyber security

2 IIoT technologies

IIoT technologies are enablers for the IIoT based solutions, and the value those bring depends on the use cases that make the actual impact to the enterprise's operations [45].

There are vast amounts of enterprises already exploiting or pursuing initiatives to build and enable IIoT solutions to achieve operational effectiveness. When enterprises are about to adopt IIoT, they should assess the entire technological stack of offerings and how it complies with their needs, current technology and legacy systems. [46]

In the following chapters enabling IIoT technologies are discussed in general, but also handling the wireless connectivity technologies in nuclear point of view, and especially cyber security. Multiple sensors can produce massive amounts of data, which needs to be handled and interpreted. Data management issues are briefly discussed in the last part of this chapter.

IIoT and other related new technologies are also considered enablers of the fourth industrial revolution, which is also referred as Industry 4.0.

Earlier the trend to use computerized systems was to develop and maintain the systems in-house at the organization. Larger systems were often also proprietary developed for each individual site, as it was often impossible to find an existing ready solution to fulfil all the requirements or there was the wish to keep the system completely self-managed. At present, digitalized systems have grown already so complex and also include parts beyond the organization borders, which makes it impossible for a single actor to develop and maintain the whole system in-house.

2.1 IIOT TECHNOLOGIES

The exploitation of Internet-of-Things technologies is continuously raising, and the number of platforms is increasing all the time. Companies are developing new Industrial Internet based business or service models by using IoT platforms as a backbone infrastructure for IIoT. Companies have already added connectivity features to new machines, vehicles and other product models. Collected and analyzed real-time data supports profitable business and efficient operations according to use cases planned. [43]

"IoT platforms help reduce the cost of developing IoT-based services and applications. Without an IoT platform, the challenges of building an IoT application are significant: developing the application logic user interface and database, and developing data analytics. However, IoT platform providers leverage the underlying technologies and assets they have, while taking into consideration their business models and customers. Understanding what each provider offers is required when evaluating IoT platforms because selection of the underlying platform can be a critical decision for an IoT-based service developer. In general, switching platforms can be messy, expensive, time-consuming, and

painful. One of the issues for the IoT community has been the proliferation of architectures and communication protocols. However, standardization bodies such as the IEEE Standards Association, the Internet Protocol for Smart Objects Alliance, the Industrial Internet Consortium, and the Open Interconnect Consortium are working on common architectures and communication protocols." [41]

The first challenge companies face, when considering the exploitation of IIoT solution, is choosing the suitable (I)IoT platform to serve their business purposes, use cases and needs. For example, "Evaluation of Internet-of-Things Platforms for Asset Management" paper presents the business and technical perspective-based approaches for evaluating IoT platforms for asset management purposes. The aim of the case study was to identify essential issues that must be noticed and to specify the requirements which the selected platform must meet to enable efficient asset management. [43]

Regarding to asset and fleet management, that is quite common use case for IIoT applications, "IoT-based Interoperability Framework for Asset and Fleet Management" paper provides a systematic outline to the ingredients of the framework and discussing their impact in an industrial setting. The paper defines a technical framework for IIoT based assets and fleet management solutions and the necessary set of functionalities that the framework should support as a base. The framework can be divided into the Operations, Data management, models and standards, User characteristics, Security considerations, and Interoperability. The framework is based on the work by The Open Group's Open Platform 3.0 initiative. [44]

In general, IIoT decisions and investments in industry are complicated because of fragmentation in industry subsectors and the mission-critical requirements of the technology. The largest industrial and technology firms are investing billions in their (I)IoT platforms. Technologies like sensors, connectivity, processing, cloud services and analytics applications are usually clear and available, but the selection of (I)IoT platform is usually a more challenging task. There are several case / enterprise specific challenges to be handled, for example integration to legacy systems / existing environment, security management, and the future of the platform / provider possibly selected. [2].

For example, Industrial Internet Consortium's (IIC) Industrial Internet Reference Architecture (IIRA) defines, what needs to be considered and addressed beyond the design phase of the system into its full lifecycle. IIRA gives viewpoints, provides guidance to system lifecycle processes from IIoT system conception, to design and implementation. The reference architecture is an architectural framework and methodology for system conceptualization and architecture highlighting important system concerns that may affect lifecycle process. During the lifecycle process Business Viewpoint guide usage, functions and implementation in the way Figure 2 depicts, whatever the application domain / industrial sector for the application is. [47]

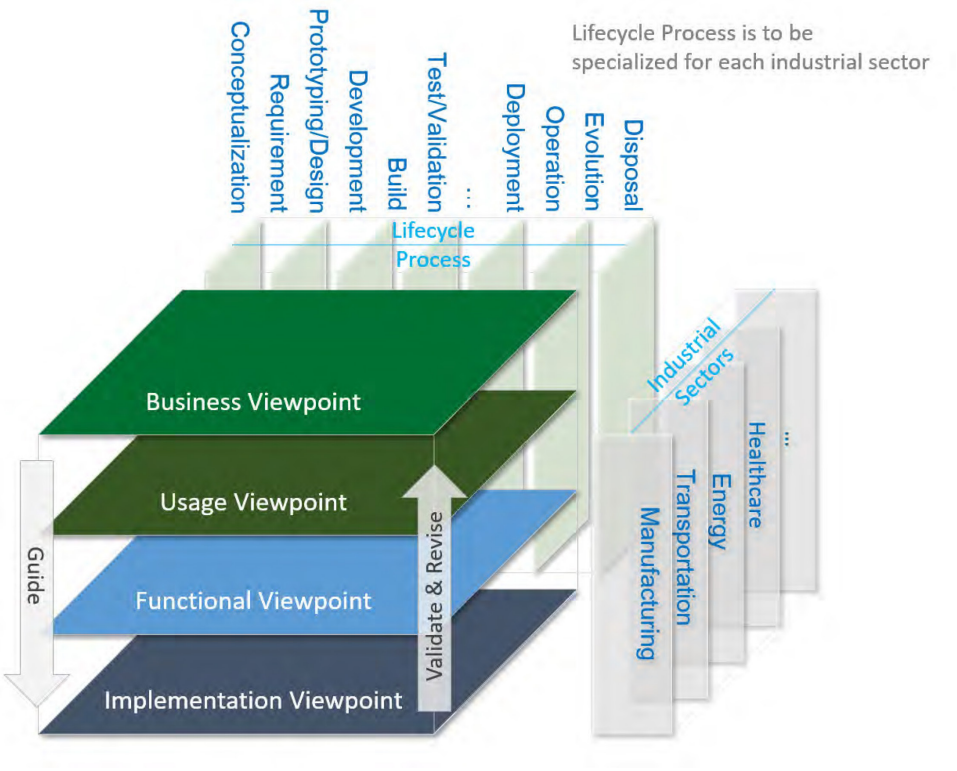


Figure 2. Industrial Internet Consortium's (IIC) Industrial Internet Reference Architecture (IIRA) [47]

Despite different IIoT consortium reference architecture efforts, there is an urgent need for standardization, governance, and regulation [3]. When considering the things / devices, a comparative overview of operating systems, communication technologies, protocols, innovative application and associated challenges for the IoTs. In the paper "Internet of Things (IoT) Operating Systems Support, Networking Technologies, Applications, and Challenges: A Comparative Review", the key requirements for IoTs applications their required architecture, proposed algorithms, language support, management of power and memory have been analyzed. The paper provides an overview of the major challenges facing IoTs and concludes that security, privacy, and interoperability are the main challenges faced by the IoT. [4]

The paper "The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview" shares the concern relating to the standards. Although the IoT enabling technologies has tremendously increased in the past decade, there are many issues to be opened and addressed. These include architecture, privacy and security, data intelligence, Quality of Service, communication protocols, GIS based visualization, etc. [6]

In nuclear sector systems are usually critical systems. Lack of standardization may lead to weaknesses of the critical systems. There are four general classes of attacks for the integrity, availability, confidentiality, access control, authentication, and nonrepudiation security aspects [23]:

1. Interruption leads to the situation where asset availability is disrupted.
2. Interception allows unauthorized asset access.
3. Modification aims for unauthorized asset tampering.
4. Fabrication tries fictitious asset creation.

Security solutions are needed to overcome these risks and protect the (I)IoT devices, networks, and sensitive data from security breaches and unauthorized access. [23]

Vendors are nowadays aware of the importance of information security in IoT. For example, an article "IoT System Security Issues and Solution Approaches" focuses on availability, which is one of the key requirements for IoT security for critical infrastructure. The article presents approaches for proceeding from problem detection to provisional measures to ensure availability, and detection technology developed by Hitachi. [37]

The cyber security issues are discussed more in the chapter 2.4, Cyber security.

2.2 WIRELESS TECHNOLOGIES

In order to transfer the data and control signals between devices and systems, communication methods play an important role in the IIoT systems. Communication between the various parts in a complex IIoT system often contain both wired and wireless communication methods. In the older nuclear plants, wireless communication has traditionally been very limited or even not existing because of several restricting guidance and rules.

In the "Wireless in Nuclear Feasibility Study" [1] existing wireless solutions used in nuclear industry and other industries and services (e.g. mining sites, factories and military) have been studied to identify and compile information about possibly applicable wireless solutions and technologies in nuclear industry.

Technological development of wireless technologies has advanced very much in recent years and novel sensors and radio technologies provide the opportunity for creating extensive wireless sensor networks to monitor and control complex systems without wires. These advancements have also enabled the mobility of personnel as well as applications creating new ways to optimize the operations in all business sectors. Nuclear industry has been very cautious to adopt wireless technologies. Reasons for this are the strict regulatory issues concerning safety and reliability and fear for new cyber security threats and electromagnetic interference with other existing nuclear power plant (NPP) legacy systems. Typical heavy wall structures of the NPPs create also the challenge for the wireless signal propagation, but there exist mitigating solutions to overcome this problem. These solutions include e.g. signal repeaters, distributed antenna systems (DAS) and directed antennas. Also, to many other thinkable disadvantages to use wireless technologies in challenging environments countermeasures have already been developed. However, the study reveals that there is an increasing interest among NPP owners and operators to start using wireless technologies and various wireless pilots have already been tested in many countries for several years. Research communities together with the nuclear industry are studying opportunities to overcome the additional obstacles and restrictions specific to the nuclear industry. Other industries are already using wireless technologies in countless ways. The NPPs, standardization bodies and regulators are in the process to accept eventually the use of wireless technology in the NPPs. [1]

Some parts of IoT systems could be built using only wired connections, but normally the modern complex IoT systems are also utilizing several wireless technologies. In the "Wireless in Nuclear Feasibility Study" report, many commonly used wireless technologies, which can be used in the IoT systems, have been introduced. These include among others the following technologies:

- 2G/3G/4G Cellular Networks
- 5G Networks
- LTE/pLTE Networks
- Satellite communications
- TETRA
- DECT
- Various wireless sensor networks (Bluetooth, Zigbee, Z-wave, …)

- Narrowband IoT (NB-IoT)
- Low Power Wide Area (LPWA) (Sigfox, LoRa)
- WLAN
- WMAN/WiMAX
- Distributed Antenna Systems (DAS)
- Ultra-WideBand, UWB
- Wireless technologies used for Location, identification and presence services
- Low frequency Wireless Technologies
- Other wireless technologies, like Optical Wireless Communication (OWC) (e.g. Visible Light Communication (VLC) or infrared communication (IrDA), also ultraviolet wavelengths can be used for optical communication).

Wireless technologies bring the advantage to free the system from the signal wires, but depending on the system, the power supply cables might still be needed. In certain environments, this is not an issue, but if the power supply cabling is hard to implement, systems can adopt other power supply solutions. Power supply for certain equipment can be provided with batteries, wireless power transmission or other energy harvesting systems.

Currently wireless technologies are using most often various radio frequency communications, but this is often considered as a risk or at least a challenge in the old NPPs, because of the electromagnetic interference (EMI) impact to the old I&C systems. When these old control systems have been designed and implemented, it has not been taken into account the existence of nearby radio transmitters. Because of this, sometimes other wireless technologies, like Optical Wireless Communication (OWC) is raised in discussions as a safer communication method, which could act as a communication method free of electromagnetic interferences. Various radio frequency communication methods are however the mainstream solution and their volumes are much higher than OWC.

In the IIoT systems, wireless communication can be used for local communication and/or long-distance communication. Locally the wireless communication can be used e.g. to transfer the data and control signals between the sensors, actuators and local gateways or in general in the locally created wireless sensor network. In the long-distance communication, the information can be transferred between geographically distant locations or even with other stakeholders, if needed.

2.2.1 4G networks, LTE-M and NB-IoT

5G is in an emerging phase and currently many IIoT systems are still using the 4G, LTE-M and NB-IoT networks for long distance communications. Besides the telecom operator run networks, private networks start getting granted licenses.

In summer 2020, there was an announcement that the Loviisa power plant was granted a private license for their own mobile network. This private network is based on a private-LTE network. According to Fortum's press release published on 07.07.2020 16:45: "The Finnish Transport and Communications Agency Traficom responds to the changing needs of digitalized society by granting the first ever license to local mobile networks. These radio networks for a limited user group implemented by mobile communications technology are intended to be used

locally in, for example, factories, ports, airports, power plants and mines for their own operations. The first, and thus historical, radio license for frequency band 2300-2320 MHz was granted to Fortum's Loviisa Power Plant." [69]

Besides operator run LTE networks, these private LTE networks have also been used in some industrial environments across the world. Danfoss is piloting and researching the benefits of the private 5G ready LTE network in their factory environment, which is producing VACON frequency changers. This example shows that the private LTE installation can also provide a pathway towards a private 5G networks.

2.2.2 5G networks

The 5th generation of mobile networks (5G) is the latest version of the cellular network family, which is currently emerging. Data rates and latencies of the 5G networks enable significantly increased operational performance compared to the earlier versions of cellular networks and it opens new business opportunities for novel applications in industry field. Figure 3 presents an example landscape of the future 5G network. Although the latest 5G standards have been finalized during 2020 by ETSI, many telecom operators have already launched their commercial 5G networks and started to provide 5G services.

During 2019 and especially 2020, operators have started their own 5G networks both in Sweden and in Finland as well as in other countries and now there exist 5G subscriptions and also equipment for the network, because also the device vendors have started to provide 5G capable devices.

Some of the big device vendors are however still warning that the 5G ecosystems are still limited and it will take few years, before they are mature enough to fully support large industrial applications.

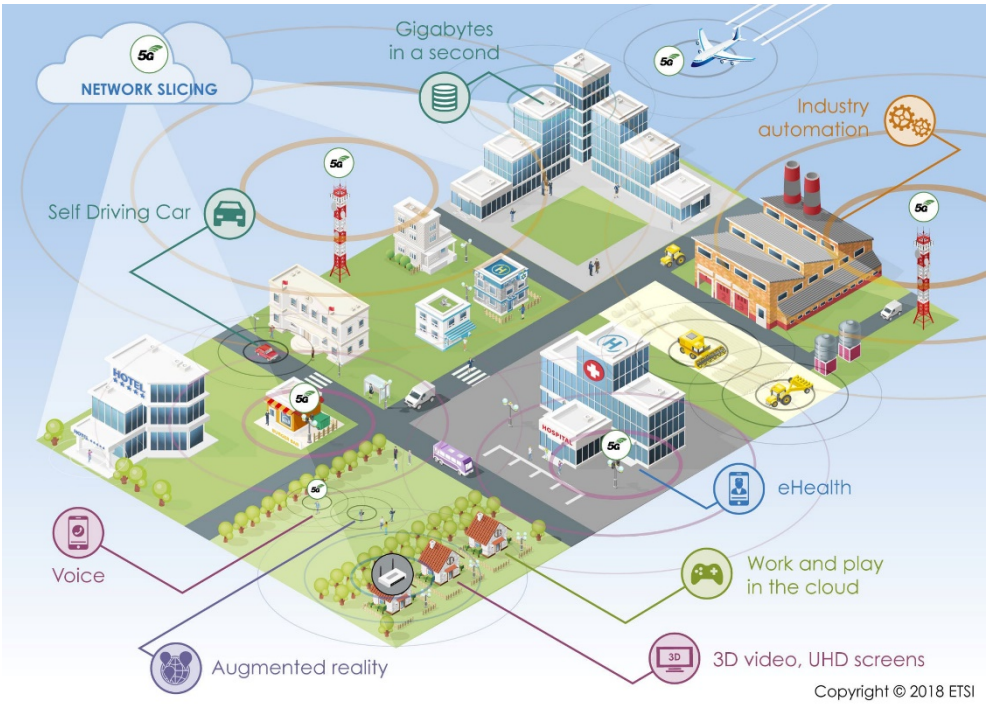


Figure 3 5G usage areas. © ETSI (https://www.etsi.org/technologies/mobile/5g)

Pilot installations of "own" 5G networks have been made and as the 5G will spread and evolve, most likely the amount will increase already in the near future. Operator Telia has had some pilots with Nokia e.g. in the Helsinki-Vantaa airport and in an ABB frequency converter factory and also in the Oulu region in Finland. Danfoss has also established a private LTE network, which is 5G ready to support their product line and warehouse management operations. Telia has also other pilots with Ericsson in another ABB factory. In Japan, Fujitsu was granted a commercial private 5G license for an AI-powered security system, which was announced May 2020. In Oulu, Finland, Nokia has been promoting the Industry 4.0 standard with Nokia's future factory, which was recognized in 2019 by McKinsey and the World Economic forum as an advanced 4th industrial revolution light house.

2.2.3 Software Defined Wide Area Networks (SD-WAN)

Various radio technologies for short range transmissions have been used for a long time in the IoT systems, but the rapid evolution of the long-distance communication suitable for the IoT systems has opened new opportunities to build larger complete systems. Network operators are offering companies software defined Wide Area Networks (SD-WAN), where hybrid networks consist of various geographical location sites fixed infrastructures, cloud environments and mobile networks.

2.2.4 Distributed Antenna Systems (DAS) and directed antennas

To overcome the reception difficulties through thick walls in the NPPs, distributed antenna systems (DAS) can be used. DAS system can be used together with directed antennas in the areas, where there are doubts of electromagnetic interference (EMI) with the old legacy I&C systems.

In USA also exclusion zones to mitigate the issue of interference with sensitive equipment is used. Exclusion zones are defined distances from the sensitive plant equipment, where radio transmitters are not allowed. Electric Power Research Institute (EPRI), U.S. Nuclear Regulatory Commission (NRC) and other instances provide guidance how to calculate the exclusion distance taking into account the power output and antenna gain of the wireless transmitter. Some experts have also expressed comments that the distances according to the calculations are overly conservative, as they are not taking into account the used frequency. Higher radio frequencies tend to cause less interference, so updating the calculation methods, smaller exclusion zones could be used, which would allow better use of wireless devices in the NPPs. [68]

2.2.5 Advantages and disadvantages to use wireless technologies in the NPPs

In the earlier wireless in nuclear feasibility study, we have collected advantages and disadvantages to use wireless technologies in the NPPs. As the predicted long-term prediction is that wireless solutions will enter in some form also into the old NPPs, the disadvantage summary table contain also the suggested countermeasures to mitigate the threats. Both the collected advantages and disadvantages with proposed countermeasures can be found from the following tables (Table 1 and Table 2). [1]

Table 1 Advantages of wireless technology usage in the NPPs [1].

Advantage of wireless	Issue	Notes
lower installation costs	No signal cable installation needed. Wireless base stations can be installed in plants at lower costs.	Cabling costs especially in a running NPP are very high. Hashemian has given an estimate of 2000$ per foot (~6000$ per meter) in his report Nuclear Power Plant Instrumentation and Control [65].
lower maintenance costs	No broken cable repairs needed.	
reduced connector failure	During time, cables and connectors can get damaged.	
rapid deployment	Installing sensors and base stations for communication is fast, when signal cables are not needed between them. No cable routing planning or mechanical work for cable installation needed.	

Advantage of wireless	Issue	Notes
less or no wires	Signal cables are not needed. Power cables do not require long routes compared to signal cables. In some locations, battery operated equipment can be used.	Battery operated equipment can be used for moving terminals and temporary / short period measurements or controls.
increased mobility and collaboration convenience of use	Network can be accessed from various locations, not only from fixed location terminals. Alarms can be transmitted to several locations and terminals, not only to control room fixed terminals.	
better access to information	Information and controls can be accessed everywhere.	E.g. in maintenance work information and support can be accessed where needed with documents and AR & VR solutions.
easier network expansion	It is easy to expand wireless networks with existing equipment, whereas a wired network often requires additional wiring.	
easier network modifications	Without cables, sensors, nodes, terminals and other equipment can easily be relocated.	
security	All communication can be encrypted. Access can be managed and monitored.	
access to difficult locations	Locations, which are hard to reach can be covered with wireless communication. Without wiring more dense measurement points can be created.	
option for guest access	Temporary access can be granted for external maintenance personnel.	
new operation possibilities	Mobility and reach of difficult places open possibilities for novel applications not earlier used in NPPs.	Wireless technologies open cost efficient ways to implement more dense measurement points than with cabled connections is feasible. Novel measuring e.g. of rotating equipment could be implemented.

Table 2 Disadvantages of wireless technology usage in the NPPs [1].

Disadvantage of wireless	Issue	Countermeasures
cyber security	Various attack scenarios, which concern both wired and wireless networks.	Follow guidelines and design principles of wireless cyber security experts. Follow guidelines and design principles of military electronic warfare and electronic counter-countermeasures.
information saturating radio waves	Information is not transmitted via known dedicated cable routes, but information is spread to the whole space and even behind walls.	Design and control appropriate power levels for transmissions. Keep perimeter restricted, where wireless network is covered. Strong encryption of all transmitted data.
eavesdropping	Unauthorized persons can listen and monitor the data transmitted.	Strong encryption of all transmitted data.
unauthorized use	Unauthorized persons can control the systems.	Strong encryption of all transmitted data. Access and user authentication management. Monitor and log access events.
jamming	Blocking or interfering authorized wireless communication.	Use wide spectrum communication (e.g. UWB), frequency hopping technologies and/or directional antennas. Use mesh network topology in wireless network (network provides several routes for the messages). Keep perimeter restricted. Use tools to detect unauthorized transmissions.
difficult planning	Wired connections are “easy” to plan. Designers have long experience in routing cables. Wireless networks are hard to design in harsh environments.	Model, test and design wireless networks with known principles and modern tools. Utilize lessons learned from other industries. Avoid use of wireless systems for automatic feedback systems, at least for critical functions.
lower reliability	wireless communication can fail	Careful planning of the network. Utilize lessons learned from other industries.

Disadvantage of wireless	Issue	Countermeasures
lower communication speed	Radio communication is slower than wired communication.	Novel radio technologies provide high speed communication. Many applications do not require massive data transfers, so speed is not a critical issue.
wireless technologies cannot be used	Heavy structures and obstacles for radio wave propagation prevents communication.	Careful planning of the network. Utilize lessons learned from other industries. Use repeaters and appropriate antennas meant for harsh environments.
interference with other NPP systems	Electromagnetic compatibility (EMC) with other NPP systems is not guaranteed. Old systems are not designed concerning wireless equipment presence. Motors and other electrical equipment generate radio noise, which prevents or disturbs wireless communication.	In the new NPPs plants already in design phase EMC and EMI issues can be take into account. In the old plants: Use low signal levels. Shield and ground equipment. Use exclusion zones, filtering and other EMI protection methods.
interference with other wireless systems	Using multiple wireless technologies, they can interfere and disturb each other.	Careful planning of the wireless system (locations, transmission levels, coexistence, radio zones). Maintenance of the plant radio frequency table.
energy sources for the wireless devices	Service time for battery operated devices is limited.	Some equipment can use normal wired electrical supplies. When signal cables are not needed, it makes still sense to use wired supply. Energy harvesting for low power equipment. Usage of zero power or nearly zero power sensors.
radiation influence	Radiation disturbs the equipment operation or prevents it.	Radiation influences all electronic equipment, wired and wireless. Similar protection against radiation effect can be used. There exist also many areas in NPPs, where wireless applications are feasible, and radiation is not an issue.

2.3 DATA MANAGEMENT

Large real time Industrial IoT systems with high-speed communication are producing massive amounts of data, which need to be processed, stored and analyzed. This is not feasible or even possible to do in the sensor nodes. Cloud and edge computing and big data analytics with artificial intelligence provide the tools to manage and store the massive amounts of data.

2.3.1 Cloud and edge computing

Large amounts of data is not feasible and often not even possible to be stored in the IoT devices. IoT nodes and components can have a local buffer memory, which can store data from certain period (e.g. hours, days or months depending on the data collection (sampling) rate. These measurements need to be transferred with some of the earlier mentioned communication methods to a bigger data storage.

This data storage can be a company specific cloud or server environment, or a commercial data operator offered cloud service built for the IoT systems. Along with the evolving 5G networks, edge computing has been introduced to make data storing more efficient. Edge computing is a distributed computing paradigm that brings computation and data storage closer to the location where it is needed, to improve response times and save bandwidth. Edge principle is presented in the following Figure 4.

With IoT, it can also improve the security of the system, as the low computing power IoT devices are not exposed to the wider networks. Edge computing can be further divided to four subcategories [66], like:

- Telecom operator Edge, which brings the processing power to the mobile network base station infrastructure.
- Enterprise Edge, which brings the processing power and intelligence to the company's own premises.
- IoT Edge, which brings the processing power to a dedicated IoT gateway, which is located near the user location.
- Device Edge, where the processing power is in the autonomic end device.

In the nuclear field, data security plays an important role and NPPs want to keep the important, confidential and safety critical data in their own servers and not use the global cloud operators.

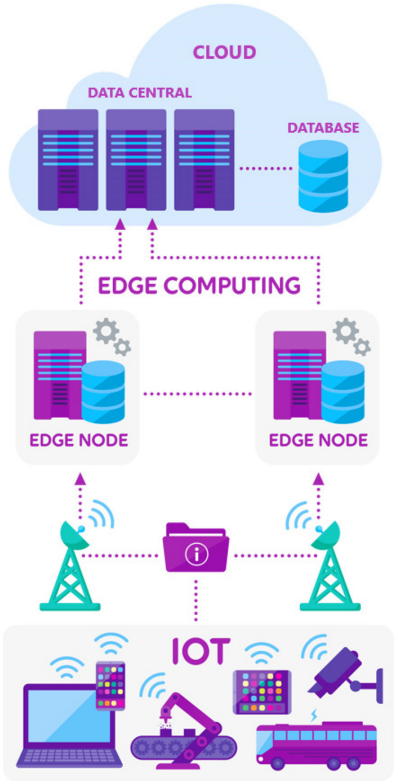


Figure 4 Edge computing principle. (Figure source Telia)

Cloud computing has also brought out new service models available for the customers compared to the traditional on-premises model, where the whole system is maintained in the company's own premises. These new models include the Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

In the Infrastructure as a Service (IaaS) model, the customer is using and managing the services and systems via a web-interface and the service provider is providing just the infrastructure platform. This model requires that the customer has experienced IT-department or other service provider to create and maintain all needed systems.

In the Platform as a Service (PaaS) model, the service provider is providing hardware and software tools over the Internet which speeds up the development, as there are ready middleware and runtime related support already in the platform.

In the Software as a Service (SaaS) model offer the whole software system as a service and it requires least from the customer, as the whole package is offered as a service. If there are many different SaaS services in use, it is possible to adopt a single sign-on (SSO) service into use, which provides user friendliness as the user needs to do only one sign-on and can then use all services without separately logging in to each of them.

2.3.2 Big data analytics

Storing massive amounts of data is not sufficient to obtain benefit from the collected data. The data also needs to be interpreted and analyzed, otherwise the data has no value. Both national and international players exist, which are offering tool frameworks for IoT and Artificial intelligence (AI) systems. Examples of such services are

- Amazon Web Services (AWS)
- Microsoft Azure
- IBM Watson
- Cloud IoT Core
- Telecom and other ICT operator IoT environments

Various telecom and ICT operators have also packaged IoT services and offer them to their customers, making it easier to adopt them into use. As noted above in the cloud and edge computing section, in the Nordic NPPs physical location of the data storage servers need to be taken into account, as there are restrictions to use servers outside of the country, where the NPP is operating. This should be remembered, when choosing the big data analytics services in the NPPs.

2.3.3 Artificial Intelligence (AI)

"AI refers to a collection of technologies that combine numerical data, process algorithms and continuously increasing computing power to develop systems capable of tracking complex problems in ways similar to human logic and reasoning. AI technologies can analyze large amounts of data to "learn" how to complete a particular task, a technique called machine learning." [51]

For example, IAEA has held a meeting discussing the use of Artificial Intelligence for nuclear applications showcased the ways in which AI-based approaches in nuclear science can benefit human health, water resource management and nuclear fusion research. [51]

As an analogy from Maslow's hierarchy of needs theory [49] in psychology, the AI hierarchy of needs can be represented as a pyramid with the more basic needs at the bottom, as depicted in Figure 5. All needs/levels of the pyramid under AI, must be fulfilled before AI can be utilized efficiently. [50]

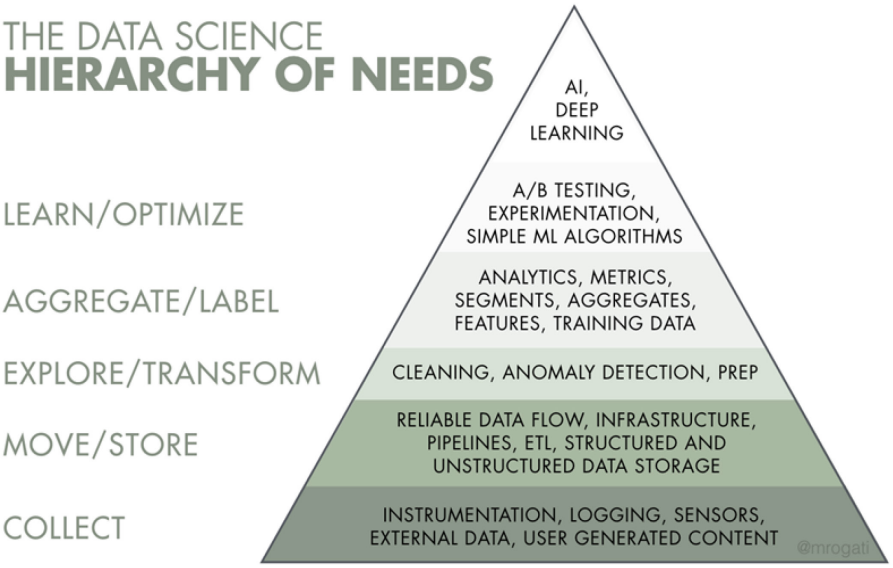


Figure 5. AI Hierarchy of Needs [50]

On the top of the AI Hierarchy of needs levels is AI that needs all the levels below it. Levels or needs Exploring/ Transforming, Aggregating/Labelling and Learning/ optimizing are typical in AI engineering as well, but the very basic lowest levels or needs relating to Collecting and Moving/storing data must be fulfilled before actual AI engineering work can begin. First of all, the data is needed, and it requires data exchange and management. [50]

2.4 CYBER SECURITY

History has shown that there is a vast group of malicious actors active who have different agendas for their cyber-attack, cyber sabotage and cyber espionage campaigns in mind. Some of them are also well resourced and have even veiled governmental support for their actions.

Cyber security is essential in (I)IoT ecosystems. Connected devices lead to complex IIoT infrastructures with multiple endpoints for cyber-attacks. The article "Why IIoT should make businesses rethink security" states that nine out of ten organizations in the operational technology sector (including critical national infrastructure providers) faced at least one damaging cyber-attack in two years. Half of those cyber-attacks resulted to downtime in the plants or operational equipment. [11]

IAEA has published a technical guidance document "Computer Security of Instrumentation and Control Systems at Nuclear Facilities" with the objective to provide guidance for the protection of I&C systems at nuclear facilities on computer security against malicious acts that could prevent such systems from performing their safety and security related functions. This publication is intended for competent authorities, including regulatory bodies, as well as nuclear facility management, operations, maintenance and engineering personnel, I&C vendors, contractors and suppliers, I&C designers, research laboratories and other organizations concerned with the safety and security of nuclear facilities. In this document, it is mentioned that new nuclear facilities and modern nuclear facility designs use highly integrated digital I&C systems. Additionally, it is also recognized that historically computer security was not given significant consideration in the design of I&C systems at nuclear facilities because hardwired or analogue systems were assumed to be invulnerable to cyber-attacks. The document presents an overview of I&C systems in use at nuclear facilities and the role of computer security in protecting these systems from cyber-attacks. Also, the relationship between computer security and safety for I&C systems is presented and the document concludes the computer security guidance to be applied in the various life cycle phases of I&C systems, including during the decommissioning of a facility. [70]

Unfortunately, the fact that historically the cyber security was not always taken seriously does not limit to old legacy systems in nuclear facilities, which were protected with other means from unauthorized access. Several early IoT systems as well as other ICT systems have also been accused of neglecting the cyber security issues, when these systems were enhanced from local connectivity to the Internet wide connectivity. As there has been several unfortunate examples, cyber security is nowadays taken more seriously. Cyber security issues need to be part of the whole life cycle of the system from design to the discharge. It should be noted that this can cause additional work, when combining old legacy systems to the new IIoT systems. Cyber security is not only an additional independent block, but an integral part of the whole system.

As presented earlier, Industrial Internet Consortium (IIC) has published the Industrial Internet Reference Architecture (IIRA). To support cyber security issues

in the IIoT architecture, IIC has also published the documents IoT Security Maturity Model: Description and Intended Use [92], which is intended for the stakeholders to understand the purpose, need and intent of the model and the Industrial Internet Security Framework: Practitioner's Guide [93], which is providing the details of the model and outlines how the model should be used. IIC recommends that the description and intended use are first read, before the practitioner's guide. "The goal of a Security Maturity Model (SMM) is to provide a path for Internet of Things (IoT) providers to know where they need to be and how to invest appropriately in sensible security mechanisms that meet their needs and requirements." [92]

In the paper "IoT Standardization - Challenges, Perspectives and Solution" [3], the IoT industry is examined and the issue of need for standardization is raised. Benefits of governance as well as the issues affecting the IoT sector due to the absence of regulation is raised as another critical issue. In the section of IoT security framework of this paper, various threats for IoT objects are depicted (Figure 6).

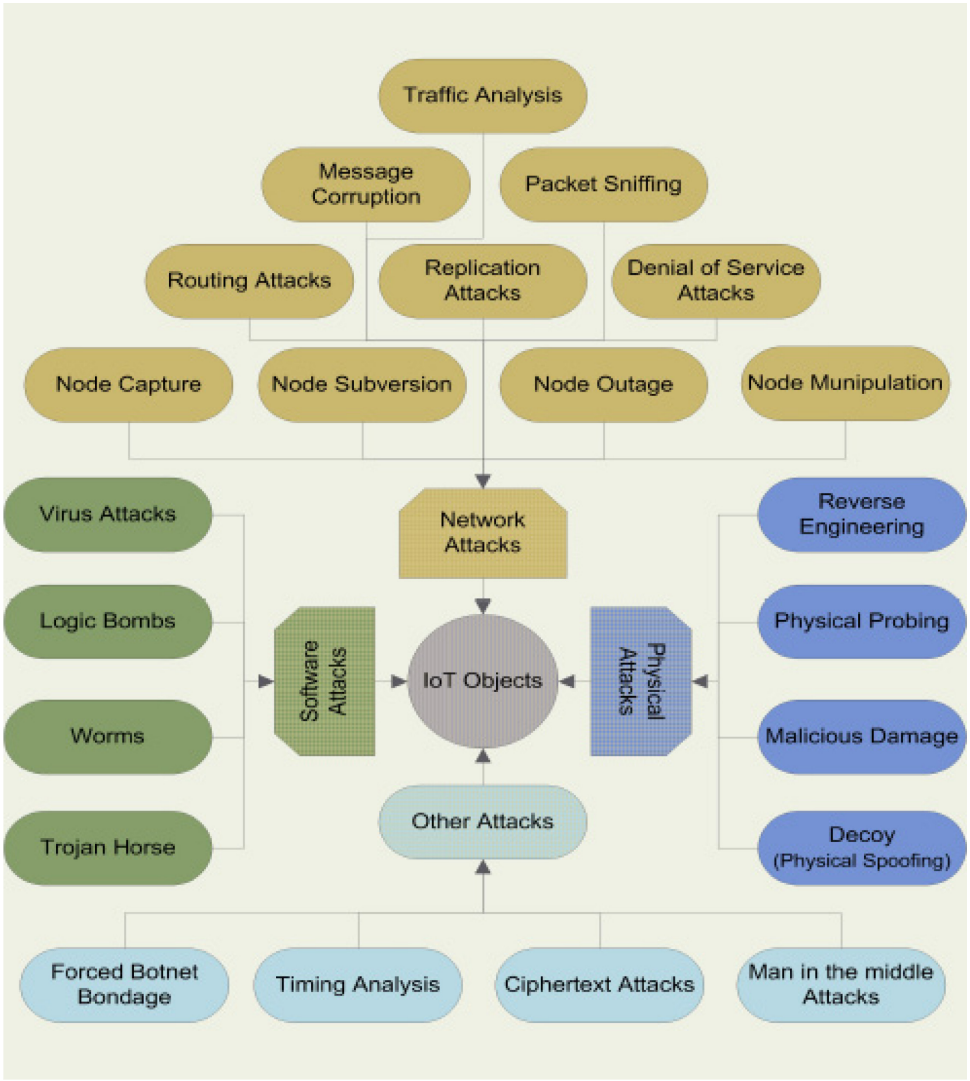


Figure 6 Brief list of attack types on IoT [3]

In the paper “Machine Learning Techniques for Security of Internet of Things (IoT) and Fog Computing Systems” among other things critical security and privacy issues with IoT devices and the ecosystem have been reviewed with examples like hacks of water treatment plants, nuclear power plant, baby monitor videos, wearable devices, and so on. The paper presents the seriousness of the security issue in (I)IoT. As solutions the paper suggests Machine Learning techniques for (I)IoT security. The paper categorizes the fundamental Machine Learning tasks used in defending (I)IoT systems and then summarized papers on machine learning for IoT Security with the focus on malware detection, intrusion detection, and anomaly detection. [16]

In addition to Machine Learning, Blockchain technology have been seen to be able to solve security and trust issues for (I)IoT. "Blockchain Transaction Protocol for Constraint Nodes" (BIoT) paradigm have been introduced in “Blockchain IoT (BIoT): A New Direction for Solving Internet of Things Security and Trust Issues”. BIoT’s idea is to insert sensor data in blockchain transactions. Because objects are not logically connected to blockchain platforms, controller entities forward all information needed for transaction forgery. Nevertheless, in order to generate cryptographic signatures, object needs some trusted computing resources. [15]

Blockchain technologies gained a lot of visibility during 2016-2018, when the outbreak of the cryptocurrencies boosted the technology into common public awareness. It should be noted that the blockchain technology is not a synonym of the Bitcoin or cryptocurrency, but it is a family of technologies which can be used in many business areas for many purposes. Often the blockchain and the distributed ledger technologies (DLT) are used as a synonym, although some experts would like to keep both as their own terms. Especially during 2016-2018, there was a race to invent and present blockchain use cases to all possible industry areas. During the early phase, use cases were presented, but actual pilots were not largely implemented. [71] The hype of the blockchain technologies has already calmed down, but the development and adoption of the technology is ongoing worldwide. European Commission is actively seeking new usage models for blockchain and the member state representatives have initiated several pilot projects. Blockchain use cases have also been presented to be used in the nuclear field. [71]

There are also patents that utilize sensor fusion to protect critical industrial IoT solutions (United States Patent, US 9,817,676 B2). [32] Sensor fusion is a concept, where combining sensor data and possibly other data will provide more reliable information than acquiring the data only from a single sensor or source.

Wireless Sensor Networks (WSN) have gained notoriety in critical environments application in conjunction with (I)IoT, especially in critical environments. In critical environments a high level of efficiency and effectiveness is required to ensure their physical integrity [28]. Because of this “Methodology Ethodology Proposal for Assessing Safety in WSN and IoT Devices in Nuclear Research Laboratory” has been researched. [25]

It has also been demonstrated several times how difficult it is to manage security even for a large company that uses standard cryptographic techniques to protect a

major product in sensor networks. In an example scenario a lightbulb worm to attack commercial smart lamps was created and demonstrated. The attack scenario was possible, because the short distance radio communication chips protocol stack, which was used in the lamps, had a software bug. As this scenario was tested by ethical researchers, they informed the lamp manufacturer, how this attack can be performed, so that the manufacturer could update their products and no harm was caused. [19]

In the paper "Security Survey of the IoT Wireless Protocols" a survey of the security of the four widely used IoT protocols is presented: Bluetooth Low Energy, LoRaWAN, ZigBee and Z-Wave. The paper discusses various vulnerabilities in the protocols and how the protocols evolved from the security point of view. [18]

As an example about the protocols, ZigBee is an IoT mesh network and application standard maintained by the ZigBee Alliance. The first ZigBee specifications were released in 2004. The latest specifications, ZigBee 3.0, which were publicly released in 2016 as one universal standard. In the past years, security weaknesses were disclosed in ZigBee specifications from leaked master keys and fallback mechanisms to unauthenticated command messages. Similar flaws are not only specific to ZigBee but also in other IoT standards, e.g., Bluetooth Low Energy. More focus on designing security measures during IoT standardization is needed to avoid threats. [7]

Middleware IoT application protocols are in major role when enabling bi-directional communication and control of (I)IoT devices. One of the widely used protocols is Message Queuing Telemetry Protocol (MQTT) that is also vulnerable to certain types of attacks. [17]

Although the IIoT technologies, as all technologies do, contain security risks, the human errors are major reasons to the realized security problems. In safety-critical applications such as nuclear power plants, safety systems are separated and isolated from non-safety systems by design. Cyber-attacks on the non-safety systems can however escalate into plant safety threats by inducing wrong operator actions. The paper "Systematic development of scenarios caused by cyber-attack-induced human errors in nuclear power plants" focuses on the operator actions that lead to the unavailability of the safety system and cause the failure of accident mitigation. In the study, the effect of safety system unavailability on plant safety was modelled by using conventional fault tree (FT) analyses. Human actions were analyzed based on emergency operating procedures. Based on the results the paper suggests a method to develop cyber-attack propagation scenarios, where a cyber-attack is linked to its consequences. [10]

Software-Defined Networking (SDN) is a strategy to increase the functionality of the network, lowering costs, reducing hardware complexity and enabling innovative research. SDN architecture models have three layers: Infrastructure layer (network e.g., switches, routers, virtual switches, wireless access point), Control layer (SDN controller(s)), and Application layer (applications for configuring the SDN e.g., Access control, traffic/security monitoring, energy-efficient networking and management of the network). One important feature of SDN architecture is its ability to extend the security perimeter to the network

access end point devices (access switches, wireless access points, etc.), by setting up security policy rules to network devices. [13]

Measured, stored and/or processed data in (I)IoT ecosystem usually contains highly sensitive information, requiring strong confidentiality. The adoption of identity-based public key cryptography provides needed end-to-end security for data across IoT-enabled industries. End-to-end encryption can be achieved using a range of public key cryptography approaches, but the (I)IoT has certain specific characteristics with new challenges. The number and variance of different devices in IIoT ecosystem is greater than in the traditional IT environments. The devices used in different kind of environments and have differences in processing capabilities, use cases, network capabilities and physical locations. The devices could also affect to health and safety. [14]

As an example, research results show a different perspective on the risks of IoT attacks to the power grid. The authors show that while immediate cascading failures or a total system blackout will be very hard to achieve, the power system will still suffer negative consequences: First, various consumers must be dropped from the power grid to prevent further damage to the grid. Second, with millions of high-energy IoT devices, the attacker can potentially cause a bifurcation of the frequency in the power grid, forcing the grid to operate as separate islands and driving it to a more vulnerable state. [8]

As always, information security is not explicit. It is always about finding the balance between risks, risks' impacts, probability of realization and the cost of the counter measures. In NPPs safety critical systems must and will most likely be separated from non-safety supporting systems. This approach has been noticed and is likely to be adopted to the other safety critical applications of IIoT in other domains. The paper "Cyber security in nuclear power plants and its portability to other industrial infrastructures" provides a view across current cyber security in different industries. This paper states that the Industry 4.0 reference architecture model presented in Figure 7 does not explicitly contain cyber security in its layers for Business, Functional, Information, Communication, Integration and Asset. It proposes that strict security controls and countermeasures familiar from NPPs could be ported to other critical industrial domains as well. Nuclear domain has always been more formally regulated and legislated than other industries. [48]

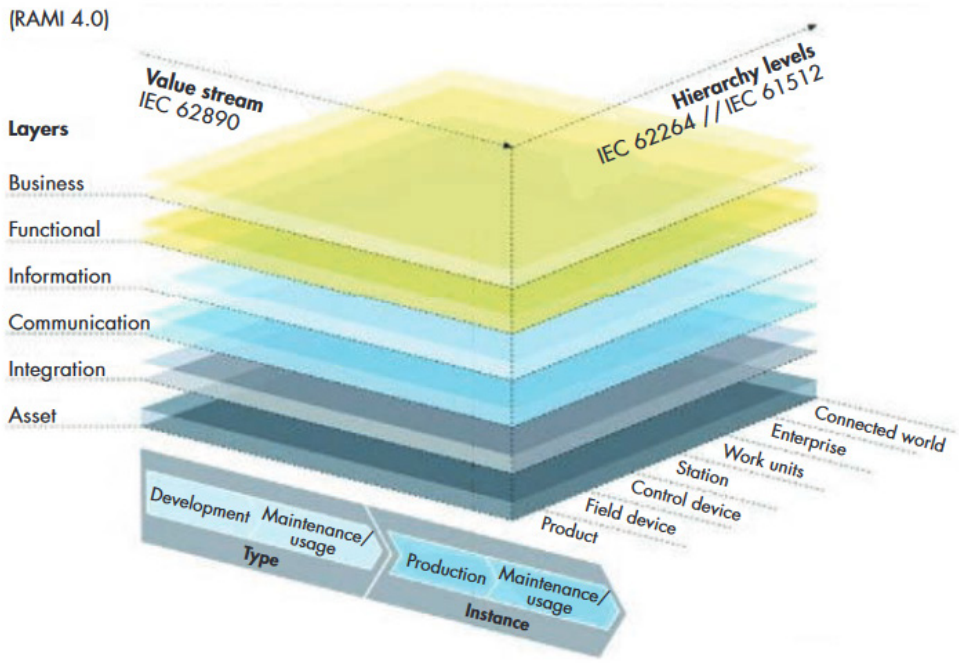


Figure 7 Reference architectural model Industry 4.0 (RAMI 4.0) by ZVEI (© Platform Industrie 4.0) [48].

The paper "Cyber-Physical-Security Model for Safety-Critical IoT Infrastructures" reviews safety-critical applications in aviation, connected cars and power plants. The paper proposes an engineering development roadmap that introduces a cybersecurity review at each design step to strengthen the robustness of IoT hardware and software. Authors have proposed the use of a cyclic cyber-physical security model after system commissioning that allows knowledge transfer between regulatory bodies through sharing of best practices. This model is presented in the following Figure 8. This helps to maintain high security levels and improve the IoT architectures during the full-service lifetime and not only at the initial planning and construction phase. [9]

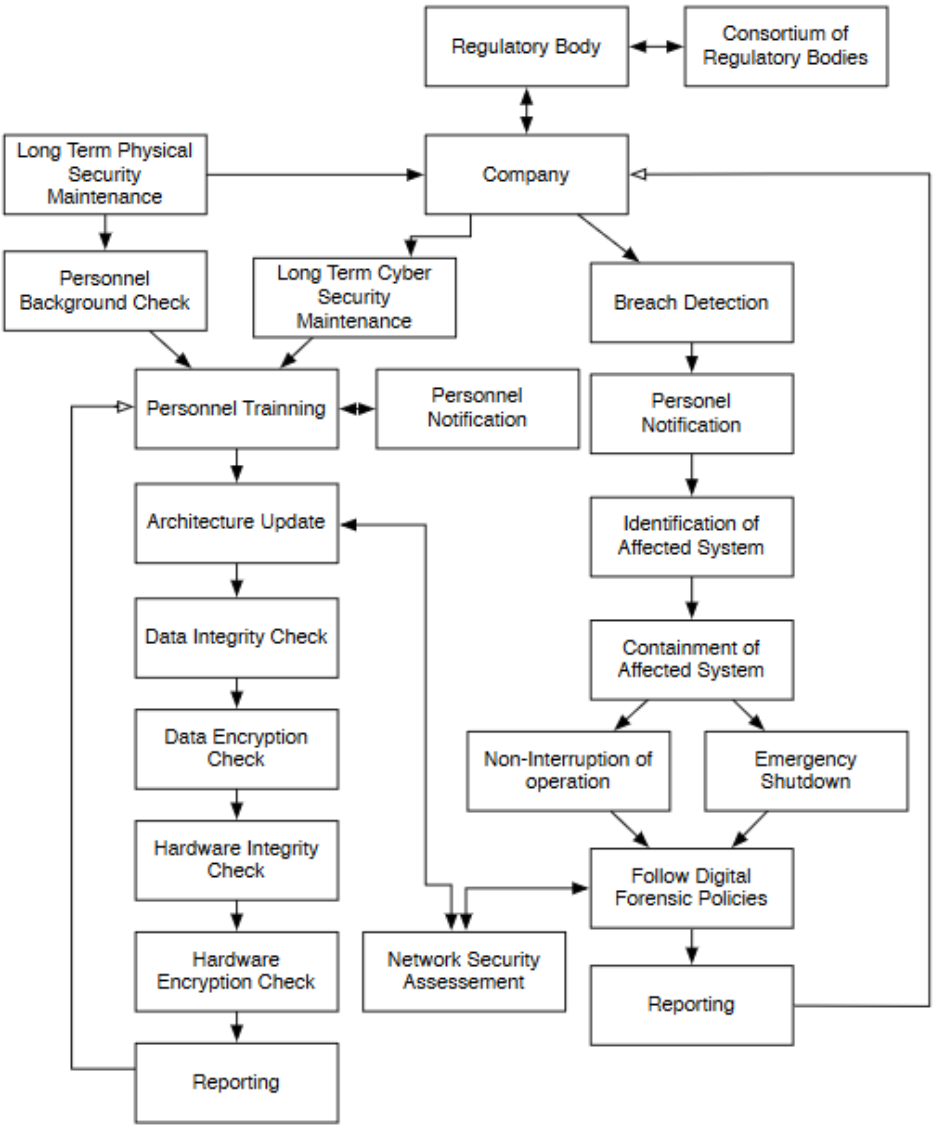


Figure 8 Cyclic security model for long-term IoT support [9]

2.5 IOT FORECASTS

IoT related technologies usage has already spread wide across the industries and they have proven their usefulness to bring cost savings and improve efficiency of systems. Many companies and institutions are making forecasts about IIoT technology evolution and expansion both technology as well as market wise. It is already evident that the IIoT will be a main-stream technology in the industry and the evolution of enabling technologies, like wireless and AI, will help new use cases to be implemented and bring new industries on-board. As many of the well-known market and technology research reports are subject to a charge and this document is publicly available, we will not be able to publish them here. But all the forecasts share the same opinion that the IIoT market share is growing fast in the following years.

Basic building blocks of IIoT, like sensor and actuator technologies have already existed a long time, but the latest development of the modern wireless technologies and data processing are boosting the IIoT. LTE and NB-IoT have already increased the use of IoT in the industry and the smooth transition to emerging 5G networks in the near future is predicted to boost IIoT.

Ericsson Mobility Report (June 2020) [72] predicts that the amount of old legacy connections (2G and 3G) for IoT will slowly start decreasing already in 2020 and the newer broadband technologies (4G and 5G as well as massive IoT, NB-IoT) will start growing a great deal during the next 5-year time period. This growing trend is outlined in Figure 9. According to the prediction, NB-IoT and Cat-M are estimated to cover 52 % of all cellular IoT connections. These technologies will also pave the road to 5G networks, which have been taken into use by various telecom operators during 2020.

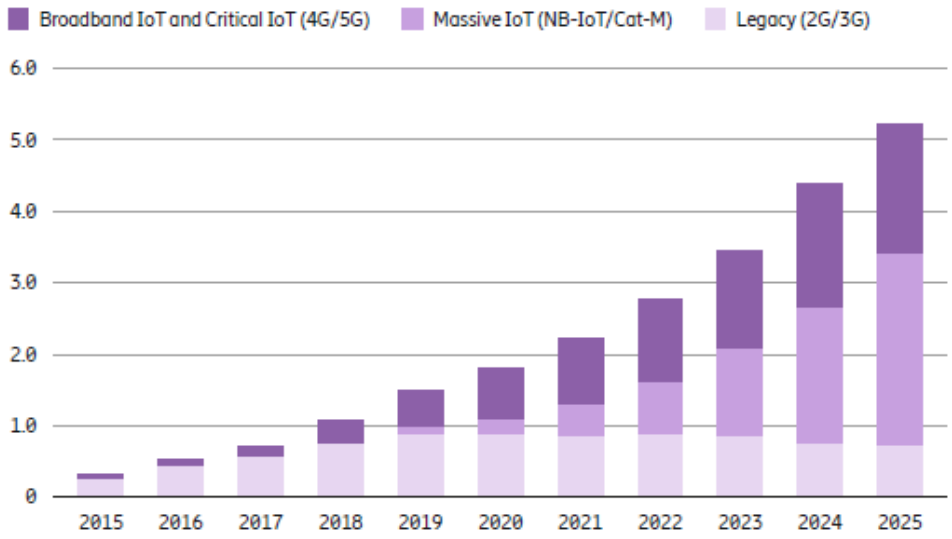


Figure 9 Cellular IoT connections by segment and technology (billion) (Ericsson mobility report, June 2020 [72]).

In a Deloitte insights, technology, media and telecommunications predictions 2020 document [73], they predict that over the next 10-20 years' time, 5G might even take place from the current LAN and WAN technologies in the newly built factories, ports or campus areas and the same article predicts that during the next 5-years ports, airports and logistic hubs could take a leap towards using the 5G technology. Another prediction is that by 2024 the sales of the edge AI chips could exceed 1.5 billion and they will be added not only to the remote data centers, but also locally on the devices as outlined in Figure 10. [73]

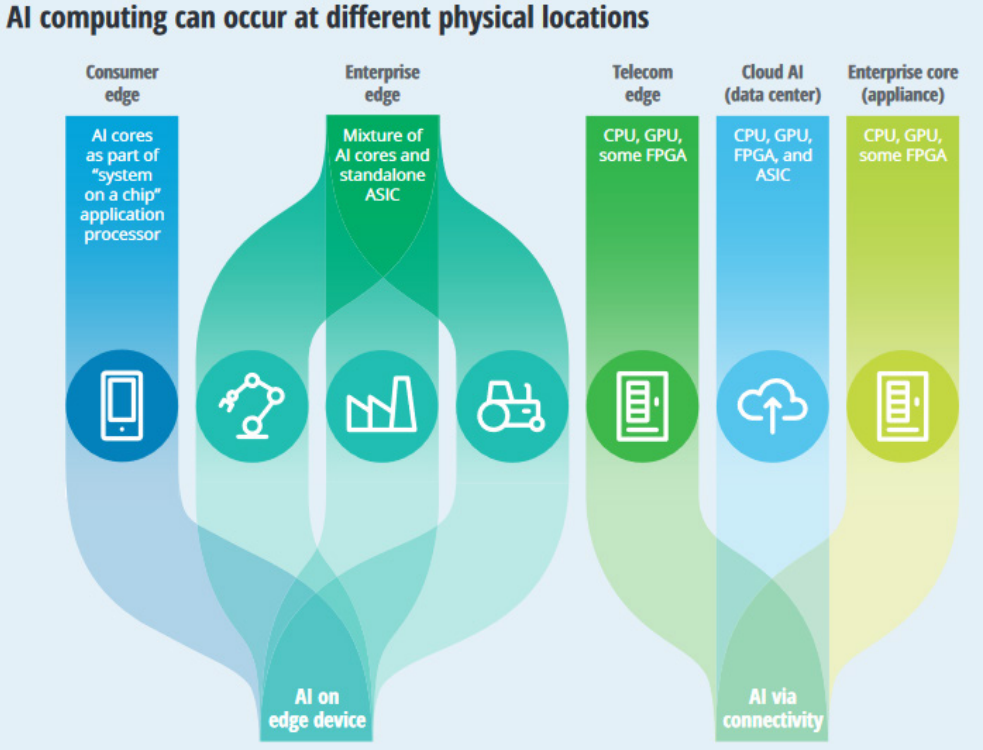


Figure 10 AI computing at different physical locations. [73]

3 IIoT applications in nuclear

Most of the world nuclear plants are designed and built before the era of digitalization and adoption of wireless technologies. Aging I&C technologies create pressure to renew equipment, but regulations, missing standards and concerns of interference from the new solutions delay or prevent decisions to adopt IIoT technologies in NPPs.

In the IAEA publication "Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications" it is noted that historically, instrumentation and control (I&C) systems in nuclear power plants have been custom developed to implement functions important to nuclear safety [74]. This has been true also in many other industries some decades ago, because of lack of existing ready solutions for complex systems. These were often built custom made according to the needs of each site. When the ICT technologies developed further and digitalization started to emerge, custom solution usage in the non-nuclear industry fields started to degrade and more commercial off the shelf (COTS) equipment were adopted in use. This document proposes also processes to justify the use of the COTS devices. Typical justification flow chart and strategy triangle are presented in following Figure 11 and Figure 12. Using COTS devices and systems bring many advantages, as the massive volumes of the production lowers the unit price and widespread usage provide extensive history of operation and improved reliability among others.

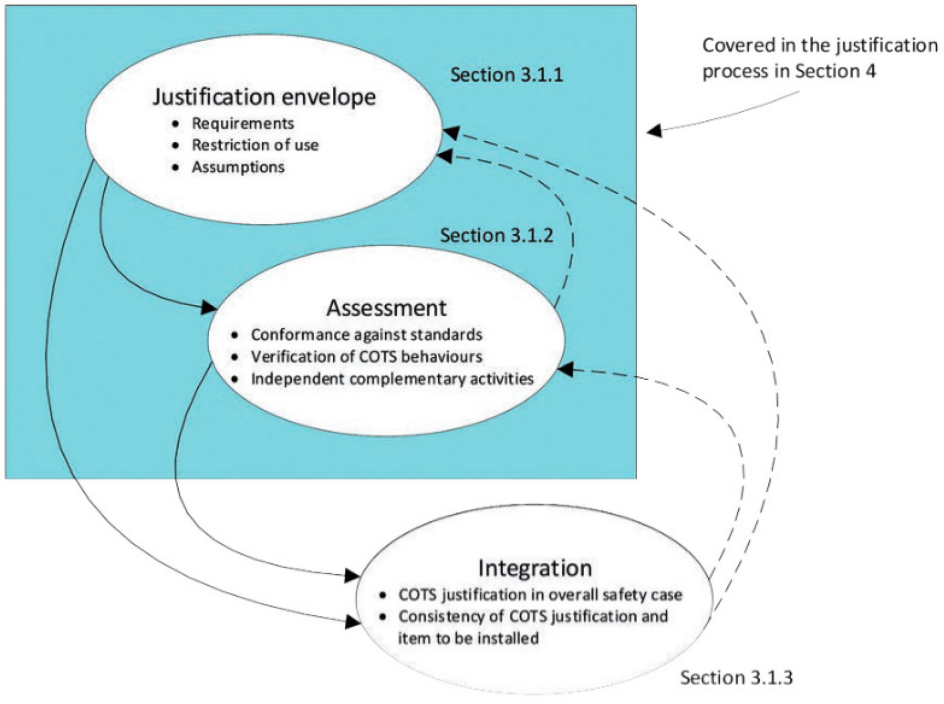


Figure 11 Typical flow chart for a commercial off the shelf (COTS) justification. [74]

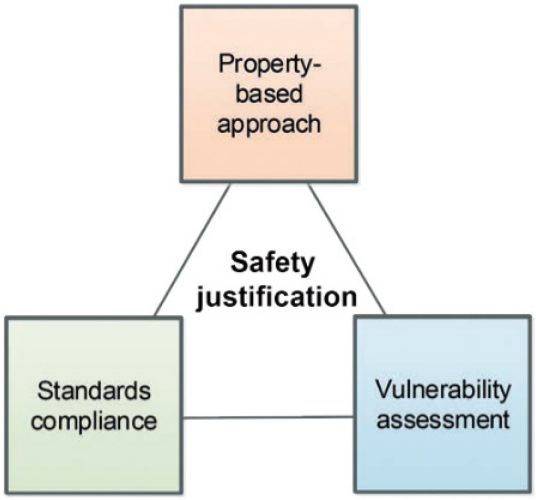


Figure 12 Strategy triangle of justification [74].

On the other hand, generalized "fits for all" solutions can have compromises in some of the implemented features and there can be additional features, which are not needed in the nuclear field. This report raises also the concern that all the COTS devices have necessarily not been designed for the more demanding nuclear functionality, safety and environmental requirements. These environmental requirements include heat, humidity, vibration, electromagnetic interference/radiofrequency interference (EMI/RFI), and seismic requirements. Depending on the usage, radiation can also bring additional challenges.

3.1 REGULATORY REQUIREMENTS AND RESTRICTIONS

National and international regulatory authorities have created guidelines and instructions for the NPPs. Both in Finland and Sweden there are national laws regulating the nuclear field on higher level regulations.

The Organization for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) is an intergovernmental agency that facilitates co-operation among countries with advanced nuclear technology infrastructures to seek excellence in nuclear safety, technology, science, environment and law. NEA is cooperating with national and international legislators to ensure sound requirements in legislation. NEA has collected regulatory and institutional frameworks for nuclear activities from member countries and a country summary of nuclear legislation from Finland [88] and Sweden [89] is available online.

In Finland the Radiation and Nuclear Safety Authority (STUK) [75] has created the nuclear safety guides (YVL Guides) [76], which all the Finnish NPPs have to follow and fulfil. The YVL Guides cover all matters and functions with a bearing on the safety of nuclear facilities: design, operation, environmental safety, nuclear material and waste, structures and equipment. These requirements are updated

continuously to keep them up to date concerning the evolving environment. The Finnish safety requirements are considered relatively strict from an international standpoint [75].

In Sweden, the Swedish Radiation Safety Authority (SSM) [77] is following and supervising the Swedish NPPs. Also, in Sweden the nuclear safety strategy is to apply continuous improvements based on regular and systematic re-assessments, aiming at ensuring compliance with modern requirements and current design basis. [76]

Nordic radiation authorities are cooperating and exchanging information as the operating environments and approaches in both countries are quite similar. As the nuclear field is very regulated and controlled, both countries representatives are members of the Western European Nuclear Regulators Association (WENRA) and International Atomic Energy Agency (IAEA). Several countries in Europe use the IAEA Safety Standards as a basis for formulating national regulations.

As an example, the Finnish YVL guide for electrical and I&C equipment of a nuclear facility sets forth detailed safety requirements concerning the electrical and I&C equipment and cables of nuclear facilities, and it describes STUK's supervision and inspection related procedures. It refers to several national Finnish Standards Association's (SFS) [78] standards as well as to ISO/IEC standards to be followed. Additionally, in this guide for electrical and I&C equipment of a nuclear facility, it is noted that:

- 311. The design, manufacturing and testing of I&C equipment in safety class 2 and equipment mentioned in Guide YVL B.1 requirement 5214 or in Guide YVL C.6 requirement 402a shall be primarily based on nuclear industry standards and guidelines or, in the absence of applicable nuclear industry standards, on international I&C equipment standards. [2019-03-15]. [79]
- 312. The design, manufacturing and testing of I&C equipment in safety class 3 shall employ applicable international I&C equipment standards. [2013-11-15]. [79]

As the Industrial IoT is a newer ICT field, it is not yet directly visible in the national nuclear regulations or guidelines. Increasing interest towards the new technology in the nuclear field has initiated many pilots and wishes and IAEA as well as other stakeholders have initiated the move for the new technology adoption.

The IAEA publication "Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications" [74], is intended to be the starting point for the member states to develop or improve their process for digital COTS justification. Justification is defined as an acceptance process undertaken to establish confidence that a digital COTS device is suitable for installation in a NPP, in a given safety application. [74] Large platforms or systems are beyond this document, but it can also be used as a support material, when addressing more complex systems.

Design of Instrumentation and Control Systems for Nuclear Power Plants Specific Safety Guide (IAEA Specific Safety Guide No. SSG-39) [80] is the revision and combination of two Safety Guides, IAEA Safety Standards Series No. NS-G-1.1 and No. NS-G-1.3. Later revision takes into account developments in instrumentation and control (I&C) systems since the publication of the earlier Safety Guides. It also includes a long list of international standards that have a strong relationship to this safety guide and the long-term structure of the IAEA safety standards series outlined in Figure 13. The purpose of this safety guide is to provide recommendations on the design of NPP I&C systems to meet the IAEA established safety standards.

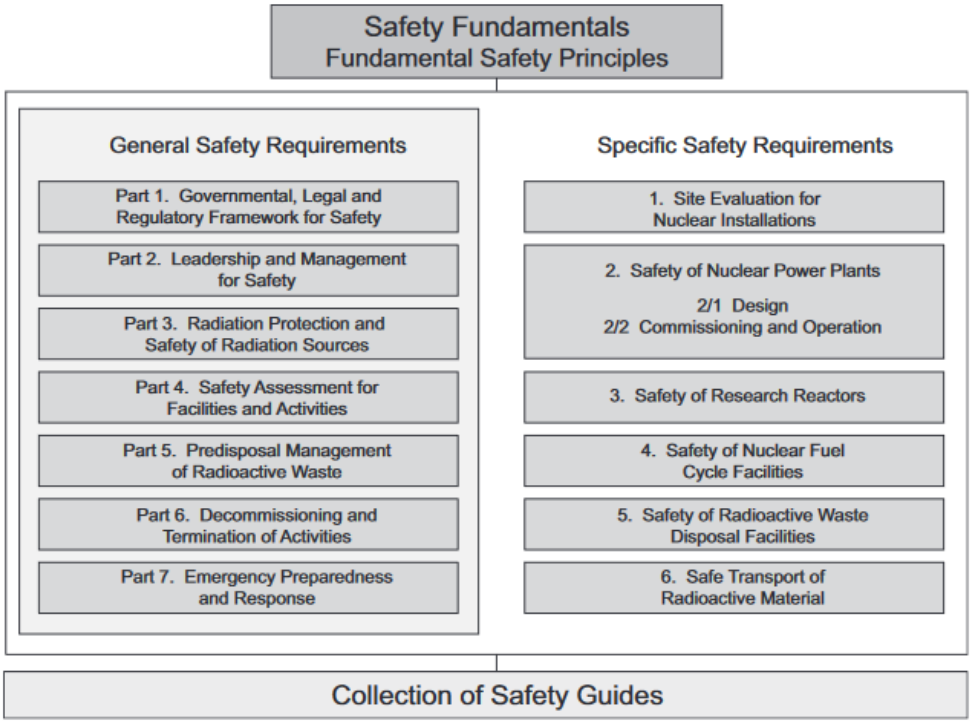


Figure 13 The long-term structure of the IAEA Safety Standards Series. [80]

3.2 IIOT APPLICATIONS IN NUCLEAR POWER PLANTS AND STANDARDISATION

Lack of standardization may lead to weaknesses of the critical systems. Security solutions are needed to overcome these risks and protect the (I)IoT devices, networks, and sensitive data from security breaches and unauthorized access. [23]

Researchers share the concern relating to the standards. There are many issues are still open and need to be addressed. For example, architecture, privacy and security, data intelligence, Quality of Service, communication protocols, and GIS based visualization. [6]

The authors of paper "Reliability and Safety of Nuclear Power Plant Instrumentation and Control Systems: New Challenges and Solutions" state that very important task for NPP I&C reliability and safety assurance is adequate activities in modernization of existed standards, development and implementation of new standards taking into account analyzed challenges. [31].

Upgrading an old NPP to obtain the data can be extremely costly and also disruptive to operations, because NPP instrumentation must be retrofitted. Alternative approaches have been invented, for example reading of an existing gauge utilizing camera and converting the reading to a digital wireless for the IoT system. [23]

Sandia National Laboratories' extensive report "Industrial Internet-of-Things & Data Analytics for Nuclear Power & Safeguards" report highlights research findings relating to the current state-of-the-art of IIoT in NPPs. In addition to the actual IIoT aspects, the report also investigates the use of machine learning tools and blockchain applications being developed for other industries. The report considers how to apply data analytics and machine learning to nuclear power and safeguards within the realm of Probabilistic Risk Assessments (PRAs), predictive maintenance & edge analytics, and proprietary data sharing.

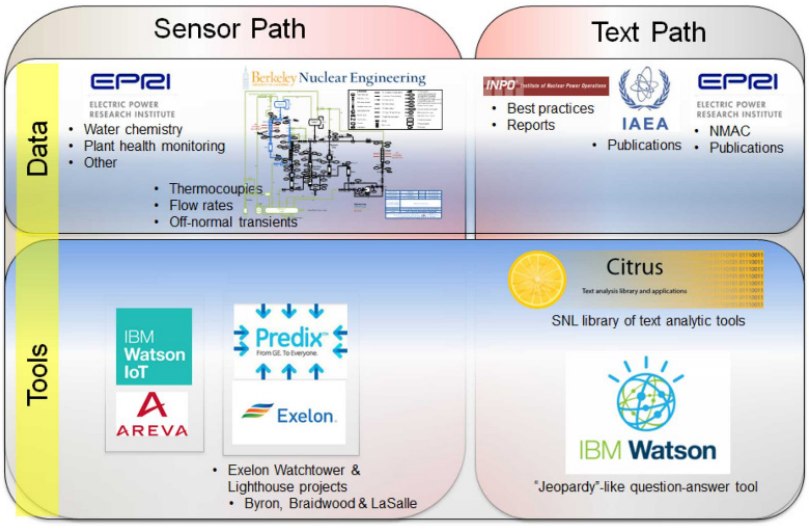


Figure 14 Data analytics applied to nuclear power. [21]

Figure 14 presents the data analytics applied to nuclear power, where the upper row outlines the data needs and the lower row the potential tools, which could be used. The report states that vast work efforts are needed for future robust utilization of data analytics in nuclear. [21]

ETSI oneM2M is the global standards initiative that covers requirements, architecture, API specifications, security solutions and interoperability for Machine-to-Machine and IoT technologies. The specifications of oneM2M provide a framework to support applications and services such as the smart grid, connected car, home automation, public safety, and health. [52]

When considering actual IoT standards, ETSI has over hundred technology standards to utilize in different parts or technologies utilized in the IoT system. [52]

The Electric Power Research Institute, Inc. (EPRI), is an American independent, non-profit organization that conducts research and development related to the generation, delivery, and use of electricity to help address challenges in the power industry, including reliability, efficiency, affordability, health, safety, and the environment. EPRI conducts research, development, and demonstration projects for the benefit of the public in the United States and internationally. The focus is on electricity generation, delivery, and use in collaboration with the electricity sector, its stakeholders and others to enhance the quality of life by making electric power safe, reliable, affordable, and environmentally responsible. [58]

EPRI has conducted research relating to (I)IoT in nuclear, and have reports and products available [59]. For example, relating technical reports about:

- Securing Nuclear Network Communications in the Age of the Internet of Things
- Wireless Sensor Survey and General Specification
- Mobile Technology Guidebook
- Communication Technology Security Architecture for Distributed Energy Resources
- Electric Power System Connectivity: Challenges and Opportunities
- 5G and Cyber Security for Utility Operational Technology Environments: Initial Assessment and Potential Outcomes
- Emerging Standards and Applications of Wireless Power Transfer

EPRI's nuclear sector conducts research supporting the safe, reliable, and environmentally responsible use of nuclear power and develops cost-effective technologies, technical guidance, and knowledge transfer tools for existing nuclear assets and new nuclear technology. For example, Plant Modernization program focuses on improved efficiency, safety and reliability through the application of new technology and more effective operational and maintenance practices. Available are quick guides, business cases, and coming modernization handbook. The handbook is said to be a comprehensive, online resource including the Modernization Quick Guides, Business Case Model with examples, and overall modernization process guidelines. [60]

IAEA has an active role to work within standardization of the nuclear related issues and to ensure safe operation of NPPs worldwide. IAEA conducted a coordinated research project (CRP) on the application of wireless technologies in nuclear power plant instrumentation and control systems from 2015 to 2017. IAEA nuclear energy series publication No. NR-T-3.29 named "Application of Wireless Technologies in Nuclear Power Plant Instrumentation and Control Systems" published in November 2020, is based on the findings of this CRP. This publication presents both codes, standards and regulatory guides, as well as wireless technologies for nuclear applications. This publication presents also lessons learned and proposals for future usage of wireless technologies in nuclear. [81]

Document was published in 2020 and it brought up the fact that at the time of the CRP execution (2015-2017), there were no international standards for the application of wireless technologies in NPPs. After the project had already ended, the IEC 62988 standard called "Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Selection and Use of Wireless Devices" [82], was published. Document notes that there are other IEC standards that have been developed for the use of wireless technologies in other industrial environments that may be applicable to NPPs.

The IIoT in NPP related standards are still to be waited as the technology is still novel, but for the NPP I&C related standards the document has collected an extensive list of standards and requirements from the following categories: [81]

- Standards or requirements for the data transmission and communications in I&C systems in NPPs (15 standards listed)
- Standards or requirements for computer security in NPPs (9 standards listed)
- Electromagnetic compatibility in NPPs (3 standards listed)

3.3 IIOT APPLICATIONS USED IN NORDIC NUCLEAR POWER PLANTS

In the Nordic countries Nuclear Power Plants have been built in Finland and Sweden. In total there are 11 (2020) reactors in 5 nuclear power plants in operation, one in construction and one planned. Summary of the reactors in the Nordic countries is presented in the following Figure 15. Commercial operation of the active NPPs has started between years 1971 and 1985. Building of the only NPP in construction phase, Olkiluoto 3, has started already in 2005. Evolution of the IIoT technologies has started later, which means that all the Nordic NPPs are lacking IIoT technologies.

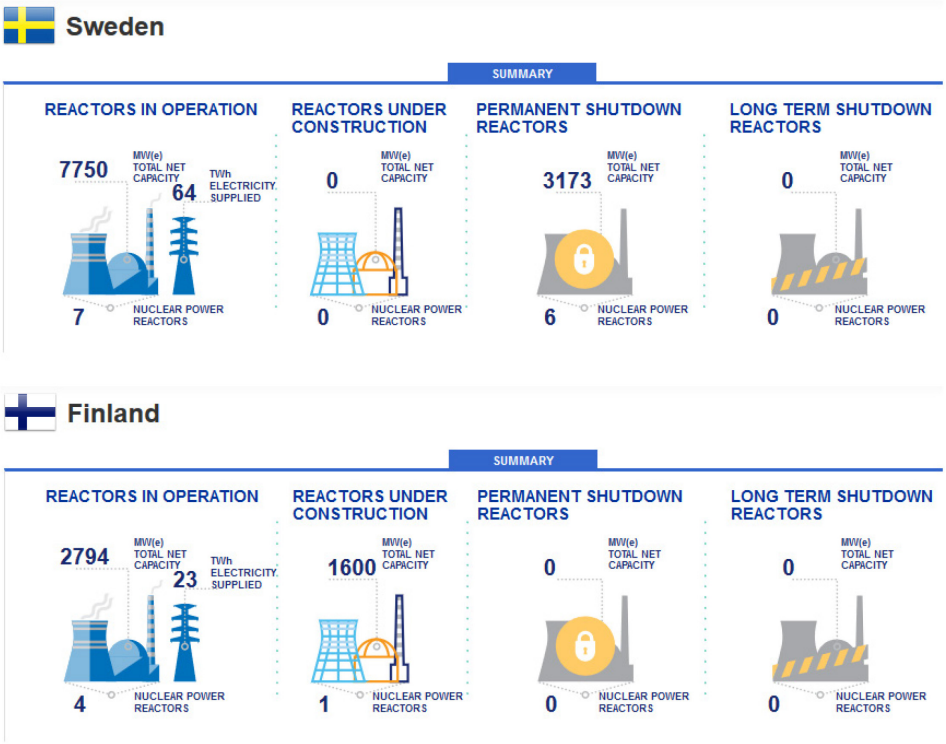


Figure 15 Reactors in the Nordic countries. Source, IAEA Power Reactor Information System (PRIS) [67]

IIoT technology usage in the Nordic nuclear plants later in this chapter has been collected via an on-line survey sent to selected NPP representatives. Survey questions to collect information can be found from the Appendix A:. Survey answers have revealed, as expected, that the Nordic nuclear plants are not very much using IIoT technologies in the plants. Nordic NPP representatives are also careful to keep the information confidential and publicly available material about the wireless or IIoT related pilot or usage information is not available.

Modernization of old NPPs is taking place in the Long-Term Operation (LTO) programs, which can provide an opportunity to bring IIoT into the Nordic NPPs. However, the existence of wireless technologies in the IIoT systems can delay the acceptance of adoption, as the wireless technologies bring out the concern of

electromagnetic compatibility (EMC) with the old legacy systems and possibility of harmful electromagnetic interference (EMI), which was not considered in the design of the plant I&C systems. On the other hand, it has been seen in the LTO definitions and processes that for many of the old legacy I&C control systems it is all the time harder to find spare parts, as these systems are not any more manufactured. In long term this will also increase the pressure to adopt novel technology in the NPPs.

Blockchain technology has been mentioned as a technology, which can be used to implement improved cyber security solutions. Nuclear related blockchain use cases have also been introduced, like we have seen in the earlier chapters of this document [15] [21]. As a Nordic example from blockchain in nuclear, the Finnish Radiation and Nuclear Safety Authority STUK, the Stimson Center and the University of New South Wales have built in collaboration a distributed ledger technology (DLT) platform called SLAFKA, which is a permissioned blockchain prototype for nuclear safeguards, which is said to be the first of its kind. It is based on STUK's current nuclear accounting database and allows nuclear facilities to record nuclear material assets on a blockchain (Figure 16). Chosen platform technology is the Hyperledger Fabric, which is a well-known and widely used permissioned blockchain framework to be used by the industry. [83] [84] [85]

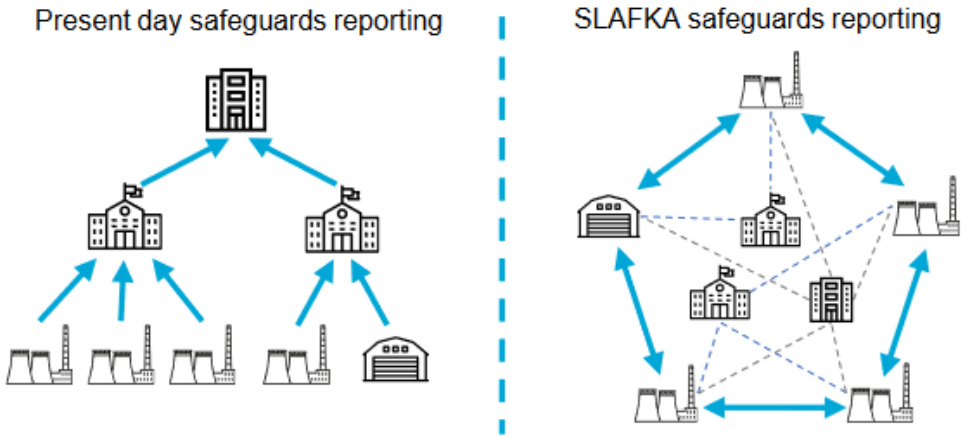


Figure 16 SLAFKA transaction model comparison for nuclear safeguard assets [83]

3.3.1 IIoT applications in use at Nordic NPPs

IIoT and wireless solutions are not yet common in the Nordic NPPs. Some local (temporary) measurements have been implemented, which are using local wireless network and local storage, e.g. wireless vibration monitoring. Some NPPs use also off-site applications.

Safeguards surveillance technologies (Seals and Cameras) are in use in Nordic NPPs. Those instruments are connected via VPN to the servers in Luxembourg and Vienna, where the status of the devices can be checked, and camera images reviewed. Also, Non-Destructive Assay technologies will be remotely controlled. Data transfer is facilitated using the same VPN data transfer capability already in use in the Finnish facilities.

The exact definition of IIoT is not clear, but for example, core supervision, vibration supervision and the use of overdetermined equation system to monitor the thermal power are examples of computational sophistication that already exist on-line. Self-diagnostics and relay protection are other examples of applications that probably could be classified as IIoT. The whole plant computer system with alarms etc. is very similar to IIoT according to the survey answers.

Although nuclear waste repositories are not directly nuclear power plants, they have to follow the nuclear facility regulations and are subjects to the same control procedures. In the Nordic countries both Svensk Kärnbränslehantering AB (SKB) (Sweden) and Posiva Oy (Finland) have researched and developed methods for encapsulation and final deposition of the spent nuclear fuel. These include also methods to monitor the repositories with monitoring systems including long range and short-range wireless communication and wireless energy harvesting for the sensors. Both of these companies have been also involved in the European Commission funded Modern2020 research project. The overall objective of the Modern2020 Project is to provide the means for developing and implementing an effective and efficient repository operational monitoring programme, that will be driven by safety case needs, and that will take into account the requirements of specific national contexts (including inventory, host rocks, repository concepts and regulations, all of which differ between Member States) and public stakeholder expectations (particularly those of local public stakeholders at (potential) disposal sites) [85]. Wireless communication and wireless energy transmission pilots in the project have been described e.g. in the project deliverables D3.2 Wireless data transmission systems for repository monitoring [86] and D6.3 Modern2020 Final Conference Proceedings [87]. Partly the physical environment of the nuclear waste repositories is even more challenging than in the NPPs as in the underground repositories the wireless transmission blocking structures are much thicker. In the Modern2020 project wireless transmission experiments were piloted for distances from 0.1 meters up to 275 meters in underground research laboratories (URL) (Table 4).

Table 3 Overview on EU Modern2020 project experiments on wireless data transmission in URLs [86]

Distance	Transmission mode	Frequency	Host rock/barrier (location)	Organization
0.1 m	Resonant cavity antenna	2.4GHz	Concrete buffer	EURIDICE
4 m	Electric dipole antenna	169 MHz	Bentonite/shotcrete (Grimsel URL)	AITEMIN
4 - 6 m	λ/4 loop antenna	2.2 MHz	(Partially) saturated bentonite (Tournemire URL)	Arquimea
5 - 10 m	Magnetic loop antenna	8.5 kHz	(Partially) saturated bentonite (Tournemire URL)	Andra
23 m	Magnetic loop antenna	125 kHz	Granite + Air (Espoo research hall)	VTT
25 m	Magnetic loop antenna	8.5 kHz	Sedimentary rock (Meuse/Haute Marne URL)	RWMC/Andra
30 m	Magnetic loop antenna	4.0 kHz	(Partially) saturated bentonite (Tournemire URL)	Amberg
30 m	Magnetic loop antenna	575 Hz	Bentonite/shotcrete (Grimsel URL)	MISL
225 m	Magnetic loop antenna	1.8 kHz.	Boom Clay & saturated sandy aquifer (Hades URL)	NRG
250 m	Magnetic loop antenna/relay system	8.5 kHz	Sedimentary rock (Horonobe URL)	RWMC
275 m	Magnetic loop antenna	8.7 kHz	Limestone & Shale (Tournemire URL)	NRG

One of these URLs in the Modern2020 project has been the ONKALO facility of Posiva Oy in Finland shown in Figure 17. More surveillance and monitoring technologies will be introduced in this site in the future, when the operation with actual nuclear waste will begin.

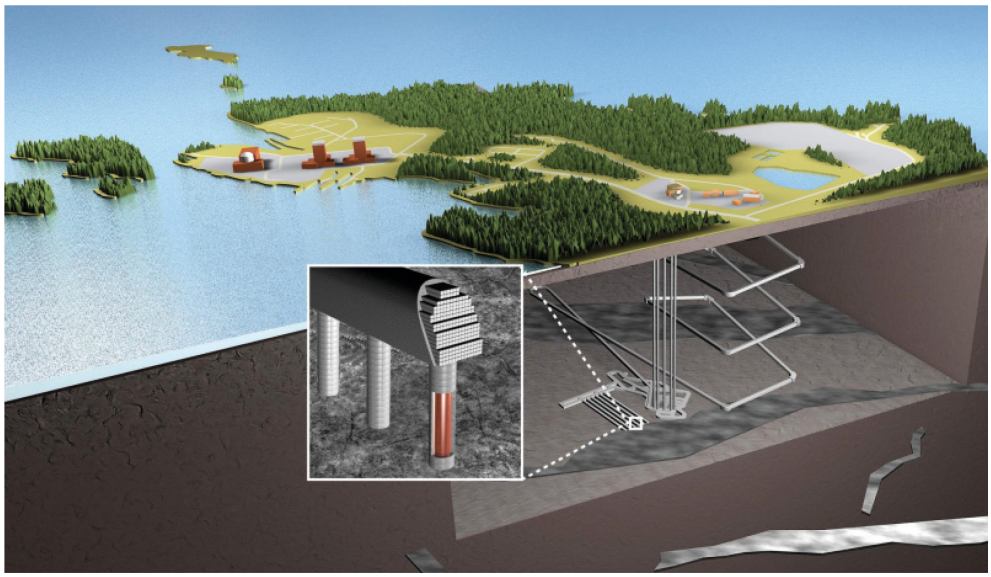


Figure 17 ONKALO underground research laboratory and future geological final disposal site. Conceptual model. (Source Posiva)

Future NPP (FH1) of Fennovoima Oy in Finland will also have remote data transfer system and newer I&C technology in use. It is taken into consideration already in the design phase and will be part of the delivery, but as this facility is still in the design phase and the final building permission has not yet been granted, the final documentation is still a subject for changes and publicly available information is not released.

3.3.2 Future wishes for IIoT usage in Nordic NPPs

The general attitude in the Nordic NPPs towards using IIoT and wireless systems in the non-safety critical systems is positive and there is a wish to increase the use of them in NPPs. Current safety and regulatory restrictions as well as the in-house control guidelines on the other hand bring out the vision that IIoT or wireless solutions should not be brought into the safety critical systems in the near future. Some stakeholders and NPP representatives consider at the moment the usage of the IIoT and wireless technologies a risk in the safety critical systems also in the long perspective. But the evolution of the mobile communication has shown that also these technologies have been adopted into use also in the NPPs, although earlier all wireless communication in the NPP area was considered to be impossible. In the longer time period, the applicability of adopting IIoT in the safety critical systems should be re-evaluated.

The following applications were mentioned by the Nordic experts in the query:

- Measurement over all systems, drones, handheld devices, positioning equipment, cameras.
- To be able to set up more sensors for example to support condition-based maintenance.
- Wireless data transfer in some areas would solve some problems.
- Applying more sensors on the Asset to start with, early warning of unexpected machine behavior, some sort of data combination for critical parameters sent to the predictive maintenance inspector, like vibration, temperature, motor current.
- Wireless can be considered as an option when there is a need for feeding measurement to data acquisition systems, particularly for non-permanent measurements.
- To be able to set up a system that uses a private plant wireless network.
- More sensors on machines where the overview of "the Assets" machinery health in the plant can be viewed on a web-paged platform, we call this Asset Portal. Information can be accessed by Devices connected to the plant network, the platform should be able to send an alarm to a smart phone or an email.

In the earlier wireless feasibility study, some future wishes for wireless usage in the Nordic NPPs were expressed. Despite of doubts and obstacles, also Nordic NPP operators would like to investigate and consider using wireless technologies in their plants. Successful experiments in other NPPs and in other industries encourage this development and by adopting some wireless applications in to use, it can be a road opener for more wireless applications. On the wireless application wish list there were topics like:

- wireless data retrieval
- movable wireless cameras
- movable temporary wireless measurements e.g. during maintenance
- wireless dosimeter system across the plant
- movable wireless detectors e.g. for radiation, gas or oxygen
- wireless document retrieval during inspections

3.4 IIOT APPLICATIONS USED IN INTERNATIONAL NUCLEAR POWER PLANTS

In this sub-chapter we have collected some examples of IIoT projects and pilots with short descriptions, which have been performed in international NPPs. It is not an all-inclusive list, but the purpose of these examples is to show that nuclear industry is interested and active to seek new technologies to improve functionality of the utilities.

Sandia National Laboratories' extensive report "Industrial Internet-of-Things & Data Analytics for Nuclear Power & Safeguards" report highlights research findings relating to the current state-of-the-art of IIoT in NPPs. In addition to the actual IIoT aspects, the report investigates also the utility of machine learning tools and blockchain applications being developed for other industries. The report considers how to apply data analytics and machine learning to nuclear power and safeguards within the realm of Probabilistic Risk Assessments (PRAs), predictive maintenance & edge analytics, and proprietary data sharing. The work of the project consists of three main topics [21]:

1. Edge Analytics: Data analytics performed at the instrument level, only important, assessed data transmitted.
2. Analytics on encrypted data: Cyber protection leaving everything encrypted, but still performing analytics to provide operator insights.
3. Blockchain IoT: Achieve instrument consensus even in the cases where some instruments are faulty or under cyber-attack.

Edge Analytics efforts are ongoing in Areva (Framatome)/IBM and Exelon/GE. The focus is on data analytics at the sensor level inside the NPP. Aim is to process the data while wirelessly streaming processed insights to operators. [21]

Exelon and GE-Hitachi have partnered to use the GE Predix at NPPs. Watchtower and Lighthouse demonstrations are ongoing. Watchtower is based on Asset Performance Management (APM) suite to reduce unplanned downtime and prevent lost power production by connecting assets. APM collects data from sensors, gives alerts about anomalies, and predicts failures. Lighthouse uses human performance data to predict plant Key Performance Indicators (KPIs). [21]

The validity and usefulness of early warning in online monitoring system for nuclear power plants has been presented in the paper "Demonstration of the validity of the early warning in online monitoring system for nuclear power plants". Early warning is one of the core functions of the online monitoring system, which uses pattern recognition to predict and alert potential problems in the equipment or system. The function was developed by using the AAKR technique (Auto Associative Kernel Regression). The early warning system has been applied to 24 plant units since 2016 to detect the abnormality through the difference between the measured values and the estimated values. The system has been confirmed operating properly and the validity and the effectiveness of the system was proved via cases. The cases identified the system detecting a fault symptom of equipment and measuring instrument and the malfunction of the system cause by external environment. [22]

"Wireless Online Position Monitoring of Manual Valve Types for Plant Configuration Management in Nuclear Power Plants" presents technology development, testing, and demonstration to support continued safe operation of fleet of light water reactors and provides the technical means of monitoring components in NPPs. The authors state that wireless-enabled valve position indicators are able to provide a continuously available position indication. A real-time availability of valve positions using affordable technologies is seen to be vital to plant configuration and it provides information that can be used for plant engineering, maintenance, and management applications. [30]

There has been a research developing an IoT based leak detection system using distributed acoustic sensors. The system extracts predictors from the raw acoustic signals applies machine learning classifiers while reducing the burden on data transmission, storage and computation. A prototype is successfully evaluated through the experiments with acoustic signals measured around a laboratory scale NPP coolant pipelines. [39]

A framework for using augmented reality to enable the next generation of smart nuclear infrastructure has been presented in the paper "Augmented Reality for Enabling Smart Nuclear Infrastructure". The author sees that emergence of augmented reality and a variety of IoT devices offers a possible solution. The paper describes a prototype of the Augmented-Reality based system for enabling smart nuclear infrastructure, its implementation and demonstration. The prototype has been implemented and demonstrated in a surrogate environment. The authors see that their work can be used as help guide when developing and deploying this kind of framework in actual nuclear infrastructure. [34]

Designing and developing a machine learning algorithm to perform predictive maintenance of nuclear infrastructure has been proposed in the paper "Predictive Maintenance Architecture Development for Nuclear Infrastructure using Machine Learning" [38].

EPRI's Next-Generation Radiation Protection project is looking at methods and technology to safely improve the cost effectiveness of radiation protection programs at NPPs. The project has also reviewed drone technologies, and developed EPRI-led Autonomous Drone able to perform inspections and collect radiological data. There is a video available that demonstrates (at Exelon's Peach Bottom Atomic Power Station in Pennsylvania) the performance of one autonomous drone coupled with a software technology to inspect components in elevated hard to access areas, search for temperature anomalies and collect dose rate surveys in radiological areas. [60]

Westinghouse has launched in June 2020 with the Guardhat IoT company a connected worker solution for the nuclear energy industry. Personnel on-location can be given real-time access to remote experts and resources for optimizing the performance of the onsite crews utilizing wearable technology. Technology has been piloted in several utilities during refueling outages. [107]

Areva has developed a long-rage wireless communication platform based in the LoRa (LongRange) technology developed by Semtech Corporation. Large number of sensors and actuators can be connected to a wireless infrastructure and the

system can provide also geolocalization of equipment in complex industrial environments, even in nuclear power plants. [108]

3.4.1 Project examples - Wireless in Nuclear: Feasibility study [1]

Wireless applications listed in the Wireless in Nuclear: Feasibility study [1] are also valid examples for IIoT applications in nuclear, as besides wireless technologies, they contain other IoT related technologies.

Wireless Technologies in NPPs using cognitive radio system. Analysis and Measurement Services AMS, located in Knoxville, Tennesee U.S. has been active on numerous wireless studies and applications. AMS has developed a cognitive radio system that has the ability to generate and output multiple wireless signals (e.g. Wi-Fi, Bluetooth, cellular communications at varying power levels and frequencies). System can be used to test equipment in training areas, simulators as well as in actual plant environment. [94]

Wireless sensor network trials in Comanche Peak Nuclear Power Plant and Arkansas Nuclear One (ANO) power generating station. In U.S. few experimental WSNs have been deployed in Comanche Peak Nuclear Power Plant and Arkansas Nuclear One (ANO) power generating station. In Comanche Peak NPP 802.11b wireless network infrastructure was established in the plant that incorporates wireless sensors for equipment condition monitoring and diagnostics. [95]

Research project for the U.S. Department of Energy. January 2009 R.J. Jarrett, H.M. Hashemian, G.W. Morton, B.D. Shumaker, and C.J. Kiger summarized in the Automation IT article "Nuclear power comeback sure to employ wireless tools" that in 2009 wireless was used in NPPs for wireless dosimetry, voice communication, equipment monitoring, laptops and PDAs, camera monitoring and heavy equipment operation. Voice communication was the most prominent wireless application in the plants at this time. [96]

Wireless radiation monitoring. Various other solutions for using wireless equipment to measure radiation in or in the perimeter of NPPs has been published e.g. from India, Hungary and Finland.

Seismic Monitoring System for Nuclear Power Plants. Geosig Seismic Monitoring System (SMS) Ambient vibration testing in the system is optionally offered fully wireless. System includes the option to retrieve common time from the GPS satellites wirelessly. [97] Similar wireless time synchronization utilizing GPS-grade time precision is also used in some of the Nordic NPPs in some other applications.

Ultra Wide Band (UWB) transmission pilot at the MIT research reactor. Ultra-wideband (UWB) technology use in electromagnetically harsh environments. Secondly, they present a novel UWB remote powering scheme that allows for battery-free operation of sensors to increase their lifetime. And finally, they present the experimental results of piloting the UWB signaling at MIT research reactor. [98]

Pilot for a NPP Wireless emergency response system (ERS). A study was conducted on wireless emergency response system (ERS) with mobile control

station (MCS) placed 30km away from the plants. In the terrestrial communication system, the system is designed based on the IEEE 802.11. [99]

WSN for Temperature and Humidity Monitoring in a Nuclear Facility at Sadhana loop, India. A wireless sensor network (WSN) implementation, where continuous monitoring of temperature and humidity are performed in the Sadhana loop, which was commissioned at the Indira Gandhi Centre for Atomic Research (IGCAR). Sensors were installed in the chimney outlets and inlets in various heights and monitored in the lower-level control room of the plant. In house developed WSN node is operating at 2.4 GHz ISM band. [100]

EPRI project - Distributed antenna systems in NPPs Catawba Nuclear Station U.S. An EPRI research project has created a combination of point-source antennas and radiating cables to build up a distributed antenna system to support voice communications, equipment monitoring, and other new technologies that the industry is adopting. With the distributed antenna system, wider coverage and greater penetration of wireless signals can be provided. System has been installed at the Catawba Nuclear Station, U.S. [101] [102]

IAEA CRP project - Application of Wireless Technologies in Nuclear Power Plant Instrumentation and Control Systems. IAEA launched a Coordinated Research Project (CRP) I31028 based on the recommendation of the Technical Working Group on Nuclear Power Plant Instrumentation and Control on 12/2014. Project was researching battery operated devices, wireless systems in the electrically noisy environment of a nuclear power plant. [103]

Nuclear decommissioning - Wireless applications in Sellafield and Magnox UK. Modern wireless instruments were installed in the Sellafield and Magnox to aid monitoring during plant closure. In the decommissioning phase new control and instrumentation is needed and wired installations would be costly and time consuming to implement. [104]

Use of robotic techniques in NPPs. OECD's R&D and Innovation Needs for Decommissioning Nuclear Facilities report handles several topics concerning research and development needs in the decommissioning and also general NPP phases. These include complex autonomous wireless networks for hazardous environment monitoring and response and use of robotic techniques in NPPs. [105]

3.4.2 Project examples - IAEA Application of Wireless Technologies in Nuclear Power Plant Instrumentation and Control Systems [81]

Earlier mentioned IAEA nuclear energy series publication No. NR-T-3.29 named "Application of Wireless Technologies in Nuclear Power Plant Instrumentation and Control Systems" [81] lists following wireless and IoT related projects. Reader is encouraged to visit the document, in case more detailed description of the projects is sought. (*Note, those projects, which were already listed in the previous section, has been removed from this list*):

Deployment of a wireless sensor network for process measurement in the Fast Breeder Test Reactor at the Indira Gandhi Centre for Atomic Research, India. As of 2017, the Fast Breeder Test Reactor WSN is functioning satisfactorily with 37

nodes. It monitors 14 thermocouples, six flow sensors, two level sensors, five vibration sensors and two vibration based condition monitoring systems. To administer and manage the WSN, an efficient graphical user interface wireless network management station has been developed.

Deployment of wireless sensor network for the measurement of sodium leak detection at the In Sodium Test Facility, Indira Gandhi Centre for Atomic Research, India. In order to reduce the complexity involved in cable routing and to test the performance of the leak detector wireless connectivity, 50 leak detectors from the In Sodium Test Facility fatigue loop were connected as a redundant system in parallel mode to a WSN developed in house. The data were communicated to a base station located in the control room to display the status of the leak detectors.

Cooling tower fan motor monitoring at the High Flux Isotope Reactor at the Oak Ridge National Laboratory, United States of America. An R&D programme was successfully completed to develop and deploy an integrated condition monitoring system utilizing wireless data delivery for the predictive maintenance of rotating equipment at the High Flux Isotope Reactor at the Oak Ridge National Laboratory.

Vibration and temperature monitoring for fan motor at Exelon's Limerick plant, United States of America. Deployment of wireless based vibration and temperature sensors to the fan motor within the duct was performed. The implementation of wireless technologies helped the plant technicians acquire condition assessment data during plant operation, thus improving reliability and reducing down time.

Motor health monitoring at Southern California Edison's San Onofre plant, United States of America. A study was conducted to implement a wireless technology-based condition monitoring system for the plant motors (1860kW installed capacity) at the San Onofre Nuclear Generating Station. An IEEE802.15.4 wireless mesh network was selected for the collection and analysis of motor temperature data in real time. The selected system enabled the plant engineers to take timely action. This system was chosen to avoid adding new cables, which helped in reducing the installation expenses with improved plant life cycle.

A wireless robotic system for severe accident applications in Japan. In a severe environments, such as a disaster area, various remote controlled robots need to be used for accurate situational assessment. To manipulate the robots smoothly, video data and robot control data need to be transmitted reliably and efficiently. The communication system for remote controlled robots, which was developed as a hybrid system of wired and wireless links. The communication between the robot operation computer and a repeater is provided via a wired network and the communication between the repeater and the robot is done via a wireless network.

4 IIoT applications in other industries

Other industries have adopted industrial Internet of Things (IIoT) in to use and they can be the signposts for the nuclear field. Best practices as well as lessons learned can be utilized in the nuclear field to avoid pitfalls when designing and building the first IIoT systems in the NPPs.

IoT is becoming commonplace in industrial environments. IIoT applications are expanding for example in manufacturing, factories, plants, process industry and in energy sector [46].

Some typical IoT application domains are energy, manufacturing and industry, connected vehicles and smart cities [53]. In industry, enabling more efficient maintenance with IoT is quite common approach. Also new Environment, Health, and Safety (EHS) operations can be enabled via IoT. Connected vehicles is also an important area in industry on the transportation point of view. Following gives an insight, some common use cases and examples in which kind of purposes IIoT are typically exploited in industrial setting.

Table 4. Typical use cases and examples of IIoT usage in industrial setting of different domains.

Domain	Use Case	Description	Examples
Energy	Transmission	Remote monitoring & control of generator assets and transmission grids	Smart monitoring and diagnostic systems at major power plants
	Distribution and metering	Smart grid monitoring & control	Smart meters. Micro grids and virtual power plants.
	Marketing, sales and service	Digital customer interface and services	Bundling energy and information services
Manufacturing / Industry	Integrated production / processes	Smart factories / plants, improving operational efficiency	Supply chain management, logistics, smart integrated production
	New business models	Shift from products to services	Product manufacturers are becoming service providers
	End-to-end digital engineering	Digital integrated engineering of integrated production and integrated products	Products on the field provide information to support engineering of new products and production

Domain	Use Case	Description	Examples
EHS	Environmental monitoring	Radiation, emission, weather etc. monitoring	Weather stations, gamma radiation measurement systems
	Disaster monitoring	Preventive monitoring of possible disasters	Dams monitoring, radiation monitoring, earthquake early detection, landslide detection, flood monitoring and control
	Ensuring safety	Ensuring healthy work environment	Portable Geiger Muller counters
Maintenance	Predictive maintenance	Vast amounts of possibilities to shift from reactive to predictive maintenance	Prognostics and system health management, fault diagnosis and prediction systems, condition-based maintenance
Transport / Vehicles	Connected enterprise solutions	Connecting enterprise's vehicles and managing its fleet	Fleet management
	eMobility	Electric vehicles (EV) remote management and charging	Energy management, charging services, EV remote management
	Automated vehicles	Assisted and automated driving	assisted driving, environment monitoring, autonomous vehicles, smart parking, intelligent traffic systems, autonomous ships
	Logistics	monitoring and controlling supply logistic	supply chain monitoring, supply drones

Domain	Use Case	Description	Examples
Smart cities	Smart city	Digitalization of the cities	Smart parking, structural health, noise urban maps, smartphone detection, electromagnetic field levels, traffic congestion, smart lighting, waste management, smart roads, smart homes
Agriculture	Smart farms	controlling and automating agriculture	Green house monitoring and control, offspring care, animal tracking

In this chapter some energy related, safety and security critical examples of IIoT applications outside nuclear domain are presented and discussed. In these applications the authors see high relevance to possible similar applications in the nuclear domain.

4.1 ELECTRIC POWER AND ENERGY SYSTEMS

A smart grid is an electrical grid which includes a variety of operation and energy measures including smart meters, smart appliances, renewable energy resources, and energy efficient resources. Smart grids are already in use widely and can be seen as IoT systems as such.

IoT's capabilities for real-time monitoring, situational awareness and intelligence, control, and cyber security are the key in evolution from Electric Power and Energy Systems (EPES) into intelligent EPES, which is more efficient, secure, reliable, resilient, and sustainable. IoT enables digitalization of the electric power ecosystem by improving visibility, management and optimization of energy and its generation. There are still several obstacles deploying IoT for EPESs. The advancements in computational intelligence capabilities can evolve an intelligent IoT system by emulating biological nervous systems with cognitive computation, streaming and distributed analytics including at the edge and device levels. There is an assessment of the role, impact and challenges of IoT in transforming EPESs available. [5]

IoT applications in smart grid have lots of advantages such as expenditure reduction, save of time, and smartness of grid equipment. Of course, there are also drawbacks that should be noticed. Concerns about security and data privacy are clear, but also complexity, safety weaknesses, possible risks of IoT have reached new levels. [62]

Merging IoT with smart grid together has shown potential. A paper "Smart grid integration of IoT" states that embedding IoT devices and technologies in the smart grid assures that data from every point in the grid is generated and transmitted fast enough to a central command point located on the power distribution system operator premises. When combined with edge computing and AI/ML the data received from devices can be utilized for predictions and to offer the state of the smart grid in near real time.

A paper "Communication Capabilities of Wireless M-BUS: Remote Metering Within SmartGrid Infrastructure" investigates the suitability of Wireless M-BUS communication protocol for possible adoption in remote metering in future housing estate. [61]

4.2 ENVIRONMENT, HEALTH AND SAFETY (EHS)

IoT seems to have significant potential in high-risk Environment, Health, and Safety (EHS) industries. The paper "Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review" reviews existing published research on IoT-based applications in high-risk EHS industries with specific emphasis on healthcare industry, food supply chain, mining and energy industries, intelligent transportation, and building & infrastructure management for emergency response operations. [27]

The prototype of meteorological and environmental gamma radiation monitoring system for early detection of radioactive material in the environment has been developed and tested around the Center for Nuclear Facilities Engineering at Serpong Nuclear Complex. The prototype consists of Arduino-based gamma radiation monitoring device, data transfer with MQTT protocol, storage of monitoring data to database, and user interface (UI) for data presentation. The presence of radioactive material was simulated using check source which emitted low dose rate gamma. Meteorological data was compared with the monitoring result from the existing meteorological monitoring system. The prototype system seems to detect the presence of gamma radiation source and meet the design requirements. [26]

Similar kind of case study in the paper "First step towards an IoT implementation of a wireless sensors network for environmental radiation monitoring" highlights also the possibility of greatly reducing costs of environmental radiological monitoring through the IoT approach [40].

Also, in another research the radiation levels have been monitored and measured in the area exposed to using a radiation sensor (GM counters), sending the data (by NodeMCUs) to a cloud from where is accessed by the concerned authorities. GPS was utilized to locate data of the radiation emitted from the radiation sources under such radiation environment. The radiation values and location mapping were remotely monitored in real time through web server configured with the radiation IoT platform. [29]

Internet of Things (IoT) based portable Geiger Muller counter has been invented. It measures radioactive particles and consists of spark fun Geiger counter developed

board (SEN-11345) and NodeMCU as host microcontroller. Radiation dose rate have been recorded and sent to cloud server via Wi-Fi gateway for connecting network through TCP/IP-based network. Blynk app stores the data and visualizes it in android mobile. The system is designed and implemented in laboratory and tested. [33]

IoT based Disaster Monitoring and Management System for Dams (IDMMSD) has been proposed. The system monitors water levels and could open the shutters at the heights pre calculated. It contains sensor nodes, smart controller and communication system to enable IoT system which will monitor and send real time parameters related to Dam and weather conditions. There will be two modes for operating: Autopilot and Manual mode. The system also includes features like SMS alert citizens and SOS for rescue operations. [35]

4.3 MAINTENANCE

The paper "Machine Learning Innovation for High Accuracy Remaining Useful Life (RUL) Estimation for Critical Assets in IoT Infrastructures" introduces a variety of algorithms that leverage time-series telemetry coupled with advanced machine learning (ML) pattern recognition for high accuracy estimation of Remaining Useful Life (RUL) of systems, components, and subsystems in business-critical and mission critical environments for Prognostics Health Management applications. RUL capability is a key enabler for Condition Based Maintenance (CBM) of customer assets. The paper states that RUL-based CBM significantly reduces operations and maintenance costs for IoT and Big Data customers in the industrial sectors of utilities, transportation, manufacturing, oil-and-gas, and enterprise data centers. [36]

Toshiba Machine has developed an IoT-based PHM system with NEC. Customers' products send failure and operating information to NEC data centers, and Toshiba Machine then uses the cloud to propose maintenance services. Nidec has developed a similar IoT-based system in conjunction with IBM. A machine at Nidec sends operating information to the data center managed by IBM. The data center provides diagnosis of the machine based on the data collected. [41]

For example, Komatsu monitors and diagnoses faults in their construction equipment products in the field via satellite communications. Similarly, GE monitors their gas turbines. Rolls-Royce monitor their jet engines in the field in real time and provide their customers with optimized maintenance. [41]

A number of organizations, for example, GE (Digital Wind Farm) and Siemens (Wind Service Solutions), now provide IoT service solutions for wind farms. These solutions aim to optimize turbine performance and equipment life by using RUL estimation models to predict maintenance requirements. [41]

For example, cars made by General Motors, Tesla, BMW, and other manufacturers have their own application programming interfaces (APIs). The APIs allow applications built by third parties to interface with the data collected on the car. This enables the development of applications for IoT-based PHM that add value by increasing connectivity, availability, and safety. [41]

Duke Energy has implemented in co-operation with partners (National Instruments, EPRI and Schneider Electric, among others) an end-to-end solution for plant-wide machine condition monitoring across 30 facilities. The solution leverages IIoT for predictive maintenance. Duke Energy recognizes that there is a great opportunity to save additional money by using more wireless sensors, which do not require costly cabling to the data acquisition systems. Development is moving toward gaining more actionable intelligence with tools that can diagnose problems, but also give recommendations for the actions needed. [57]

The problem of fault diagnosis and prediction from IoT data collected in the process industry has been considered. A solution has been proposed to make use of IoT enabling technologies offered by SAP. The proposed solution first discovers the causal relationship of the physical devices by analyzing only the device sensor data without the knowledge of the physical manufacturing system. While faults of certain devices can be detected by monitoring the healthy index of these devices in real-time, possible faults of other devices can be predicted based on the causal relationship discovered in the previous step. This prediction capability enables new predictive maintenance applications where appropriate actions can be recommended to operators of the manufacturing system. [42]

In order to improve the maintenance efficiency and save the maintenance cost, IoT-based remote handling maintenance process has been designed for fusion reactor. It has been seen improve the traditional maintenance process and save time and cost based on IoT. [20]

TemLab S.r.l.'s TEMLAB system [56] is a patented IoT system for remote monitoring of concrete corrosion. The Temlab system is based on measuring the electrochemical corrosion of embedded steel and chlorides concentration and pH, via sensors embedded in the structure. The measurements, focused on pH, chloride concentration, conductivity, temperature and humidity, can be taken on site or remotely. Sensors can be installed either during concrete casting or after. The system has been developed to monitor bridges and buildings. It can be seen that technology could be beneficial to the nuclear sector, providing a safe and cost-efficient solution to monitor concrete structures. AB5 Consulting [55] is bringing the solution and promoting it also to the nuclear domain. [54]

4.4 SOME NORDIC TELECOM OPERATOR IOT EXAMPLES

Nordic telecom operators have been traditionally eager to adopt and promote the newest mobile technology solutions. Like mentioned earlier in this document, also they are offering IoT platforms to their customers. They are also potential partners for cooperation for the Nordic NPPs, as they most likely already provide some services for the NPP organizations. Nordic telecom operators offer IoT platforms, IoT ecosystems and data management services. They advertise also their know-how with various case studies that they have made with their customers and white papers. Some of the telecom operators have formed and joined to the IoT World Alliance [106], which purpose is to offer for their multinational customer seamless IoT device connectivity around the world. Some telecom operators are also offering

small scale development kits without a charge to make proof of concept testing for a limited time.

Telecom case study examples with customers:

- Air condition system remote monitoring
- Connected personal alarm system
- Connected vehicles
- Delivery logistics
- Elderly safety
- Electric speedboats with connected sensors
- Electric vehicle battery condition monitoring
- Electric vehicle charging infrastructure
- eScooter infrastructure
- Fleet management
- Indoor air quality monitoring
- IoT for agriculture - Geofencing livestock, robotics in the field
- Monitoring remote assets with IoT
- Public transport management
- Real estate monitoring
- Site asset location service
- Smart factory
- Smart heating and energy in buildings
- Smart traffic
- Supply chain management

5 Final considerations and future work

IIoT technologies provide the opportunity to add instrumentation and enhance monitoring options of the NPP equipment. IIoT systems can either be used to replace current legacy systems, which are lacking spare parts or add enhanced redundancy in monitoring the NPP equipment operation. Using the wireless communication option, instrumentation can be added to novel locations, which would otherwise hard or impossible to be reached.

5.1 SUMMARY AND FINAL CONSIDERATIONS

This report presents a short overview of existing industrial Internet of things (IIoT) solutions and related technologies in nuclear power plants (NPP) and other industries, which could be applicable to be used in the Nordic NPPs. All the Nordic nuclear plants, which are currently in operation, are old and built before the digital age. This makes the adoption of IIoT and wireless technologies in them challenging, as there are many constraints hindering the decisions.

Digitalization is the current trend both in industry and in society. New IIoT solutions are piloted and built with increasing speed across industries, which provide positive examples to harvest the best practices to be adopted also in the nuclear field. IAEA, regulators and other stakeholders are piloting and creating guidelines to help the transition to start the digitalization of the NPPs.

Although the old Nordic NPPs will not be the front runners to adopt the latest emerging technologies, there is a wish to adopt digital IIoT technologies including wireless communication into use. The LTO-programs of the NPPs can also create a need for IIoT adoption in some form, as the replacement of the old I&C technologies will most likely turn more difficult in the future, when manufacturers of the spare parts for the old I&C systems stop their operation.

Unfortunately, there is no one single correct way to successful IIoT adoption. As a first step, nuclear plant owners, operators and other stakeholders need to define an IIoT strategy, why and how they would take the IIoT in use. Nuclear industry is more restricted and regulated than other industries, which results to the fact that other industry IIoT strategies cannot be copied one-to-one. But still other industry strategy and other examples should be taken as a starting point and modify them as needed, instead of starting from an empty table. In the next chapter have collected some guidelines for IIoT usage planning for the NPPs.

Summarizing these facts and presented wishes and doubts both from the Nordic NPP stakeholders and also global actors, the most probable pathway for IIoT adoption in the Nordic NPPs will be a gradual increase of IIoT equipment starting from small scale successful pilot experiments. These pilot experiments could be the needed enablers, which lead to broader use of IIoT in NPPs.

A

5.2 GUIDELINES FOR IIOT USAGE IN NUCLEAR POWER PLANTS

We have outlined in this report that IIoT is not a single technology, but it consists of many technological sectors. In order to successfully implement an IIoT system, one need to master all of them. Typically, NPP I&C systems have been closed and isolated systems. IIoT systems on the other hand are utilizing networking and connectivity and wireless communication opens new opportunities, but also new threats to the information and communication technology (ICT) systems.

It should be noted that this report is not an all-inclusive step-by-step guide, which leads to an IIoT enabled nuclear plant. We want to provide some background for various stakeholders and starting points, where to start the journey towards IIoT adoption. Even, if the purpose is to make some small pilot experiments to try the technology, the IIoT strategy and roadmap work should be started as early as possible.

According to McKinsey report "The Internet of Things: How to capture the value of IoT" [91], which is based on interviews, mentions that although the IIoT is foreseen and advertised as a massive opportunity and lot of positive promises are given, the adoption of IoT is still slow. In the report it is also said that "The reality of IoT is that businesses tend to focus too narrowly when thinking about how to use it." In this report, it is stated that although there are intentions and wishes to adopt IIoT technologies into use, there are many gaps, which slow the process. The three most important ones, which all are also very valid for the nuclear industry, were:

1. Integrating IoT solutions into existing business workflows
2. Managing data
3. Identifying use cases and applications

The capability gaps according to the McKinsey survey are depicted in the following Figure 18.

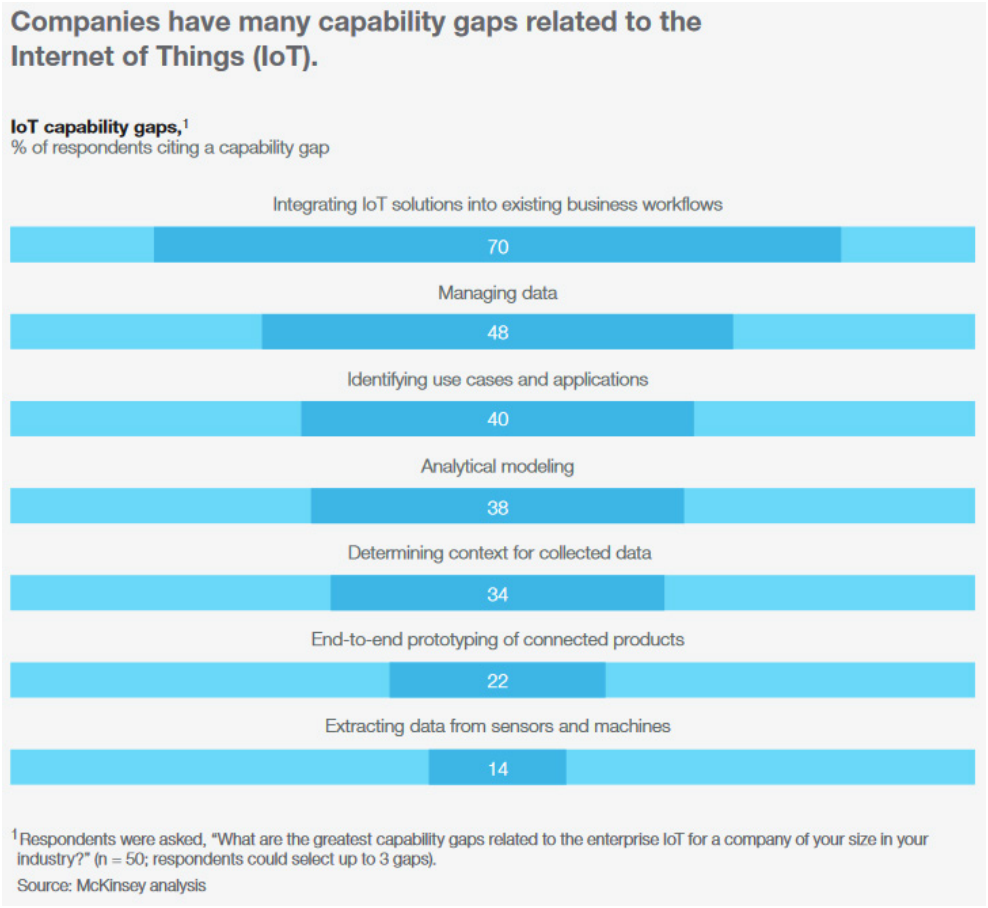


Figure 18 IoT capability gaps according to the McKinsey analysis. [91]

Even for a small pilot IIoT trial, the big picture should be kept in mind. There is a need for a communication infrastructure, most likely including wireless communication, data management plan and also the overall cyber security aspects need be taken into account. Especially the use of wireless technologies can cause extra complications in the strategy planning and implementation because of the regulatory and other restrictions, like possible interference with legacy I&C. Additionally, the connection to the old legacy systems needs to be considered, at what level the connection can be established or should there be two parallel systems to increase resilience. Figure 19 outlines the various fields of technologies, which need to be considered and defined for the pilot system. It also reveals that it requires a lot of work to establish the first IIoT pilot in operation.

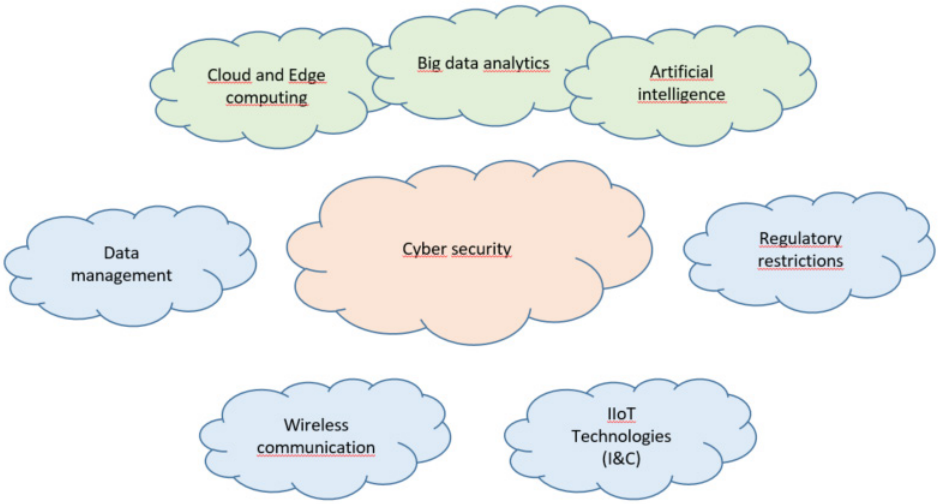


Figure 19 Technological fields to take a stand on during strategy planning.

5.2.1 Business case

To initiate a project, like adopting IIoT, a business case to support the project should be found. Otherwise, there is a danger that the project will not receive funding or the support from the organization is too weak to successfully finish the project with sufficient dimension. Nuclear plant is not the end product in this perspective, but it is a manufacturing plant, which the IIoT adoption should improve. IIoT will not increase the production but can bring cost savings and improved efficiency. IIoT business planning and strategy planning are very tightly connected and should be performed parallel in an iterative way.

One emerging "business case" for the Nordic NPPs is the aging of original I&C systems. In the long run there is a high probability that there will be no vendor support for some of the original equipment. Long Term Operation (LTO) planning is a forum, where IIoT adoption should be taken in, as IIoT systems can be potential replacements for obsolete parts in the NPP. Vendor support will not stop for the whole NPP at once, but during time the amount of unsupported equipment is likely to grow.

This fact raises a potential challenge for the NPPs. Components should not be replaced as isolated systems but keeping the big picture in mind. However, replacing the outdated components with traditional currently available components without full IIoT features, is faster and more cost-effective in a short time period. Adopting IIoT systems into use, would require more infrastructure planning and building, before they can be taken into use. Our surveys have revealed that the missing IIoT infrastructure is a major obstacle for the adoption. If the decision to start using IIoT and build the needed infrastructure is pushed to the far future, more legacy equipment will be replaced with non-IIoT systems.

Considering the existing doubts among stakeholders and regulatory restrictions, replacing the existing I&C systems might be the long-term plan. Additional new IIoT (pilot) implementations will be a more probable way for the IIoT to enter the NPPs. When the needed infrastructure for the IIoT is in place (wired and wireless

networks, cyber security and data management) the next enhancements and new use cases are easier to take into use. Finally, possibly also the replaced I&C systems could be modified and connected to the IIoT system.

Potential starting points for IIoT business case definitions in the Nordic nuclear plants can be:

1. Improve internal processes with enhanced monitoring.
2. Bring cost savings with predictive maintenance and analytics.
3. Improve security.
4. Improve safety.
5. Improve resilience.
6. Improve data collection, management and analytics.
7. Increase automation.
8. Track assets.
9. Improve logistics.
10. Replace existing legacy I&C systems in small scale.
11. Replace existing legacy I&C systems in large scale.
12. Create digital twins.

The three last ones, replacing existing legacy I&C systems and creation of digital twins might be considered cases, which will not be the first ones to be implemented.

To test the chosen business case, it might be good to build a proof-of-concept implementation to convince the decision makers to approve or disapprove the chosen case. Proof of concept implementation can be also very valuable asset in the iteration process, when the IIoT business case and strategy are further defined, as they can help to find the gaps and pain spots of the chosen strategy, which need improvement.

5.2.2 Strategy planning

IIoT strategy planning is initiated by the internal team and internal capabilities, resources and knowledge gaps should be mapped. It would be very important that in-house experts, who can provide the necessary nuclear related know-how will be able to define at least the requirements for the IIoT system. Internal contribution to the implementation process can have a positive impact on the final solution, so in-house IIoT capabilities is good to have.

Other involved parties, like software providers, system integrators, cloud providers, communication providers and hardware providers should be selected and engaged to the definition process in an early phase. The selection of external partners needs to be done carefully. Although vendor locks should be avoided, changing partners later can cause substantial additional costs. Regulatory and company policies will have an impact, which partners and offerings are eligible to deliver the needed services and how they should be delivered. Cost model of the various service providers need to be carefully analyzed in order to ensure that there will not come surprises, when IIoT system is scaled up. Scalability and lifetime of the system as well as its components is important to keep in mind, even

if the first pilots would be small-scale proof of concept implementations. Built IIoT infrastructure should serve also the future implementations.

The previously mentioned McKinsey report [91] highlights also that one single IoT pilot will probably not yet show the transformative impact of IoT in full scale. To achieve convincing impact, pilots should have sufficient breadth and there should be several use cases implemented. Financial impact of IoT Use Cases is outlined in Figure 20

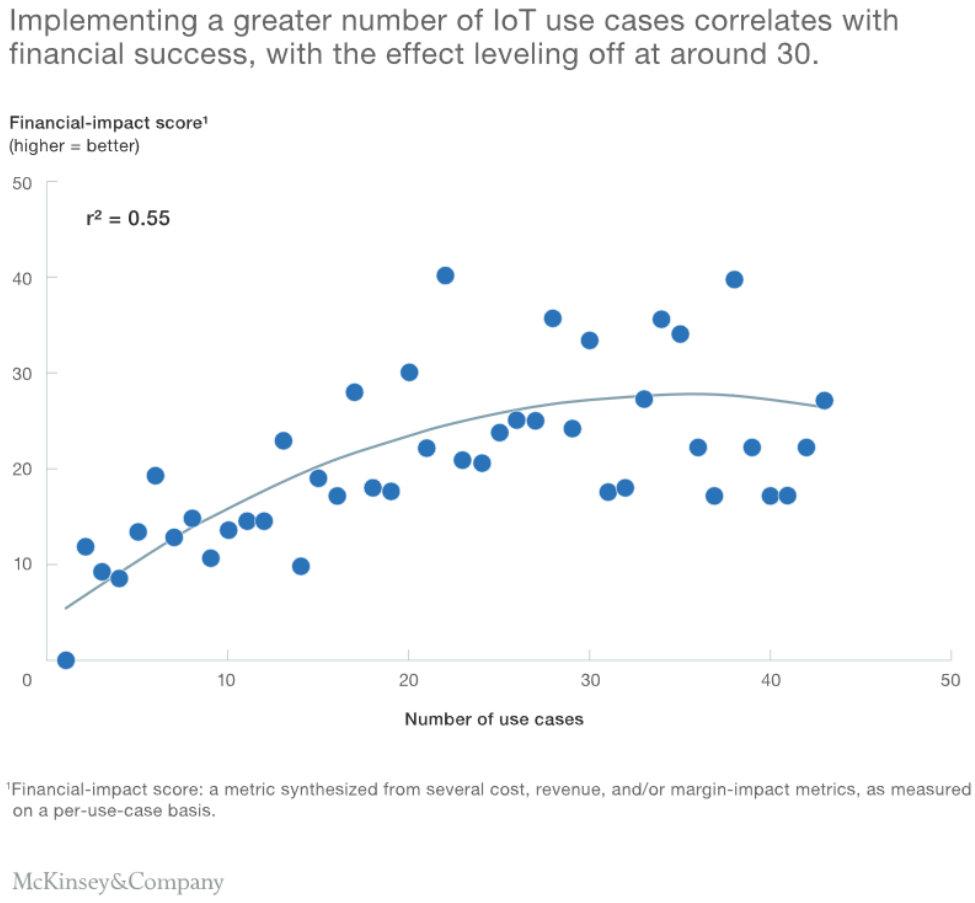


Figure 20 Multiple IoT Use Cases create higher financial impact. [91]

One important strategic decision is, what kind of service model NPP would like to pursue for the IIoT system. Is it the Infrastructure as a Service model (IaaS), where only the platform is provided and most of the work is done in-house with own personnel. Second option is the Platform as a Service (PaaS) model, where the service provider is providing hardware and software tools, but still moderate amount of work needs to be done with own personnel. Third option is to choose the Software as a Service (SaaS) model, which offers the whole software system as a service and only minor own work is required to maintain and run the system. Economic wise the question is to make the balance with the internal and external investments, when choosing the preferred model. Organization's resourcing possibilities is naturally also affecting to the decision. Will the implementation of

the IIoT system be considered as strategic and important issue, or is IIoT considered as a tool among other tools.

Possible changes to the original business processes and IT-strategies need to be carefully evaluated. IIoT adoption can impact to the work processes and require changes to them, which in some cases can be a problem, as resistance to change is a common phenomenon in organizations.

5.2.3 Planning the IIoT system

In this report we have presented several research papers and other publications to provide information about IIoT. Technology and service providers, which will be involved in the design and implementation process, will offer guidelines and tools to help the planning, but the buyer should be aware of possibilities and pitfalls. Figure 19 outlined the technological fields, which need to be covered in the planning and implementation process.

We have presented earlier that industrial technology providers have IIoT offerings for products, devices, and services. As some examples following were mentioned: IBM's Watson, GE's Predix. Schneider's EcoStruxure, Honeywell's Sentience. Domestic and global telecom and ICT operators are also providers of IIoT services and platforms, which can act as partners in the process.

A book "Enterprise IoT: Strategies and Best Practices for Connected Products and Services" acts as a guide by introducing a dedicated methodology for businesses preparing to transition towards IoT-based business models. The book contains a set of best practices based on case study analysis, expert interviews, and the authors' own experience. Outlined Ignite | IoT Methodology delivers actionable guidelines to assist with IoT strategy management and project execution. The book also includes a detailed case study of a project fully developed with the methodology. [53]

Industrial Internet Consortium (IIC) has IIoT RFP Toolkit for creating and managing request for proposals (RFPs) for the Industrial Internet (Copyright 2020: Industrial Internet Consortium, The IIC RFP Toolkit is using the Ignite IoT Methodology; license: CC BY 4.0). Aim of the toolkit is streamlined IIoT solution process enabling acquisition of better solutions, delivered by suppliers in time and at best cost, and to avoiding typical IIoT procurement and project risks. The toolkit includes tools for different phases: Challenges, risks and mitigation, Project planning, RFP creation, IIC RFP wizard, and RFP distribution & vendor selection. [64] Online toolkit can be found from the URL https://hub.iiconsortium.org/rfp-toolkit

To support cyber security issues in the IIoT architecture, IIC IoT Security Maturity Model: Description and Intended Use [92] and the Industrial Internet Security Framework: Practitioner's Guide [93], which providing the details of the model can be used together with the RFP Toolkit (See Figure 21).

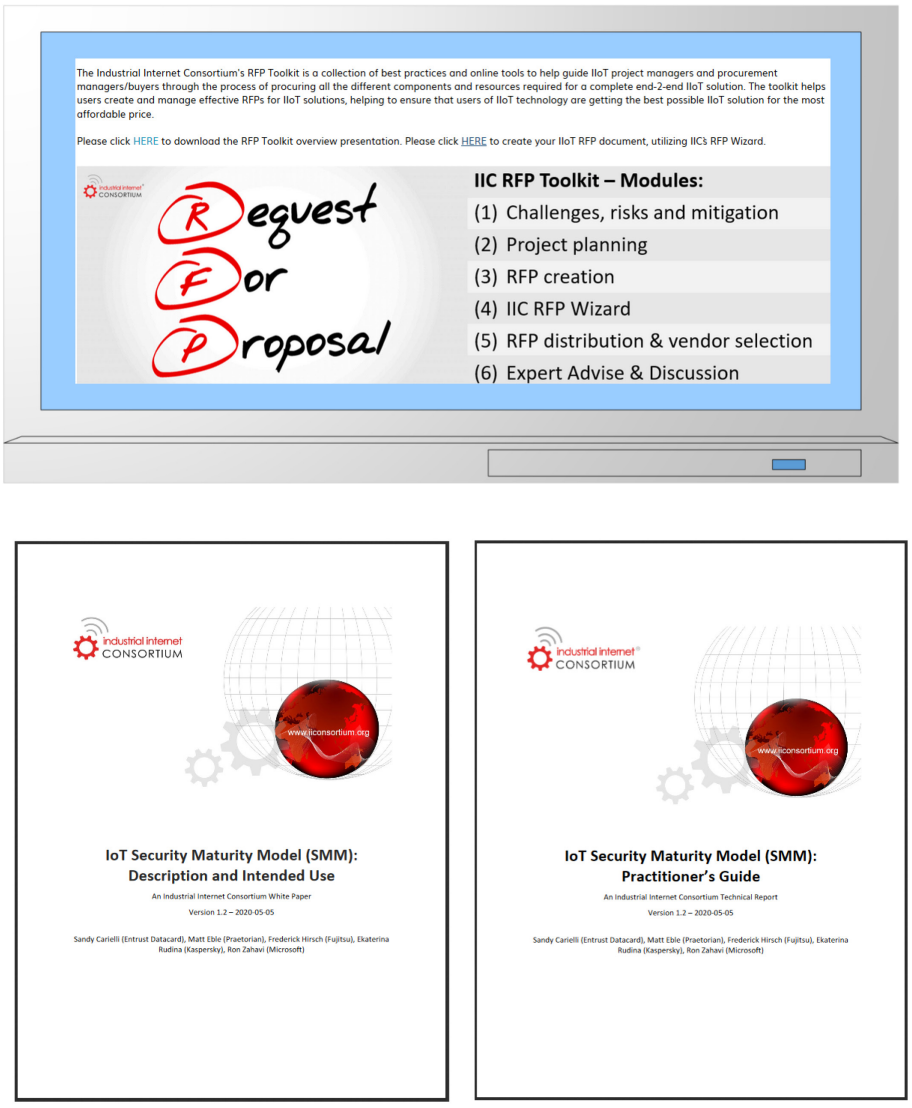


Figure 21 Industrial Internet Consortium RFP Toolkit and IoT Security Maturity Model (SMM) documentation. [64] [92] [93]

When adopting new technologies, like IIoT, resilience is required from Critical Infrastructures (CIs). A research called "Resilience framework for critical infrastructures: An empirical study in a nuclear plant" provides a qualitative resilience framework helping CIs improving their resilience level. The framework integrates socio-technical, technical, organizational, economic and social aspects. The framework also states that internal and external stakeholders involved in the crisis management process. The authors have performed an empirical study in a nuclear plant, and it proved framework's value in improving resilience level. [24]

A methodology to evaluate the reliability of the use of levels security with IoT devices for nuclear installations using WSNs has been proposed. The proposal consists of 5 main stages and 21 sub-stages, which are part of the category of a

function in groups of cyber security results that are linked to programmatic needs and specific activities of mandatory execution. The application of the defense-in-depth concept of anomaly solution management and prevention against atypical events to provide an effective safety mechanism, ensuring its safe use in these high critical environments. The stages and sub-stages of the proposal are depicted in Figure 22. [12]

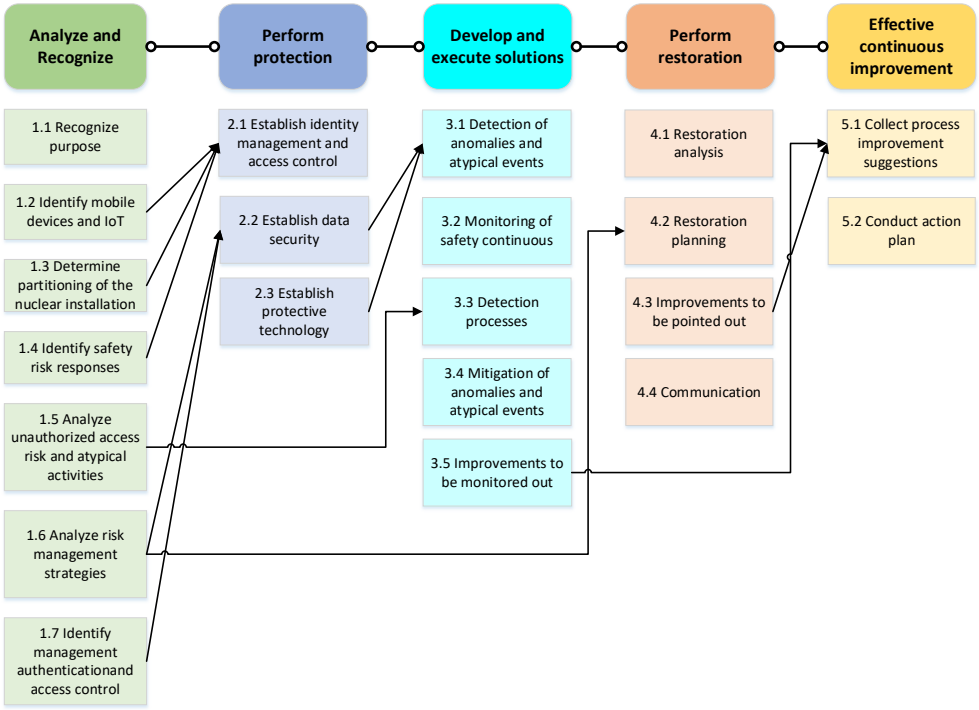


Figure 22 Functional diagram of the interconnections of the stages and sub-steps of the methodology. [12]

In addition to the IIoT strategy and other planning tool usage, nuclear industry related guidelines and recommendations should be applied parallel during the definition process. As an example of such document, IAEA's "Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications" [74] provides guidelines to justify commercial off the shelf (COTS) device and system usage in the nuclear plants. Document proposes techniques and processes to be used as well as related standards. Figure 23 outlines an example of the COTS product justification process steps proposed in the document.

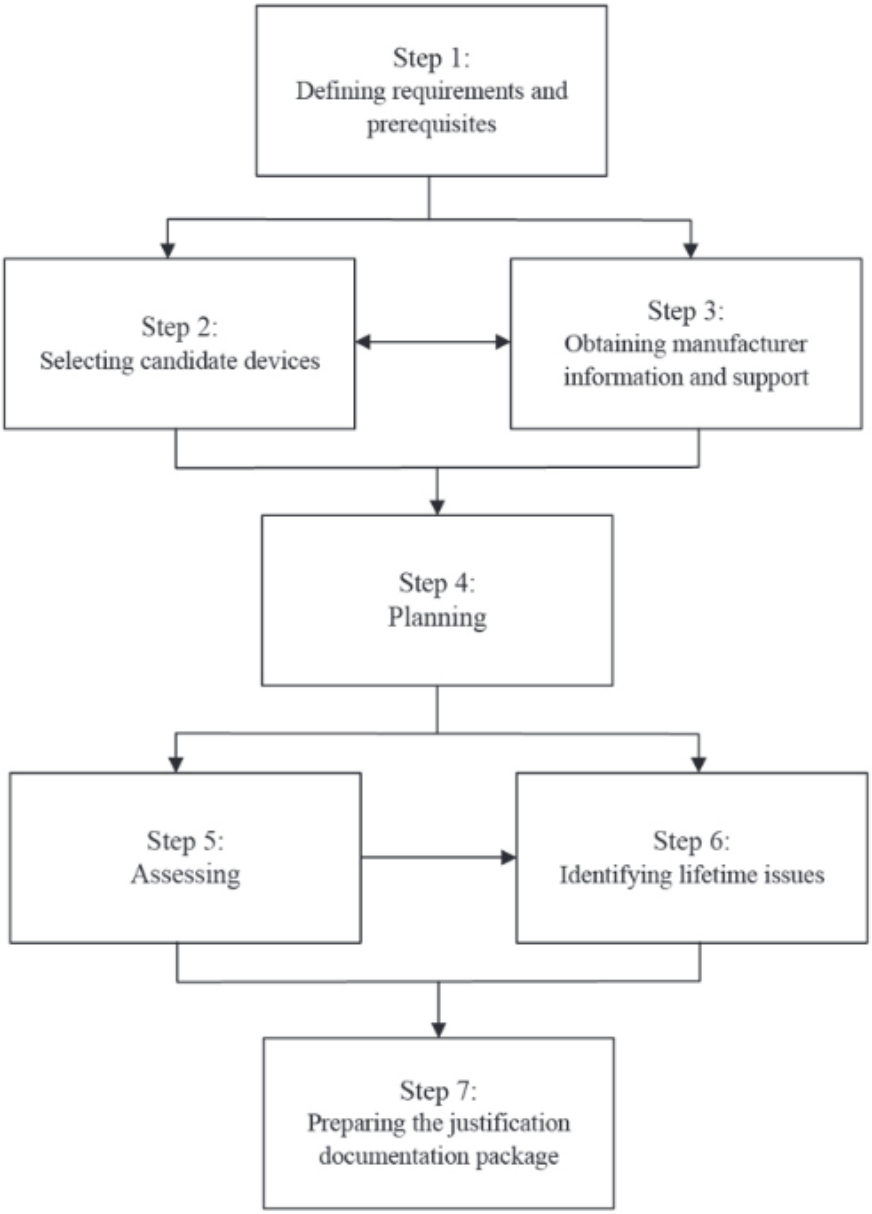


Figure 23 IAEA commercial off the shelf product justification process steps. [74]

5.3 FUTURE WORK

IIoT technologies have already been been adopted widely in use in many non-nuclear industries. Rapid evolution of different IIoT sub technologies, like sensors, wireless and cloud technologies as well as advanced data management including artificial intelligence guarantee the increase of IIoT usage across industries.

Nuclear industry, regulators and standardization bodies have followed the development and are already on the way to start adopting IIoT and wireless technologies in to use in NPPs. IIoT with wireless trials and pilots have been implemented already several years ago and when regulators and standardization bodies have created frameworks for the IIoT use adoption of IIoT can really start in the NPPs.

Development in the nuclear IIoT standardization and IIoT activities in other international NPPs should be followed as especially for the older NPPs successful best practices adopted from other NPPs are the most probable way to start using IIoT technologies. Another path to IIoT adoption is to create pilots with research communities and commercial partners and seek approval for the new solutions together.

6 References

[1] Laikari, A., Flak, J., Koskinen, A., & Häkli, J. 2018. Wireless in Nuclear: Feasibility study. Energiforsk report 2018-513.

[2] Bowen, P., Goel, A., Schallehn, M., & Schertler, M. 2017. Choosing the Right Platform for the Industrial IoT. Bain & Company Inc.

[3] Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. 2018. IoT Standardization - Challenges, Perspectives and Solution. ICFNDS' 18, June 26-27, 2018, Amman, Jordan.

[4] Javed, F., Afzal, M.K., Sharif, M., & Kim, B-S. 2018. Internet of Things (IoT) Operating Systems, Support, Networking Technologies, Applications, and Challenges: A Comparative Review. IEEE Communications Surveys & Tutorials, Vol. 20, No. 3, Third Quarter 2018.

[5] Bedi, G., Venayagamoorthy, G.K., Singh, R., Brooks, R.R., & Wang, K-C. 2018. Review of Internet of Things (IoT) in Electric Power and Energy Systems. IEEE Internet of Things Journal, Vol. 5, No. 2, April 2018.

[6] Bhuvaneswari, V., & Porkodi, R. 2014. The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview. International Conference on Intelligent Computing Applications 2014.

[7] Morgner, P., & Benenson, Z. 2018. Exploring Security Economics in IoT Standardization Efforts. Workshop on Decentralized IoT Security and Standards (DISS), 18 February 2018, San Diego, CA, US.

[8] Huang, B., Cardenas, A.A., & Baldick, R. 2019. Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks. The Proceedings of the 28th USENIX Security Symposium. August 14–16, 2019, Santa Clara, CA, USA.

[9] Bellekens, X., Seeam, A., Nieradzinska, K., Tachtatzis, C., Cleary, A., Atkinson, R., & Andonovic, I. 2015. Cyber-Physical-Security Model for Safety-Critical IoT Infrastructures. Wireless World Research Forum Meeting 35, Copenhagen, Denmark.

[10] Kim, H.E., Son, H.S., Kim, J., & Kang, H.G. 2017. Systematic development of scenarios caused by cyber-attack-induced human errors in nuclear power plants. Reliability Engineering and System Safety, Vol 167, pp. 290-301.

[11] Herbert, S. 2019. Why IIoT should make businesses rethink security. Network Security, July 2019, pp. 9-11.

[12] Savoine, M.M, de Menezes, M.O., & de Andrade, D.A. 2018. A Proposal for WSN Cybersecurity Levels for IoT Devices in Nuclear Research Facilities. IFIP Latin American Networking Conference, IFIP LANC 2018, São Paulo, Brazil, October 3-4, 2018.

[13] Flauzac, O., Gonzalez, C., & Nolot, F. 2015. New Security Architecture for IoT Network. Procedia Computer Science. Vol. 52, 2015, pp. 1028-1033.

[14] Hodgson, R. 2019. Solving the security challenges of IoT with public key cryptography. Network Security, January 2019, pp. 17-19.

[15] Urien, P. 2018. Blockchain IoT (BIoT): A New Direction for Solving Internet of Things Security and Trust Issues. 3rd Cloudification of the Internet of Things (CIoT), 2018.

[16] Moh, M., & Raju, R. Machine Learning Techniques for Security of Internet of Things (IoT) and Fog Computing Systems. 2018 International Conference on High Performance Computing & Simulation.

[17] Firdous, S.N., Baig, Z., Valli, C., & Ibrahim, A. 2017. Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol. 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).

[18] Krejˇcí, R., Hujˇnák, O., & Švepeš, M. 2017. Security Survey of the IoT Wireless Protocols. 2017 25th Telecommunication Forum (TELFOR), Belgrade, 2017.

[19] Ronen, E., O'Flynn, C., Shamir, A., & Weingarten, A-O. 2017. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. 2017 IEEE Symposium on Security and Privacy.

[20] Zhang, R., & Liu, X. 2014. IoT-Based Maintenance Process Design for Fusion Reactor Remote Handling System. Journal of Fusion Energy (2014) Vol. 33. pp. 653–657.

[21] Farley, D.R., Negus, M.G., & Slaybaugh R.N. 2018. Industrial Internet-of-Things & Data Analytics for Nuclear Power & Safeguards. Sandia National Laboratories.

[22] Min, J.H., Kim, D-W., & Park, C-Y. 2019. Demonstration of the validity of the early warning in online monitoring system for nuclear power plants. Nuclear Engineering and Design, Vol. 349, pp. 56-62.

[23] Sim, H. 2018. IoT Will Not Deliver on Potential Without Solving This Challenge. Natural Gas and Electricity, October 2018, pp. 21-24.

[24] Labakan, L., Hernantes, J., & Sarriegi, J.M. 2015. Resilience framework for critical infrastructures: An empirical study in a nuclear plant. Reliability Engineering and System Safety, Vol. 141, pp. 92-105.

[25] Savoine, M.M., Andrade, D.A., & de Menezes, M.O. 2019. Methodology Ethodology Proposal for Assessing Safety in WSN and IoT Devices in Nuclear Research Laboratory. 2019 International Nuclear Atlantic Conference - INAC 2019, Santos, SP, Brazil, October 21-25, 2019.

[26] Susila, I.P., Istofa, Kusuma, G., Sukandar, & Isnaini, I. 2018. Development of IoT Based Meteorological and Environmental Gamma Radiation Monitoring System. AIP Conference Proceedings 1977.

[27] Thibauda, M., Chi, H., Zhou, W., & Piramuthu, S. 2018. Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review. Decision Support Systems, Vol. 108 (2018), pp. 79-95.

[28] Kim, S., Lim, H., Lim, S., & Shin, I.. 2018. Study on cyber security assessment for wireless network at nuclear facilities. 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya.

[29] Muniraj, M., Qureshi, A.R., Vijayakumar, D., A.R., Viswanathan, & Bharathi, N. 2017. Geo Tagged Internet of Things (IoT) device for radiation monitoring. 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, 2017, pp. 431-436.

[30] Agarwal, V., Buttles, J.W., Beaty, L.H., Naser, J., & Hallbert, B.P. Wireless Online Position Monitoring of Manual Valve Types for Plant Configuration Management in Nuclear Power Plants. IEEE Sensors Journal, Vol. 17, No. 2, January 15, 2017, pp. 311-322.

[31] Yastrebenetsky, M., & Kharchenko, V. 2016. Reliability and Safety of Nuclear Power Plant Instrumentation and Control Systems: New Challenges and Solutions. 2016 Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management.

[32] Tatourian, I.A., Nayshtut, A., Pogorelik, O., & Hunt, S. 2017. Cognitive Protection of Critical Industrial Solutions Using IoT Sensor Fusion. United States Patent, US 9,817,676 B2.

[33] Mahammad D.V. 2019. Design and Development of IoT based Geiger Muller counter. International Research Journal of Engineering and Technology (IRJET), Vol. 6 Issue 12, December 2019.

[34] Mascareñas, D., Harden, T., Morales, J., Boardman, B., Sosebee, E., Blackhart, C., Cattaneo, A., Krebs, M., Tockstein, J., Green, A., Dasari, S., Bleck, B., Katko, B., Moreu, F., Maharjan, D., Aguero, M., Fernandez, R., Trujillo, J., & Wysong, A. 2019. Augmented Reality for Enabling Smart Nuclear Infrastructure. Frontiers in Built Environment, June 2019, Vol. 5, Article 82.

[35] Varghese, A.J., Jolly, A.T., Peter, A., Rajeev, B.P., Sajitha, K.S., & George, D. E. 2019. IoT based Disaster Monitoring and Management System for Dams (IDMMSD). 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Chennai, India, 2019.

[36] Gross, K.C., & Li, D. 2018. Machine Learning Innovation for High Accuracy Remaining Useful Life (RUL) Estimation for Critical Assets in

IoT Infrastructures. International Conference on Internet Computing and Internet of Things (ICOMP'18).

[37] Tanaka, S., Fujishima, K., Mimura, N., Ohashi, T.,& Tanaka, M. 2016. IoT System Security Issues and Solution Approaches. Hitachi Review Vol. 65 (2016), No. 8. URL: https://www.hitachi.com/rev/archive/2016/r2016_08/pdf/r2016_08_111.pdf.

[38] Gohel, H.A., Upadhyay, H., Lagos, L., Cooper, K., & Sanzetenea, A. 2020. Predictive Maintenance Architecture Development for Nuclear Infrastructure using Machine Learning. Nuclear Engineering and Technology, Article in press.

[39] Oh, S.W., Bae, J., Yoon, D., Yang, B., Kim, G. J., & Kim, H.S. 2018. A study on Improvement of Resource Efficiency for IoT-based Pipe Leak Detection. 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, pp. 1423-1425.

[40] Tocchi, A., Roca, V., Angrisani, L., Bonavolontà, F., & Moriello, R.S.L. First step towards an IoT implementation of a wireless sensors network for environmental radiation monitoring. 2017 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Turin, 2017.

[41] Kwon, D., Hodkiewicz, M.R., Fan, J., Shibutani, T., & Pecht, M.G. 2016. IoT-Based Prognostics and Systems Health Management for Industrial Applications. IEEE Access, Vol. 4, 2016. pp. 3659-3670.

[42] Wang, C., Vo, H.T., & Ni, P. 2015. An IoT Application for Fault Diagnosis and Prediction. 2015 IEEE International Conference on Data Science and Data Intensive Systems, pp. 726-731.

[43] Backman, J., & Helaakoski, H. 2016. Evaluation of Internet-of-Things Platforms for Asset Management. In K. T. Koskinen, H. Kortelainen, J. Aaltonen, T. Uusitalo, K. Komonen, J. Mathew, & J. Laitinen (Eds.), Proceedings of the 10th World Congress on Engineering Asset Management (WCEAM 2015) (pp. 97-104). Springer. Lecture Notes in Mechanical Engineering https://doi.org/10.1007/978-3-319-27064-7_9

[44] Backman, J., Väre, J., Främling, K., Madhikermi, M., & Nykänen, O. (2016). IoT-based Interoperability Framework for Asset and Fleet Management. In Emerging Technologies and Factory Automation (ETFA), 2016 IEEE 21st International Conference on (pp. 1-4). IEEE Institute of Electrical and Electronic Engineers. https://doi.org/10.1109/ETFA.2016.7733680

[45] PTC, ThingWorx. 2016. IoT Value Roadmap, Version 1.0, Part Number: J5452_PTC_IoT_VRM_1.0.

[46] Biron, J., Kelly, S., Immerman, D., & Lang, J. 2019. The State of Industrial Internet of Things 2019: Spotlight on Operational Effectiveness. PTC. J12987–State–of–IIoT–WP–EN–0319.

[47] IIC - Industrial Internet Consortium. 2019. The Industrial Internet of Things Volume G1: Reference Architecture. Version 1.9, June 19, 2019.

[48] Champigny, S., Gupta, D., Watson, W., & Waedt, K. 2017. Cyber security in nuclear power plants and its portability to other industrial infrastructures. VGB PowerTech, Vol. 5., pp. 27-32.

[49] Maslow, A.H. (1943). A Theory of Human Motivation. Psychological Review, 50(4), pp. 370–396.

[50] Rogati, M. (2017). The AI Hierarchy of Needs. URL: https://hackernoon.com/the-ai-hierarchy-of-needs-18f111fcc007

[51] IAEA (2020). The Future of Atoms: Artificial Intelligence for Nuclear Applications. URL: https://www.iaea.org/newscenter/news/the-future-of-atoms-artificial-intelligence-for-nuclear-applications

[52] ETSI. URL: www.etsi.org

[53] Slama, D., Puhlmann, F., Morrish, J., & Bhatnagar, R.M. 2015. Enterprise IoT: Strategies and Best Practices for Connected Products and Services. O'Reilly Media, 2015.

[54] Bonnardel-Azzarelli, B. 2019. IoT opportunity. Nuclear Engineering International, 28th August 2019. URL: https://www.neimagazine.com/features/featureiot-opportunity-7388490/

[55] AB5 Consulting. URL: https://www.ab5consulting.com/temlab

[56] Temlab. URL: http://www.temlab.online/

[57] West, A. 2018. Duke Energy Leverages IIoT for Predictive Maintenance Applications. IHS Markit Technology, January 2018.

[58] EPRI. URL: https://www.epri.com

[59] EPRI. Products. URL: https://www.epri.com/research/products/

[60] EPRI. Nuclear sector. URL: https://www.epri.com/research/sectors/nuclear

[61] Masek, P., Hudec, D., Krejci, J., Ometov, A., Hosek, J., & Samouylov, K. (2018) Communication Capabilities of Wireless M-BUS: Remote Metering Within SmartGrid Infrastructure. In: Vishnevskiy V., Kozyrev D. (eds) Distributed Computer and Communication Networks. DCCN 2018. Communications in Computer and Information Science, vol 919. Springer.

[62] Davoody-Beni, Z., Sheini-Shahvand, N., Shahinzadeh, H., Moazzami, M., Shaneh, M., & Gharehpetian, G. B. 2019 Application of IoT in Smart Grid: Challenges and Solutions. 2019 5th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS), Shahrood, Iran, 2019, pp. 1-8.

[63] Cornel - Cristian, A., Gabriel, T., Călin-Arhip, M., & Zamfirescu, A. 2019. Smart grid integration of IoT. 2019 54th International Universities Power Engineering Conference (UPEC), Bucharest, Romania, 2019.

[64] IIC - Industrial Internet Consortium. 2020. IIoT RFP Toolkit Creating and Managing RFPs for the Industrial Internet, DXWG June 11, 2020. URL: https://www.iiconsortium.org/pdf/IIoT-RFP-Management.pdf

[65] Hashemian H.M. 2011. "Nuclear Power Plant Instrumentation and Control. Chapter 3 in InTech book, Nuclear Power - Control, Reliability and Human Factors, European Open Access Publisher, http://intechweb.org/ Nuclear Power / Book 4, ISBN 979-953-307-855-6. pp. 49-66.

[66] Rokka H. 2018. Edge Computing is challenging but not breaking. Commercial article, online magazine Tivi.

[67] IAEA Power Reactor Information System PRIS. URL: https://pris.iaea.org/PRIS/

[68] Laikari, A. 2018. Wireless in Nuclear Applications: Seminar Report. Wireless in Nuclear Applications - Stockholm, Sweden 03/2018. https://energiforskmedia.blob.core.windows.net/media/24841/wireless-in-nuclear-applications-seminar-report-energiforskrapport-2018-514.pdf

[69] Fortum press release. 07.07.2020. The Finnish Transport and Communications Agency Traficom responds to the changing needs of digitalized society by granting the first ever license to local mobile networks". https://www.traficom.fi/en/news/new-leaf-turns-history-telecommunications-fortums-loviisa-power-plant-gets-its-own-mobile

[70] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018). https://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf

[71] Backman, J., Valtanen, K., Laikari, A., Vallivaara, V., & Ilomäki, J. (2017). Blockchain review: BOND project (Blockchains Boosting Finnish Industry) report. VTT Technical Research Centre of Finland. VTT Technology No. 330 https://www.vtt.fi/inf/pdf/technology/2017/T330.pdf

[72] Ericsson Mobility Report, June 2020, https://www.ericsson.com/49da93/assets/local/mobility-report/documents/2020/june2020-ericsson-mobility-report.pdf

[73] https://www2.deloitte.com/content/dam/insights/us/articles/722835_tmt-predictions-2020/DI_TMT-Prediction-2020.pdf

[74] INTERNATIONAL ATOMIC ENERGY AGENCY, Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications, Nuclear Energy Series No. NR-T-3.31, IAEA, Vienna (2020).

[75] Säteilyturvakeskus (STUK), Radiation and Nuclear Safety Authority, www.stuk.fi

[76] Regulatory Guides on nuclear safety and security (YVL) (online) https://www.stuk.fi/web/en/regulations/stuk-s-regulatory-guides/regulatory-guides-on-nuclear-safety-yvl-

[77] Stråls säkerhets myndigheten, Swedish Radiation Safety Authority, www.ssm.se

[78] SFS Finnish Standards Association (SFS), www.sfs.fi

[79] STUK, YVL E.7, Electrical and I&C equipment of a nuclear facility, 15.3.2019, https://www.stuklex.fi/en/ohje/YVLE-7

[80] IAEA. 2016. Design of Instrumentation and Control Systems for Nuclear Power Plants Specific Safety Guide (IAEA Specific Safety Guide No. SSG-39). https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1694_web.pdf

[81] IAEA Nuclear Energy Series. Nov. 2020. No. NR-T-3.29. Application of Wireless Technologies in Nuclear Power Plant Instrumentation and Control Systems. https://www-pub.iaea.org/MTCD/Publications/PDF/P1869_web.pdf

[82] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Selection and Use of Wireless Devices, IEC 62988:2018, IEC, Geneva (2018).

[83] STUK (2020). SLAFKA, a permissioned blockchain prototype for nuclear safegueards. https://www.stuk.fi/documents/12547/273805/SLAFKA_Infographic_2020.pdf/4e84cac4-ebaf-705a-2021-c8ba7400160e?t=1583742072832

[84] STT news (2020, Mar. 10). Blockchain offers new opportunities for safeguards of nuclear materials. STT. https://www.sttinfo.fi/tiedote/blockchain-offers-new-opportunities-for-safeguards-of-nuclear-materials?publisherId=64456131&releaseId=69876403

[85] Hyperledger platform. URL https://www.hyperledger.org/

[86] Modern2020 Consortium. 2019. D3.2 Wireless data transmission systems for repository monitoring. http://www.modern2020.eu/fileadmin/Deliverables/Modern2020-_D3.2_Wireless_data_transmission_systems_JB.pdf

[87] Modern2020 Consortium. 2019. D6.3 Modern2020 Final Conference Proceedings. http://www.modern2020.eu/fileadmin/user_upload/Modern2020-_D6.3_PU_Conference_proceedings_FINAL-web.pdf

[88] OECD / NEA. 2019. Nuclear Legislation in OECD and NEA Countries, Regulatory and Institutional Framework for Nuclear Activities, Finland, https://www.oecd-nea.org/law/legislation/finland.pdf

[89] OECD / NEA. 2008. Nuclear Legislation in OECD and NEA Countries, Regulatory and Institutional Framework for Nuclear Activities, Sweden, https://www.oecd-nea.org/law/legislation/sweden.pdf

[90] Bohm R. 2018. Industrial Internet of Things for Developers. ISBN 978-1-119-45693-3 (pbk). Wiley 2018. https://www.ge.com/digital/sites/default/files/download_assets/GE-Industrial-Internet-of-Things-for-Developers.pdf

[91] McKinsey & Company. 2018. The Internet of Things: How to capture the value of IoT. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20How%20to%20capture%20the%20value%20of%20IoT/How-to-capture-the-value-of-IoT.pdf

[92] Carielli S., Eble M., Hirsch F. Rudina E., Zahavi R. IIC - Industrial Internet Consortium. 2020. IoT Security Maturity Model (SMM): Description and Intended Use. Version 1.2, May 5, 2020. https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf

[93] Carielli S., Eble M., Hirsch F. Rudina E., Zahavi R. IIC - Industrial Internet Consortium. 2020. IoT Security Maturity Model (SMM): Practitioner's Guide. Version 1.2, May 5, 2020. https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf

[94] Lowe C. L., Kiger C. J., Jackson D. N., Young D. M., Analysis and Measurement Services, Implementation of Wireless Technologies in Nuclear Power Plants' Electromagnetic Environment Using Cognitive Radio System, NPIC&HMIT 2017, San Francisco, CA, June 11-15, 2017

[95] JIANG J., CHEN D., BARI A., HASHEMIAN H. M., Technical Survey on Applications of Wireless Sensor Networks in Nuclear Power Plants, ISOFIC/ISSNP 2014, Jeju, Korea, August 24-28, 2014.

[96] Jarrett R.J., Hashemian H.M., Morton G.W., Shumaker B.D., and Kiger C.J., Nuclear power comeback sure to employ wireless tools, 2009 ISA Automation IT.

[97] Seismic Monitoring System for Nuclear Power Plants, https://www.geosig.com/files/geosig_npp_documents_public.pdf

[98] Nekoogar F. and Dowla F., A ROBUST WIRELESS COMMUNICATION SYSTEM FOR ELECTROMAGNETICALLY HARSH ENVIRONMENTS OF NUCLEAR FACILITIES, NPIC&HMIT 2017, San Francisco, CA, June 11-15, 2017

[99] Son G.-S., Kim C.-H. and Kang H.-G., Performance Evaluation of Terrestrial Emergency Communication System in NPPs, ISOFIC/ISSNP 2014, Jeju, Korea, August 24~28, 2014.

[100] Baghyalakshmi D., Chandran T., Ebenezer J., S.A.V. Murty S., Wireless Sensor Network for Temperature and Humidity Monitoring in a Nuclear Facility, 2013 Fifth International Conference on Advanced Computing (ICoAC), DOI: 10.1109/ICoAC.2013.6921951.

[101] Nuclear wireless advances seen as a 'game changer' for analytics, Nuclear Energy Insider Nov. 29 2017, https://analysis.nuclearenergyinsider.com/nuclear-wireless-advances-seen-game-changer-analytics

[102] A Wireless Eye in Nuclear Plants, EPRI Journal July/August 2017, http://eprijournal.com/wp-content/uploads/2017/07/A-Wireless-Eye.pdf

[103] https://www.iaea.org/NuclearPower/Engineering/CRP/AWT/index.html

[104] Nobes T., Murphy C., UK Nuclear Industry First Wireless Applications, Measurement and Control 2014, Vol. 47(2) 55-57, DOI: 10.1177/0020294014521156.

[105] OECD, R&D and Innovation Needs for Decommissioning Nuclear Facilities, 2014, https://www.oecd-nea.org/rwm/pubs/2014/7191-rd-innovation-needs.pdf, 318 p.

[106] IoT World Alliance. URL: https://iotworldalliance.org/

[107] Westinghouse news. Westinghouse Launches WEConnect™ System. 2020. https://www.westinghousenuclear.com/about/news/view/westinghouse-launches-weconnect-system

[108] Areva news. Areva develops a smart network for industrial site management. https://www.sa.areva.com/EN/news-10357/areva-develops-a-smart-network-for-industrial-site-management.html

Appendix A: Nordic nuclear power plant survey questions

Energiforsk IIoT feasibility in nuclear survey

VTT Technical Research Centre of Finland Ltd. is making a feasibility study for Industrial Internet of Things (IIoT) technology usage in nuclear for the Energiforsk "Digitalization in nuclear applications"-program. The aim of this study is to identify and compile information of existing IIoT solutions used in nuclear industry and in other demanding environments, which could be applicable in the Nuclear industry. This feasibility study report will be based on literature studies and surveys or interviews with selected experts from the Nordic utilities. Results will be published in an Energiforsk's standard report format later this year. Answers of the survey and possible further interviews will be anonymised and merged and no personal information will be published or used in the report. At the end the survey, you can express, if you can be later contacted for a short additional interview, in case some additional questions would be raised based on your answers. Participation to this additional optional interview is completely voluntary. You have been chosen to receive this survey, because the researchers of this study have earlier been in contact with you or the Energiforsk's "Digitalization in nuclear applications"-program steering group members have proposed you as a contact person to be interviewed for this study. You can consult with your colleagues prior to filling the survey to bring out the common view of your utility. We hope that you would have time to fill this survey and bring out valuable information for the study. Looking forward hearing your point of view concerning the usage and/or wishes concerning IIoT usage in the Nordic NPPs. The questions concern IIoT usage in three levels - The NPP you are representing - Your possible view/vision about the other Nordic NPPs - Your possible view/vision about the global NPPs If you do not have a comment for some specific question, you can leave the answer blank. There are 24 questions in this survey, but some of the questions come only visible, depending how you have answered the previous question. In case you have any questions related to this survey or the report, you can contact the core researchers of this study. You can find the contact information below. Thank you for your cooperation.

Energiforsk Ab
- https://energiforsk.se/en/

VTT Technical Research Centre of Finland Ltd.
- https://www.vttresearch.com/en

1. In which Nordic NPP or other instance are you involved or answering on behalf of?

- Forsmark (SE)
- Oskarshamn (SE)
- Ringhals (SE)
- Loviisa (FI)
- Olkiluoto 1-2 (FI)
- Olkiluoto 3 (FI)
- Hanhikivi (FI)
- Stråhl säkerhets myndigheten (SSM) (SE)
- Säteilyturvakeskus (STUK) (FI)
- other

2. How are your utility's / intance's general attitudes towards to usage of following technologies usage in your NPP?

	Should not use	Should decrease	Current state is ok	Should increase	Should increase widely
Usage of wireless technology in non-safety critical systems.					
Usage of wireless technology in safety critical systems.					
Usage of IIoT technology in non-safety critical systems.					
Usage of IIoT technology in safety critical systems.					

3. Do you or your utility / instance think that changing regulatory restrictions will allow in the future in following five (5) year period?

	Totally disagree	Disagree	No change to the current situation	Agree	Totally agree
More use of wireless technologies in non-safety critical systems.	○	○	○	○	○
More use of wireless technologies in safety critical systems.	○	○	○	○	○
More use of IIoT technologies in non-safety critical systems.	○	○	○	○	○
More use of IIoT technologies in safety critical systems.	○	○	○	○	○

4. What kind of Industrial Internet-of-Things (IIoT) applications and solutions are already in use in the NPP you represent?

5. What kind of IIoT applications and solutions have already been or will be piloted in the near future in the NPP you represent?

6. What are IIoT usage future wishes in the NPP you represent?

7. What kind of IIoT applications and solutions you know that are already in use in other Nordic NPP(s)?

8. What kind of IIoT applications and solutions you know that have already been or will be piloted in the near future in other Nordic NPP(s)?

9. What are IIoT usage future wishes you know that Nordic NPP(s) have?

10. What kind of IIoT applications and solutions you know that are already in use in other international NPP(s)?

11. What kind of IIoT applications and solutions you know that have already been or will be piloted in the near future in other international NPP(s)?

12. Do you know some standards or standardization aims relating to utlilization of IIoT in NPPs?

- Yes
- No

13. What are these standards?

14. Do you know some IIoT applications and solutions from other industry domains that can be seen valid also from NPPs point of view?

- Yes
- No

15. What other industry domains you see are most close to NPPs needs from IIoT applications point of view?

16. What are these IIoT applications in other industrial domains?

17. Do you know some already proven and suitable frameworks for IIoT applications and solutions frameworks for piloting, proof-of-concepts, etc.

- Yes
- No

18. What are these frameworks?

19. What regulatory requirements and restrictions there are to utilize IIoT applications and solutions in the NPP you represent

20. What regulatory requirements and restrictions you know there are to utilize IIoT applications and solutions in other Nordic and international NPP(s)

21. What kind of cyber security requirements and restrictions there are to utilize IIoT applications and solutions in the NPP you represent?

22. Are there other restrictions to utilize IIoT applications and solutions in the NPP you present?

23. The researchers of this study can contact me for possible additional questions, if needed?

- Yes
- No

24. My email address for possible further questions from the researchers for this study.

INDUSTRIAL INTERNET OF THINGS IN NUCLEAR

Industrial Internet of Things, IIoT is a rapidly growing phenomenon across industries. These technologies provide the opportunity to add instrumentation and enhance monitoring options of the nuclear power plant equipment.

Industrial Internet of Things systems can either be used to replace current legacy systems, which are lacking spare parts or add enhanced redundancy in monitoring the equipment operations.

This study reveals that the Nordic nuclear power plants are not yet using Industrial Internet of Things solutions very much because they have been built in the time before the digitalization era. Despite of the doubts to bring modern technologies for Industrial Internet of Things into the old nuclear power plants, which might interfere with the legacy I&C systems, there is the desire to adopt the new technology with applicable solutions into use.

Energiforsk is the Swedish Energy Research Centre – an industrially owned body dedicated to meeting the common energy challenges faced by industries, authorities and society. Our vision is to be hub of Swedish energy research and our mission is to make the world of energy smarter!

Energiforsk