Smart Nuclear Power Plants Operating System Through IoTs

Amanat Ali[1], Yasin Gudarzi[2], Bassma Abouabdellah[3], T. Elzayat[4], Mohammad Furqan Ali[5], and Gaurav Saini[6]
[1]Dept. of Mech. Engg., University of Petroleum & Energy Studies, India
[24]Dept. of Nuclear Fuel Cycle, Tomsk Polytechnic University, Russia
[3]Dept. of Génie Électrique, et Électronique, École Nationale Des Sciences Appliquées d'Agadir, Morocco
[5]School of Computer Science & Robotics, National Research Tomsk Polytechnic University, Russia
[6]Center of Excellence for Green Energy & Sensor System, IIEST Shibpur, Howrah, India

Abstract—**The potentials of the wireless network has made it possible to access a variety of technological operations through the folk of internet-connected devices. This exponential hike and trade of wireless carriers could be a platform to operate and deploy in highly radiated remotely accessed areas such as Nuclear Power Plants (NPPs). The internet-connected devices play the most significant role to improve and build up a smart NPP operating system. The promising internet of things (IoTs) method has enabled interaction between advanced instrumentation and control devices that contributes a new paradigm in the digital world towards the advanced futuristic wireless networks as 5G or 5G beyond (5GB) communication system in industrial research. From this point of view, we investigate the important features and arduously execute a novel approach to operate of smart NPP system for safety concerns by the deployment of internet-connected devices. Therefore, due to security reasons, the IoTs are patched up with a communication between the user and corresponding component at the site. Monitoring and surveillance of NPP safety concerns IoT have become the replacement solution of manpower. In this study, we are summarizing the affecting factors for smooth functioning of NPP, human health diseases cause radiation and a big impact of remotely accessed modern NPP system. This study is also carried out a wide discussion and comprised the existing operational views. Additionally, the major key components of wireless connections are used for security and safety monitoring in NPP systems through IoTs. Finally, the future extendable work is also summarized.**

Index Terms—Internet of Things (IoTs), Smart Nuclear Power Plant (NPP) System, Safety and Security in Nuclear Power Operations.

I. Introduction

Since the incidence of the 3-miles Island, Chernobyl, and Fukushima, issues with regards to the safety of Nuclear Power Plants (NPPs) have become a preferable research field of investigation. For instance, critical accidents are distinguished by a very brief and high-intensity radiation pulse, which could then be followed by further pulses to maintain a steady-state power level on a continuous basis. There is no possibility for personnel in the area of such occurrence to avoid the initial pulse exposure [1]. With regard to standard safety concerns, the system could achieve the critically conditions followed by a sudden jump in power level when neutrons fluxes trigger the nuclear sustainable chain reactions within the system. This is a more significant approach for critical safety, a system can experience transients operation modes which could lead to a super-prompt critical condition that is undetected by personnel or standard radiation monitoring and control instruments. For being continuously radiation, International Commission on Radiological Protection (ICRP) stated that the maximum effective dose equivalent of 20 mSv/year as occupation exposure averaged over a 5 year period [2]. It is also noted that every biological organs and tissues have differing probabilities of developing radiogenic cancer, due to healthcare safety is the major concern to study nuclear safety.

To cope with these issues, Medical Technology (MT) is another approach that helps in monitoring health parameters and sustains the health care of patients [3]. MTs are employed in diverse areas such as monitoring systems for satisfactory levels and better scanning types of equipment to receive reliable treatment remotely accessed. The potential of the internet has altered the means of communication and re-search in different scientific fields. The approach of interaction wirelessly is required internet productive devices generally called as the internet of things (IoTs). This concept provides a communication bridge among transceivers and users. In another way, IoTs open the doors of a new paradigm to connect the massive number of devices in various applications and promise to improve human-assisted lives in better quality. Due to this, IoT has gained attention from researchers and engineers all around the globe. Moreover, the IoT is related to a new way of connecting various sorts of sensors to the internet which represent the next big leap ahead in the in-formation and communications technology (ICT) sectors. The integration of internet-connected devices in healthcare sector is proposed as Internet of Health Things (IoHTs) to support the new development of modern medical systems by embedding wireless sensors and medical equipment, combining them with the internet with achieving a full integration among hospitals, patients, and medical equipment.

Currently, the medical architectural and health care facilities have been taken care of by the IoHTs. Some major applications of the IoHTs include medical equipment medication control, medical information management, telemedicine, and mobile medical care, personal health management. Throughout this study, it supports an overview of IoTs and their most significant role in operating and control of NPP assessments in the safety and security concerns. This proposed study supports the main characteristic features of the safety concerns and the relevance in applications towards IoT scenarios in NPP systems. An overview of nuclear power plant operation remotely throughout the internet connection is depicted by Fig.1.

A. Paper Structure

The main objective of this study is to provide a problematic solution and consider safety patterns of remotely accessed NPP systems. Therefore, the importance of the proposed concept is presented in section II. The development of the smart nuclear power plant system and the major role of internet-connected devices in NPP system are discussed in section III. Through the remote operation of power plants the safety parameter most importantly taken into an account and summarized in section IV. The deployment of wireless communication system, the affecting factors and channel impairments are widely in consideration in this study. Finally we summarizing the whole work in section V.

B. Motivation and Contribution

The number of devices are connected to the internet and have been constantly growing in connectivity. The IoT is quickly diffusing across many areas from home appliances to entertainment devices, lighting, transportation, health care instruments, which that are considered at the consumer level of usage. Accordingly, the trade of IoT becomes one of the major communication and highly demandable approach that links the internet with sensors and working devices for an all internet protocol (IP) based architecture [4]. However, very few research works are presented in the literature to address the applications of IoT in the NPP operational domain including refueling, outage, and maintenance. Consequently, the m-IoT is a new approach that corresponds to the capabilities of m-health and IoT for a new and innovation towards the next generation of wireless networking applications. In the principle of *m*-IoT, it introduces a new healthcare connectivity paradigm that interconnects IP-based communication technologies [5]. Motivated this over-viewed research in digital communication domain, covers the following points as follows:

- A clear concept of the deployment IoTs in NPP operation in control systems for the safety and security concerns. The uniqueness of IoTs as a problematic solution for various communication hurdles;
- Sensing the physical phenomena of the related environment such as the exposure dose radiation, leakage of highly radioactive materials, and environmental effect;
- The ubiquitous data exchanging through proximity wire-less carriers in terms of spectrum availability or via radio signals.

II. Importance of IoTs in Nuclear Industries

It is believed that we are at the edge of a new technological transformation leading to the fourth industrial revolution which is built on the predecessors (water-steam, electricity, and electronics) and characterized by the convergence of various technological areas. These new materials, biotechnology, nanotechnology, and advanced digital production (ADP) technologies are characterized by exploit extensive digitalization in industries mentioned in Fig. 2.

The key component that helps to fill the gap between these technologies is digitalization with the help of IIoT are summarized in [6]. Further, in 2017 International Energy Agency (IEA) predicted that during 2016-2040s, digitalization in the power sector saved 80 billion per year or about 5% of the total annual power generation cost through reducing operations and maintenance costs. Additionally, improving power plant and network efficiency reducing unplanned out-ages and downtime, and extending the operational lifetime of assets are the main concerned [7]. It seems that why the interest for digitalization is growing on the energy sector. However, the potentials of digitalization in IIoT are being gradually understood and implemented by big companies in nuclear power as well. The key technological products for their implementation approaches are Predix (an IIoT edge-to-cloud based platform intended for data gathering from NPP and digitizing), Digital Twin (a software for performing predictive analytics on the data transformed by Predix), Watchtower (a system for obtaining real-time status of plant equipment), and Lighthouse (a service for risk analysis based on historical data, enabling to predict the adverse effect three months in advance) [8], [9], respectively. The work flow of General Electric Predix Platform (GEPP) is shown in Fig.3.

The communication system is considered as one of the major way in NPP remote operations. The communication systems have existed in all building blocks those need to interact within the NPP system, including the nuclear island buildings, conventional island buildings, and balance of plant buildings. It stands as the main system for operators and engineers to communicate throughout the nuclear power plant. In addition to that, it undergoes an important function of the communication system for emergency conditions. In general, this communication function that supports the control of emergency response is carried out by an emergency communication sys-tem, which is the most important communication sub-system in NPP operation. In [10], the authors have demonstrated a conceptual approach of an emergency communication system corresponding to severe nuclear accidents based on a wireless channel NPP system. IoT is a new technology that is associated with the contemporary era and is marked by its small size and user handy devices over limited storage and functionality. It is primarily concerned with dependability, performance, security, and privacy. IoT refers to an addressable protocol and collaboratively interconnection among devices network. These are based on intelligent and self-configuring devices, which are connected with the global network infrastructure [11]. The strategy of the implementation of these devices are used to monitor and cope with the modified environment with

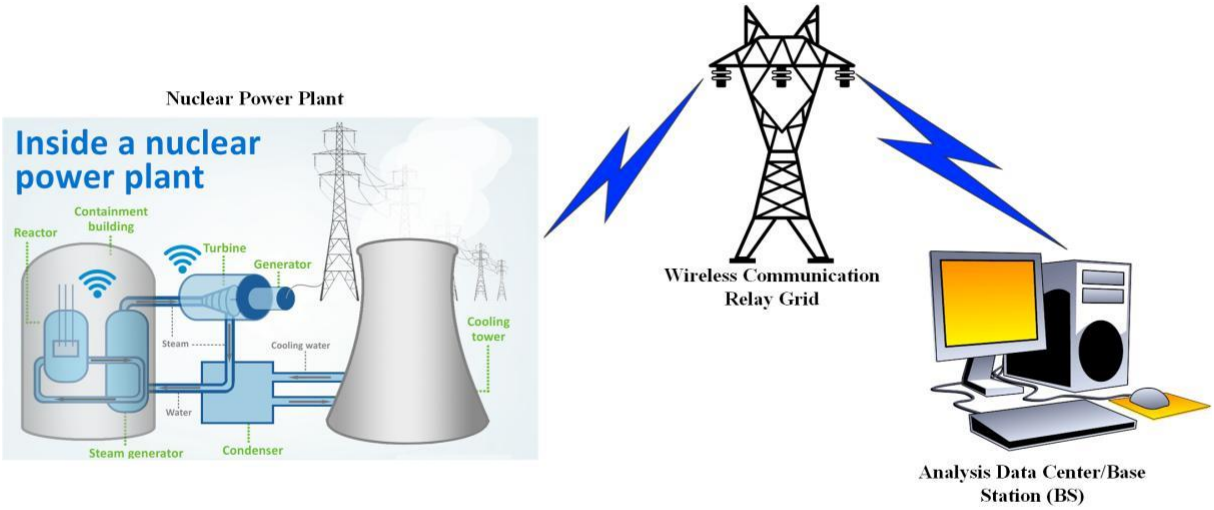

Fig. 1. The proposed scenario of nuclear power plants through remotely operation. The picture is depicted, the smooth function of the site remotely and monitoring the plants through internet connected devices.

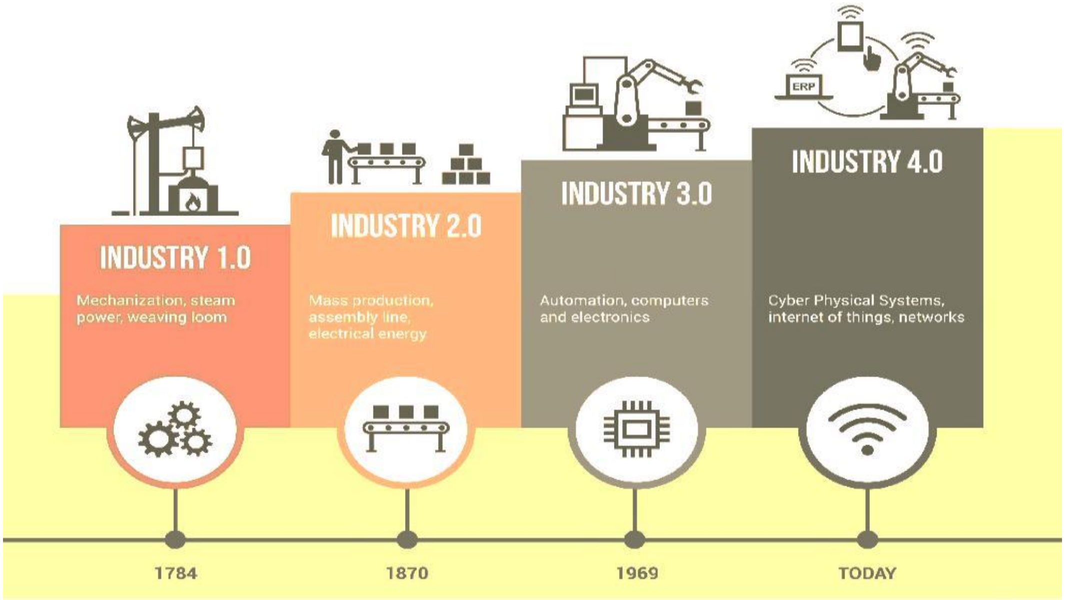
INDUSTRY 1.0
Mechanization, steam power, weaving loom
INDUSTRY 2.0
Mass production, assembly line, electrical energy
INDUSTRY 3.0
Automation, computers and electronics
INDUSTRY 4.0
Cyber Physical Systems, internet of things, networks
ERP
1784
1870
1969
TODAY

Fig. 2. The aspect of four industrial revolutionary generation [8], where the further development is depicted in each of individual duration.

respect to time. The IoTs have distinguished effects on assisted living and domestic scenarios with respect to next-generation perspectives [12].

The strategic approach of IoT underneath implementing of advance networking architectural devices are used to monitor and fully understand the concepts of changed circumstances and environments over time. IoT is being more advanced and a variety of communication technology which comprises daily basis objects such as clothing, food, business equipment, home appliances, and industrial surveillance, etc, [13]. As the industrial sphere is adapting the challenges of smart manufacturing towards the industry 4.0 perspective. The adoption of the industrial internet of things (IIoTs) is revolutionized for industrial operational standards. Nevertheless, the challenges still have strategies to boost transformation efforts while maintaining securities amid increased connectivity.

Enlighten of internet advances, a big impact of the integration of IIoT supports the industrial manufacturing processes to enhancing mass production, workers safety concerns, reduce dwelling time of machines, exponentially improve productivity rate, and diminishing mishappening, incidents, and casualties at the working platform. The operational methods of the industry could be predicted to be well-versed in aspects that include employee safety and product quality. Safety is an essential significant concern, across different industrial verticals. Due to this, an implementation of IIoTs in safety-as-a-service (Safe-aaS) industrial architecture is widely detailed in the recent open literature [25]. The authors in [14], are widely discussed the necessity of block-chain Safe-aaS IIoTs architecture and presented the five layers including device, edge decision, decision virtualization, and application.

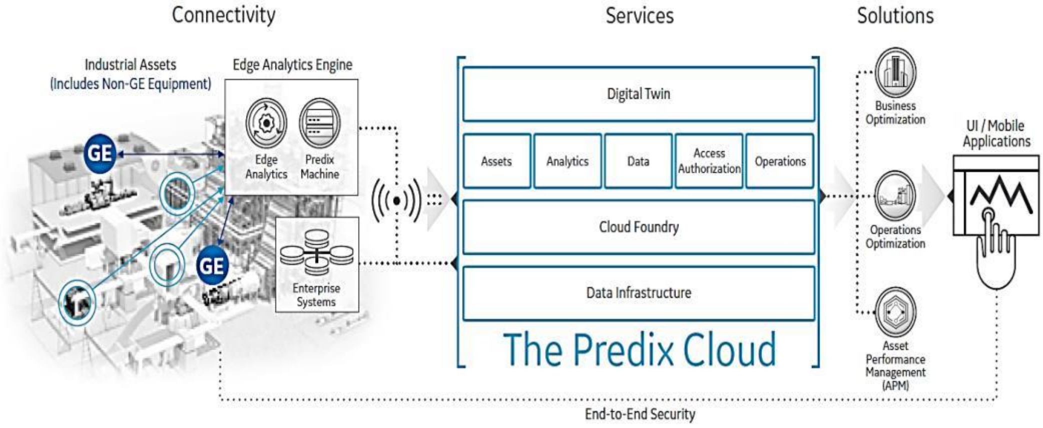

Fig. 3. The work flow of General Electric Predix Platform [11]

III. Infrastructure Development for a Smart NPP System

Generally, the digitalization in NPP system deals with big data analysis. This implies that the application of IoT devices in nuclear industry is closely connected with both data analytic and machine learning to ensure safety, security and safeguard measures. Therefore, a generic work plan for implementation of IIoT should enclose the following areas:

- Data analytic at the instrument level and transmit only important evaluated data through a secure wireless network. This also is called edge analytic;
- Encryption of data (for privacy-preserving aims), and analysis of the encrypted data using well-established algorithms.

Application of a method such as machine learning or block chain to achieve a robust consensus algorithm and protection against cyber-attacks. There are two approaches to data analytic at the instrument level are proposed as Sensor Path (SP) and Text Path (TP), each of which is depend on their specific data and tools for data processing. In the sensor path, large voluminous data are produced by sensors and then labeled to be processed by machine learning tools. In theory, the existent data from past operations, events and accidents can be used they should be refined and labeled, or else generation on new data is inevitable. As an example of implementation of data analytic by following the data path, may refer to the joint proposal by Sandia Laboratory an UC Berkeley to be implemented for a compact test facility (CIET). In this plan, sensor data along with the data gained from RELAP code simulations is gathered and then labeled according to the off-normal transient initiated, and this data fed into several modern machine learning tools (Principal Component Analysis (PCA), Support Vector Machines (SVM), and KNN). The possibility of performing real-time FFTs (Fast-Fourier Transforms) on the incoming sensor data streams to assess instrument degradation is also envisaged in the system. After machine, learning models are trained on the labeled experimental and simulated data streams, the trained models on to a Field-Programmable Gate Array (FPGA) device that could then identify the off-normal events in real time as illustrated by Fig. 4.

In the TP, a large number of text data resources such as IAEA safety publications, best practices reports, regulatory documents, research and technical documents should be processed to enable their usage for machine learning applications. However, availability of proprietary documents and diverse format of the documents (e.g. digital vs. hardcopy or encrypted vs. non-encrypted) are the main challenges for data analytic in Data Path (DP). At present, the most reliable tools for implementation of data analytic are IBM Waston platform, GE’s Predix, Google Tensorflow’s Word2Vec and Sandia’s Citrus text analytics library.

Aforementioned, one of the challenge is accessing the operational data of NPPs is the proprietary related issues. This issue can be addressed by encryption of a data and using the concept of privacy-preserving Multi-Party Computation (MPC) which enables secret sharing of data required for special nuclear material accountancy, safeguard measures and sensitive data such as proprietary operational data. In this concept the computation (asking a question) can be run with-out exposing the source data to the opposing party. The two main approaches for the implementation of privacy-preserving computations are secret sharing schemes, and more efficient Boolean garbled circuit protocols and compilers are summarized as in [15]. In secret sharing schemes, solve the problem of secrecy of data by dividing the total (secret) data into to shares distributed among different parties. The final desired results i.e. min/max, intersections, linear regressions, etc. are obtained by combining (Add and Multiply operations) the result of individual calculation performed by all parties. This result can be publicly shared without exposing the individual source data shares [16].

Although, the cyber security and standardization in this domain are essential aspects for IIoT connected devices. Ma-chine learning has been frequently proposed for ensuring IIoT network security. Some of the machine learning algorithms used for tasks like discovering a pattern in existing data, detecting outliers, predicting values, and feature extraction are listed in Table I [17].

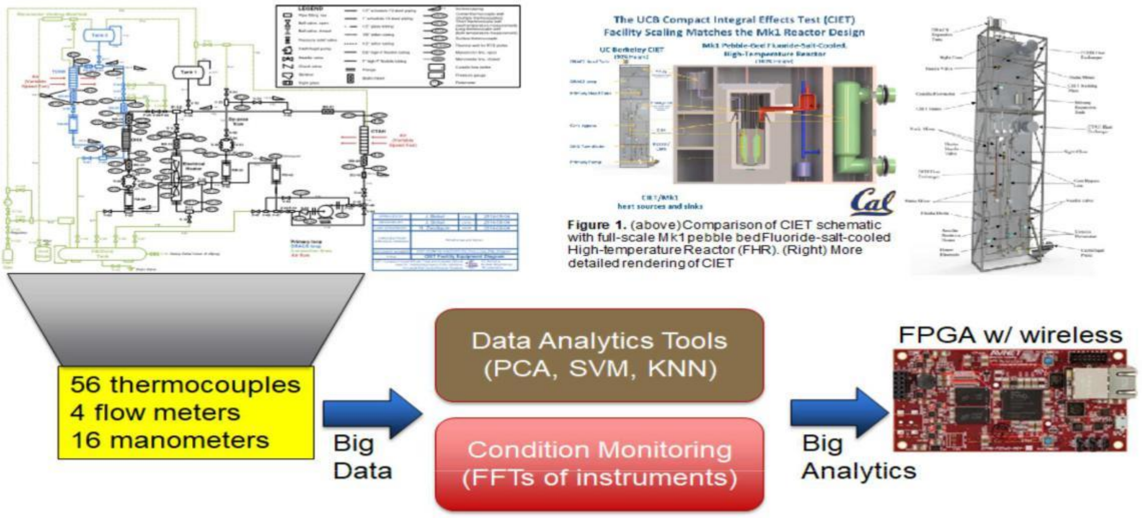
The UCB Compact Integral Effects Test (CIET) Facility Scaling Matches the Mk1 Reactor Design
UC Berkeley CIET
Mk1 Pebble-bed Fluoride-Salt-Cooled, High-temperature Reactor
CIET/Mk1 heat sources and sinks
Cal
Figure 1. (above) Comparison of CIET schematic with full-scale Mk1 pebble bed Fluoride-salt-cooled High-temperature Reactor (FHR). (Right) More detailed rendering of CIET
56 thermocouples
4 flow meters
16 manometers
Big Data
Data Analytics Tools (PCA, SVM, KNN)
Condition Monitoring (FFTs of instruments)
Big Analytics
FPGA w/ wireless

Fig. 4. A modern machine learning tools proposed for operation of UC Berkeley's Compact Test Facility [12]

Additionally, the block-chain technology is another important direction for solving security and trust issues for IoT with the outbreak of the crypto-currencies during 2016-2018s. The block-chain technologies are gained a numerous visibility in this specific ear for wireless securities. In another words, it defines as the family of technologies which can be use in various business areas for many purposes. In another study, it is carried out by IBM [18]. Further some of the block-chain benefits to IIoT are enumerated as follows:

- Facilitates adding the large numbers of IIoT devices without required central administration;
- Use excess capacity of under-used physical assets (block-chain contracts re-direct workflows);
- Block-chain can be used to track the sensor data measurements and prevent duplication with any another malicious data;
- Deployments of IoT devices can be complex, and a distributed ledger is well suited to provide IoT device identification, authentication and seamless secure data transfer;
- A distributed ledger eliminates a single source of failure within the ecosystem, protecting a IoT devices data from tampering;
- Block-chain enables device autonomy (smart contract), individual identity, and integrity of data and supports peer-to-peer communication by removing technical bottlenecks and inefficiencies;
- The deployment and operation costs of IoT can be reduced through block-chain since there is no intermediary; IoT devices are directly addressable with block chain, providing a history of connected devices for troubleshooting purposes.
- Providing aid in smart diagnostics (erroneous nodes might indicate a maintenance issue), supply chain tracking, product certification. machine-to-machine (M2M) transactions, registry of assets & inventory.

The above factors reveal the need for robust, redundant consensus mechanism for ultra-dependable systems, such as nuclear power plants. Beyond consensus, it appears block chain can provide further assurance regarding data integrity and chain of custody. There are also patents that utilize sensor fusion to protect critical industrial IoT solutions (United States Patent, US 9,817,676 B2) [19]. A cyclic cyber-physical security model [20] is proposed to use after system commissioning that allows knowledge transfer between regulatory bodies through sharing of best practices by the Fig. 5.

IV. SAFETY REQUIREMENTS AND ANALYSIS

Nuclear safety necessitates the use of an emergency communication network including reactivity control of nuclear reactor residual heat decay removal in addition to the radioactivity containment function. Nevertheless, the function provided by the emergency communication system aids in the emergency response. The emergency communication system should satisfy the specifications of IAEA SSG-39 and HAF102-2016 [2]. As a result, it should be usable in all postulated incidents as well as in accidental scenarios. To meet this requirement, the architecture of an emergency communication system should provide a range of safety precautionary measures. The measures against LOOP (Loss of Offsite Power) and Station Supply Black Out (SBO) accidents in nuclear power stations are taken into account. To prevent interfering with the safety function of adjacent safety classified systems and components in nuclear power stations, communications network equipment should also maintain stability throughout unforeseen natural catastrophes such as tsunamis, earthquakes, and volcanic eruptions. The maintenance of network components must also be taken into account when designing emergency communication systems based on the operational regulations of nuclear power plants.

A. Sensor Monitoring Effective NPP Operation

To accomplish intelligent monitoring, wireless sensor net-work (WSN) technology can be established in main types of nuclear reactors such as pressurized water reactors (PWRs)

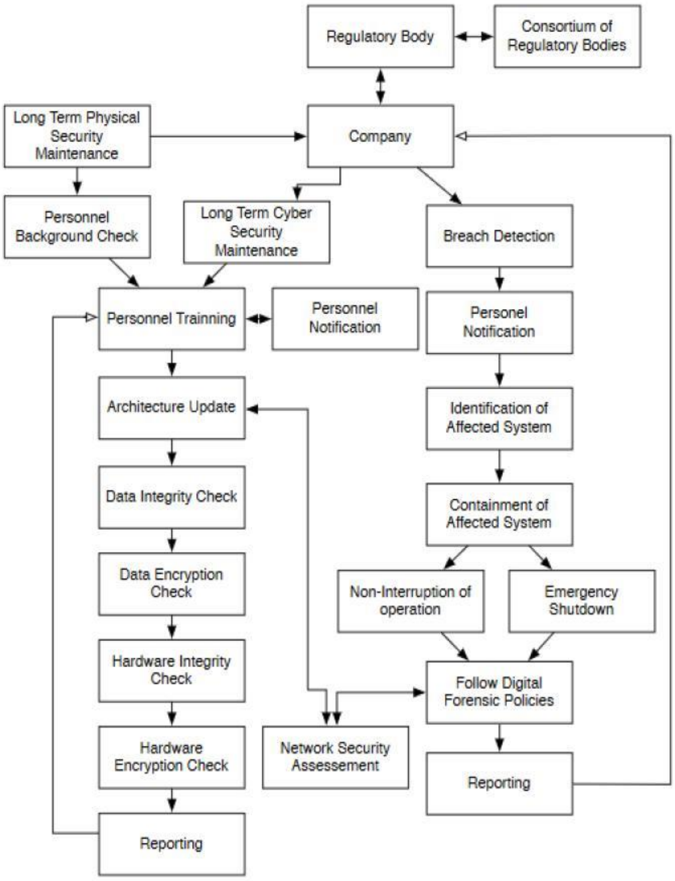
Regulatory Body
Consortium of Regulatory Bodies
Long Term Physical Security Maintenance
Company
Personnel Background Check
Long Term Cyber Security Maintenance
Breach Detection
Personnel Trainning
Personnel Notification
Personel Notification
Architecture Update
Identification of Affected System
Data Integrity Check
Containment of Affected System
Data Encryption Check
Non-Interruption of operation
Emergency Shutdown
Hardware Integrity Check
Follow Digital Forensic Policies
Hardware Encryption Check
Network Security Assessement
Reporting
Reporting

Fig. 5. The cyclic security flow model for long-term IoT supports [20]

and boiling water reactors (BWRs). Intelligent monitoring with WSN will not only decrease the significant cost of regular monitoring but will also support a variety of functions such as defect detection and recovery, condition-based maintenance, which will optimize the operation and maintenance of NPP systems. Moreover the sensors with wireless communication capabilities can work together to monitor physical or environ-mental conditions. A sensor can be a self-contained device that includes a sensing constituent, a radio transceiver, a microcontroller, and a source of energy altogether in the same module. It could also be a customary instrument linked to a wireless data transmitter, with sensed data wirelessly transmitted to a data processing center. There are various considerations that must consider in order to make the entire module operate more efficiently at operating NPPs by utilizing IT technology, all NPPs are working to achieve efficient, safe, and reliable operation and a decrease in operator error. Typically, voice communication has also been used as an analog desk phone is assembled in the phone booth or operator computer during the operation. Nevertheless, wireless technology has been used during the overhaul period of domestic NPPs on the basic principle of the primary concern safety procedures.

B. The Role of Wireless Network in Nuclear Operation

Generally, the most of internet-connected devices are used to facilitate, nuclear control and operational activities. How-ever, the Nuclear Regulatory Commission (NRC) is anticipating the nuclear trade to provide a wireless network among the various application and data transmission along with the protected cybersecurity requirements. The current trends of cellular carriers and deployment in nuclear industries are limited in order to non-safety-related applications. The current applications of digital signaling support data transmission among devices and employees within the field crews, supervisory control, and with the substations. The safety concerns and analysis are quite compatible the wireless network. Nevertheless, the higher data rate and the wireless link provided as an advantage. The cellular carriers minimize the acceptable errors rather than the local errors inbuilt in existing systems. The wired links support common errors as repetition, deletion, insertion, incorrect sequences, respectively. Another diversity of the probability is the plenty errors that occur in the system. As an example, communication errors are responsible for higher bit error rates, and fading environment wireless signals also affect the mobility, and interference at the user end.

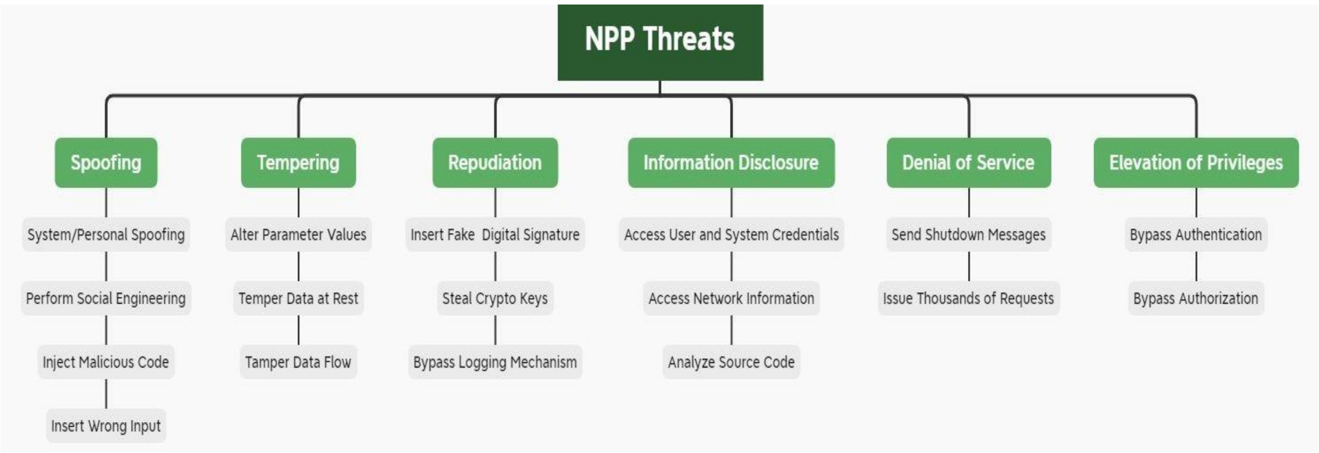

Fig. 6. The nuclear power plants threats hierarchy tree in cyber security. The corresponding issues occur in order to operating the NPP systems and the related types of threats with corresponding attackers.

C. Cyber issues

In general, the wireless communication system should imply the basic security objectives. The system security properties could described by confidentiality, integrity and availability (CIA) [28]. The corresponding significance of CIA is related to the requirements of specific application. The unnecessary violations of the security parameters are typically arise via known attack technique. However, the hacking attacks are classified according to the function of attackers as active and passive attacks. Therefore, within the passive attack the attackers by hacking the wireless network. The different types of attacker and types threat are summarized and depicted as in Fig. 6. The attackers monitor the specified network and encrypt the data, including authentication credentials and could be attack at any point in the wireless link, while the active attacks are relied based on the ability of an attacker for link interruption. Addionally, an intentional jamming could be held in active attack category. The consequences in unexpected attacks by amending, or modifying the data or in other ways it could be misused. The necessity of the basic security system should be imply by an encryption, device authentication, and enabled physical security. All of above measures, are beneficial for various encryption and physical security for the secure wireless systems.

D. General Wireless Security Concern

The relative importance of the CIA also concerns the importance of the precise application; therefore, the requirements for its performance are being reviewed. Although the violations of those security standards are usually arose via unrecognized attack mechanisms. The perspective attacks are often categorized in terms of the attackers function. A brief classification of those attacks include passive and type active attacks are mentioned in earlier section. The corresponding access to physical network is important to send messages or receive them. The wireless networks function by means connected with wireless devices, those broadcast signals through the air. Thus, the transmission is often heard by anyone within range. Although things are superfluous, the receiver's objection can receive signals of the target because the communication protocols uniform commercial readily available. It is typically challenging that the adaptation of the transmission state which could interfere the transmissions of other nearby or prevents their independence rights.

The Federal Communications Commission (FCC) regulates product sold within the radio jamming as oftenly easy if the structure of all the knowledge about the communication protocols is available. Surely, confusion or objection must be in close proximity so as to receive sufficient signal. The communications system should not be built using commercially available radios. The best practices should be adopted by the ministry of defense for the utilization of economic radio or internal devices. It is easier in wireless networks eavesdropping, the injection of messages harmful to the network, and sending a message previously registered, denial of service (DoS) as jamming. Additionally, entire vulnerabilities during a wireless network also exist for the wireless network.

Almost the wired and wireless links experience the similar vulnerabilities of attacking events. The basics or the fundamental principles could be different cause the nature of the threats detection [22]. Attacks on the wired network are often established in remote areas of the wire, while the attack point of the wireless network could be detect within the range of the attackers wireless devices. Usually, the safety features of the wireless network are weaker. The reason is that the wireless networks usually ready to provide less resources and connected devices with less complexity. Since, the RF signals are broadcasted, each packet that reaches the receiver is an unknown source and must be validated. It has been validated at the beginning of the session; the intruder still is probably going to hive the session. An intruder guards to the wireless link and bypass firewall, therefore it gains unauthorized access to protected information assets.

E. Security Control for Wireless Networks

Security concerns are required different treatments, health and safety, access control, confidentiality, and protection, such as to make sure proper transmission of data. Firstly, the information send via wireless connections that must be encrypted and keep confidential, because the information sent weak or non-encrypted is subject to interference by the hacker and therefore the origin of messages received via wireless connections must be validated. The integrity and validity of incoming messages must be verified. The current state-of-the-art practices within the security of wireless networks depend upon suppliers to provide strong security protocols for wireless devices to guard them against possible attacks, within the case of a security breach to detect and stop the attack. It's incumbent upon individual organizations to adopt security measures and practices in accordance with their security needs. The Law of data Security Management federal (LSMF) to all or any federal agencies (United States of America Civil government departments and agencies/agency contractors) develop and implement agency-wide information security programs to guard information technology assets and data. It offers an up-to-date federal information since 1999s [23] common methodology for assessing risks that threaten the confidentiality of unpatched systems integrity and availability. As, NIST SP 800-53 sets the inspiration of technical management and operational controls that has got to be included within the system to a minimum and make sure the security of low, medium, high-risk systems [24]. Before deploying a wireless network, the organization should assess its security needs and therefore the potential consequences of a security violation. In conducting the evaluation, the organization should consider existing security policies, known threats and vulnerabilities, legislation and regulations, safety, reliability, system performance, and security-related life cycle costs and technical requirements.

V. Conclusion

Internet is the most widely used wired and wireless device connectivity service provider. Nowadays, internet-connected devices make easy communication and observatory facilities in almost every critical field. The remote operation of nuclear power plants is more challenging which could be simplified by the implementation of IoTs. These internet-connected de-vices support the real-time monitoring, observation of smooth functioning of NPP systems and play the most significant role in nuclear safety. In this proposed work we over-viewed the integration of IoTs in highly radiated and critical systems. The NPP threats and cyber-security are also majorly studied in this study towards the next generation of wireless networking systems. The main perspectives are of this investigated work for smart and futuristic nuclear power plant operations through wireless connections and internet-connected devices.

REFERENCES

[1] K. Nagatani, S. Kiribayashi, Y. Okada, K. Otake, K. Yoshida, S. Tadokoro, T. Nishimura, T. Yoshida, E. Koyanagi, M. Fukushima et al., "Emergency response to the nuclear accident at the fukushima daiichi nuclear power plants using mobile rescue robots," Journal of Field Robotics, vol. 30, no. 1, pp. 44–63, 2013.

[2] C. Cousins, D. Miller, G. Bernardi, M. Rehani, P. Schofield, E. Vañó, A. Einstein, B. Geiger, P. Heintz, R. Padovani et al., "International commission on radiological protection," ICRP publication, vol. 120, pp. 1–125, 2011.

[3] J. DePasse, A. Caldwell, D. Santorino, E. Bailey, S. Gudapakkam, D. Bangsberg, and K. Olson, "Affordable medical technologies: bringing value-based design into global health," BMJ Innovations, pp. bmjinnov– 2015, 2016.

[4] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart mobile-internet of things (m-iot): A survey," IEEE Access, vol. 8, pp. 167 123–167 163, 2020.

[5] B. Chanda, P. K. Mallick, and G.-S. Chae, "An analytical study of the role of m-iot in healthcare domain," in Hybrid Artificial Intelligence and IoT in Healthcare. Springer, 2021, pp. 75–96.

[6] P. Ross and K. Maynard, "Towards a 4th industrial revolution," pp. 159– 161, 2021.

[7] I. Parfis. (2017) Digitalization and Energy. [Online]. Available: https://www.iea.org/reports/digitalisation-and-energy

[8] J. W. C. L. K. C. N. D. Michael Rnecheck, Bob Bement and F. Salman, "New Plants & Vendor Advetorial," Nuclear Plant Journal, Tech. Rep., 2017.

[9] I. Parfis, "Digital Solutions for Power Utilities," 2017. [Online]. Available: www.ge.com/digital/power-utility

[10] R. Lin, Z. Wang, and Y. Sun, "Wireless sensor networks solutions for real time monitoring of nuclear power plant," in Fifth World Congress on Intelligent Control and Automation (IEEE Cat. No. 04EX788), vol. 4. IEEE, 2004, pp. 3663–3667.

[11] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," Future generation computer systems, vol. 56, pp. 684–700, 2016.

[12] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in 2010 seventh international conference on information technology: new generations. Ieee, 2010, pp. 804–809.

[13] K. Evangelos A, T. Nikolaos D, and B. Anthony C, "Integrating rfids and smart objects into a unifiedinternet of things architecture," Advances in Internet of Things, vol. 2011, 2011.

[14] C. Roy, S. Misra, and S. Pal, "Blockchain-enabled safety-as-a-service for industrial iot applications," IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 19–23, 2020.

[15] D. R. Farley, M. G. Negus, and R. N. Slaybaugh, "Industrial internet-of-things & data analytics for nuclear power & safeguards." Sandia National Lab.(SNL-CA), Livermore, CA (United States), Tech. Rep., 2018.

[16] B. Mood, D. Gupta, H. Carter, K. Butler, and P. Traynor, "Frigate: A validated, extensible, and efficient compiler and interpreter for secure computation," in 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016, pp. 112–127.

[17] M. Moh and R. Raju, "Machine learning techniques for security of internet of things (iot) and fog computing systems," in 2018 International Conference on High Performance Computing & Simulation (HPCS). IEEE, 2018, pp. 709–715.

[18] I. I. for Business Value, "Device democracy: Saving the future of the Internet of Things," 2015.

[19] I. A. Tatourian, A. Nayshtut, O. Pogorelik, and S. Hunt, "Cognitive protection of critical industrial solutions using iot sensor fusion," Nov. 14 2017, uS Patent 9,817,676.

[20] X. Bellekens, A. Seeam, K. Nieradzinska, C. Tachtatzis, A. Cleary, R. Atkinson, and I. Andonovic, "Cyber-physical-security model for safety-critical iot infrastructures," in Wireless world research forum meeting, vol. 35, 2015, p. 18.

[21] J. Chen, T. Wang, Y. Du, and S. Zhai, "Research for emergency communication system design in nuclear power plant based on safety requirements," in 2019 IEEE 11th International Conference on Commu-nication Software and Networks (ICCSN). IEEE, 2019, pp. 722–725.

[22] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," in 2018 International Conference on Artificial Intelligence and Data Processing (IDAP). IEEE, 2018, pp. 1–5.

[23] F. Pub, "Standards for security categorization of federal information and information systems," NIST FIPS, vol. 199, 2004.

[24] M. A. Haque, S. Shetty, K. Gold, and B. Krishnappa, "Realizing cyber-physical systems resilience frameworks and security practices," in Security in cyber-physical systems. Springer, 2021, pp. 1–37.

AMANAT ALI is working as a Research Assistant (RA) and pursuing masters in Nanotechnology from National University of Science and Technology MISIS, Russia. He received bachelor of technology (B.Tech) in Mechanical engineering from University of Petroleum and Energy Studies, India in 2020. His research interests are Nanotechnology, Wireless Communication and Internet of Things (IoTs).

Yasin Goudarzi is pursuing Ph.D in nuclear engineering at Tomsk Polytechnic University in Russia. He received a bachelor's degree in atomic physics and a master's degree in nuclear physics from Shiraz University in Iran. His current field of research is the application of thorium fuel cycles in 4th generation reactors. He is interested in fuel cycle optimization, safety analysis of nuclear reactors, fuel behavior modelling, inertial confinement fusion and new technologies in modern reactors.

BASSMA ABOUABDELLAH is pursuing master in Electrical Engineering from National School of Applied Science Agadir, Morocco. She has completed bachelor in Electrical Engineering as well. Her research interest in wireless communication, Internet of Things (IoTs) and Power Engineering.

Tarek Elzayat is pursuing Ph.D. in Nuclear Engineering at the school of nuclear science & engineering at National Research Tomsk Polytechnic University, Russia. He received M.Sc. degree in nuclear and thermal energy from department of theoretical and experimental physics of nuclear reactors, National Nuclear Research University, Russia. His research work primarily includes modeling and simulation (M&S) of nuclear fuel cycle and advanced nuclear reactors design through Monte Carlo neutronic codes.

MOHAMMAD FURQAN ALI is working as a research engineer and pursuing Ph.D. in Computer Science and Wireless Communication Engineering from the School of Computer Science and Robotics, National Research Tomsk Polytechnic University, Russia. He received M.Sc. degree (Distinction & Gold medalist) from "National Research Tomsk Polytechnic University Russia" in 2018, and B.Tech (Bachelor of Technology) degree in 2013 from "UP Technical University Lucknow, India. His research interests include Optical communication, Underwater Visible light communication (UVLC), 5G wireless networking, Internet of Things (IoTs) and Hybrid-cooperative underwater wireless communication.

Dr. Gaurav Saini is presently working as the Post-Doctoral Fellow in the Department of Sustainable Energy Engineering, Indian Institute of Technology, Kanpur. He had served as the assistant professor in the School of Advanced Materials, Green Energy and Sensor Systems, Indian Institute of Engineering Science and Technology (IIEST) Shibpur India. He received his Ph.D in Renewable Energy (Hydrokinetic Turbines) in the year 2020 and M.Tech. (Fluid Machinery and Energy System) in the year 2014 from Indian Institute of Technology Roorkee, Uttarakhand India. Prior to joining IIEST Shibpur, he was working as Project Fellow in the Department of Hydro and Renewable Energy, Indian Institute of Technology Roorkee. His research areas include Renewable Energy (Hydrokinetic Energy, Wind Power, and Biomass), Computational Fluid Dynamics (CFD) and Fluid Mechanics & Fluid Power. He has published several research publications on renewable energy technologies in different international journals of repute. He has also presented his research at different international and national platforms and he received accolades from various peers working in the same area across the globe. Dr. Gaurav is skilled in Computational Fluid Dynamics (CFD) - numerical modelling and roto-dynamics analysis, Multiphase flow analysis, Modeling of various renewable energy resources viz. wind, marine, solar and hydrokinetic energy for rural applications, wind and hydrokinetic-Technology selection and design, Installation strategies, Performance evaluation and O&M issues.