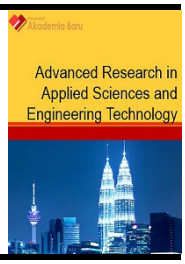
Penerbit Akademia Baru

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage: www.akademiabaru.com/araset.html
ISSN: 2462-1943



Review of cyber security applications in nuclear power plants

Open Access

Muhammad Adil Khattak [1,*], Muhammad Khairy Harmaini Shaharuddin [1], Muhammad Saiful Islam Haris [1], Muhammad Zuhaili Mohammad Aminuddin [1], Nik Mohamad Amirul Nik Azhar [1], Nik Muhammad Hakimi Nik Ahmad [1]

[1] Department of Nuclear Engineering, Faculty of Chemical & Energy Engineering, Universiti Teknologi Malaysia, 81310 Skudai Johor, Malaysia

ARTICLE INFO

Article history:
Received 15 April 2017
Received in revised form 9 May 2017
Accepted 23 May 2017
Available online 27 May 2017

Keywords:
Nuclear power plant cyber security, software security, secure system, cyber security hazard

ABSTRACT

It is essential to ensure the nuclear power plant system are not compromise and avoid failure that can result in significant economic loss and physical damage to the public. However, a very little attention was given to software and cybersecurity hazard. This review paper discusses about the cybersecurity in nuclear power plant, history of accident, implementation and future plan on cybersecurity deeply. About 51 published studies (2006-2017) are reviewed in this paper. It is marked from the literature survey articles that it is important for the cybersecurity of a nuclear power plant to be at par with the evolution of hardware and software and to counter the increasing risk on cyber vulnerabilities. Moreover, it should be addressed as a concern and major priority for researches and policy-makers.

1. Introduction

The uses of energy play important role in human daily life [1]. Nuclear energy plays a vital role as it become one of the most important energy supply in the world [2]. The first commercial nuclear power station has started an operation in 1950. There are over 440 of commercial nuclear reactor for producing electricity operable in 31 countries with capacity over 390,000 Mwe. Nowadays, they provide about 11% of the world electricity as continuous, a reliable source of energy without carbon dioxide emission [3]. Hence, because of its importance in supplying energy, when nuclear reactor would be built and design, three key factors in building and designing in nuclear reactor are which is 3S's safety, safeguard and security.

As noted by Endo [4], the expanding number of nuclear reactors on the planet these days can build the issue and dangers in wording safety, security, and safeguards, and these three perspectives must be considered while presenting nuclear power era. People in general individual conclusion

* *Corresponding author.*
E-mail address: muhdadil@utm.my (Muhammad Adil Khattak)

needs to feel protected and secure in regards to with nuclear issue by the aftereffects of the 2010 Eurobarometer on Nuclear safety. This negative view and observation unmistakably was influenced by the expansion and security specific in radioactive waste safe transfer. Among these three perspectives, safety is the principal viewpoint to be considered, trailed by safeguards, and finally is security angle [4]. This is alluded by IAEA with the nuclear 3S's idea [20-21]; assist these same ideas have been over and again expressed amid late G8 [22] and Nuclear Security Summits [24-26].

As characterized by IAEA in 2014, the primary rule of safety control is to shield the populace and nature from radiation and different dangers brought about by the operation of nuclear power plants and other nuclear offices at all phases of life cycle, and additionally stockpiling, transportation and radioactive materials use including spent nuclear fuel and radioactive waste. Nuclear security from CNND discernment implies that measures intended to address the dangers related with robbery and trafficking in nuclear and radio legitimate materials, harm of nuclear offices, and the peril of fear mongers getting and utilizing it for a nuclear weapon. As expressed by IAEA [4], nuclear safeguards by configuration is characterized as an approach whereby universal safeguards necessities and targets are completely coordinated into the outline procedure of a nuclear office, from introductory arranging through plan, development, operation, and decommissioning.

"Nuclear security" infers measures expected to address the risks related with robbery and trafficking in nuclear and radio consistent materials (meaning the benefit of would-be multiply), mischief of nuclear offices, and the hazard of dread based oppressors acquiring and using a nuclear weapon. Notwithstanding late advances overall nuclear security is lacking. Since an important nuclear security event would have clearing comes about, feasible nuclear security must be an overall concern. However, for the most part countries see nuclear security as fundamentally a national concern, committing lacking thought to the change, headway and utilization of widespread measures [4]. As attempts in the nuclear ventures, Nai Fovino I [45] presented the aftereffect of information and communication technology (ICT) security assessment concentrating on an operational power plant. The results exhibit that the weakness of a plant to noxious assault is extraordinary. Lee [46] exhibited a practice for an advanced security chance examination in power plants as required by RG. 1.152-2006.The appraisal comprises of an objective framework investigation, resource examination, danger examination, defencelessness examination, chance investigation, and interruption tests to recognize the dangers.

The nuclear security organization involves abstentions, bearings, resolutions and principles that either existed or were close being done before 2010. Help progress has been made in national execution since pioneers' level Nuclear Security Summits (NSS) begun in 2010. National endorsements of settlements and a couple endeavours were revived so they could be accounted for at the summits. Regardless, nuclear security still falls well behind the other nuclear organizations for security, guards and arms control. The present organization is reliant totally on national protection and control systems in those countries that have nuclear and radio consistent materials. It ought to be more entire as opposed to incremental, covering all materials and all workplaces by any extend of the creative energy times; fused rather than different and piecemeal; and upheld by overall instruments with a particular true objective to make the organization both solid and flexible. It similarly needs fruitful watching necessities, and pro, techniques and establishments for approving agreed obligations: without these, duty is missing and states can't have assurance in the all-inclusive nuclear security structure.

From this, the paper is more concern about cyber security. Nowadays, the modern and more technology world are become more openly and vulnerable for this type of attack. The therefore there are some guideline that been point by Nuclear Regulatory Commission (NRC) for safety of cyber-attack [31]. NRC developed it in 2009 a comprehensive cyber security regulations.

- Establish a devoted cyber security appraisal group under its cyber security arrange.
- Identify basic frameworks and basic computerized resources that fell inside the extent of the NRC necessities.
- Isolate key control frameworks utilizing either air-crevices or hearty equipment based disconnection gadgets.
- Implement vigorous controls of versatile media and gear, (for example, thumb drives, CDs, and tablets), including limiting the utilization of gadgets that are not kept up at the plant, checking gadgets for infections both prior and then afterward being associated with plant hardware, and actualizing extra security measures when the wellspring of the information or gadget begins outside the plant.
- Enhance resistances against insider dangers by executing preparing and insider moderation programs that incorporate cyber traits, expanding security screening of people who work with advanced plant gear, and expanding cyber security preparing and behavioral perception.

In January 2010, the NRC published Regulatory Guide, RG 5.71 [29]. It provided guidance to licensees and license applicants on an acceptable way to meet the cyber security requirements. Also, a nuclear energy facilities are intended to close down securely if essential, regardless of the possibility that there is a rupture of cyber security. A cyber-attack has a low likelihood of influencing basic frameworks in a nuclear energy facilities or their wellbeing capacities. Among different measures, these basic frameworks are not associated with the Internet or to an office's interior system. The confinement of basic security frameworks limits the pathways for a cyber-attack. Nuclear energy facilities likewise are intended to consequently disengage from the power lattice if there is an unsettling influence that could be brought about by a cyber-attack.

2. Accident Happened in NPPs Due to Cyber Security

The accident occurred at Hatch nuclear power plant near Baxley, Georgia. The burden happened after an originator from Southern Company, whom manages the advancement operations for the plant, introduced a product refresh on a PC working on the plant's business organize. The PC being alluded to was used to screen compound and indicative information from one of the office's essential control frameworks, and the product refresh was intended to synchronize information on both frameworks. As demonstrated by a report recorded with the Nuclear Regulatory Commission, when the revived PC rebooted, it reset the data on the control structure, making security systems errantly decode the nonattendance of data as a drop in water supplies that cool the plant's radioactive nuclear fuel poles. Accordingly, modernized prosperity systems at the plant set off a shutdown. PC security experts say the occurrence is the latest sign of issues that can happen when corporate PC frameworks at the country's most basic systems are associated with delicate control frameworks that were never composed in view of security which defenceless against digital assaults [10]. The digital fear based oppression for nuclear power plants (NPPs) is examined for the explanatory review taking after the South Korean case on December 2014 [39].

Different accidents occur in South Korea where obscure individual or gathering utilizing a record named "leader of the anti-nuclear reactor group", posted plans of nuclear reactors via web-based networking media. These programmers were putting outlines and manuals of plant gear possessed by Korea Hydro and Nuclear Power Co (KHNP) however fortunately the danger that was made with the spilled information did not undermine the wellbeing of the reactors [16,42].

Next accident because of cyber is the Stuxnet virus. Stuxnet, known as clearly annihilating a fifth of Iran's atomic centrifuges by making it turn insane. The worm which pass on into Natanz through

an authority's pen drive moreover expanded the weight on turning centrifuges while showing the control room that everything appeared to be common by replaying recordings of the plant's assurance framework values amid the assault. The arranged effect was not beating rotators, yet rather diminishing lifetime of Iran's tomahawks and making the Iranians' support control systems appear outside their capacity to appreciate [8]. The long range interpersonal communication is utilized for the nuclear fear episode displaying and its counteractive action systems [40].

Before the Stuxnet virus accident, accident had occurred at David-Besse nuclear power plant because of viruses of the Slammer worm [41]. On January 25, the Slammer worm began mishandling powerlessness in Microsoft SQL Assistant. Inside ten minutes, it had debased seventy thousand servers around the globe. The layout of Slammer was essential; it didn't stay in contact with itself to the hard drive, delete records, or gain system control for its maker. Or maybe, it settled in structure memory and checked for various hosts to sully. Removing the worm was as clear as rebooting the server in the wake of closing framework port 1434, Slammer's purpose of entry. Introducing a fix Microsoft had discharged six months before would take out the weakness Slammer abused and keep another disease [9,33-36]. The majority of the materials were utilized without further decontamination.

3. Cyber security requirements

By the time of 2010 and 2011 U.S. NUCLEAR REGULATORY [29] have been issued some of rule for nuclear cyber security. In 2010 the issued was "Cyber security program for nuclear facilities" RG. 5.71-2010, which is depict in term of the specialized technique and security exercises for the operation and support of a nuclear power plant (Table 1). The developer guidelines or procedures contain a self-checklist for software design principles, such as accuracy, clarity, loose coupling, and strong cohesion are imperative amid establishment [47].

Table 1
Summary of RG.1.152-2011

Sections	Descriptions
Concept	*Establish a secure operational environment *Identify potential security vulnerabilities *Remote access should not be implemented
Requirements	*Define security functional requirements *V&V role *Pre-development software should be addressed *Secure development process
Design	*Spesific design configuration items *Developer should take the standards and procedures
Implementation	*Implement security procedures and standards *Testing to address undocumented codes
Test	*Verify security functions *A test should cover overall system

In 2011, USNRC issued the RG. 1.152-2011, "Criteria for use of computers in safety systems of nuclear power plants," which utilizes the waterfall life-cycle stages as a structure to depict the framework security direction. The system comprises of five stages: the concept, requirement, design, implementation, and test phases.

To accomplish conformance with both sorts of direction, it is important to mix the security necessities of RG. 1.152-2011 and RG. 5.71-2010 into each phase of the framework life cycle. We coordinated the five areas of RG. 1.152-2011 and the principle exercises of RG. 5.71 into three phases: planning stage, development stage, and operation and maintenance phase. Before going any further, we will clarify quickly the RG. 5.71-2010 and RG. 1.152-2011 perspectives for programming security underneath (Table 2):

- High potential dangers from information technology (IT): There is no difference that data technologist fundamental on the planet today, and psychological warfare constitutes a noteworthy risk to the IT business. By and by, nuclear security frameworks depend on IT, for example, Commercial Off The-Shelf (COTS) items and Ethernet systems as information correspondence and process control. In reality, the nuclear business likewise confronts a danger of psychological warfare.

- Seamlessly tending to the security contemplation of advanced well being frameworks: A blend of RG. 1.152-2011 and RG. 5.71-2010 can flawlessly address the safe plan, improvement, and operation of advanced well being frameworks. The previous locations the security issues amid well being framework improvement, and the last gives automatic security direction to operation and upkeep.

- The fundamental issues of RG. 1.152-2011: The well being framework outline for a protected operational condition ought to address the physical and coherent access to the framework capacities, the utilization of security framework administrations, and information correspondence with different frameworks. Likewise, models and methods ought to be executed for a protected improvement condition.

- The primary components of RG. 5.71-2010: A resistance top to bottom methodology is an action to build up numerous layers of assurance to protect security frameworks containing critical digital assets (CDAs), as the disappointment of a solitary layer ought not bring about a trade off of CDAs. The utilization of security controls delegated specialized controls, operational controls, and administration controls is likewise a vital action that makes up shield or defensive measures tending to the potential cyber dangers of CDAs. Consistent checking of their viability is additionally a basic movement amid the plant operation arrange.

Table 2
Summary of RG.5.71-2010

Sections	Descriptions
Cyber security program establishment	*Cyber security team, training plan *Critical digital assets analysis *Defense-in-depth strategy *Implement security controls
Cyber security program maintaining	*Continuous monitoring *Periodic assessment and audit *Change control *Cyber security program review

In 2009, NRC built up its exhaustive cyber security controls. Each nuclear power plant administrator has gotten NRC endorsement for a cyber security arrange for that depicts how it is executing its cyber security program and a timetable portraying steps it has taken to completely actualize the program. NRC has checked on these calendars and frequently assesses nuclear power plant cyber security. NRC required each nuclear power plant to [14]:

- Establish a devoted cyber security appraisal group under its cyber security arrange.

- Identify basic frameworks and basic advanced resources that fell inside the extent of the NRC necessities.

- Isolate key control frameworks utilizing either air-holes or hearty equipment based disconnection gadgets.

- Implement vigorous controls of versatile media and gear, (for example, thumb drives, Cds, and portable PCs), including limiting the utilization of gadgets that are not kept up at the plant, checking gadgets for infections both prior and then afterward being associated with plant hardware, and actualizing extra security measures when the wellspring of the information or gadget begins outside the plant.

- Enhance resistances against insider dangers by actualizing preparing and insider relief programs that incorporate cyber properties, expanding security screening of people who work with computerized plant hardware, and expanding cyber security preparing and behavioral perception.

NRC's cyber security group incorporates innovation and danger appraisal specialists who group with other Government organizations and the nuclear business to assess and help settle issues that could influence advanced frameworks. This group makes suggestions to different workplaces inside the NRC and is likewise outlining a cyber security review program for future usage. All locales will be required to fulfill those review prerequisites.

4. NPPs' Cyber Security Implementation

As expressed in the past segment, USNRC had distributed two new rules with respect to digital security: USRNC (2006) and USNRC (2010). These two rules alongside 10 CFR are universally utilized as references for the outline and development of nuclear plant offices [32].

By referring to USRNC (2006), it depicts what the staff of the NRC considers commendable to follow the bearings for propelling high viable trustworthiness, diagram quality, and cyber security for the usage of automated PCs in the NPPs' security systems. It requires the system segments and change practices for cyber security to be executed and performed through the structure headway lifecycle [32]. While in USNRC (2010), it underscored that, "Cyber security programs for nuclear offices", which portrays the particular methods and security practices for the operation and support of a nuclear plant. Cyber security segments should be created and completed in the midst of the change organize before the site foundation of the systems, as any later treatment of the structures for security may achieve unpredicted defects in the structures or may be realized with less reasonable security measures. This suggests security controls stressed in RG. 5.71-2010 should in like manner be organized, arranged, and completed in the midst of the security structure headway organize. Regardless, it doesn't give specific lifecycle-based techniques [30].

The usage of cyber security at NPPs has been depicted in USNRC (2010), R.G 5.71, which expressed that the NRC staff considers worthy for the assurance of advanced PC and correspondence

frameworks and systems, as put forward in 10 CFR 73.54, 10 CFR 73.55, and 10 CFR 50.34. The NRC arranged a back fit investigation for the proposed directions at 10 CFR 73.55, from which the prerequisites of 10 CFR 73.54 have been determined. The NRC has verified that, as per 10 CFR 50.109(a)(3), a generous increment in the general insurance of the general wellbeing and security or the normal barrier and security will be gotten from the back fit related with 10 CFR 73.54, and the immediate and aberrant expenses of execution are advocated in perspective of this expanded assurance [29].

4.1 Relationship between Cyber Security Activities and V&V Activities

An exceptional current standard, IEEE, 2004, grasped by the nuclear regulatory body gives specific activities for software verification and validation (V&V) of mechanized security systems. The security examination determined in the standard has been interpreted as the possibility of physical security figuratively speaking. Considering late regulatory positions, it is palatable that the security examination should be driven for the cyber security of cutting edge systems. In this way, this survey breaks down the standard necessities into three important parts, software V&V, prosperity examination, and cyber security examination. The examination comes to fruition for each part through the headway stages are dispersed uninhibitedly [32]. In Fig. 1 demonstrates that the cyber security arranges inside the V&V plan of the framework.

All things considered, structure engineers use qualified commercial-off-the-shelf (COTS) things as the phase of security systems. Software V&V and a security examination simply focus on method of reasoning source codes that are as of late made inside the things. By virtue of a security examination, the security limit in the past does not ensure a similar feasibility at this moment due to reliably progressing cyber risks. Appropriately, this paper recommends that the gear and software of the COTS are consolidated as review things in the security examination [32].

4.2 A Cyber Security Plan

This section proposes a cyber security mastermind including a cyber security team (CST) affiliation and security practices execution. The cyber security assemble contains a gathering pioneer and associates. The real missions of the gathering are according to the accompanying [32]:

- supervision of the protected advancement condition,
- examination of the framework weakness and entrance test to the framework,
- presenting cyber security necessities,
- following and settling security issues,
- surveying security affect on the framework honesty, and
- exploring the aftereffects of improvement stages [43-44].

As a review done by J. Park *et al*. [32], they have built up a framework show for the advanced framework, surely understood as waterfall configuration display, which comprises of the idea, prerequisite, plan, execution, and test stages. Their review adds security exercises to the outline model to play out the security team missions. The arrangement and exercises for the model are as take after which be explained in detail in Figure 2:

- Attack Path Analysis,
- Penetration Test,
- Security Requirements V&V,
- Security Design V&V,
- Security Implementation V&V,

- Security Test V&V, and
- Final Security Evaluation.

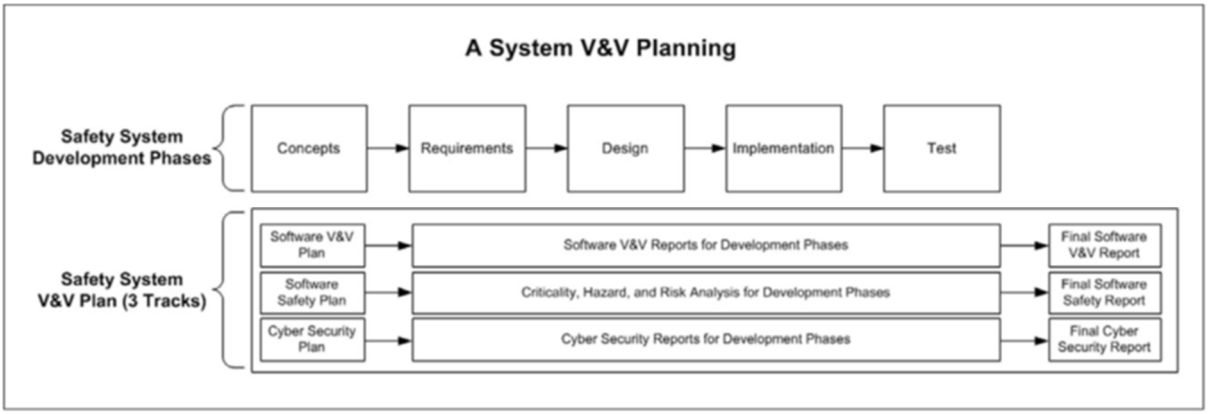


Fig.1. System V&V plan with cyber security implementation [32].

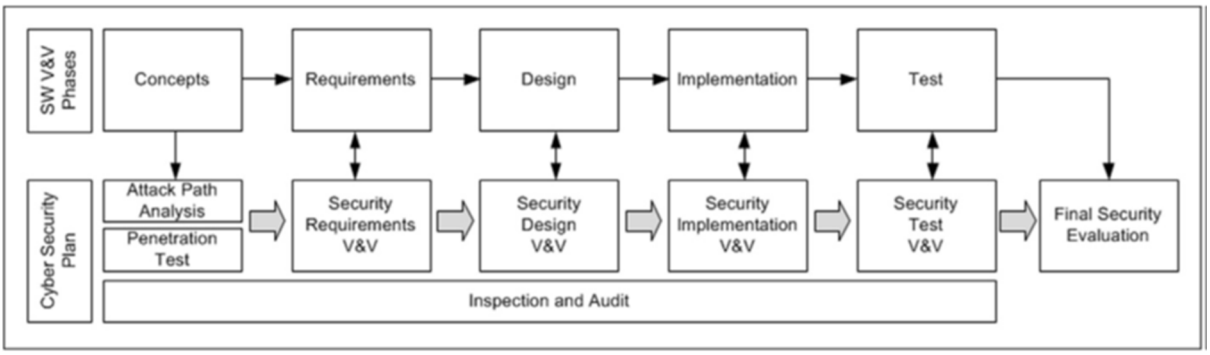


Fig. 2. Cyber security plan and activities [32].

5. Software in NPPs' Cyber Security

Nuclear power plants had been upgraded and improved from analogue-based manual system to implement a computer based control system and several software [12]. The control system in nuclear power plants perform a task that's included data acquisition and, control actuation and information indication based software. Existing operator actions, such as the monitoring of hardwired panels and the manual control of hand switches, have been swapped with computer-based visualization and automatic actuation. It also backings faster reactions in plant operation and cut the human resources and costs.

The product in SCADA frameworks is multi-tasking and utilizes on-going database(s) [37]. Chance, as per Byres et al. (2004), relies on framework architecture and conditions, countermeasures set up, difficulty of attack, discovery probability and assault cost [38]. Be that as it may, improvement in programming security had frequently been disregarded in nuclear safety software development [12]. Additionally, by utilizing PC based framework and software, nuclear power plants are vulnerable against digital assault and software dangers. For instance, an nuclear office in Iran encountered a cyber-assault, in particular, "Stuxnet", in 2010 [15]. In this manner, nuclear power plants are utilizing

and created numerous sorts of PC based framework and software to fortify the digital cyber and anticipate cyber mischance.

The operation in time of the fundamental hardware's in nuclear power plants takes years. Thus, a work in progress of framework for power engineering, nuclear power plants apply arrangements in the robotized procedure control system (APCS), which empower to work, repair, and update the introduced hardware without halting the technology procedure [7]. Additionally, this prerequisite, giving high dependability, survivorship, and wellbeing are the key necessities.

At current, V.A. Trapeznikov Institute of Control Sciences actualizes the advancement of the software of the upper level control system (ULCS) of the "Kudankulam" NPP APCS [5-6,11,13,17]. The ULCS is an arrangement of programmed examining, storing, showing data on a present status of mechanical and technological plants subject to control (TPSC) and mechanized remote framing charges of control of TPSC mechanism and system by utilization of the APCS calculations and algorithm.

The reason for making the ULCS is giving centralization of checking and control of the mechanical and technological procedure for:

- Economically productive assembling the electrical power.
- Observing the operation edges.
- Observing the edges and states of safe operation of the gear.
- Improving qualities of technological procedures and execution of the mechanical and technological gear.
- Decreasing the work yield apportion of the equipment execution, enhancing equipment repair capacity, diminishing the quantity of administration personnel, enhancing customer attributes of APCS components.
- Improving work force work conditions and diminishing the number and lessening the results of blunder activities of operators.

The ULCS is perplexing software and hardware framework, upheld by a computer helped outline. Furthermore, tuning system, and planned to join in a one of a kind framework all subsystems of the robotized procedure control system APCS [7].

6. Future Plan for Cyber Security

It is important for the cybersecurity of power plant (nuclear) to be updated evolution to software and hardware as stated as the Committee on Improving Cybersecurity Research report. Increasing risk on cyber vulnerabilities address a concern that should be the major priority for policy makers and researches [27,48].

One of future for this issue is to improve the nuclear administrative commission and amended the security necessity for any nuclear computer based framework. For instance, the regulatory commission, for example, USNRC in 2011 additionally issued another correction of RG 1.152 in which entitle "Criteria for utilization of PCs in wellbeing frameworks of nuclear power plants," which utilizes the life-cycle stages as structure to portray the framework security direction. This modification of control is guaranteed the security and wellbeing of atomic power plant are dependably be refresh. The five stages structure comprises of idea, prerequisite, outline design, execution, and test stages [28].

In addition, proposes a coordinated development process handle appropriate for the safe improvement requirements and system security necessities depicted by different regulatory bodies, for example, expressed in paper of 'A Development Framework for Software Security in Nuclear

Safety Systems: Integrating Secure Development and System Security Activities' [30] are also helping the future plan improvement for cybersecurity. Which the paper is expected to contribute comprehensive development process approach on both secure development regulations and the security regulations for nuclear safety software, emphasizes software design and engineering for meeting nuclear regulation requirements and give software developers and licensees to better understanding the regulation requirement.

Moreover, besides enhances the nuclear regulatory body, future plan cybersecurity also depends on the researchers' study [48-49]. Numerous ranges should be talk about and additionally enhance, for example, "pervasive computing" and innovation encapsulated in computer into interconnected ordinary things. For instance, in light of International Journal of Information Management (IJIM) there are six agenda that should be inspected in the fundamental body of the content [27]. The six classes are;

- Deterring would-be attackers
- Limiting & blocking compromise of the impact
- Accountability Enabling
- Speculative research
- Deployment promoting
- Illustrative cost –cutting

Inside the six categories, the major issues include that need to be address for the cybersecurity are stated below;

- Development and testing
- Secure design
- Biological approaches to security
- Usable security
- Cybersecurity metrics
- Anomaly and misuse detection systems
- Policy security
- Cyber retaliation
- Cybersecurity related to legal issues
- The economics of cybersecurity
- In security cyber defence
- Spam dealing

Digital security occurrences have happened at nuclear power plants, crossing as far as possible among imagination of data innovation and process control frameworks (PCF) and reactors, shutting down so far the potential for hurting an nuclear reactor appears to be hypothetical. Scott Lunsford, from IBM government says requested protections would shield a programmer from setting off an emergency of cyber security. Up to now, no damage has come to a digital assault against an nuclear office. The same can't be said for different fragments, as by virtue of the Stuxnet attack has demonstrated that states are likely pushing the headway of new procedures and capacities web [50-51].

7. Conclusion

In spite of the fact that the experience of the nuclear division waits behind that of non-nuclear offices in digital security and process control frameworks (PCF), power plants ought to in like manner

comply with more grounded more grounded regulation and reviews. Despite the way that he NRC's digital bearings are so far being made, its present controls have put a couple of occurrences on general society record that would have gone unreported by non-nuclear plants. Nuclear Regulation Commission (NRC) was to execute a similar kind of thorough investigation and announcing necessities for cyber security as for safety and physical security, as it might open the field up to more prominent public examination and goad the venture expected to better ensure importance of the frameworks.

References

[1] Jorgenson, Andrew K., Alina Alekseyko, and Vincentas Giedraitis. "Energy consumption, human well-being and economic development in central and eastern European nations: A cautionary tale of sustainability." *Energy Policy* 66 (2014): 419-427.

[2] Gralla, Fabienne, David J. Abson, Anders P. Møller, Daniel J. Lang, and Henrik von Wehrden. "Energy transitions and national development indicators: A global review of nuclear energy production." *Renewable and Sustainable Energy Reviews* (2016).

[3] www.world-nuclear.org. *Nuclear Power in The World Today*. (2017).

[4] Zakariya, Nasiru Imam, and M. T. E. Kahn. "Safety, security and safeguard." *Annals of Nuclear Energy* 75 (2015): 292-302.

[5] Byvaikov, M. E., E. F. Zharko, N. E. Mengazetdinov, Aleksei Grigor'evich Poletykin, Iveri Varlamovich Prangishvili, and Vitalii Georgievich Promyslov. "Experience from design and application of the top-level system of the process control system of nuclear power-plant." *Automation and Remote Control* 67, no. 5 (2006): 735-747.

[6] Cherdantseva, Yulia, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. "A review of cyber security risk assessment methods for SCADA systems." *computers & security* 56 (2016): 1-27.

[7] Jharko, Elena Ph. "Software Tools to Model and Investigate Technological and Economical Efficiency of Nuclear Power Plants: A Real Case Study." *IFAC-PapersOnLine* 48, no. 3 (2015): 1320-1325.

[8] Kelley, M. B. "*The Stuxnet attack on Iran's nuclear plant was 'far more dangerous' than previously thought. Business Insider*." (2013).

[9] Kesler, Brent. "The vulnerability of nuclear facilities to cyber attack." *Strategic Insights* 10, no. 1 (2011): 15-25.

[10] Krebs, Brian. "*Cyber incident blamed for nuclear power plant shutdown*." Washington Post, June 5 (2008): 2008.

[11] Miller, Bill, and Dale Rowe. "*A survey SCADA of and critical infrastructure incidents*." In Proceedings of the 1st Annual conference on Research in information technology, pp. 51-56. ACM, 2012.

[12] Moreira, Naiara, Elias Molina, Jesús Lázaro, Eduardo Jacob, and Armando Astarloa. "Cyber-security in substation automation systems." *Renewable and Sustainable Energy Reviews* 54 (2016): 1552-1562.

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

[14] Park, Jaekwan, and Yongsuk Suh. "A development framework for software security in nuclear safety systems: integrating secure development and system security activities." *Nuclear Engineering and Technology* 46, no. 1 (2014): 47-54.

[15] Shin, Jinsoo, Hanseong Son, and Gyunyoung Heo. "Development of a cyber security risk model using Bayesian networks." *Reliability Engineering & System Safety* 134 (2015): 208-217.

[16] Ward, M. *S Korea nuclear firm to hold cyber-attack drills after hack*. (2014).

[17] Zharko, E. F. "Flexible modeling complex for the operator support systems of UPP's with VVER-1000 reactor." *Automation and Remote Control* 67, no. 5 (2006): 748-758.

[18] Collins S, McCombie S. Stuxnet: *the emergence of a new cyber weapon and its implications*. J.Polic Intell Count Terror 2012;7:80–91. http://dx.doi.org/10.1080/18335330.2012.653198.

[19] Poletykin, A.G., Jharko, E.Ph., Zuenkova, I.N., Promyslov, V.G., Byvaikov, M.E., and N.E. Mengazetdinov "Software for nuclear power engineering", *Automation in industry*, (2006). no. 8, pp. 52-56. (in Russian)

[20] International Atomic Energy Agency, International Atomic Energy Agency, *Milestones in the Development of a National Infrastructure for Nuclear Power*,(2007) Ng-G-3.1

[21] Suzuki, M., Y. Izumi, T. Kimoto, Y. Naoi, T. Inoue, and B. Hoffheins. "*Investigating 3S synergies to support infrastructure development and risk-informed methodologies for 3S by design*." In Proceedings of the IAEA Safeguards Symposium. IAEA-CN-184/64, 2010.

[22] International Initiative, *International Initiative on 3s-Based Nuclear Energy Infrastructure*, G8 Summit Hokkaido Toyako.

[23] Camp David Declaration, *Camp David Declaration*, G8 Summit 2012

[24] Communiqué Of The Washington, *Communiqué of the Washington Nuclear Security Summit*, 2010

[25] Communiqué Of The Seoul, *Communiqué Of The Seoul Nuclear Security Summit*, 2012
[26] Hague Nuclear Security, *The Hague Nuclear Security Summit Communiqué*, 2014.
[27] National Research Council. *Toward a safer and more secure cyberspace*. National Academies Press, 2007.
[28] USNRC. Regulatory Guide 1.152 Revision 3, "*Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*", 2011
[29] USNRC. Regulatory Guide 5.71, "*Cyber Security Programs for Nuclear Facilities*", 2010
[30] Park, Jaekwan, and Yongsuk Suh. "A development framework for software security in nuclear safety systems: integrating secure development and system security activities." *Nuclear Engineering and Technology* 46, no. 1 (2014): 47-54.
[31] Homeland Security, "*Nuclear Reactors,Materials, and Waste Sector-Specifc Plan An Annex to the NIPP 20*13" , 2015
[32] Park, JaeKwan, YongSuk Suh, and Cheol Park. "Implementation of cyber security for safety systems of nuclear facilities." *Progress in Nuclear Energy* 88 (2016): 88-94.
[33] Stephen D. Dingbaum. "*NRC's Planned Cyber security Program (OIG-08-A-06)". Memorandum Report from the Office of the Inspector General* (March 18, 2008).
[34] Nuclear Regulatory Commission, "*Information Security Strategic Plan*". May 18, 2009.
[35] International Atomic Energy Agency. "Security of Information and Instrumentation & Control Systems at Nuclear Facilities", *IAEA Nuclear Security Series No. XX Technical Guidance*. 2007, page 13.
[36] Albright, David, Paul Brannan, and Christina Walrond. "Stuxnet malware and natanz: Update of isis december 22, 2010 report." *Institute for Science and International Security* 15 (2011): 739883-3.
[37] Daneels A, Salter W. What is SCADA? *International conference on accelerator and large experimental physics control systems*, Trieste, Italy, 1999.
[38] Byres, Eric J., Matthew Franz, and Darrin Miller. "*The use of attack trees in assessing vulnerabilities in SCADA systems*." In Proceedings of the international infrastructure survivability workshop. 2004.
[39] Cho, Hyo Sung, and Tae Ho Woo. "Cyber security in nuclear industry–Analytic study from the terror incident in nuclear power plants (NPPs)." *Annals of Nuclear Energy* 99 (2017): 47-53.
[40] Woo, Tae Ho, and Sang Man Kwak. "Social networking-based simulations for nuclear security: Strategy assessment following nuclear cyber terror on South Korean nuclear power plants (NPPs)." *Annals of Nuclear Energy* 81 (2015): 91-97.
[41] Kim, Do-Yeon. "Cyber security issues imposed on nuclear power plants." *Annals of Nuclear Energy* 65 (2014): 141-143.
[42] Sklyar, Vladimir. "Cyber Security of Safety-Critical Infrastructures: a Case Study for Nuclear Facilities." *Information & Security* 28, no. 1 (2012): 98.
[43] Song, Jae-Gu, Jung-Woon Lee, Cheol-Kwon Lee, Kee-Choon Kwon, and Dong-Young Lee. "A cyber security risk assessment for the design of I&C systems in nuclear power plants." *Nuclear Engineering and Technology* 44, no. 8 (2012): 919-928.
[44] Jamieson, Rodger, and Meliha Handzic. "*A framework for security, control and assurance of knowledge management systems*." In Handbook on Knowledge Management 1, pp. 477-505. Springer Berlin Heidelberg, 2004.
[45] Fovino, Igor Nai, Luca Guidi, Marcelo Masera, and Alberto Stefanini. "Cyber security assessment of a power plant." *Electric Power Systems Research* 81, no. 2 (2011): 518-526.
[46] Lee, Cheol-Kwon, G. Y. Park, K. C. Kwon, D. H. Hahn, and S. H. Cho. "Cyber security design requirements based on a risk assessment." *Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies* (2009): 1638-1646.
[47] Mark D, John MD, Justin S., "*The art of software security assessment*", Addison-Wesley (2007).
[48] Beckmerhagen, I. A., H. P. Berg, S. V. Karapetrovic, and W. O. Willborn. "Integration of management systems: focus on safety in the nuclear industry." *International Journal of Quality & Reliability Management* 20, no. 2 (2003): 210-228.
[49] David, Paul A., and Julie Ann Bunn. "The economics of gateway technologies and network evolution: Lessons from electricity supply history." *Information economics and policy* 3, no. 2 (1988): 165-202.
[50] Farrell, Joseph, and Garth Saloner. "Standardization, compatibility, and innovation." *The RAND Journal of Economics* (1985): 70-83.
[51] Lee, Cheol-Kwon, G. Y. Park, K. C. Kwon, D. H. Hahn, and S. H. Cho. "Cyber security design requirements based on a risk assessment." *Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies* (2009): 1638-1646.