Security Application in the Context of Critical Infrastructure Protection and Resilience

FRANCIS MUSA ASHIMI

Master's Thesis
2020

Tomas Bata University in Zlín
Faculty of Applied Informatics

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Francis Ashimi Musa**
Osobní číslo:	**A16854**
Studijní program:	**N3902 Engineering Informatics**
Studijní obor:	**Security Technologies, Systems and Management**
Forma studia:	**Prezenční**
Téma práce:	**Bezpečnostní aplikace v kontextu vybraného odvětví kritické infrastruktury v Nigérii**
Téma práce anglicky:	**Security Applications in the Context of Selected Critical Infrastructure Sectors in Nigeria**

Zásady pro vypracování

1. Elaborate a literature review on critical infrastructure.
2. Discuss the general principles of critical infrastructure protection.
3. Do the evaluation of various types of security application used in selected critical infrastructure sector.
4. Analyze the current state of selected critical infrastructure sector protection in Nigeria.
5. Design and propose suitable security applications for selected critical infrastructure sector protection in Nigeria.

Rozsah diplomové práce:
Rozsah příloh:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. European Commission. (2019). Evaluation of Council Directive 2008/114 on Identification and Designation of European Critical Infrastructures and the Assessment of the need to improve their protection (SWD/2019/310).
2. Bologna, S., Bertocchi, G., Carducci, G., Carrozzi, L., Cavallini, S., Lazari, A., Oliva, G., Traballesi, A. (2016). Guidelines for Critical Infrastructure Resilience Evaluation. Roma: Italian Association of Critical Infrastructures? Experts.
3. Brown, T. (2008). Infrastructure Dependency Indicators. In J.G. Voeller (Ed.), Wiley Handbook of Science and Technology for Homeland Security. Hoboken, NJ: John Wiley & Sons. DOI: 10.1002/9780470087923.hhs248.
4. DHS. (2013). The National Infrastructure Protection Plan 2013: Partneringfor Critical Infrastructure Security and Resilience. Washington, DC: The Department of Homeland Security.
5. Fekete, A. (2011). Common Criteria for the Assessment of Critical Infrastructures. International Journal of Disaster Risk Science, 2(1): 15-24. DOI: 10.1007/s13753-011-0002-y.
6. Řehák, D., Hromada, M. (2018). Failures in a Critical Infrastructure System. In T. Nakamura (Ed.), System of System Failures. London: IntechOpen, pp. 75-93. DOI: 10.5772/intechopen.70446.

Vedoucí diplomové práce: **doc. Ing. Martin Hromada, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

I hereby declare that:

- I understand that by submitting my Diploma thesis, I agree to the publication of my work according to Law No. 111/1998, Coll., On universities and on changes and amendments to other acts (e.g. the Universities Act), as amended by subsequent legislation, without regard to the results of the defence defense of the thesis.
- I understand that my Diploma Thesis will be stored electronically in the university information system and be made available for on-site inspection, and that a copy of the Diploma/Thesis will be stored in the Reference Library of the Faculty of Applied Informatics, Tomas Bata University in Zlin, and that a copy shall be deposited with my Supervisor.
- I am aware of the fact that my Diploma Thesis is fully covered by Act No. 121/2000 Coll. On Copyright, and Rights Related to Copyright, as amended by some other laws (e.g. the Copyright Act), as amended by subsequent legislation; and especially, by §35, Para. 3.
- I understand that, according to §60, Para. 1 of the Copyright Act, TBU in Zlin has the right to conclude licensing agreements relating to the use of scholastic work within the full extent of §12, Para. 4, of the Copyright Act.
- I understand that, according to §60, Para. 2, and Para. 3, of the Copyright Act, I may use my work - Diploma Thesis, or grant a license for its use, only if permitted by the licensing agreement concluded between myself and Tomas Bata University in Zlin with a view to the fact that Tomas Bata University in Zlín must be compensated for any reasonable contribution to covering such expenses/costs as invested by them in the creation of the thesis (up until the full actual amount) shall also be a subject of this licensing agreement.
- I understand that, should the elaboration of the Diploma Thesis include the use of software provided by Tomas Bata University in Zlin or other such entities strictly for study and research purposes (i.e. only for non-commercial use), the results of my Diploma Thesis cannot be used for commercial purposes.
- I understand that, if the output of my Diploma Thesis is any software product(s), this/these shall equally be considered as part of the thesis, as well as any source codes, or files from which the project is composed. Not submitting any part of this/these component(s) may be a reason for the non-defence of my thesis.

I herewith declare that:

- I have worked on my thesis alone and duly cited any literature I have used. In the case of the publication of the results of my thesis, I shall be listed as co-author.
- That the submitted version of the thesis and its electronic version uploaded to IS/STAG are both identical.

In Zlin; dated: .....

Student´s Signature

ABSTRAKT

Czech abstract

Elektrická energie je klíčem k sociálně-ekonomické udržitelnosti a rozvoji všech aspektů společnosti, což z ní činí klíčovou kritickou infrastrukturu pro jakýkoli národ. Spolehlivá funkčnost zdroje generace je zásadní pro celkovou výrobu. Cílem studie je podívat se na rizika, zranitelnosti a hrozby spojené s elektřinou jako kritickou infrastrukturou. Diplomová práce představuje rizika spojená s elektrárnami na výrobu vodních elektráren s důrazem na osobní rizika a doporučení ke zmírnění těchto rizik pro kontinuální a efektivní výrobu elektrické energie.

Klíčová slova: Elektřina, pohonná jednotka, kritická infrastruktura, riziko, zranitelnost, personál, analýza

ABSTRACT

English abstract

Electric power is key to the socio-economic sustainability and development of every aspect of the society, making it a key critical infrastructure to any nation. The reliable functionality of the source of generation is vital to the overall production. The goal of the study is to look at the risk, vulnerabilities and threats associated with Electric power as a critical infrastructure. The Diploma thesis presents risks associated with Hydropower generating plants with emphasis on personnel risks and recommendations on mitigating these risks for continuous and efficient electric power generation.

Keywords: Electricity, Powerplant, Critical Infrastructure, Risk, Vulnerability, Personnel, Analysis

ACKNOWLEDGEMENTS

I use this opportunity to express my sincere gratitude to my Supervisor, **Assoc. Prof. Martin Hromada**, Ph.D., for his relentless support throughout my study and the course of the thesis. You are a mentor and am proud to have passed through your tutelage.

My sincere appreciation goes to **Assoc. Prof. Marek Kubalcik, Ph.D.** and **Assoc. Prof. Jiří Vojtěšek, Ph.D.** for all their support and guidance.

To my lecturers and other members of the UTB community, I remain eternally grateful for without you there won't be this thesis.

To the creator of the Universe, I come with thanksgiving for the opportunity to serve by learning and for all that he has brought my way thus far.

Content

INTRODUCTION

General Background

Since the development of civilizations, there has always been a need to protect structures or facilities the society felt essential for their existence. Like the Romans already protected their Critical Infrastructures (CI) such as aqueducts, food supply routes, military roads, and territories. Nations have always created means to protect their key infrastructure from foreign/enemy invasion e.g. European war, World War I, World War II and the cold war era.

Countries have realized the importance of prioritizing their assets for continuous socio-economics development, making CI identification, protection and resilience a key indicator for sustainable growth.

Problem Statement

The electric power which is identified as a key element of CI serves as the cornerstone for sustaining and development of any economy has been a problem in Nigeria due to various reasons. The electricity crisis in Nigeria has lingered for decades with a high negative index on economic development. There is an extreme electricity deficiency in Nigeria and the causes of this deficiency are related to financial, sociopolitical, and structural issues [4].

Objectives

The goal of this study is to apply security measures in reducing the personnel risks inherent in the generation unit of the power system to optimize production, enhance efficiency and service delivery.

Methodology

SWOT analysis which is a semi-quantitative method of risk analysis and assessment was used to determine the risks associated and resilience evaluation of security areas.

Limitations

Information/ data used was sourced on a qualitative level thereby limiting the scope of risk analysis and assessment in the generation unit.

I. THEORY

1 HISTORY DEVELOPMENT OF CRITICAL INFRASTRUCTURE PROTECTION

Since the development of civilizations, there has always been a need to protect structures or facilities we the society felt was essential for their existence. Like the Romans already protected their Critical Infrastructures (CI) such as aqueducts, food supply routes, military roads, and territories. Nations have always created means to protect their key infrastructure from foreign/enemy invasion e.g. European war, World War I, World War II, and the cold war era.

In the US, the European war brought about the first form of critical infrastructure protection by the Congress including language in the Army's appropriations legislation in August 1916 to establish a Council of National Defense (CND) and related Advisory Committee to streamline industrial mobilization in support of the defense. CND membership consisted of six secretaries: War, Navy, Interior, Agriculture, Commerce, and Labor. The Advisory Committee's seven members included a college president, a leading railroad engineer, the president of Sears, the president of the American Federation of Labor, the head of the American College of Surgeons and stockbroker Bernard Baruch. The Council was charged with the "coordination of industries and resources for the national security and welfare" and with the "creation of relations which render possible in time of need the immediate concentration and utilization of the resources of the Nation." But the pace at which the work frustrated white house and led to the formation of a fast-moving and more vigorous War Industries Board (under Bernard Baruch and peopled with more representatives from industry and the military).[1]

The Executive Order 13010, signed by President Bill Clinton on July 15, 1996, defined the term 'critical infrastructures' for the first time in official federal policy. The Executive Order states that critical infrastructures are systems that are "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States". Eight sectors of critical infrastructure were identified: telecommunications, electrical power, gas and oil, banking and finance, transportation, water supply, emergency services, and continuation of government. Since then, the definition of critical infrastructures has evolved due to the growth and complexity of technology, interdependencies, and interconnectivity to include additional sectors that support public health, assure continuity of government services and maintain public confidence (such as the security of national

monuments and special events). Then, the official list of critical infrastructure sectors had expanded to thirteen and included many subdivisions. The exercise in defining critical infrastructure is useful, but also limited. [1]

In the United States, the Oklahoma City bombing and Omnibus Counterterrorism Act of 1995, made the protection planning process a function of the government, other organizations, and agencies[2]. In May 1998, President William Jefferson Clinton solidified and defined the new emphasis and challenge, by issuing Presidential Decision Directive 63 (PDD-63), which recognized parts of the national infrastructure is critical to the national and economic security of the United States and required steps to taken to protect it.

The collapse of Twin-towers due to the September 11, 2001 attack, "9/11 events" caused the inoperability of many infrastructures (electricity, water, gas, communication, steam distribution, metro, operations of key financial institutions) in a broad area of Manhattan. An update on PDD-63 on 17 December 2003 by President George W. Bush through Homeland Security Presidential Directive 7 for critical infrastructure identification, prioritization, and protection, which described that some critical infrastructures are so vital that by incapacitating or destroying such systems and assets would have a debilitating impact on security, national economic security, national public health or safety. This critical infrastructure now included 16 sectors: chemical, communications, dams, emergency services, financial services, government facilities, information technology, transportation, commercial facilities, critical manufacturing, defense industries, energy, food/agriculture, healthcare/public health, nuclear reactors/waste, and water/wastewater. On 12 February 2013, the White House released Presidential Policy Directive 21 (PPD-21), which outlined and emphasized the federal role in critical infrastructure protection – especially the leadership of the U.S. Department of Homeland Security.

The European Council of June 2004 called on the European Commission to prepare an overall strategy to protect critical infrastructure (CI). The Commission adopted on 20 October 2004 a Communication on Critical Infrastructure Protection (CIP) in the Fight against Terrorism, which put forward suggestions on what would enhance European prevention, preparedness, and response to terrorist attacks involving Critical Infrastructures [2].

The Council came to a conclusion on "Prevention, Preparedness, and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks" which was adopted and endorsed in December 2004 with the intention of the

Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP) and also a Critical Infrastructure Warning Information Network (CIWIN). In November 2005, the Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP), which provided policy options on how the Commission could establish EPCIP and CIWIN. The 2005 December Justice and Home Affairs (JHA) Council Conclusions on Critical Infrastructure Protection called upon the Commission to propose a European Programme for Critical Infrastructure Protection. This Communication sets out the principles, processes, and instruments proposed to implement EPCIP. The implementation of EPCIP will be supplemented where relevant by sector-specific Communications setting out the Commission's approach concerning particular critical infrastructure sectors [EPCIP] namely; energy, transportation, and finance [3]. In 2013, the European Commission after evaluating the progress made by EPCIP decided to launch a new phase with a more practical approach of analyzing the European critical infrastructure that could be vulnerable to threats namely; The EU's electricity transmission grid, The EU's gas transmission network, EUROCONTROL, GALILEO – the European programme for global satellite navigation [3].

Other nations (China, Canada, and Australia) and member states of the European Union have since set up a framework for Critical Infrastructure Protection. Countries such as the United Kingdom, Sweden, the Netherlands, Germany, France, Italy, and Switzerland are already quite advanced in translating CIP and/or Critical Information Infrastructure Protection (CIIP) initiatives into real measures while others are striving to align their internal policy process with current and mature CIP policy [4].

South Africa is the only country in Africa that passed a bill in August 2018 towards the adoption of a legislative framework for critical infrastructure protection. In Nigeria, the Critical Infrastructure protection bill has been submitted since 2008 but yet to pass the final reading.

Critical Infrastructure has evolved to a multidimensional point of view due to the growing need for prioritization of individual sectors of the economy making it more manageable for countries to plan, strategize and manage resources. The advancement of technology and processes have made it more important for countries to adopt Critical Infrastructure protection with a common guideline to help in implementation, monitoring and future collaborative development.

2 LEGISLATIVE FRAMEWORK IN EUROPEAN UNION/ NIGERIA

In Europe, the European Programme for Critical Infrastructure Protection (EPCIP) is saddled with the responsibility of setting the overall framework for activities aimed at improving the protection of critical infrastructure in Europe - across all EU States and in all relevant sectors of economic activity [5]. Its' establishment came as a result of the 2006 Directive on European Critical Infrastructures.

The Directive establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection with an emphasis on the energy and transport sectors. The Directive also requires owners/operators of designated ECI to prepare Operator Security Plans (advanced business continuity plans) and nominate Security Liaison Officers (linking the owner/operator with the national authority responsible for critical infrastructure protection). [5]

The framework as contained in the 2006 communication on a European Programme for Critical Infrastructure Protection consist of the following:

2.1 A procedure for the identification and designation of European Critical Infrastructures (ECI)

A procedure for the identification and designation of European Crit-ical Infrastructures (ECI) and a common approach to the assess-ment of the needs to improve the protection of such infrastructures.

An EU level mechanism is required to serve as the strategic coordination and cooperation platform capable of taking forward work on the general aspects of EPCIP and sector-specific actions. Consequently, a CIP Contact Group will be created. The CIP Contact Group will bring together the CIP Contact Points from each Member State and will be chaired by the Commission. Each Member State should appoint a CIP Contact Point who would coordinate CIP issues within the Member State and with the other Member States, the Council, and the Commission. The appointment of the CIP Contact Point would not preclude other authorities in the Member State from being involved in CIP issues. European Critical Infrastructures constitute those designated critical infrastructures that are of the highest importance for the Community and which if disrupted or destroyed would affect two or more MS, or a single Member State if the critical infrastructure is located in another

Member State. This includes transboundary effects resulting from interdependencies between interconnected infrastructures across various sectors. The procedure for the identification and designation of European Critical Infrastructures (ECI) and a common approach to the assessment of the needs to improve the protection of such infrastructures will be established by employing a Directive.

2.2 Measures designed to facilitate the implementation of EPCIP including an EPCIP Action Plan

Measures designed to facilitate the implementation of EPCIP including an EPCIP Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of CIP expert groups at the EU level, CIP information sharing processes and the identification and analysis of interdependencies.

EPCIP will be an ongoing process and regular review will be carried out in the form of the EPCIP Action Plan (Annex). The Action Plan will set out the actions to be achieved along with relevant deadlines. The Action Plan will be updated regularly based on the progress made.

The EPCIP Action Plan organizes CIP related activities around three workstreams:

- Work Stream 1 will deal with the strategic aspects of EPCIP and the development of measures horizontally applicable to all CIP work.
- Work Stream 2 dealing with European Critical Infrastructures and implemented at a sectoral level.
- Work Stream 3 will support the Member States in their activities concerning National Critical Infrastructures.

The EPCIP Action Plan will be implemented considering sector specificities and involving, as appropriate, other stakeholders.

The Critical Infrastructure Warning Information Network (CIWIN) will be set up through a separate Commission proposal and due care will be taken to avoid duplication. It will provide a platform for the exchange of best practices in a secure manner. CIWIN will complement existing networks and could also provide an optional platform for the exchange of

rapid alerts linked to the Commission's ARGUS system. The necessary security accreditation of the system will be undertaken in line with relevant procedures.

Stakeholder dialogue is crucial for improving the protection of critical infrastructures in the EU. Where specific expertise is needed the Commission may, therefore, set up CIP expert groups at EU level to address clearly defined issues and to facilitate public-private dialogue concerning critical infrastructure protection. Expert groups will support EPCIP by facilitating exchanges of views on related CIP issues on an advisory basis. These expert groups constitute a voluntary mechanism in which public and private resources are blended to achieve a goal or set of goals judged to be of mutual benefit both to citizens and the private sector. CIP expert groups will not replace other existing groups already established or which could be adapted to fulfill the needs of EPCIP, nor will they interfere with direct information exchanges between industry, the MS authorities, and the Commission.

An EU level CIP expert group will have a clearly stated objective, a timeframe for the objective to be achieved, and identified membership. CIP Expert Groups will be dissolved following the achievement of their objectives.

Specific functions of CIP expert groups may vary across CI sectors depending on the unique characteristics of each sector. These functions may include the following tasks:

- Assist in identifying vulnerabilities, interdependencies, and sectoral best practices;
- Assist in the development of measures to reduce and/or eliminate significantly vulnerabilities and the development of performance metrics;
- Facilitating CIP information-sharing, training and building trust;
- Develop and promote “business cases” to demonstrate to sector peers the value of participation in infrastructure protection plans and initiatives;
- Provide sector-specific expertise and advice on subjects such as research and development.

The CIP information sharing process among relevant stakeholders requires a relationship of trust, such that the proprietary, sensitive or personal information that has been shared voluntarily will not be publicly disclosed and that that sensitive data is adequately protected. Care must be taken to respect privacy rights. Stakeholders will take appropriate measures to protect information concerning such issues as the security of critical infrastructures and protected systems, interdependency studies, and CIP related vulnerability,

threat, and risk assessments. Such information will not be used other than to protect critical infrastructure. Any personnel handling classified information will have an appropriate level of security vetting by the Member State of which the person concerned is a national.

Also, CIP information exchange will recognize that certain CIP information, though unclassified may still be sensitive and therefore needs to be treated with care.CIP information exchange will facilitate the following:

- Improved and accurate information and understanding about interdependencies, threats, vulnerabilities, security incidents, countermeasures and best practices for the protection of CI;
- Increased awareness of CI issues;
- Stakeholder dialogue;
- Better-focused training, research, and development.

2.3 Identification of interdependencies

The identification and analysis of interdependencies, both geographic and sectoral, will be an important element of improving critical infrastructure protection in the EU. This ongoing process will feed into the assessment of vulnerabilities, threats, and risks concerning critical infrastructures in the EU.

Support for the Member States concerning National Critical Infrastructures (NCI), which may optionally be used by a particular Member State. A basic approach to protecting NCI is set out in this Communication. With due regard to existing Community competences, the responsibility for protecting National Critical Infrastructures falls on the NCI owners/operators and the Member States.

The Commission will support the Member States in these efforts where requested to do so. To improve the protection of National Critical Infrastructures, each Member State is encouraged to establish a National CIP Programme. The objective of such programs would be to set out each Member State's approach to the protection of National Critical Infrastructures located within its territory. Such programmes would at a minimum address the following issues:

- The identification and designation by the Member State of National Critical Infrastructuresaccording to predefined national criteria. These criteria would be devel-

oped by each Member State taking into account as a minimum the following qualitative and quantitative effects of the disruption or destruction of a particular infrastructure;

- Scope - The disruption or destruction of a particular critical infrastructure will be rated by the extent of the geographic area which could be affected by its loss or unavailability.
- Severity - The consequences of the disruption or destruction of a particular infrastructure will be assessed based on:
    - Public effect (number of population affected);
    - Economic effect (significance of economic loss and/or degradation of products or services);
    - Environmental effect; Political effects;
    - Psychological effects; Public health consequences.

Where such criteria do not exist, the Commission will assist a Member State, at its request, in their development by providing relevant methodologies.

The establishment of a dialogue with CIP owners/operators.

- Identification of geographic and sectoral interdependencies.
- Drawing-up NCI related contingency plans where deemed relevant.
- Each Member State is encouraged to base its National CIP Programme on the common list of CI sectors established for ECI.

The introduction of similar approaches to the protection of NCI in the Member States would contribute to ensuring that CI stakeholders throughout Europe benefit from not being subjected to varying frameworks resulting in additional costs and that the internal market is not distorted.

2.4 Contingency planning.

Contingency planning is a key element of the CIP process to minimize the potential effects of disruption or destruction of critical infrastructure. The development of a

a coherent approach to the elaboration of contingency plans addressing such issues as the participation of owners/operators of critical infrastructure, cooperation with national authorities, and information sharing among neighboring countries should form an important element of the implementation of the European Programme for Critical infrastructure protection.

2.4.1 **An external dimension.**

Terrorism, other criminal activities, natural hazards, and other causes of accidents are not constrained by international borders. Threats cannot be seen in a purely national context. Consequently, the external dimension of Critical Infrastructure Protection needs to be fully taken in to account in the implementation of EPCIP. The interconnectedness and interdependent nature of today's economy and society mean that even a disruption outside of the EU'sborders may have a serious impact on the Community and its Member States. Equally true the disruption or destruction of critical infrastructure within the EU may have a detrimental effect on the EU's partners. Finally, working toward the goal of increasing the protection of critical infrastructure within the EU will minimize the risk of the EU economy being disrupted and thereby contribute to the EU's global economic competitiveness. Consequently, enhancing CIP cooperation beyond the EU through such measures as sector-specific memoranda of understanding (e.g. on the development of common standards, undertaking joint CIP related studies, identification of common types of threats and exchanging best-practices on protection measures) and encouraging the raising of CIP standards outside of the EU should, therefore, be an important element of EPCIP. External cooperation on CIP will primarily focus on the EU's neighbors. Given however the global interconnectedness of certain sectors including ICT and financial markets, a more global approach would be warranted. Dialogue and the exchange of best practices should nevertheless involve all relevant EU partners and international organizations. The commission will also continue promoting improvements in the protection of critical infrastructures in non-EU countries by working with G8, Euromed, and EuropeanNeighbourhood Policy partners through existing structures and policies, including the"Instrument for Stability".

Accompanying financial measures and in particular, the proposed EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013, which will provide funding opportunities for CIP related measures having a potential for EU transferability. Within the general objectives, and unless covered by other financial instruments, the programme will stimulate, promote

and develop measures on prevention, preparedness and consequence management aimed at preventing or reducing all security risks, in particular risks linked with terrorism, where appropriate based on comprehensive threat and risk assessments. Funding under the programme, by way of grants and Commission, initiated actions, will be used in particular toward the development of instruments, strategies, methodologies, studies, assessments, and activities/measures in the field of the effective protection of critical infrastructure (at both EU and MS levels).

In Nigeria, no law talks about the identification, planning and protection of the critical infrastructures. On 23rd July 2019, a bill titled ''Critical National Assets and Infrastructure centre (Establishment)Bill, 2019 m[HB. 221]'' past its' first reading under the 9th National Assembly. Until now there has not been any address to the bill.

The EPCIP provides a standard framework for defining, identification, designation, protection, reporting and support of critical infrastructures amongst member countries. It states the implementation process and means of communication and collaboration amongst countries willing to adopt without a wholistic approach but according to the needs and priority.

Without the implementation of laws to guide society, it's existence and development will always be vulnerable to persons/nations with a more structured ideology. For sustainability growth and development of the nation is imperative that a law that identifies and protects critical infrastructures is established to enhance the socio-economic development of Nigeria.[5]

3 GENERAL AND SPECIFIC APPROACHES OF RISK ANALYSIS

3.1 Definition of terms

Defining the basic terminologies that constitute the framework for critical infrastructure protection analysis is important.

Risk *(R)*

The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability. In practice, risk can be defined mathematically as;

$$R = A.T.V \qquad (1)$$

Where;

Asset: An asset is what we're trying to protect (people, property, and information). People may include employees and customers along with other invited persons such as contractors or guests. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records, and many other intangible items.

Threat: Anything that can exploit a vulnerability, intentionally or accidentally, to access, modify, obtain, damage, destroy and asset.

Vulnerability: Any weakness or loophole in our security program or structure that can be exploited by threats to gain unauthorized access to an asset. [6]

3.2 General Risk Analysis Methods

Applying risk analysis to Critical Infrastructure protection entails choosing the appropriate methodology for the scenario/ system under consideration. These methodologies can be categorized as qualitative and quantitative as listed below.

3.2.1 Qualitative Risk Analysis

The main purpose of the qualitative risk analysis is prioritizing risks according to their probability and impact. A project can be exposed to a large number of different risks. [7]

3.2.2 Hazard and Operability (Hazop) Study

Hazop is a systematic and detailed method that was developed in the process industry. Different guidewords (such as 'no', 'less', 'higher', 'instead') are used to identify potential deviations in a system. The method is qualitative, and the aim is to find potential problems in a system.

Consequences, causes, current protection, and recommended actions are usually described and displayed in a table.

3.2.3 Failure Mode and Effect Analysis (FMEA)

Failure Mode and Effect Analysis (FMEA) is a method used to identify and eliminate faults or deviations in a system before they cause problems. Each function in a system is analyzed and it can easily be very extensive. It is a qualitative method and the results are displayed in a table.

The results may include causes of failure, effect, frequency, severity, probability and recommended actions.

3.2.4 Fault Tree Analysis (FTA)

An FTA aims to identify all causes of an unwanted event. The method is a top-down approach where the analyst starts with an unwanted event and identifies all the different root events or causes. The result is a logical diagram and the FTA can be either qualitative or quantitative depending on whether probabilities are assessed or not. The difference is that quantitative FTA results in an estimation of the probability of the top event, which depends on the probabilities of the root causes.

3.2.5 Event Tree Analysis (ETA)

Event Tree Analysis (ETA) starts with an undesired event and tries to determine the consequences of the event. The course of the event is thus not analyzed. The method is appropriate for use when planning activity and issuing licenses and permits and can be used both quantitatively and qualitatively. It is suited for production systems with safety systems and emergency routines adapted to prevent the development of damage. Quite often it is followed by a quantitative consequence analysis for some specified events of damage and can preferably be combined with for example Quantitative Risk Analysis and Fault Tree Analysis. The results are presented graphically and are drawn as a logical diagram.

3.2.6 Human Reliability Analysis (HRA)

Human Reliability Analysis (HRA) studies human reliability, meaning the probability that the person will correctly perform some system-required task given certain time. This is a group of many different methods, one of the most commonly used of which is called THERP (Technique for Human Error Rate Prediction), where human reliability is thoroughly assessed.

The results from an HRA, e.g. probabilities of human error, could be used for instance in an FTA.

3.2.7 Quantitative Risk Analysis (QRA)

Quantitative Risk Analysis (QRA) is a method commonly used in the process industry. The technical systems are the focus and the aim is to foresee how these might affect technique, equipment, processes, process conditions, and the siting of the plant. Several scenarios are identified (starting events) and then the risk, as defined in the report, is analyzed. The results of a QRA are shown graphically either on an individual level or societal level. The individual risk is shown as contour maps that illustrate the different levels of risks around the studied object and its surroundings on a map. When society is concerned the results are shown as a graph, a so-called F/N-curve chart, where F stands for the frequency of the damaging event, and N stands for the number of victims (those killed) of the damaging event.

3.2.8 Conflict Analysis (CA)

Conflict Analysis (CA) is a systematic mapping of competing interests during planning. The analysis should be performed as early as possible during the planning to avoid one activity rendering another desirable activity impossible. The method is very brief and gives no specific support for how to handle the issues of risks. The advantage is that possible conflicts and problems could be identified at a very early stage, thus lessening the costs of taking measures later on in the process or perhaps even preventing the process from coming to a dead end.

3.2.9 Expected Damage-Cost Analysis (EDCA)

Expected Damage-Cost Analysis (EDCA) is used to determine the frequency of different kinds of hazards and the result is an estimation of the expected damage costs per year. The results also include suggestions for precautionary measures such as investments and de-

sign/planning. The frequencies of different hazards are estimated and a factor of vulnerability is considered.

Human, technique and environment are studied, as are the economic consequences for the production plant if something is damaged.

*3.2.10 **Vulnerability Analysis (VA)***

Vulnerability Analysis (VA) evaluates how an organization, or a part of an organization, will be affected by different negative events. This is done by using analyzing scenarios based on realistic events. VA is an in-depth analysis that is time-consuming and is very useful for different kinds of processes and/or plants. The results from a VA provide advice on precautionary measures. The organization is studied, and a survey consequence analysis is performed. [8]

Quantitative analysis means the opposite, to measure by quantity rather than quality. When we do quantitative analysis, we are exploring facts, measures, numbers, and percentages. When we do quantitative work, we work with numbers, statistics, formulae, and data [9]

The Quantitative Risk assessment (QRA) is an objective risk assessment tool used to project threat impacts. The QRA provides an estimate of the magnitude of consequences for each identified budget threat. The estimated costs to the program are summarized into a total probabilistic budget threat estimate. An estimate can be a range of possible costs from a range of possible values; meaning the cost will fall within the estimated range. QRA systematically determines the likelihood of threats occurring and evaluates the cost (cents/$) of the occurrence QRA sets out to define, measure, predict, and provide a confidence level of likelihood and occurrence of threat impacts [10]

3.3 Specific Risk Analysis Methods

*3.3.1 **RAMCAP-Plus***

The RAMCAP-Plus methodology has been developed by ASME (American Society of Mechanical Engineers) as an all-hazards risk and resilience assessment methodology. The scope of the methodology covers all infrastructures, intending to address protection of na-

tions critical infrastructures (avoiding hazardous events or their consequences) and resilience (rapid return to full function after disruptive events).

The methodology is based on a seven-step approach namely:

1. Asset characterization,
2. Threat characterization,
3. Consequence analysis,
4. Vulnerability analysis,
5. Threat assessment,
6. Risk and Resilience assessment,
7. Risk and Resilience Management.

The methodology is particularly interesting as it incorporates several important features for risk assessment of infrastructures. The first element is that the methodology avoids unnecessary detail by focusing on the most critical assets at a facility. The second important element is that the developers of the methodology have identified the necessity for cross-sectoral risk comparisons which is rarely offered by the existing risk assessment methodologies. Finally, the methodology has a simplified approach and it is based on existing risk assessment techniques, but the high-level approach is pronounced.

The target group of this methodology are CI operators and decision-makers.

Resilience is addressed in this methodology. It constitutes a central element of the methodology, a feature that is not developed at this level by any other methodology analyzed in the present report. [11]

4 MEASURES FOR CRITICAL INFRASTRUCTURE PROTECTION

The EPCIP is generally divided into two subsystems namely; a technical subsystem, which is responsible for the production and transmission of electric power, and an economic subsystem, which caters for marketing transmission and distribution services. A legal framework regulates both subsystems.

The thesis aims to look at security in the technical subsystem. The technical subsystem of an electric power system consists of the hardware that physically produces and transports electric energy to customers as well as the equipment in which the electric energy is

consumed. It further consists of the people and organizations that build, maintain, operate and control the equipment. The structure of the technical subsystem is determined by the nature of the components of the power supply system: the power stations, the transmission network, the distribution networks and the consumer equipment. [12]

4.1 Technical Security of Electric Power Critical Infrastructure

Technical security can be defined in the context of EPCI as a set of essential requirements and measures for the protection of infrastructure elements. Technical security deals with continuous application of security measures which can be grouped as physical security, regime measures and technical as shown in Fig.1.

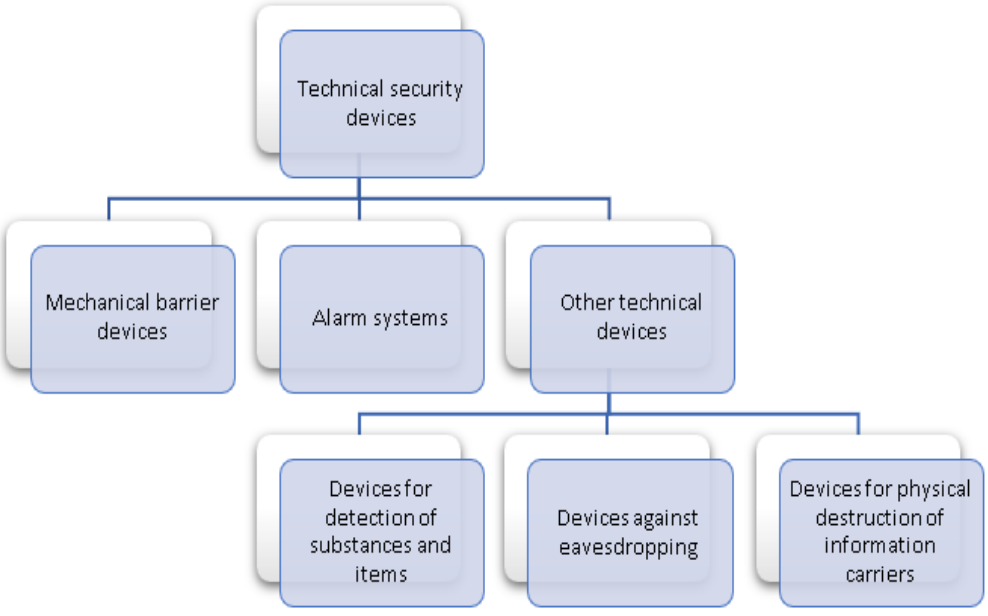

Fig.1: Classification of technical security devices. *[Source: Vidrikova et al., 2017]*

The security measures can further be divided into; Physical security, Information security, Administrative security, Personnel security, Crisis management and planning units. Their application in context on ECIP is explained:

4.1.1 Physical Security

Physical security is achieved by combining three basic elements: physical protection systems, response team/activity and regime protection.

i. Physical protection systems – is divided into two basic areas of mechanical barrier systems and technical protection systems.

- **a.** Mechanical barrier systems in object concepts as the building are walls, roofs, floors, doors and windows objects. Example: safety locks, grilles, security film, security and toughened laminated glass, safe, safety deposit boxes.
- **b.** Technical protection systems are Intruder and/or Hold-up Alarm System (I&/or HAS); Security Camera System (CCTV system, CCTV surveillance system); Fire alarm system (FAS); Access Control System (ACS); Mechatronics System.

ii. **Response team/activity** - can be carried out by own resources, security, private security service employees, or by police or army. This type of protection is expensive but very active and effective. The core is a response of a human element to impulses related to danger/ security disruption/ object protection such as. breaking in, technological breakdown etc. Impulses for a response team reaction are carried out by an alarm system.

iii. **Regime protection/measure** – consists of a compilation of administrative and organizational measures for securing protected interests and values. Generally considered the most important are:

- **a.** Input and output mode of persons and means of transport which includes namely checking the entrance of employees, clients, visitors and foreigners into the object and its parts, checking the leaving of persons and vehicles from the object, a right to take out objects and materials.
- **b.** Mode of the employee's movement in the object which also includes a determination of a part of an object with limited accessibility for employees and designation of their affiliation to certain transports, working places etc.

c. Material and expedition mode sets the procedure when receiving, storing, exporting and movement of material. This way the property is protected against theft, damage and devaluation

d. An operational mode which secures continuity and security of operation and working when an exceptional event occurs

e. The key mode of operation which serves to determinate the marking, assignment, handing over of keys, the way they are used, the making of spare keys, changing of locks in important parts of the object etc.

f. Operational mode related to the working of technical protection systems.

4.1.2 Information Security

Information security management is key to the protection of critical assets ranging from information managed by databases, information accessed, processing of information through applications to management of other units of security. The main areas of information security are; Security policy - defines the basic rules and requirements to ensure the protection and security of information in an organization. After approval of the management serves as a binding regulation for employees.

i. Management of physical access - ensuring the physical access to key components of the IS for personnel only, including the option of supervision. This area is intertwined with Physical protection systems.

ii. Folder services, authentication and authorization - central database of users, enabling the management of their identification and access data, including logging in and access monitoring. A potential expansion can be systems for identity management, single sign-on or systems for multi-factor authentication.

iii. Security supervision and management system – an important element of security that enables gathering information about events from various systems, unifying them into one place and subsequently evaluating them.

iv. Invasion checking – all operational activity or measures within security must be checked from the perspective of keeping the defined security policy or the occurrence of vulnerability – compliance monitoring, vulnerability scanning and penetration tests.

v. Antivirus protection – often makes up the base of IS security. It is important to build one or more barriers into the potential route of a dangerous code in the direction of the organization's information system – so-called multi-layer antivirus protection. The essential element is central management and monitoring of antivirus solution and further protection against new kinds of attacks (combined attacks, phishing, spyware, installers, rootkits etc.)

vi. Protection for the web's perimeter – used for the web's separation from web's of other subjects and public webs. Often composed of firewall, IDS/IPS sensor, content filters, antispam and antivirus protection. Content check - namely filtering the content on the web's perimeter to eliminate unwanted content when transferring into the organization's web or the other direction.

vii. Data encryption - a system to prevent tampering with data, their possible theft or modification. It is used to protect data stored on disk storage, removable media and communication through untrusted networks. In particular, these are systems for online disk encryption, file systems, parts, electronic mail, symmetric and asymmetric encryption of data streams - VPN.

4.1.3 Personal and administrative security

In this area which observes the "life cycle of an employee", the security measures can be divided into 3 categories; pre-employment, employed/post-employment, termination of appointment.

i. Pre-employment: It is necessary to carry out inspections with the new employees to ensure the security of the CI. Techniques such as identity verification according to documents, verification of education or training documents, etc. A higher level can be carrying out of personal profile analysis, reference verifying, or business register check or insolvency register. The highest form can be proving integrity based on the extract from the crime register or other special methods. Herein, when verifying, it is necessary to pay attention to the fact that all activities are carried out thoroughly following the effective laws. The last stage of accepting an employee is negotiating exact conditions for work, which should also include a specification of an employee's responsibilities and duties about maintaining security.

ii. Employed/post-employment: For the development of personal security during the employees' activity in an organization, three safety measures are important:

a. Senior employees' responsibility – including acquainting subordinates with safety rules and their motivation to following these rules.

b. Broadening the security consciousness – realized via schooling, seminars, training and other educational activities. The aim is to project the designated rules into the actual behavior of all employees, which is a very difficult and everlasting task.

c. Disciplinary proceeding – meant for situations when the designated rules have been broken. The aim is to discipline and draw attention to detected misconduct. With subtle misconduct, oral reprehension is enough. More serious issues could result in financial sanctions, change of position and in extreme cases even in termination of the employment relation or lawsuit.

iii. Termination of appointment: The last stage of the employee's life cycle in the organization is the termination of his/her employment relation. The main security measure is a clear and unequivocal determination of responsibilities related to the termination of the employment relation. The primary issue is to co-ordinate relations between human resources and line managers. Concerning the leaving employee, it is important to draw attention to the fact that his obligation of reticence continues even after his employment relation termination. Another measure is returning of all borrowed devices. The most difficult issue here is data deletion on the private devices of the employee. The basic task of employees involved in the working of information and communication technologies is locking and deletion of access accounts and closing of all access routes into the organization for the leaving employee. That includes the area of physical protection.[13]

4.1.4 Crisis Management and Planning

i. *Risk and crisis management*

The strategy for risk and crisis management and planning is a systemic process consisting of five phases representing the fundamental scope of process-based risk and crisis management used by both private enterprises and Government. The phases are as follows;

a. preliminary planning to establish a system of risk and crisis management;

b. risk analysis;

c. specification of preventive measures;

d. implementation of a system of crisis management;

e. regular evaluation of phases 1 through 4.Business continuity planning as shown in **Fig.2**.

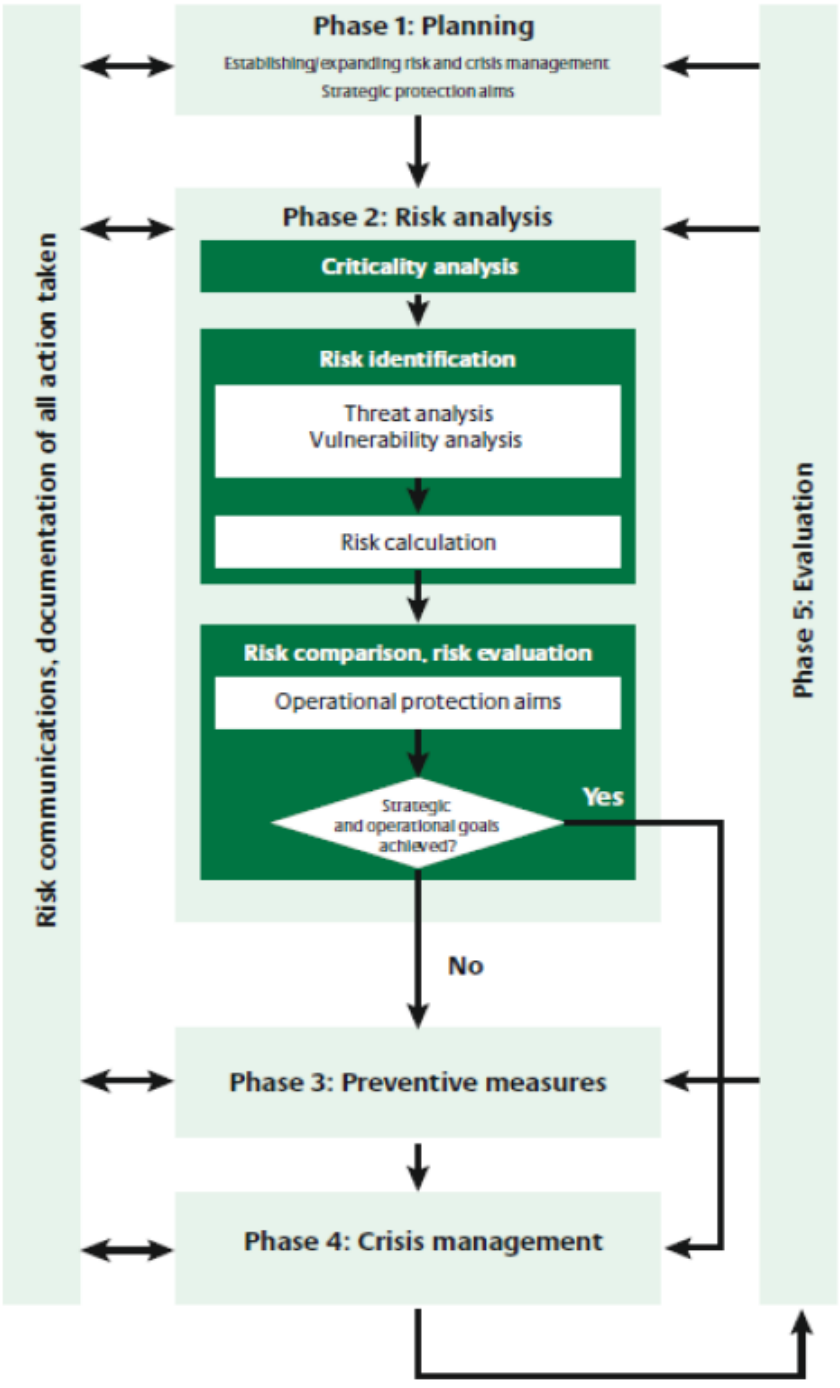

Fig.2: Five phases of risk and crisis management *[Source: Ludek Lukas et. 2011]*

ii. *Business Continuity Plan*

The complexity of business processes exposes organizations to risks of varying magnitude involving people, processes and technology. Organizations need to have a Business Continuity Plan (BCP). A business continuity plan (BCP) is a document that outlines how a business will continue operating during an unplanned disruption in service. It contains a disaster recovery plan and contingencies for business processes, assets, human resources and business partners – every aspect of the business that might be affected.

Business continuity plan typically contain a checklist that includes supplies and equipment, data backups and backup site locations. Plans can also identify plan administrators and include contact information for emergency responders, key personnel and backup site providers. Plans may provide detailed strategies on how business operations can be maintained for both short-term and long-term outages. Fig.3 describes the processes involved in the cycle regarding IT security.[14]

Fig.3: BCP in IT Security *[Source: Ludek Lukas et. 2011]*

The theoritical part of the thesis looked at the history of CI and it's evolution with growth in technology and interdependencies of various economic sectors with the adoption of Laws (Legistlative Framework) for the identification, protection, communication and building of resilience across critical infrastructures.

5 OVERVIEW OF THEORY

The theoretical part of the thesis covered; Chapter 1, the history of critical infrastructure and how the development over centuries led to the creation of laws to define it. Chapter 2, looks at how the need for protection of national assets led to the development of laws [legislative framework] across continents, which describes ways of identification, planning, protection, communication and resilience of the critical infrastructure. Chapter 3, briefly describes methods of identifying the vulnerabilities and risks associated with critical infrastructure. Chapter 4, introduces measures for the protection of critical infrastructure elements with emphasis on the technical part of the electric power system.

In other to apply security measures, it is important to look at the types of risks inherent in the EPCIP and methods on how they can be measured.

The ECPIP general structure was introduced with emphasis on the technical subsystem and the measures for its protection.

The Analytical part will be the analysis of a generating hydropower plant, considering the risks and choosing a suitable security application that mitigates them.

II. ANALYSIS

6 ELECTRIC POWER CRITICAL INFRASTRUCTURE

Electric power critical infrastructure is unique in that it supports other critical infrastructure and key resource sectors. The electiricity system consists of; generation part for production of electricity; the transmission part for transporting the generated electricity; distribution part and technical control rooms for managing the whole system.

6.1 INTRODUCTION

The evolution of electricity from an individual point of generation/demand overtime to an interconnected network of multiple sources of generation, transmission, and delivery as a service has given room to complexity in the system. Almost all critical infrastructure sectors are interdepended, and all rely on the electricity power supply as shown in Fig.4, a disruption in any of the related parts of the process will affect the nation. An example is the 2019 Venezuela, a power outage that affected 18 of its 23 states causing food shortage, chaos in health and transport systems with 26 deaths recorded [15].

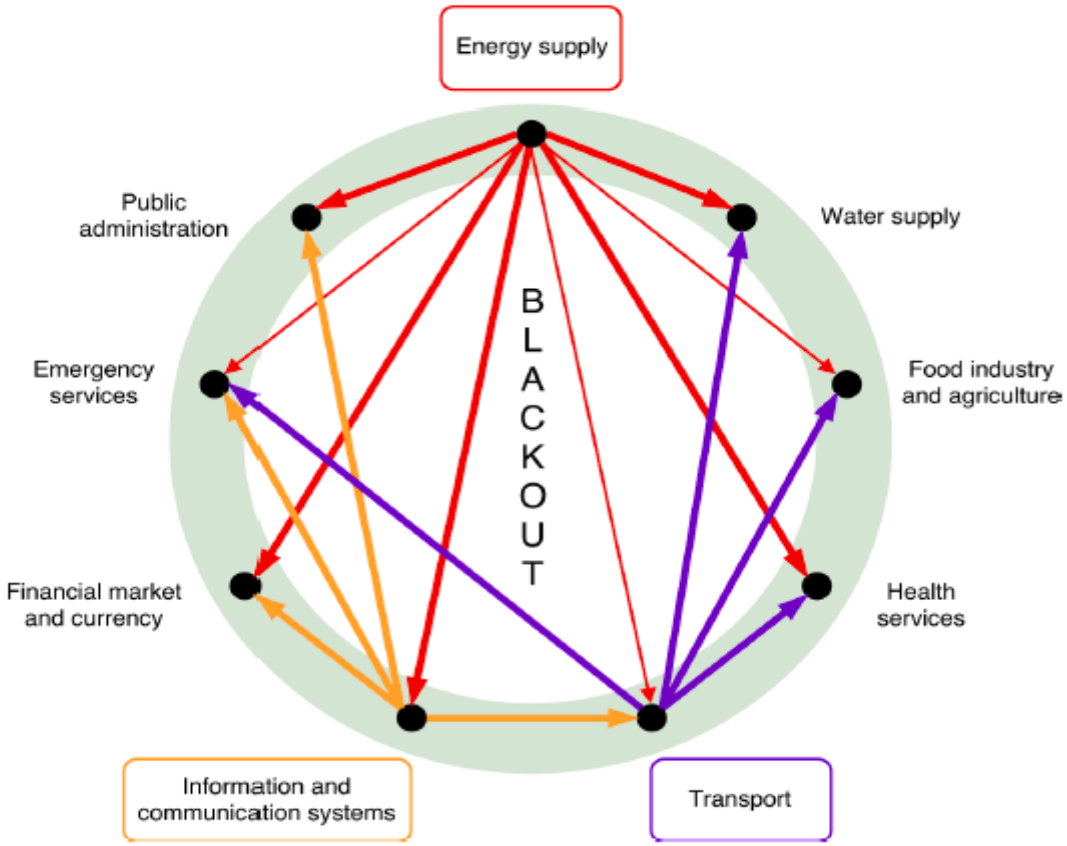

Fig.4: *Interdependency of critical infrastructure on electric power supply.[Source: David Rehak et. 2020]*

6.2 TYPES OF INTERDEPENDENCIES IN EPCI

The most relevant types of interdependencies are; physical, geographical, logical, and cyber.

1. Physical Interdependency:

   This can be defined as when the output of one infrastructure is needed as input to another infrastructure. For example, a production plant will need electricity from the electric power company for production which is provided using a physical link (Transmission lines).

2. Geographical Interdependency:

   This is when elements of multiple infrastructures are in close spatial proximity. For example, an electrical line and a fiber-optic communications cable slung under a bridge connect (geographically) elements of electric power, telecommunications, and transportation infrastructures.

3. Logical Interdependency

   This when the state of two infrastructures depends on the state of each other via a mechanism not described by other interdependencies. An example is a control schema that links an agent in one infrastructure to an agent in another without any connection.

4. Cyber Interdependency

   This can be defined as the state of infrastructure depending on the information transmitted through the information infrastructure. Cyber interdependencies connect infrastructures through information and communication systems output serving as input. An example is the SCADA system that controls the power grid.[16]

6.3 ELECTRIC POWER SYSTEM

Electric power system could be defined as a process involving; production, transmission, delivery of electric power, and other related services. It comprises 3 parts namely; Legal framework, Economic subsystem, and Technical subsystem. The whole system comprises different elements as defined below;

1. Part: smallest component of a system that can be identified in the analysis.

2. Unit: a functionally related collection of parts (e.g., a steam generator).
3. Subsystem: an array of units (e.g., a secondary cooling system).
4. System: a grouping of subsystems (e.g., a nuclear power plant).
5. Infrastructure: a complete collection of like systems (e.g., the electric power infrastructure).
6. Interdependent Infrastructures: the interconnected web of infrastructures and environment.

For our discussion emphasis will be laid on the Technical subsystem as shown in Fig.5.

The Electrical power system model shows the different units; the Generation Unit, Transmission Network, Distribution Network, and Load (Consumer).

1. Power Generation: This unit represents power plants that convert fossil fuel energy (coal, oil, natural gas or enriched uranium) or renewable energies (water, wind and solar) into electric energy
2. Transmission Network: The generated electric power is transported through transmission lines at various voltages from the step-up transformer at the generation unit to a step-down transformer at the distribution unit for onwards distribution.
3. Distribution Network: Each unit comprises of subunits and cannot function independently, hence the need for interconnectivity.

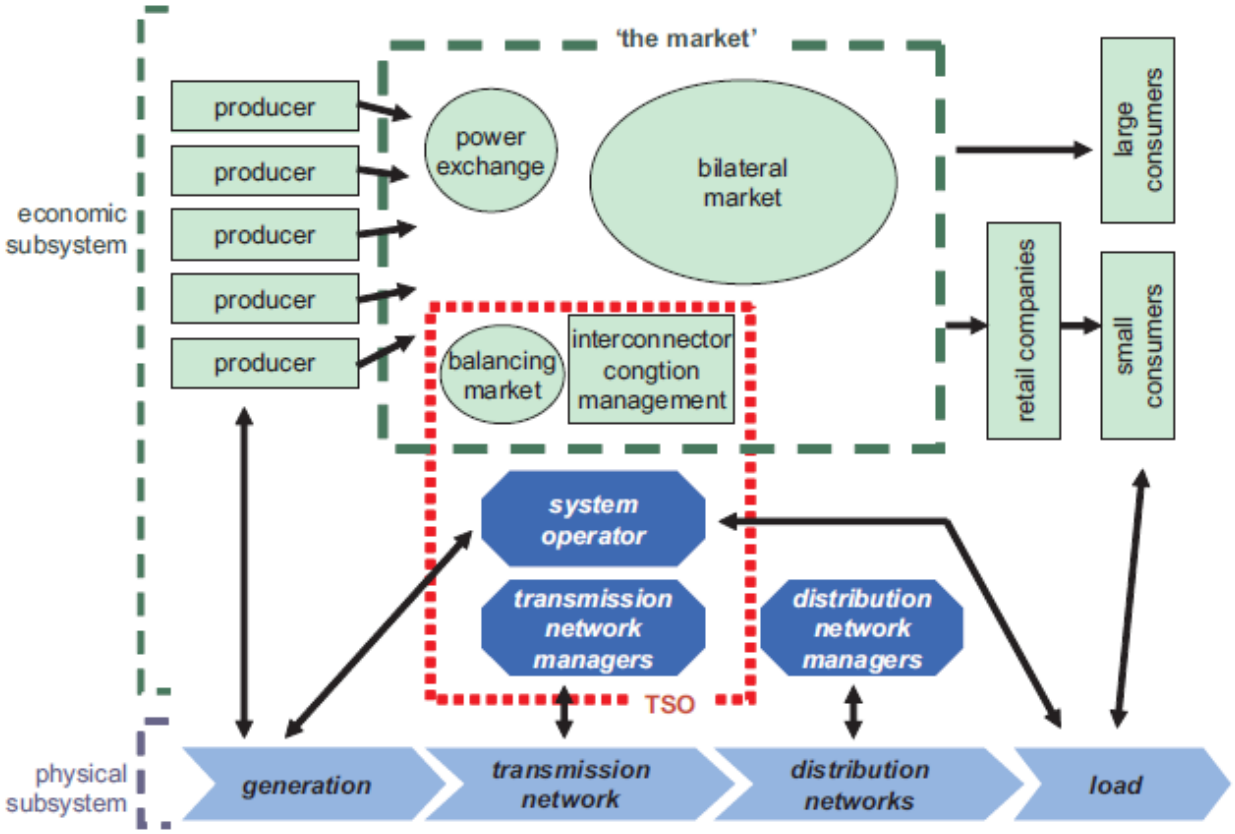

Fig.5 *Electrical Power System Model. [Source: Knops et al 2004]*

The EPCI comprises of technology, raw materials as input, and humans. From input (raw materials) conversion in the generation unit to transmission unit and delivery of the output(electricity) to the consumer, information and communication systems are used to make the control flow of the entire system reliable, efficient, and manageable. However, each component of EPCI has a potential vulnerability but the most susceptible are the human component who controls the entire system and the highest level of risk is non-functionality of the generation plant. [17]

6.4 TYPES OF VULNERABILITIES FOUND IN ELECTRIC POWER CRITICAL INFRASTRUCTURE

In considering the vulnerabilities in EPCI, the following groups of assets are considered in the production, transmission and distribution parts: Thermal power and heating plants; Hydropower plants;Electrical stations; Dispatching building and power line.

The vulnerability of the electric power grid ranges from technology, processes, and implementation. Cyber Interdependency is vital to the proper functioning of the entire grid thus encompassing the highest level of vulnerability.

1. Open Communications

   Open and unprotected communication lines between protection and control system components, as well as between power infrastructure facilities:

   I. Lack of Identity Verification

      Due to poor implementation of authentication of interacting agents, a random device on the technological network can send incorrect or malicious control commands to a top-level system that in turn, could cause a dispatching operator to execute invalid actions

   II. Open Standards and Open Data Transmission

      The data transmission protocols used are based on publicly available, open, and well-documented standards. Free implementations of protocols and their source code, together with tools for analysis and emulation are publicly available. Data transmitted in such networks is usually open for capturing, reading, modification and replay, simplifying access and threat execution for potential intruders

   III. High Level of Network Communications

      The high levels of communication between IEC 60807-5-10x and IEC 61850 MMS protocols are a normal aspect of their operation. But these open communications can also facilitate simple denial of service attacks on technological infrastructure devices (for example, dispatching center process control system, or protection terminals) via the mass sending of invalid data packets

   IV. Connections to Public Networks

      The corporate and technological networks of a modern industrial facility may have multiple interconnections at almost every hierarchy level of the control system, which increases the risk of unauthorized external access to technological equipment

2. Lack of Cybersecurity Awareness Among Employees

A limited number of technical personnel maintain large numbers of devices that are often distributed on territory and function without permanent monitoring. On-site personnel often lack even a basic knowledge of cybersecurity:

I. Privileged Remote Access From An Untrusted Network

For easy maintenance and convenience, technical staff often enable full-privilege access to remote facility equipment. Such access is often organized unofficially and insecurely, for example, from corporate workstations with Internet access

II. Lack of Password Protection and User Control Policies

With the large number of devices maintained by a limited of personnel, it is difficult to organize and maintain device access policies, including password protection and user control policies. As a result, technological devices are often operated with default passwords, simplifying unauthorized access

III. Outdated Software

IED software is seldom updated during its lifecycle on the technological facility. Known software bugs are not eliminated unless they directly affect industrial processes

IV. Maintenance from Unsafe Workstations

Portable workstations (notebooks) used in the course of technological infrastructure maintenance are often also used as regular corporate workstations as well as “test lab” equipment for software testing or personal needs

V. Lack of Regular Configuration and Software Control

Device configuration and software verification checks are performed manually and irregularly, not more often than once a year

3. Security Requirements are Not Followed

Information Security requirements are rarely considered in the device or software design and development processes for technological infrastructures.

I. Weak Resistance To Hacking

Developers do not usually consider the vulnerability of their code to targeted attacks or illegitimate actions on technological infrastructure and its elements. This means resistance to devise hacking is generally weak.

II. Invalid or Insufficient Network Security Settings

Invalid settings of network segmentation and access control between network segments in the technological network, the Absence of specific network design solutions in PACS implementation projects is a typical problem. For this reason, the quality of the network infrastructure setup usually depends on the skills and qualifications of the installation team.

III. Absence of Data Protection When Transmitted via Open Channels

There is a lack or absence of secure means for data transfer over open communication lines;

- Absence of role-based access controls can enable incorrect access permissions to devices, allowing users access that does not correspond to their official duties
- The absence of compatible solutions to protect computer systems from unauthorized application startup often leaves systems unprotected from the launch of unauthorized software in industrial environments. General tools for application startup control are often incompatible or ineffective with industrial systems (incompatibility with technological software, insufficient resources on specific technological systems, etc.)
- Absence or Insufficiency of Security Event Registration Tool

  There are no specific monitoring and cybersecurity event registration tools within process control systems, or their functionality is insufficient to provide the correct interpretation of a situation.

4. Complexities of Contractor Access Control

The use of contracting organizations for certain types of maintenance work is common. Consequently, it is extremely important to provide only temporary access to a limited amount of equipment that does not influence other system components. Cancellation of access on completion of the work is vital.

5. Long Lifetime of Vulnerable Components

   The lifetime of devices and protection and control systems is 20-30 years; insecure systems installed today will only be replaced in a couple of decades or so. The partial upgrade is usually extremely difficult as soon as secure solutions (for example, those using encryption) are often incompatible with standard vulnerable solutions. In addition to the technical issues listed above, there are also important organizational issues. Firstly, the lack of guides defining actions to be taken when suspicious activity is detected within automated systems. Secondly, the lack of documents and practices relating to the investigation of disturbances in technological environments including malicious influence on control systems through information technologies. For example, due to their age, some reference documents for the investigation and classification of technological disturbances do not even consider cybersecurity incidents as a possible cause of the malfunction. If such an incident even takes place, the real causes will not be revealed. As a result, the appropriate measures will not be taken and the incident may reoccur. [18]

The socio-economic growth of every nation depends on how it prioritizes it resources, and the adoption of critical infrastructure protection legislative framework is the most suitable approach.

Electric power is a key element of critical infrastructure due to interdependencies with other elements. The process of delivering electricity as a commodity comprises the generation, transmission and distribution. There are risks associated with each of the mentioned stages which could be internal or external. For efficiency and reliability of service delivery, it is important to understand these risks.

The risks are results of vulnerabilities inherent to the system. It is of high significance that the levels of risks are analyzed using risk models suitable to the system in order to prioritize and apply the necessary security models to mitigate the risk for optimization of service delivery to meet consumer demands.

7 ANALYSIS OF HYDRO POWER PLANT

The hydro power plant analysis aims to highlight the strength, weakness, opportunities and threats in the system to determine the units that posses great risks and how they can be mitigated.

7.1 Overview

The hydropower plant occupies a 34km2 land with a rock-filled concrete-faced dam that is 115m high and 700m long. The dam site has a reservoir of 7bM3. It has a powerhouse building comprising several support services. It has an electrical distribution network comprising 11/0.41kV distribution network and 11/0.415kV sub-stations (110-200kVA). Assets consist of civil structures, the Primary Electro-Mechanical Plant, non-core assets, and balance of the plant assets (overhead cranes, fire protection systems). There are four hydraulic turbines, four generators, gates and hoists, plant auxiliaries including a powerhouse portable water treatment plant, sewage treatment plan, lubricating oil treatment plant, one chlorination plant, two flood-control pumps, and reservoir management equipment. The available capacity is 600MW. [19]

Fig. 6: *Pictorial view of the Hydropower plant.[Source: Gbadomosi et. Al 2015]*

Fig.7 is a flow diagram showing the hydropowerplant and Table.2 shows desrcibes the parameters related to the components.

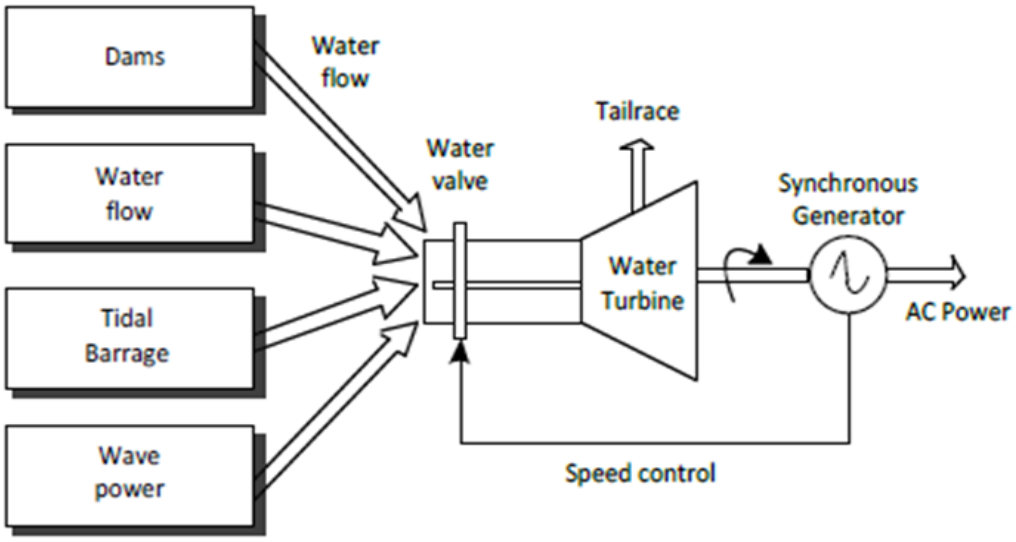

Fig.7: *Flow diagram of Hydro-Electric Generation [Source: Gbadomosi et. Al 2015]*

7.1.1 Computing/ Control System

The system is controlled using an intelligent system that requires a power supply and internet connection for almost 5 years and it has software design, a sensing module,

1. It is host to SCADA-operated national control center and the station is also equipped with switchyard facilities that include a technical "step down" function for enhanced distribution into the national grid, an advanced control room, and modern training facilities [20].
2. Hp z type computer with Windows 10 Pro core™ processors, ultra 3D certified graphics: visualization software with NVIDIA Quadro® P5000 graphics. Windows 10 Pro for Workstation 64, Intel® Xeon® E processor, 16 GB memory; 512 GB SSD storage, NVIDIA® Quadro® P2200 (5 GB GDDR5X dedicated. There are also Backup systems readily available.
3. Software Design Modules: The software used for the design is an android software application that is applicable on an android phone for ease control and it is outsourced for its design.
4. Sensing Module: The module is deployed to monitor and control devices in the outside power plant or turbine layout and entire physical layout of the generating station. The layout station is classified:
    I. Security unit with 3 different interlinks together

II. Power plant unit

III. Staff quarter outlet unit

In each section of the modules, the sensors were interfaced with the devices for monitoring and controlling purposes and the sensors include current and voltage sensors.

Elements	**Technical parameters**	**Expected Performance with time frame**	**Topological structure**	**Key technology: classification**	**Element redundancy and risk**	**Physical protection of the element**
Storage Reservoir	No	-	-	-	-	-
Dam	1. 7 billion cubic meters and concrete rock-filled dam	95% with 100 years	River	-	The dam content must be reduced when the design peak is reached and it occurs mostly in the rainy season. The flow is decongested and it is announced on radio to people downstream or villages to know about that and it is consequences 2 weeks earlier.	Concrete rock-filled and two gates before the dam.
Trash Racks	Net type	95%	-	-	-	-

Draft Tubes	-	-	-	-	-	-
Prime Movers/Water Turbines	#4 Vertical Francis Turbine		#18 vertical blades	181.3 flow rate per metre meter cube and speed of 150 rpm	Capabilty The capability of all working simultaneously to generate maximum power.	At intervals

Table.1: *Parameters of the Generation unit.[Source – Hydro power plant Management]*

7.1.2 **Staffing**

The hydropower plant is made up of 143 employees (sample size) comprising of different departments and roles. The production correlation to other elements and time sensitivity varies between 24 hours – 4 months depending on department and the level timing is between 40 to 70% time increment in the worst situation. The main objective for each department and procedure for achieving the target is represented in Table.2.

No.	**DEPT.**	**SIZE**	**Main objective (output, product, and service)**	**Procedure for achieving target activities**	**The topological structure of the evaluated objective**	**Available technology/ System of operation**
1.	**Administrative/Human resources**	**16**	Managing of entire system activities and recruitment.	It is based on the organisational structure through the creation of a file, documented of a file and with the appropriate executive of	Life cycle system management for record-keeping and the use of internet facilities. Creation of: Policy and subject files,	internet facilities, CD and hard disk, computer for documenting the purpose.

				directors.	personnel files, data input sheets, Computerise generated data. Bureau of Public Procurement Act for the management process.	
2.	**Corporate/ Legal Advice**	**4**	Legal backing	The company hire corporate people for legal issue and protection.	Since the company is partially owned at 60% by private: corporate legal adviser is adopted	Documented using record-keeping
3.	**Engineering & Technical Services**	**27**	This section contains works: mechanical and electrical majority while civil for minor restructuring: To ensure the maintenance of power plant gadgets are in order.	The process ensures all engineering activities through staff training, equipping the workshop and using ISO 9001:2015 standard.	Assurance of engineering and technical know-how of the plant is adequate within a limited time. Training of engineering personnel.	Tools base on ISO 9001:2015 Quality standard.

4.	**Health & Safety**	**7**	HSE responsible safety of the system through a protocol	Through ISO 9001: 2018 HSE standard	Assurance of safety of the workers and visitor through the procedure Training of HSE personnel	ISO 9001/2018:45001 HSE system standard

Table.2: *Objectives of the Hydropower plant departments. [Source – Hydro power plant Management]*

No.	**DEPT.**	**SIZE**	**Main objective (output, product, and service)**	**Procedure for achieving target activities**	**The topological structure of the evaluated objective**	**Available technology/ System of operation**
5.	**Power plant utilities & Maintenance**	**39**	Ensuring power plant itself is in order during generating of power	The process ensures all engineering activities through staff training, equipping the workshop and using ISO 9001:2015 standard	Assurance of power plant and maintenance is adequate within a limited time 2. Training of her personnel	Tools base on ISO 9001:2015 Quality standard

6.	**Process operation & Public affair**	**6**	Relating internal and external concerning the company such as announcing the warning of water discharge when dam over filled	Public procurement act (PPA) and ISO 9001: 2015 requirement	This ensures that internal and external process are in order	
7.	**Quality control & Assurance**	**8**	Ensuring quality process	Strictly work on ISO 9001: 2015	To ensure generated frequency of power is produced at a quality level within the control room 2. Training of her personnel	
8.	**Supply chain**	**10**	Ensuring supply chain and logistics of power plant utilities and other needed material within the system	Public procurement act (PPA) and ISO 9001: 2015 requirement	Provision of logistic and outsourcing. warehousing of power plant components	
9.	**Security**	**26**	It is hired to ensure secure place against terrorist	Strictly work on ISO 9001: 2015	Ensuring the security of the entire system and training of her personnel	

Table.2: *Objectives of the Hydropower plant departments. [Source – Hydro power plant Management]*

7.1.3 Security

The physical security is divided into two with the outside perimeter been guarded by Army personnel and other affiliated units. The second entry point is guarded by a private security outfit.

CCTV camera is positioned at every important or sensing unit in the facility.

Intelligent sensors are applied from power source to sensor detector and next signal conditional processing unit and transformed into an electronic or visual unit which is mounted at each or various units.

7.2 THREATS AFFECTING THE ELECTRIC POWER CRITICAL INFRASTRUCTURE

The hydropower plant is exposed to threats that are both internal and external and range from technology, processes, and implementation. Cyber Interdependency is vital to the proper functioning of the entire grid thus encompassing the highest level of vulnerability.

Threats are broadly categorized into three groups as shown in Table.3;

1. External threats (Global): This group of threat exists naturally throughout the entire world. Anthropogenic threats are war/conflict-related threats.
    I. Climatic threats relate to changes in climate and it's resulting impacts such as global heating, drought, precipitation, rising sea-levels, floods, hurricanes, and blizzards.
    II. Raw Material Threats refers to the natural resources used in the operation EPCI
2. External threats (Regional): These are threats that impact on regional level ranging from natural to human pioneered threats.
    I. Meteorological Threats refer to depletion in normal atmospheric activities resulting in; strong winds, storms, hurricanes, and snow disasters.

II. Geological Threats relates to abnormal activities in the geosphere with negative impact, such as earthquakes, volcanic activity, or landslides.

III. Biological Threats refer to the spread of harmful viruses and bacteria that may cause epidemics, pandemics, or epizootics that affects the personnel handling the infrastructure.

IV. Cascading Threats are threats arising from cascading effects within a critical infrastructure system (CIS). The risk is especially related to dependent elements, specifically elements dependent on electricity power supplies [21].

V. Physical Threats are intentional anthropogenic behavior from external environments, for example, acts of terrorism or criminal activity (Morgan et al., 2012). Examples are physical theft, physical loss, physical damage, injury, and threat.

VI. Cyber Threats are related to the deliberate disruption of information and communication systems in a critical infrastructure element. Examples are; Data breaches, Ransomware, Information leakage, Cyberespionage, Identity theft. The most famous case in recent years was the cyber-attack on Ukraine's energy network (Knake, 2017). [22]

3. Internal threats: This group of threats comprises threats arising from processes, technology, and personnel.

I. Process and Technology Threats include the technological breakdown of the affected elements, for example, radiation accidents, dangerous chemical leaks, extensive civil engineering disruptions, and water-distribution and water resource-related accidents.

II. Personnel Threats are situations when an employee or other authorized person is a risk factor. These threats can be further categorized into unintentional and intentional (Morgan et al., 2012). Unintentional Personnel Threats include an insufficient awareness of security, insufficiently qualified personnel, or human error. The most famous example is the Chernobyl nuclear power plant accident in 1986, which occurred as a result of the insufficiently attempted and inadequately competent personnel (NEI, 2015). By contrast, intentional personnel threats are, for example, personal enrichment, revenge, or achieving ulterior goals (i.e. the essence of terrorism).

	Naturogenic	Technogenic	Anthropogenic
External threats (Global)	Climatic threats Raw material threats	X	Conflict/War threats
External Threats (Regional)	Meteorological threats Geological threats Biological threats	Cascading threats	Physical threats Cyber threats
Internal threats	X	Process and technological threats	Personnel threats

Table.3: *Security threat to electric power critical infrastructure [Source: David Rehak et. al 2020]*

7.2.1 Risk Analysis of the Hydropower plant

The risk analysis was performed using a semi-quantitative approach that considers three risk components namely; asset, threat, and vulnerability. Where;

- Asset means part of the system or data relevant to the company.
- The threat is considered as the occurrence of any activity leveraging weaknesses in the system either intentionally or unintentionally to hinder confidentiality, integrity and availability of the asset.
- Vulnerability is defined as a weakness or bug that when exploited will result in a threat to the asset, leading to injury, asset loss, denial of service, or incapability of proper functioning of the asset.

Each component is assigned a value as shown in Table.4.

Numerical value	Asset value	Threat level	Level of vulnerability
0	none or non rated	unlikely or unrated	**none or non rated**
1	low	very unlikely	**low**
2	insignificant	unlikely	**insignificant**
3	middle	moderately likely	**middle**
4	high	very likely	**high**
5	very high	highly probable or certain	**very high**

Table.4: *Risk components assessment*

Equation (1) was used to calculate the risk level of the component.

The output of the risk assessment which comprises of both physical and information security is presented using SWOT analysis in Table.5a & b.

SECURITY GROUPS	RISK PRIORITIES		
Physical	**Primary**	**Secondary**	**Tertiary**
	Fire. Back power failure. Server failure. CCTV element failure. Lock system failure Software failure. Working procedures failure.	Flood. Heavy rain. Lightning. Electromagnetic radiation. Power cut Air contamination with dangerous gas. Workstation failure.	Air conditioning failure. Threats of bomb placement – by phone, e-mail. Mails and parcels with dangerous content. Use of annoying agents.

	Lack of material resources. Lack of human resources. Security service failure. Unauthorized access of a third party to the area. Technical security system elements (TSS). Destruction of cooling equipment. Destruction or retirement of permanent service.	Wiring failure. Inappropriate working procedures. Intentional damage by an employee. Impersonation of user identity. Staff sabotage. The forcible intrusion of a stranger into space. Destruction of overhead lines Blackmail of employees. Abduction of employees. Destruction of technological premises for data processing and transmission.	

Table.5a: *Physical risks observed in the Hydropower plant.*

SECURITY GROUPS	RISK PRIORITIES		
Information systems	**Primary**	**Secondary**	**Tertiary**
	Impersonation of employees by contractors/third parties. Unauthorized use of application. Introduction of destructive and harmful programs. Incorporate malicious programs. Corporate espionage. Application failure. Computer fault in network management. Network technical failure. System or network software failure.	Misuse of system resources. Computer malfunction. Memory device technical failure. Hardware maintenance Operation error. User error. Software error.	Lack of personnel.

Table.5b: *Information systems risks observed in the Hydropower plant*

7.2.2 Swot Analysis of hydropower plant

Given the risks found in the electricity power critical infrastructure, SWOT analysis was used to understand the strength, weaknesses, opportunities associated with the hydropower plant as shown in Table.6.

The powerplant was found to have security flaws from a technical point of view which encompasses regimes measures, physical security and technical security. These flaws which are represented as weaknesses and threats in Table.7 are all human-controlled, hence the need for the application of personnel security.

STRENGTH	**WEAKNESS**
• ***Location of Power plant*** • ***Skilled workforce*** • ***Layered physical security*** • ***Use of Army for outer perimeter security*** • ***Reliable Backup system*** • ***Mechanical barrier devices***	• *Climate change* • *Inadequate supply of input resources* • *Water levels* • *Maintenance* • *Internet service provider* • *Device against eavesdropping* • *Use of known technology* • *Continues training of employee on the latest security trends*
OPPORTUNITIES	**THREATS**
• ***New technology*** • ***Integrated security system*** • ***Use of computing systems with manufacturer support***	• *Corporate espionage* • *Technology advancement* • *Arial security* • *Devices against eavesdropping* • *Susceptibility of malicious attack* • *Zero-day attack* • *Devices for physical destruction of information carriers.* • *Phishing attacks*

Table.6: *SWOT analysis of the hydropower plant.*

8 PERSONNEL SECURITY

Personnel security protects the employees, information, and assets by enabling the power-plant by:

- reducing the risk of harm to its‘ employees, customers and partners
- reducing the risk of information or assets being lost, damaged, or compromised
- encouraging confidentiality, integrity and availibilty companys‘ official or important information and assets
- promoting effecient operation and contiinous service delivery.

Table.7 is a checklist of security measures and it’s implementation level in the hydropower plant.

Controls	**Checklist**
Physical Security	
Card key Acess	Yes
Biometric technology	No
Guard services	Yes
X-Ray screening	No
Metal detector	Yes
Visitor control	Yes
Mail screening	No
Panic Button	No
Property removal/control	No
Fire safety/system	Yes
Barriers	Yes
Personnel security	
Background screening	Yes

Security awareness	No
Employee routine audit	Yes
Group Policy across units/departments	No
IT usage policy	No
Emergency Action Plan	No

Table.7: *Security control checklist in the hydropower plant*

Personnel security focusses on reducing the risks associated with insider threats [18].

A catalogue of selected personnel threats as sourced from electric companies is presented in Table.8 with their severity; Red = High; Yellow = Medium and Green = Low

Index	Risk
High	Failure to observe workflows Lack of material resources Lack of human resources Security service failures
Medium	Extortion of employees Hostage situations Employee operational error Intentional damage by employee Acquiring information about site protection measures
Low	Destruction of outdoor power transmission lines Phishing attacks Distributed denial of service

	Impersonation of third-party employees' physical identities Malicious software

Table.8: *Catalogue of personnel risks in the hydropower plant.*

8.1 Swot Analysis of personnel security risks

Based on the personnel risk assessment, SWOT analysis was performed to determine the strength, opportunities, weaknesses and threats of the powerplant as presented in Table.9.

STRENGTH	**WEAKNESS**
• ***Responsibilities, obligations, powers*** • ***Employment activity – performance conditions*** • ***Personnel management*** • ***Human resources management***	• *Staff training* • *Physical access restriction* • *Employee scrutiny* • *Security service failures* • *Employee operational error*
OPPORTUNITIES	**THREATS**
• ***Data protection agreements*** • ***Disciplinary processes*** • ***Termination of the employment relationship***	• *Destruction of outdoor power transmission lines* • *Phishing attacks* • *Distributed denial of service* • *Impersonation of third party employees' physical identities* • *Malicious software* • *Extortion of employees* • *Hostage situations*

Table.9: *SWOT analysis of the personnel risks in the hydropower plant.*

9 RECOMMENDATION OF MEASURES

The development and sustainability of every nation is in harnessing and managing its' resources both internally and externally. Critical infrastructure protection framework serves as a guide for determining, identifying, protecting and managing various sectors of the economy with prioritization. Determination of the risks associated with the key sectors is very important and the right model must be used in assessing these risks. When these risks are identified appropriate measures applicable to each sector must be implemented. The functionality of the overall structure is dependent on people from planning, implementing and maintenance.

Personnel security is of high significance to the establishment, continuous operation and productivity of the powerplant. To ensure it meets standards that can minimize risk and maximize business continuity it is important to make sure the following are in place and routinely checked based on business strategy and staff strength.

The adoption of an intergrated security system (ISS) is the most suitable approach for protection of the hydro powerplant. ISS units of application is as detailed below.

1. Physical security;
    I. Deepwater controlled alarm sensors for monitoring objects in the water.
    II. Video surveillance system (VSS).
    III. Access control systems (ACS): Logical anti-passback, timed anti-passback, area controlled anti-passback.
    IV. GPS tracking and monitoring system.
    V. Devices for the detection of substances and items.
    VI. Devices that detect and eavesdropping.
    VII. Provide an additional layer of security for computing and mobile devices used by employees.

The areas of application for some of the security devices recommended for physical security are listed below in Tables 10 and 11.

Areas of application	Location - area, object - building, space parameters
Perimeter area	External fencing
	Entrances (gateway)
	Entrances (entrance and siding gate)
	Buildings in the perimeter
Exterior	Outdoor power station energy equipment
	Parking areas inside the building with stored property
	Inputs to through cable channels
Interior spaces and buildings	Entrance (outside) doors and gates in the building envelope incl. emergency exits and entrances from through or through cable ducts
	Locking system or padlock in the entrance (outside) door and gate to the building
	Self-closing mechanism on the main entrance door to the building
	Glazed parts (doors, windows) in the building shell
	Glazed parts (cellar windows) in the building shell, which are below the level of the surrounding terrain
	Other technical openings in the building shell
	Solid ladders on the building shell leading to the roof

Table 10: Mechanical barriers.*[Source: Rehak et al., 2016; Deloitte Advisory, 2012]*

Areas of application	Location - area, object - building, space parameters
Perimeter area	External fencing
	Entrances (gateway)
	Entrances (entrance and siding gate)
	Buildings in the perimeter
	Other penetrations
Exterior	Outdoor power station
	Parking areas inside the building with stored property
	Inputs to through cable channels

	Evidence of entry in the outdoor premises of the building
	Transmission of alarm and other functional states of AS to the power control center
	Transmission of alarm and other functional states of AS to the regional supervisory workplace
Interior spaces and buildings	Entrance (outside) doors and gates in the building shell incl. emergency exits and entrances from through or through cable ducts
	Glazed parts (doors, windows) in the building envelope
	Glazed parts (doors, windows) in the building envelope accessible from accessible places (walkable cornices and roofs, ladders, balconies)
	Glazed parts (cellar windows) in the building envelope, which are below the level of the surrounding terrain
	Other technical openings in the building shell
	Solid ladders on the building shell leading to the roof
	Outgoing or through cable duct outlet (to / from the interior of the building)
	Entrance (internal) doors to the premises, respectively. rooms related to the operation of the building
	Spaces, respectively. rooms related to the operation of the building
	Spaces, respectively. rooms related to the operation (management) of the building and continuous presence of persons (permanent service)
	Interior spaces at the entrance door to the building (vestibule) and other common areas (corridors, staircases)
	Space or room with installed AS
	Evidence of entry into the building and evidence of entry into selected areas or rooms related to the operation of the building (in AS or ACS)
	Transmission of alarm and other functional states of AS to the power control center
	Transmission of alarm and other functional states of AS to the regional supervisory workplace

Table 11: Alarm systems, CCTV, ACS. *[Source: Rehak et al., 2016; Deloitte Advisory, 2012]*

2. Cyber security:

    I. Implementation of Cyber Security Risk and Compliance policy.

    II. Asset management policy.

III. Adoption of Group Management Policy.

IV. Multi-factor authentication.

V. Data loss Prevention.

VI. Proxy firewalls.

VII. Network segmentation.

VIII. Deploy the security operation unit for continuous monitoring.

IX. Logical access control.

X. Event recording and audit.

XI. Software Integrity.

XII. Data backup and shredding.

XIII. Network resilience.

XIV. System testing.

XV. Protection against harmful programs.

XVI. System management control.

XVII. Operational controls.

XVIII. Public Key Infrastructure.

XIX. Software change check.

XX. Customer Authorization

XXI. Vulnerability analysis.

XXII. Document / media checks.

XXIII. Virtualization.

XXIV. Identification and authentication.

3. Personnel security:

I. Responsibilities, duties and powers.

II. Examination of employees.

III. Information protection agreements.

IV. Conditions of work performance.

V. Staff training.

VI. Responding to security incidents and failures.

VII. Disciplinary process.

VIII. Termination of working relationship.

4. Administrative security:

I. Responsibilities, duties and powers

II. Marking and classification of documents

III. Document handling

IV. Loss of documents and their media - media

V. Administrative security in personnel changes

5. Crisis management and planning: The proposed structural and functional requirements for individual areas of crisis management and planning optimize the process of dealing with an emergency / situation in the system, while maintaining the basic functions of the selected area and their recovery.[23]

I. Personnel structure of CMS: Standard areas of responsibility and action at each level of management and planning in a selected critical infrastructure area;

i. Organization Representative for Emergency Management / Liaison Security Officer.

ii. Organization crisis management manager.

iii. Guarantor of crisis management organization for the section.

iv. Solver.

v. Employees.

II. Crisis team management level: In the event of an emergency crisis situation, increased emphasis is placed on formulating the optimal form of crisis management and dividing the management process into several levels namely;

   i. Operational level,

   ii. Tactical level,

   iii. Strategic level.

Power generation is one of the most important and vulnerable elements of critical infrastructure globally. Hence, the need for identification of vulnerable elements to ascertain the risk levels for proper implementation of the most appropriate security measures to enhance the safety and reliability of production.

Proper and timely implementation of security measures increases the redundancy of critical infrastructure thereby enhancing the socio-economic growth of the nation.

Since critical infrastructure is made up of people, technology and processes which keeps evolving for better management and efficiency, the need to keep up with the trend of new technology and better education of the people will further enhance the resilience of the critical infrastructure profer better operability and optimization of the entire system.

10 OVERVIEW OF ANALYSIS

The practical part of the thesis started with; Chapter 6, an introduction to electric power critical infrastructure with a brief description of the interdependencies; overview of the electric power system; introduction of types of vulnerabilities common to the electric power critical infrastructure. Chapter 7, a general description of the chosen hydropower plant; risk and SWOT analysis of the hydropower plant to determine the risk levels. Chapter 8, SWOT analysis was performed for risk associated with personnel in the organization as identified from previous analysis, and Chapter 9, concluded with a recommendation of security measures for the hydropower plant as a major critical infrastructure element.

CONCLUSION

The hydropower plant has been identified as one of the most important elements of critical infrastructures. After considering potential risks, personnel threat possesses the most significant threat because organization prepares for external attacks more than internal attacks making insider threat of utmost significance. This threat can lead to undesirable events that might harm the business and its' customers on a large scale. Security revolves around technology, people and processes, so it's an on-going routine that needs to be checked from planning, implementation, maintenance to back up and of the life cycle.

BIBLIOGRAPHY

[1] KATHI ANN BROWN (2006): A brief history of critical infrastructure protection in the US. *https://cip.gmu.edu/wp-content/uploads/2016/06/CIPHS_CriticalPath.pdf*

[2] KAY C. GOSS (2014): Critical Infrastructure Protection: History, Overview & Update. *https://www.domesticpreparedness.com/preparedness/critical-infrastructure-protection-history-overview-update*

[3] European Commission, Protection of critical infrastructure. *https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure.*

[4] DR. AIKATERINI POUSTOURLI ET.AL (2019): An Overview of the European Union and the United States Critical Infrastructure Protection Policies. Available online at Research gate. Retrieved on February 2019

[5] https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en.

[6] https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/

[7] https://study.com/academy/lesson/qualitative-risk-analysis-definition-purpose-example.html

[8] https://pdfs.semanticscholar.org/88d9/0381f5f2fe1f343565652eb349d5ac544454.pdf

[9] https://www.shiftcomm.com/blog/understanding-qualitative-quantitative-analysis/

[10] https://www.nasa.gov/sites/dfault/files/files/45_NASA_2015_Cost_Symposium_QRA_pitch.pdf

[11] LOUIS ANTHONY COX, JR. (2002): Risk Analysis Foundations, Models, and Methods

[12] A.V. GHEORGHE, M. MASERA, M. WEIJNEN, AND L. DE VRIES (2066): Critical Infrastructures at Risk; Securing the European Electric Power System

[13] LUDEK LUKAS, LUBOS NECESAL (2011): Measures for Critical infrastructure protection

[14] IBM Services (2019): Adapt and respond to risks with a business continuity plan (BCP) Available: https://www.ibm.com/services/business-continuity/plan

[15] SAM JONES (2019): Venezuela blackout: what caused it and what happens next? https://www.theguardian.com/world/2019/mar/13/venezuela-blackout-what-caused-it-and-what-happens-next 09/04/2020

[16] JAMES P. PEERENBOOM (2002): Identifying, understanding, and analyzing critical infrastructure Interdependencies G

[17] Kaspersky Industrial Security (2019): Cybersecurity for Electric Power Infrastructure.

[18] S.L. GBADAMOSI ET.AL (2015): Evaluation of Operational Efficiency of Shiroro Hydro-Electric Plant in Nigeria

[19] PERSONNEL SECURITY RISK ASSESSMENT, 4th Edition (2013): Centre or Protection of National Critical Infrastructure.

[20] DAVID REHAK, MARTIN HROMADA, PETR NOVOTNY (2016): European Critical Infrastructure Risk and Safety Management: Directive Implementation in Practice

[21] Armstrong's Handbook of Human Resource Management Practice: Accidental Risk Assessment Methodology for Industries in the framework of SEVESO II directive 2014

[22] CHRISTOPHER LAING, ATTA BADII, PAUL VICKERS (2013): Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection

[23] Martin Hromada, David Rehak, Neil Walker (2020):Electricity Infrastructure Technical Security

[24] LUCAS AND LEONARDO (2014): Critical Infrastructure Protection: Threats, Attacks and Countermeasures.

[25] NATIONAL ACADEMY OF ENGINEERING. CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW.

[26] CHRISTOPHER LAING, ATTA BADII, PAUL VICKERS (2013): Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection

[27] VIDRIKOVA D., BOC K., DVORAK Z., REHAK D. (2017). Critical Infrastructure and Integrated Protection. Ostrava: Association Of Fire And Safety Engineering.

[28] Deloitte Advisory. 2012. Methodology to ensure of critical infrastructure protection in the area of electricity generation, transmission and distribution. Prague: Deloitte Advisory. (in Czech) Act No. 240/2000 Coll. on Crisis Management as amended.grated Protection. Ostrava: Association Of Fire And Safety Engineering.

[29] David Rehak, Martin Hromada, Tomas Lovecek, (2020). Personnel threats in the electric power critical infrastructure sector and their effect on dependent sectors: Overview in the Czech Republic

[30] Bologna, S. et al. (2016): Guidelines for Critical Infrastructure Resilience Evaluation. Roma, Italy: Italian Association of Critical Infrastructures? Experts. 101 p. ISBN 978-88-9349-090-0

[31] Action Plan for Critical Infrastructure (2014-2017): Ottawa: Public Safety Canada. 14 p. ISBN 978-1-100-23291-1.

LIST OF ABBREVIATIONS

ACS	Access control systems
CA	Conflict Analysis
CCTV	Closed-circuit television
CI	Critical Infrastructures
CND	Council of National Defense
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CIWIN	Critical Infrastructure Warning Information Network
EU	European Union
EPCIP	European Programme for Critical Infrastructure Protection
ECI	European Critical Infrastructures
ETA	Event Tree Analysis
EDCA	Expected Damage-Cost Analysis
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
GPS	Global Positioning System
HRA	Human Reliability Analysis
Hazop	Hazard and Operability study
NCI	National Critical Infrastructures
PDD-63	Presidential Decision Directive 63
PPA	Public procurement act
QRA	Quantitative Risk Analysis
RAMCAP-Plus	Risk Analysis and Management for Critical Asset Protection
SCADA	Supervisory control and data acquisition
THERP	Technique for Human Error Rate Prediction
VA	Vulnerability Analysis
VSS	Video surveillance system

LIST OF FIGURES

LIST OF TABLES