World Academy of Science, Engineering and Technology
International Journal of Industrial and Manufacturing Engineering
Vol:9, No:10, 2015

Production Structures of Energy Based on Water Force, Its Infrastructure Protection, and Possible Causes of Failure

Gabriela-Andreea Despescu, Mădălina-Elena Mavrodin, Gheorghe Lăzăroiu, Florin Adrian Grădinaru

***Abstract*—**The purpose of this paper is to contribute to the enhancement of a hydroelectric plant protection by coordinating protection measures / existing security and introducing new measures under a risk management process. In addition, plan identifies key critical elements of a hydroelectric plant, from its level vulnerabilities and threats it is subjected to in order to achieve the necessary protection measures to reduce the level of risk.

***Keywords*—**Critical infrastructure, risk analysis, critical infrastructure protection, vulnerability, risk management, turbine, Impact analysis.

I. Introduction

THE growth as never in the history, in the last decades, of the risks, dangers and threats to the vital objectives of the states and international organizations, together with the increase of their number and vulnerabilities lead to sedimentation and defining the new concept generically called critical infrastructure.

Infrastructures represent an essential condition of human life. They are a part of the material support for civilization. They are material ways for security of human life, they define the human life style, take a part of human nature, from human reality. By this reason, the quoted European Directive gives a special attention for defining, identifying and its security [6].

The Directive considers that ICE owners/operators should be granted access, especially through specialized authorities from member states, to best practices and methodologies regarding the protection of critical infrastructures. She defines the critical infrastructures and other notions related to them, as following:

(a) Critical infrastructure means an element for maintenance of vital social functions, of health, safety, security, good social life or economical of persons and whose perturbation or destruction would have a significant impact in a member state as result of the incapacity in keeping those functions;
(b) European critical infrastructure or ECI means a critical infrastructure localized in member states, whose perturbation or destruction will have a big impact on at least two member states. The importance of impact is evaluated from the perspective inter-sectorial criteria. This includes the effect that results from inter-sectorial relationship and from dependency of other types of infrastructures;
(c) Risk analysis means significant threats scenario analyzing, for vulnerability evaluation and potential impact of perturbation or of critical infrastructures destruction [3];
(d) Sensitive information regarding critical infrastructures protection means information regarding a critical infrastructures that may be used, in case of disclosure, for planning and fulfillment of some actions that will lead to perturbation or the destruction of some critical infrastructures installations;
(e) Protection means any activity that has as purpose the assurance of functionality, continuity and critical infrastructures integrity to discourage, reduce and neutralize a threat, a risk or a vulnerable point;
(f) ECI owners/operators means those entities responsible with investigation in specific element, system or its component, designate as ECI, through direct presence and/or with its current handling [8].

Critical infrastructure owners and operators prioritize and implement risk mitigation activities based on their cost-effectiveness, feasibility, and potential for risk reduction.

Risk management actions include measures designed to deter, disrupt, and prepare for threats and hazards; reduce vulnerability to an attack or other disaster; mitigate consequences; and enable timely, efficient response and restoration in a post-event situation, whether a terrorist attack, natural disaster, or other incident [2]. The risk management approach focuses attention on that prevention, protection, mitigation, response, and recovery activities that bring the greatest return on investment, not simply the vulnerability reduction to be achieved [5].

Risk management activities also may include the means for reducing the consequences of an attack or incident. These actions are focused on mitigation, response, and/or recovery. Often it is more cost effective to build security and resilience into assets, systems, and networks than to retrofit them after initial development and deployment. Accordingly, critical infrastructure partners should consider how risk management, robustness, and appropriate physical and cyber security enhancements can be incorporated into the design and construction of new critical infrastructure and the redesign or repair of existing infrastructure [4].

Gabriela-Andreea Despescu is with the Politehnica of Bucharest, Romania (e-mail: gabriela.despescu@yahoo.com).

II. Vulnerabilities, Hazards and Threats to Critical Infrastructure in Romania

Assessment of vulnerability in relation to critical infrastructure is becoming increasingly important due to the urgent need to protect them against natural disasters, against the exploitation of technological failure, disasters caused by human factor, voluntarily or involuntarily, and against other types of interruptions that may affect these items. The vulnerability can be defined broadly as a combination of risks associated with an entity and its ability to resist and overcome internal and external emergencies [1].

In Romania, threats to physical infrastructure are all the more notable as the vulnerability of such infrastructures has increased over the years due to ineffective or inconsistent optimization in terms of physical integrity of the systems that constitute ICN (transport infrastructure numerous industrial and general built environment).

This paper seeks to address critical infrastructure risk management from an organizational perspective. Considering that this activity (risk management) is a task of prime importance in fulfilling the mission received by law component processes are analyzed in terms of effectiveness, while watching them to be updated and improved. Operator Security Plan (OSP) identifies elements of critical infrastructure (CI) and existing security solutions implemented for their protection [7].

A concrete example of this is a turbine failure.

A. Risk Assessment Based on Threat Scenarios

1. Type of Hazard / Threat

Stop the turbine operation FVM 24-158 (vertical Francis with metal casing) by breaking the metal casing.

2. Background

On the morning of February 2, 2015 after maintenance activities at both turbines were observed ruptured metal part of the turbine FVM 24-158. Cracks have developed rapidly observed, occurring phenomenon of failure and automatic shutdown of the turbine casing's operation

3. The Causes that Led to the Scenario

- Carrying out regular maintenance and repair delay.
- Failure to regular technical inspections and occasional;
- Failure program performance monitoring construction activity

4. Early Warning

- Touching the alert threshold, at which were observed occurrence of the first cracks in the metal housing is announced management plant hydropower and Dispatch area energy and national level which will announce inspectorate emergency situations and all settlements downstream of the possibility shutdown the supply of electricity;
- It will switch to power up the possibility CHE (electric generator).
-

5. Reference Incidents

- towns downstream of HPP by electricity nonfood
- towns downstream of HPP by evacuating the maximum flow allowed by the surge secondary (which is linked to the surge accumulation HPP).

6. People, Goods, and Other Systems at Risk

- In the first 30 minutes of the incident will be affected 59 households, economic and 8 social objectives. A total of 80 people with non-food electricity supply;
- After 60 minutes of incident 464 households will be affected, 10 economic and social targets and a total of 380 people with electricity non-food supply;
- 90 minutes of the incident will be affected 653 households, 25 economic social targets and a total of 590 people with electricity non-food supply.

B. Establish Probability of the Chosen Scenario

For determining the probability, it was adopted a scale (Table I):

TABLE I
Probability of Chosen Scenario

Level / Associate score	Probability determination	Periods
1 - Very low	It has a very low probability of happening. Normal measures are necessary to monitor the evolution of the event	More than 13 years
2 - Low	The event has a low probability of occurring. Further efforts to reduce the probability and / or impact mitigation.	10 – 12 years
3 - Medium	The event has a significant probability of happening. Significant efforts are needed to reduce the probability and / or impact mitigation.	7 – 9 years
4 - High	The event has a probability of happening. Priority efforts are needed to reduce the likelihood and mitigate the impact.	4 – 6 years
5 - Very	The event is considered imminent. Immediate and extreme measures are needed to protect the lens to an alternate location evacuation / safe area where impact requires.	1– 3 years

The likelihood of the chosen scenario is low (2) with a production period of 13 years.

Setting the severity of the consequences the proposed scenario

Given the gravity of the consequences are the worst levels of vulnerability and impact.

C. Vulnerability and Capabilities Analysis

TABLE II
VULNERABILITIES AND CAPABILITIES

Vulnerability and capacity	Level
1. ICN placement in terms of road traffic or pedestrian areas	Very low Low Medium High Very high
2. The level of HPP staffing	Very low Low Medium High Very high
3. The degree of specialization of HPP staff	Very low Low Medium High Very high
4. Hydroelectric power facilities with specific equipment	Very low Low Medium High Very high
5. Worn turbine	Very low Low Medium High Very high
6. The level of competence of personnel involved in the operation / maintenance of equipment, technical assistance on equipment	Very low Low Medium High Very high
7. The technological equipment and facilities status	Very low Low Medium High Very high

D. Impact Analysis

Impact analysis is an analysis of management at certain levels to identify the impact of the loss of ICN Resources. It will consider the scenario severity of all impacts and then will determine the severity of the consequences of producing hazard / threat scenario considered. It has chosen the highest level of severity levels associated impacts.

TABLE III
THE IMPACT ANALYSIS

Impacts	Level	
Potential deaths	☑ 1 – Very low	0 - 5
	☐ 2 - Low	6 – 10
	☐ 3 - Medium	11 – 15
	☐ 4 - High	16 – 20
	☐ 5 – Very high	> 21
Potential damage or damage to infrastructure within the site that provides the main utilities (transport, electricity, drinking water, communications**)**	☐ 1 – Very low	temporal
	☐ 2 - Low	Significant damages
	☐ 3 - Medium	medium damages
	☐ 4 - High	high damages
	☑ 5 – Very high	Very high damages
Potential damage to equipment or property damage of those to whom services are provided by ICN concerned(public, commercial, private**)**	☑ 1 – Very low	0 – 10%
	☐ 2 - Low	11 – 20%
	☐ 3-Medium	21 – 30%
	☐ 4 - High	31 – 40%
	☑ 5 – Very high	More than 41%
Potential damage or environmental damage	☑ 1 – Very low	0 – 20%
	☐ 2 - Low	21 – 40%
	☐ 3 - Medium	41 – 60%
	☐ 4 - High	61 – 80%
	☐ 5 – Very high	peste 81%
Potential social impacts	☐ 1 – Very low	0 – 10%
	☐ 2 - Low	11 – 20%
	☐ 3 - Medium	21 – 30%
	☑ 4 - High	31 – 40%
	☐ 5 – Very high	

Level and associate score	Severity of consequences
☐ 1 – Very low	The event produces a minor disruption in activity without damage.
☐ 2 - Low	The event cause minor material damage and disruption activity limits.
☑ 3 - Medium	Product Injuries staff, and / or some loss of equipment, facilities and delays in service delivery.
☐ 4 - High	Serious injuries of personnel, significant loss of plant equipment and facilities, delays and / or denial of service.
☐ 5 – Very high	The consequences are catastrophic resulting in deaths and serious injuries of personnel, major loss of equipment, installations and facilities and cease providing the service.

TABLE IV
CALCULATING THE RISK LEVEL

PROBABILITY			Very high 5				
			High 4				
			Medium 3				
			Low 2			turbine turn off	
			Very low 1				
			0	V.low1	Low 2	Medium 3	High 4	V. high 5
Risk Level calculated	Level	Score	GRAVITY CONSEQUENCES				
	V. low	1-3					
	Low	4-6					
	Medium	7-12					
	High	13-16					
	V. high	17-25					

Note: The risk is given by the product of the probability of a hazard / threat and severity of the consequences.

Calculated risk has a **value of 8** (Severity 4 x Probability 2) therefore there is a risk of producing medium chosen scenario. **Turbine turn off** has serious consequences "High" (value 4) while the probability of the scenario chosen is "Low" (value 2).

E. Risk Treatment

To reduce the risk reduction measures to be taken the vulnerabilities and/or capabilities (Table V):

TABLE V
PROPOSED MEASURES

Vulnerability and/or capability	Proposed measures
HPP facilities with specialized equipment	- verification of existing equipment and the degree of wear - Installation of reliable and resistant to corrosive media
Condition of technological equipment	- checking the status of equipment and technological system - installation of new technological equipment

Protection of critical infrastructure consists of all the measures established to reduce risks unlocking operation or destruction of a critical infrastructure.

After applying measures to reduce the risk resulting:

TABLE VI
RESULTS

Vulnerability identified		After applying measures
HPP facilities with specialized equipment	Very low	Very low
	Low	Low
	Medium	Medium
	High	High
	Very high	Very high
Vulnerability	**Identified**	**After applying measures**
Condition of technological equipment and facilities	Very low	Very low
	Low	Low
	Medium	Medium
	High	High
	Very high	Very high

TABLE VII
RECALCULATING THE SEVERITY OF THE CONSEQUENCES

Level and Related score	The severity of the consequences
1 – Very low	The event produces a minor disruption in activity without damage.
2 - Low	The event cause minor material damage and disruption activity limits.
3 - Medium	Product Injuries staff, and / or some loss of equipment, facilities and delays in service delivery.
4 - High	Serious injuries of personnel, significant loss of plant equipment and facilities, delays and / or denial of service.
5 – Very high	The consequences are catastrophic resulting in deaths and serious injuries of personnel, major loss of equipment, installations and facilities and cease providing the service.

TABLE VIII
THE RISK LEVEL AFTER ABATEMENT MEASURES

PROBABILITY			Very high 5				
			High 4				
			Medium 3				
			Low 2		**turbine turn off**		
			Very low 1				
			0	Very low 1	Low 2	Medium 3	High 4	Very high 5
Calculated risk level	Level	Score	**GRAVITY CONSEQUENCES**				
	V. low	1-3					
	Low	4-6					
	Medium	7-12					
	High	13-16					
	V. high	17-25					

Risk recalculated has a **value of 4** (Severity 2 x Probability 2) therefore there is a low risk of producing treated chosen scenario. **Turbine turn off** has serious consequences "Low" (value 2) while the probability of the scenario chosen is "Low" (value 2).

TABLE IX
PREVENTION, CONTROL AND MITIGATION

Vulnerability and/or capability	Proposed measures
CHE facilities with specialized equipment	- execution injections to restore sealing veil -checking existing equipment and their degree of wear - installation of reliable and resistant to corrosive media
Condition of equipment and technologic system	- checking the status of equipment and technology - Installation of new technological equipment

III. CONCLUSION

As well as protected critical infrastructure will always have a high degree of vulnerability, as a rule, are the first target when seeking to destabilize and even destroy a system or a process. The identification, optimization, and securing critical

infrastructure is an undisputed priority for managers of systems and processes.

To reduce the risk has proposed measures to reduce vulnerabilities and / or improvement of capabilities.

ACKNOWLEDGMENT

The work has been funded by the Sectorial Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU 187/1.5/S/155420.

REFERENCES

[1] Cohen. F., *What makes critical infrastructures Critical?,* International Journal of Critical Infrastructure Protection, 2010

[2] Antonioni, G., Spadoni, G. and Cozzani, V., *A methodology for the quantitative risk assessment of major accidents triggered by seismic events,* Journal of Hazardous Materials, 2007.

[3] *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, February 2003.

[4] *Role of Dams on the development and management river basins*, Bulletin 149, Commission Internationale des Grands Barrages, Paris 2014.

[5] *Gheorghe ILIE,* Revista de Stiinţe Militare, "Protecţia infrastructurilor critice în corelaţie cu strategia de securitate naţională. Coordonarea cu acţiunile Alianţei Nord-Atlantice si Uniunii Europene", Nr. 2 (19), 26 May 2010.

[6] Cf. Hotărârii Guvernului nr. 762/2008 *pentru aprobarea Strategiei naţionale de prevenire a situaţiilor de urgenţă*.

[7] ARION, Stelian, Protecţia infrastructurilor critice - managementul securităţii la nivelul deţinătorilor şi al operatorilor (www.revista-alarma.ro), Retrieved data: 05/12/2008.

[8] Directive 114/2008 of the European Union Council.