Industrial Risk Management of a Combined Cycle Power Plant

Inês Heitor Frazão Ferreira

Instituto Superior Técnico – Universidade Técnica de Lisboa
Av. Rovisco Pais, 1049-001 Lisboa, Portugal

Abstract

In order to cope with the changing business environment due to the liberalization of the electricity market in Portugal and Spain and the change of power purchase agreements, EDP Produção intends to improve its technical and financial performance by implementing an Integrated Risk Management System. Therefore, EDP Produção has considered the areas of occupational and environmental risks and asked an external party to carry out a risk assessment study.

This paper presents the methodology used for the risk assessment of EDP's Ribatejo Power Plant, in Portugal, and the development of a risk treatment plan.

In this context, concepts are reviewed and some methods of risk assessment are presented. A recognized risk management process is also presented. A risk assessment analysis was carried out, leading to the development of a risk treatment plan where mitigating measures are dealt with, considering some criteria and the available resources of Ribatejo Power Plant.

Key-words: Industrial risk, risk assessment, mitigating measures, risk treatment, plan.

Introduction

Along the years, EDP Produção has been revealing a constant concern with environmental and safety aspects. In this context Environment Management Systems and Prevention and Safety systems were implemented in a single system called Integrated Environmental and Safety Management System (SIGAS). The purpose of this system is to enable EDP's Power Plants to achieve a better conformity between Environmental and Safety objectives.

In order to cope with the changing business environment and to promote SIGAS improvement, an integration of the Industrial Risk Management System has become indispensable.

To develop the Industrial Risk Management System, EDP Produção asked an external party to carry out a study concerning industrial risks.

The purpose of this project was to work as a pilot project, in order that the applied methodologies could be extended to other EDP's power plants and in the limit to the whole of EDP Produção.

The external party carried out a risk assessment of the electricity production process of EDP's Ribatejo power plant and analyzed an agreed set of prioritized risks. Related to the risks, mitigation actions were determined with their risk reduction effects. This was done by bringing together appropriate EDP personnel and contractors with the external party consultants.

On completion of the risk assessment study, the external party presented a final report to EDP. Following this report EDP Produção felt the need to do further work in this field.

Consequently, the goal of the work described in the present paper was to analyze the risk assessment report and develop a risk treatment plan for the industrial risks of Ribatejo power plant.

Concepts and Theory

Risk management is a key business within both the private and public sector around the world. Sound and effective implementation of risk management is part of best business practice at a corporate and strategic level as well as a means of improving operational activities.

In a power plant, risk management is not only about avoiding or reducing the chance of something going wrong, but is also about taking the opportunities to improve electricity production performance.

The meaning of risk

The risk represents the uncertainty and its impact. The uncertainty all alone doesn't lead to risk. Is the uncertainty simultaneously with the impact of the consequences that create risk events.

Hull (1992) asserts that, in a general way, risk can be described as the probability of occurrence of an unexpected event (P) times the severity of the consequences of that event (C),

$$R = P \times C \qquad [1]$$

The risk can also be represented graphically, having the probability on an axis and the severity of the consequences on the other axis.

It is also very common to represent risk by means of a risk matrix, where the level of risk is ranked based on the probability and on the severity of the consequences (Coelho, 2007).

The next figure shows an example of a risk matrix.

		Probability				
		A	B	C	D	E
Severity	I	1	1	2	3	4
	II	1	2	3	4	4
	III	2	3	4	4	5
	IV	3	4	4	5	5

Severity:	Frequency:	Risk:
I = Low	A = High unlikely	1 = Low
II = Medium	B = Unlikely	2 = Medium
III = High	C = Sometimes	3 = High
IV = Very High	D = Often	4 = Severe
	E = Very often	5 = Very severe

Figure 1 Risk Matrix

The ALARP principle

The elimination of all risks is an impossible task. Thus, companies strain continuously to achieve the maximum safety as possible.
Therefore, to make effective and sustainable investment decisions, companies should create criteria and boundaries to delineate levels of risk admissibility.

The simplest risk criterion separates risks that need treatment from those which do not. However, a common approach is the ALARP principle (As Low As Reasonably Practicable) (AS/NZS 4360:2004).

The ALARP principle divides risks into three bands:

a) The upper band where adverse risk are intolerable whatever benefits the activity may bring, and risk reduction measures are essential whatever their cost;
b) The middle band where costs and benefits are taken into account and opportunities balanced against potential adverse consequences, called ALARP region);
c) The lower band where risks are negligible, or so small that no risk treatment measures are needed.

The next figure illustrates the ALARP concept.

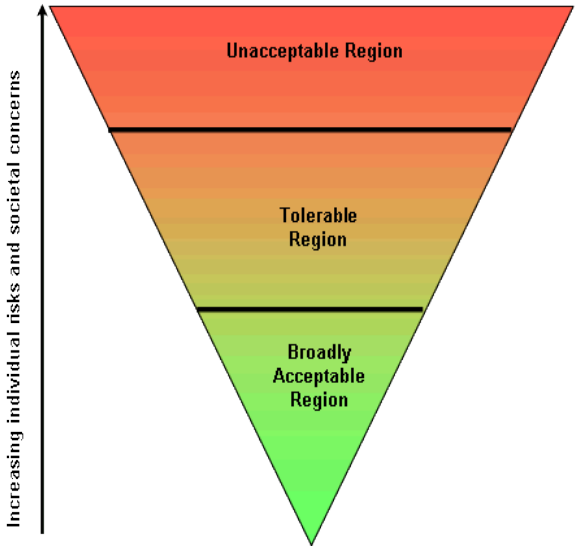

Figure 2 The ALARP Principle

Risk Management Process Overview

Risk management is a complex process. A survey of the existing literature shows that different authors have different definitions for the phases of the risk management process. Therefore, in the context of this work a key reference was chosen, the AS/NZS 4360:2004 of Standards Australia/Standards New Zealand, and the definitions used come from this source.

Risk management is an interactive process of continuous improvement that ideally should be embedded into existing practices.

The main elements of the risk management process are the following:

a) *Communicate and Consult*
   Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole;
b) *Establish the context*
   Establish the context external, internal and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis defined;
c) *Identify risks*
   Identify where, when, why and how events could prevent or degrade the achievement of the objectives;
d) *Analyse Risks*
   Identify and evaluate existing controls. Determine consequences and probabilities and hence the level of risk. This analysis should consider the range of potential consequences and how these could occur;
e) *Evaluate risks*
   Compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and the nature of treatments required and about priorities;
f) *Treat risks*
   Develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs;
g) *Monitor and review*
   It is necessary to monitor the effectiveness of all steps of the risk management process. This is important for continuous improvement.

Risk Assessment Methods

Preliminary Risks Analysis (PRA)

The PRA is a semi-quantitative method for hazard identification and analysis. It is frequently used in the design phase of a system to identify the risks that could emerge in the operational phase and hence to define safety requirements.
It is also very useful in the operational phase when reviewing systems, because it allows the detection of hazards that were unnoticed (Aubry, Bied-Charreton, & Mazouni, 2007).
The aim of this analysis is to identify the hazards that could lead to unexpected and undesirable events, produce accident scenarios and define the risk of the system.

Hazard And Operability Technique (HAZOP)

HAZOP is a method for hazards identification. Its methodology is based on guide words which allow developing diverse scenarios.

This method tries to identify operability or safety problems related to deviation of some parameters or variables of the process.

It considers the normal function of an equipment or process and analyzes all possible deviation scenarios.

Fault Tree Analysis (FTA)

FTA follows a deductive methodology, determining all the faults that can lead to an undesirable event, called top event.
The logical relations are represented in the form of a tree. Starting with the top event, its causes or the combination of causes that could generate it are determined.

Event Tree Analysis (ETA)

ETA is a logical and inductive method that is used to identify the possible consequences of an undesirable event.
An event tree is built starting with the undesirable event and identifying all the possible consequences that event could generate. The sequence of consequences created could represent or not a possible accident (Barata, Soares, & Teixeira, 2001).

Failure Mode, Effetcs and Criticality Analysis (FMECA)

FMECA is a method that aims to analyze the frequency of the failure modes of a system and its consequences, to identify the existing safeguards and, when the risk is high, to define mitigating measures.

The methodology followed by FMECA is described below:

1. Study the system analyzing all the existing information;
2. Identify the failure modes, its causes and consequences;
3. Quantify the frequency, the severity of consequences and the probability of the safeguards fail;
4. Define the levels of tolerability of the risk;
5. Determine mitigating measures;
6. Quantify the residual risk.

The risk can be classified using a risk matrix (figure 1) or RPN.
The RPN is calculated as shows the next equation.

$$RPN = F \times P \times C \qquad [2]$$

Where,

F : Frequency of the failure mode;

P : Probability of the current safeguards fail;

C : Impact of the consequences that may result.

FMECA allows the identification of problematic areas and possible failure modes of an installation and the need of corrective actions, helping management on decision making (Wei, 1991).

Case study

This paper presents the methodology used for the risk assessment of EDP's Ribatejo Power Plant, in Portugal, and the development of a risk treatment plan.

Ribatejo Power Plant

It is a Combined Cycle Power Plant with three units of 392 MW each. The fuel is natural gas.
Power is provided to the grid at a voltage of 220 kV (unit 1) and 400 kV (units 2 and 3).

Risk Assessment Plan

Risk assessment analysis aims to identify and quantify the risks and to determine mitigating actions for its decrease or elimination.

To achieve this goal, a risk treatment plan should be developed.

The risk treatment plan developed for Ribatejo Power Plant includes information about risk analysis method, systems, people involved, risk quantification method, levels of risk tolerability, and type of mitigating measures.

The risk assessment method used was FMECA. The risk identification and analysis has been done through workshops bringing together subject matter experts of EDP and contractors. The workshops were facilitated by a person selected by the external party who is very familiar with risk assessment methods and capable of managing the group interaction.

The following systems were analyzed:

- Gas turbine;
- Boiler;
- Feed water system and steam system;
- Condensate system;
- Cooling system;
- Steam turbine;
- Generator;
- Fuel supply;
- Water supply and disposal;
- Power transmission and auxiliary power supply;
- Instrumentation & control;
- Grid and distribution system;
- Sampling systems;
- Ancillary system, in particular stationary compressed air supplies and fire protection system;
- Emergency auxiliary generator plant.

For each item a value from 1 to 7 was adopted, as the following tables show.

Table 1 Numbers used for frequency

Failure Mode	Frequency	Number used in the risk assessment
Highly unlikely to occur	Once per 10 000 years or less	1
Unlikely to occur	Once per 1000 years	2
Occurs occasionlly	Once per 100 years	3
Occurs sometimes	Once per 10 years	4
Occurs regulary	Once a year	5
Occurs often	10 times a year	6
Occurs very often	100 times a year or more	7

Table 2 Numbers used for safeguards fail

Current safeguard	Probability per demand	Number used in the risk assessment
Failure of four safeguards or more	0,0001	1
Failure of three safeguards	0,001	2
Failure of two safeguards	0,01	3
Failure of one safeguards	0,1	4
Event noticed but consequence is dificult to prevent in time	0,2	5
Event noticed by accident and safeguard taken	0,5	6
No safeguard at all	1	7

Table 3 Numbers used for impact of consequences

Consequence	Number used in the risk assessment
Minor	1
Less E-production or emergency shutdown or earlier or longer outage	2
Unit trip	3
Accelerating event, no E-production for a couple of days	4
Machine damage or no E-production for longer time	5
Reputation loss, extensive machine damage	6
People wounded, death, impact o n the surroundings	7

Three levels of risk were defined:

i. *High risks*: risks higher than or equal to 60, i.e., measures must be taken;

ii. *Intermediate risks*: risks lower than 60 but higher than or equal to 30, i.e. measures may be taken depending on the involved cost and the risk reduction effect;

iii. *Low risks*: risks lower than 30, i.e. no measures are needed.

The mitigating measures suggested by the external party in the the risk assessment study can be divided into:

- Technical measures;
- The application of already existing procedures/policies;
- The creation of new procedures or policies;
- Measures on maintenance and checks;
- Measures on keeping awareness on new or increased risks;
- Making agreements with external parties;
- Other actions.

Results of Risk Assessment

Risk assessment analysis was able to identify 320 risks, of which 33 were classified as high, 167 as intermediate and 120 as low.

For the intermediate risks an indirect trade off was made during the workshops between the risk reducing effect of a measure and the roughly estimated costs involved in its implementation, leading to either accepting the risk or implementing that measure.
The intermediate risks were classified into two types: tolerable risk or non tolerable risk.

A number of recommendations of mitigating measures were derived.

The risk assessment report suggests further study on risks that were high and for which the measures appeared not to be effective enough to reduce them.

The risk assessment also revealed a number of failure modes, which do not have high risk, but whose risks may increase in time if attention for maintenance is fading.

Risk Treatment Plan

The aim of the Risk Treatment Plan was to establish priorities to implement the best possible arrangement of treatments.

In order to define treatment priorities, two criteria were established:
Criterion 1 – The basis of this criterion is the value of RPN. It says that all high risks must be treated as soon as possible. The other risks follow criterion 2;

Criterion 2 –This criterion is based on the nature of the mitigating measures. The intermediate risks that are not tolerable have higher priority than the other. Within the tolerable risks the ones that have more efficient mitigating measures have higher priority.

a) Mitigating measures that reduce an intermediate and non tolerable risk to a low risk have higher priority;
b) Next, the risks with mitigating measures that reduce the risk from intermediate and non tolerable to intermediate and tolerable should be treated;
c) Then the risks with mitigating measures that reduce the risk just a little and the level of risk stays intermediate and non tolerable should be treated.

EDP Produção and the external party decided that tolerable risks don't need mitigating measures because those risks are to be accepted hence it was decided to exclude intermediate tolerable risks and low risks from the risk treatment plan.
Thus, Ribatejo Power Plant needs to implement 151 mitigating measures to treat 106 risks, 33 high risks and 73 intermediate risks.

However, it is impossible to analyze 33 risks at the same time hence to develop the treatment plan it was necessary to prioritize them based on RPN.

The next steps were followed to create the risk treatment plan for Ribatejo power plant:

1. Select from the risk assessment report all information related to high and intermediate risks;
2. Identify the resources available;
3. Create assumptions of the plan;
4. Prepare the plan;

For each measure the need for human resources was identified using a dichotomous scale. The equipment resources were defined using the same method.

The time needed to implement a measure is most of the time conditioned by some factors that lead to delay. Thus the time required to implement a mitigating measure is represented bellow.

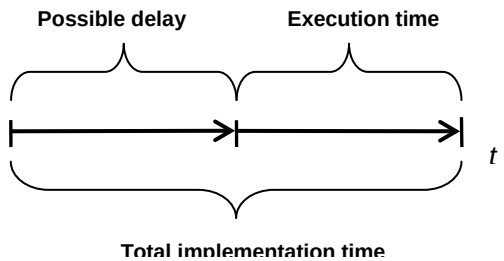

Figure 3 Implementation time

Factors that could delay the implementation of the measures are: the need for a unit outage, the delivery time of materials, problems that can occur on the supply of material, e.g. equipment is already discontinued, and the inefficient communication between people.
To define the time required was created the following scale.

Table 4 Time scale

Scale	Time
+	Up to 1 month
+ +	From 1 month to 1 year
+ + +	More than 1 year

The financial resources scale is based on the level of delegated competence.

Table 5 Cost scale

Scale	Delegated Competence	Cost of investment
NA	Director of Ribatejo power plant	Low cost, no investment
€	Director of Ribatejo power plant	Less than 50 000€
€ €	Director of EDP power production	Between 50 000€ and 250 000€
€ € €	Executive Board	More than 250 000€

Three types of assumptions were defined: cost, human resources and time.

Cost assumptions:

- At maximum three measures with a cost of € € € can be implemented in the same year;
- At maximum six measures with a cost of € € can be implemented in the same year;
- At maximum twelve measures with a cost of € can be implemented in the same year;
- The total cost can't exceed twelve "€", for example, if three measures of € € € are planned to be implemented, three measures of € or two of € € and one of € can also be implemented in the same year;
- Measures that don't need investment (NA) don't have cost limitation;
- The total cost of a measure is imputed at the beginning of the implementation;
- The measures with higher cost have higher priority.

Human resources assumptions:

- At maximum six teams can work at same time;
- Teams only work at the execution phase, assuming that a possible project phase will be done by an external party.

Time assumptions:

- The unit outages match the final of four-month periods;
- Three outages are done in a period of a year for each unit a major outage and two minor outages;
- The measures that require unit outage have higher priority.

The next phase was to prepare the plan by defining how to represent the measures and their required resources.

Two plans were developed: a *priority plan* and a *time plan*.

In the priority plan measures are arranged according to risk priority. This plan is of importance to management.

In the time plan measures are distributed in time and do not reflect the priority of the risks. The recipient of this plan is the general commissioner who allocates tasks to employees.

Results of the Risk Treatment Plan and Future Work

According to the developed plan, the time required to implement all the mitigating measures is of four years and one month. In the beginning of fourth year all high risks are treated.

The measures with higher cost (€ € €) are planned to be implemented in the first three years.

Human resources are best optimized. Six teams work at same time all months.

For future work, a detailed cost-benefit analysis for intermediate risk is suggested.

Another risk assessment analysis for the risks whose measures were inefficient and stayed at the same level is also suggested.
Following health and safety at work legislation, consulting of employees and their representatives is recommended.
In conclusion, EDP should analyze if the treatment objectives are being achieved and if the treatment plan is being efficient.

The developed plan will allow Ribatejo power plant to eliminate and reduce some of industrial risks with resource's optimization.

Hence, industrial risk management is extremely important in the power production process since it enables power plants to achieve a higher performance, creating a safer place to work and respecting the environment and society.

References

AS/NZS 4360:2004. *Risk Management Guidelines - Companion to AS/NZS 4360:2004.* Zealand, Standards Australia/Standards New.

Barata, J., Soares, C. G., & Teixeira, A. P. (2001). Curso de Especialização em Segurança e Higiene no Trabalho - Análise de Riscos. IST.

Coelho, J. M. (2007). A Matriz Harmonizada de Risco - O "Canivete Suiço" dum Sistema Integrado de Gestão do Risco Industrial. In P. Antão, C. G. Soares, & A. P. Teixeira (Ed.), *Riscos Públicos e Industriais* (pp. 269-286). Lisboa: Edições Salamandra.

Hull, K. (1992). Risk Analysis Techniques in Defence Procurement. *Proceedings of IEEE Colloquium on Risk Analysis Methods and Tools, 3 de Junho*, (pp. 3/1 - 317).

Bibliography

Kletz. (1992). *Hazop and Hazan - Identifying and Assessing Process Industry Hazards* (3.ª edição ed.). Institution of Chemical Engineers, Rugby, UK.

Rausand, M. (2005a, Outubro 7). Retrieved from http://frigg.ivt.ntnu.no/ross/slides/fmeca.pdf

Rausand, M. (2005b, Outubro 7). Retrieved from http://frigg.ivt.ntu.no/ross/slides/pha.pdf

Rausand, M. (2005c, Outubro 7). Retrieved from http://frigg.ivt.ntnu.no/ross/slides/hazop.pdf

Rausand, M. (2005d, Outubro 7). Retrieved from http://frigg.ivt.ntu.no/ross/slides/eta.pdf

Wei, B. C. (1991). A Unified Approach to Failure Mode, Effects and Criticality Analysis (FMECA). *Proceedings of Reliability and Maintainability Annual Symposium, 29 - 31 January*, (pp. 260 - 271).