A LOPA APPLICATION TO THE HYDROGEN COOLING SYSTEM OF THE MAIN ELECTRIC GENERATOR OF A NUCLEAR POWER PLANT

Flavia. M. Vasconcelos, flaviamvasconcelos@gmail.com
P. F. Frutuoso e Melo, frutuoso@con.ufrj.br
COPPE/UFRJ – Programa de Engenharia Nuclear, Caixa Postal 68509, 21945-970 Rio de Janeiro, RJ, Brasil

P. L. Saldanha, saldanha@cnen.gov.br
Coordenação de Reatores – CODRE/CNEN Rua General Severiano, 90 – Sala 421, 22294-900, Rio de Janeiro, RJ, Brasil

Abstract. *The Layer of Protection Analysis (LOPA) is a powerful analytical tool for assessing the adequacy of protection layers used to mitigate risks in a process plant. LOPA applies semi-quantitative measures to evaluate the frequency of potential incidents and the probability of failure of protection layers. This paper presents an application of the Layer of Protection Analysis technique to a nuclear power plant in order to evaluate the cooling system of an electric generator, so as to identify scenarios that might lead to a plant shutdown. Next, the frequencies of occurrence of these events and the probability of failure on demand of the independent protection layers are determined. Here a difficulty is related to the lack of failure and initiating event data. The consequences identified are listed as impact events and are classified as to their severity level. The initiating causes are listed for each impact event and the likelihood is estimated for each initiating cause. Independent Protection Layers (ILPs) are listed. The mitigated event likelihood is studied and additional ILPs can be evaluated and added to reduce the risk. As a conclusion, LOPA demonstrated that the hydrogen inner-cooling electric generator system is in compliance with the risk scenarios adopted for this study. Some suggestions were made in order to automate some manual actions to increase the system reliability.*

Keywords*: LOPA, Hydrogen Cooling, Main Electric Generator, Nuclear Power Plant*

1. INTRODUCTION

The Layers of Protection Analysis (LOPA) is a powerful analytical tool for assessing the adequacy of protection layers used to mitigate risks in process plants. LOPA applies semi-quantitative measures to evaluate the frequency of potential incidents and the probability of failure of protection layers. One advantage of this approach is the fact that a plant survey as to risk can be quickly obtained, so that critical scenarios can be readily identified. In many instances, a formal quantitative risk analysis, or a probabilistic safety assessment (as this technique is usually named in the nuclear field) is not available, so that applying LOPA can be a useful step towards a more effective decision making, Alves (2007) and Vasconcelos (2008).

LOPA provides specific criteria and restrictions for the evaluation of independent protection layers (IPLs), eliminating the subjectivity of qualitative methods at substantially less cost and time than fully quantitative techniques.

This paper presents an application of the LOPA technique to the cooling system of the electric generator of a nuclear power plant, in order to identify scenarios that can lead to a plant shutdown. Next, the frequencies of occurrence of these events and the probability of failure on demand of the independent protection layers are determined. Here a difficulty is related to the lack of failure and initiating event data. LOPA, as applied to chemical process plants, normally employs recommend industry data. The application to the hydrogen system revealed the lack of data for performing the analysis. Different data banks were used and this issue must be properly addressed if LOPA is to be of use outside the chemical process industry. Using LOPA the risks of each scenario were estimated and it was checked whether additional safeguards were necessary to mitigate the risk.

Generator cooling is required to remove the heat produced by electrical losses resulting from the large currents flowing through the generator conductors. As the generator electrical output ratings increase, additional heat is generated and must be removed through the use of effective cooling systems, in this case, hydrogen inner cooling. Compared with air, hydrogen is preferred as the cooling fluid. It has excellent thermodynamic and heat transport properties, is lighter than air, and is 10 to 20 times more efficient as a cooling medium than air. One important shortcoming of hydrogen cooling is the explosive mixture formed by hydrogen and air over a wide range of hydrogen concentrations. Therefore, seals are provided at the boundaries of the generator frame to prevent hydrogen leakages.

2. LOPA – LAYERS OF PROTECTION ANALYSIS – CASE STUDY

The primary purpose of LOPA is to determine whether there are sufficient layers of protection against an accident scenario. Many types of protective layers are possible as illustrated in Fig. 1. A scenario may require one or many protection layers depending on the process complexity and potential severity of a consequence. For a given scenario, only one layer must work successfully for the consequence to be prevented. However, since no layer is perfectly effective, sufficient protection layers must be provided to render the risk of the accident tolerable.

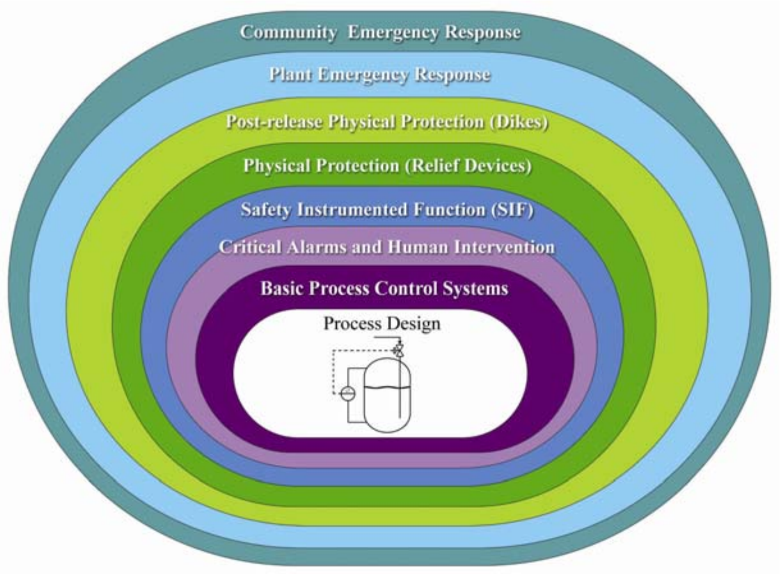
Community Emergency Response
Plant Emergency Response
Post-release Physical Protection (Dikes)
Physical Protection (Relief Devices)
Safety Instrumented Function (SIF)
Critical Alarms and Human Intervention
Basic Process Control Systems
Process Design

Figure 1: Layers of defense against a possible accident.

LOPA is limited to evaluating a single cause-consequence pair as a scenario. Once a cause-consequence pair is selected for analysis, the analyst can use LOPA to determine which engineering and administrative controls (often called safeguards) meet the definition of IPLs, and then estimate the risk of the scenario. The results can then be extended to make risk judgments and to help the analyst decide how much additional risk reduction (additional IPLs) may be required to reach a tolerable risk level. Some of the LOPA benefits are:

- LOPA helps solve conflicts in decision making by providing a consistent, simplified framework for estimating the risk of a scenario and provides a common language for discussing risks.
- LOPA provides a means of comparing risks from unit to unit or plant to plant, if the same approach is used throughout the company.
- LOPA provides more defensible comparative risk judgments than qualitative methods due to the more rigorous documentation and the specific values assigned to frequency and consequence aspects of the scenario.
- LOPA can be used to help an organization decide whether the risk is “as low as reasonably practicable” (ALARP), which may also serve to meet specific regulatory requirements.
- Information from LOPA helps an organization decide which safeguards to focus on during operation, maintenance, and related training.

The limitations imposed on LOPA result in a work process that is much less complex than quantitative risk analysis, while generating useful, somewhat conservative, estimates of risk. LOPA can be divided into the steps described below, Summers (2003) and CCPS (2001):

- Step 1: Identify the consequence to screen the scenarios.
- Step 2: Select an accident scenario.
- Step 3: Identify the initiating event of the scenario and determine its frequency.
- Step 4: Identify the IPLs and estimate the probability of failure on demand of each IPL.
- Step 5: Estimate the risk of the scenario by combining the consequence, initiating event, and IPL data.
- Step 6: Evaluate the risk to reach a decision concerning the scenario.

3 CASE STUDY

Since a mixture of hydrogen and air is explosive over a wide range of proportions, the design of the machine and specified operating procedures are such that the explosive mixtures are not possible under normal operating conditions. Under normal operating conditions the hydrogen purity is maintained at 95% or greater by volume, which is well outside the hydrogen-air explosive range. The generator gas system has the following main functions: (a) to provide means for safely putting hydrogen into or taking hydrogen out of the generator, using carbon dioxide as the scavenging medium; (b) to maintain the hydrogen gas pressure in the generator at the desired level; (c) to provide indication to the operator at all times of the condition of the machine with regard to gas pressure, gas temperature, gas purity and if liquid is present in the machine; and (d) to dry the gas and remove any water vapor which might get into the machine from the seal oil.

The operation of the generator gas system includes five separated steps: (1) replacing air with carbon dioxide; (2) replacing carbon dioxide with hydrogen; (3) replacing hydrogen with carbon dioxide; (4) replacing carbon dioxide with air; and (5) maintaining hydrogen gas in generator while in operation, Westinghouse (1984).

This application of LOPA to a nuclear power plant is based on the original work of CCPS (2001), however some adaptations were made to consider typical features of the system to be analyzed.

An initiating event is an event that creates a disturbance in the plant and has a potential to lead to damage, depending on the successful operation of the various plant mitigating systems. Initiating events are grouped into three general types: external events, equipment failures, and human failures. Initiating events can be the result of various underlying root causes such as external events, equipment failures, or human failures. Root causes are not the same as initiating events, and care should be taken to avoid going too far into root causes in identifying initiating events.

A scenario requires the identification and documentation of all important steps for an event from the initiating event to the consequence. Each factor that can affect the calculation of its frequency or consequences must be documented. This is important to keep the link between a specific initiating event, a specific consequence and the specific ILPs.

The first step is the identification of the consequences of each scenario, for which a qualitative analysis must be performed. The most common technique for this purpose is HAZOP, IEC (2001). The consequence (including its impact) is evaluated and its magnitude is estimated. Each step of the process is evaluated. All possible deviations of normal operating conditions (and how they can occur) are listed and the measures to detect the possible deviations that can lead to hazardous events or operability problems are identified, ABNT (1997). The results of scenario 1 will be presented and discussed in detail.

The general expression for the initiating event frequency evaluation of a scenario (number of events per year) with a specific consequence is displayed in Eq. (1). For this scenario, the initiating event frequency is multiplied by the product of the probability of failure on demand of all ILPs (PFD).

$$f_i^C = f_i^I \times \prod_{j=1}^{J} PFD_{ij} = f_i^I \times PFD_{i1} \times PFD_{i2} \times \ldots \times PFD_{ij} \qquad (1)$$

where

f_i^C frequency for consequence *C* for initiating event *i*;

f_i^I initiating event frequency for initiating event *i*;

PFD_{ij} probability of failure on demand of the *j*-th IPL that protects against consequence *C* for initiating event *i*.

The result of Eq. (1) can be used as an input for comparing the calculated risk to scenario risk tolerance criteria for decision-making, CCPS (2001).

- **Step 1:** Identification of the consequence to screen the scenarios.

Tab. 1 presents the results of the HAZOP study for the Hydrogen Cooler System, which generated 10 possible deviations. The magnitudes of the consequences are estimated in Tab. 2 (CCPS, 2001).

Table 1: HAZOP for the Generator System

Item	Deviation	Cause	Consequence	Protection
1	High hydrogen temperature	Failure in hydrogen cooler	Explosion	Automatic control valve and panel alarm
2	High hydrogen pressure	Failure of reduction pressure valve	Rupture / leakage	Panel alarm
3	Air entrance in generator	Failure of seal oil system	Explosion	Seal oil system
4	Low hydrogen pressure	Pressure control valve failure	Hydrogen leakage	Panel alarm
5	Small crack in the generator	Air entrance	Hydrogen leakage	-
		Vibration		
		Corrosion		
6	High contaminant concentration (liquid)	Gas drier failure	Corrosion/ hydrogen flux problems / insulator flashing	Liquid detector
		Drain valves failures		
		Heat exchanger tube rupture		
7	High hydrogen consumption	Small crack in the hydrogen line	Leakage	Panel alarm
8	Less carbon gas flow	Valve partially opened	Frozen gas in line	Human protection
9	High carbon gas temperature	Fire below carbon gas cylinder	Explosion	Safety valve
10	High carbon gas pressure	Fire below carbon gas cylinder	Explosion	Safety valve

Table 2: Consequence Categorization

Consequence Characteristic	Magnitude of Loss			
	Spared or non essential equipment	**Plant outage < 1 month**	**Plant outage < 1 to 3 months**	**Plant outage > 3 months**
Mechanical damage to main generator	Category 2	Category 3	Category 4	Category 5
Mechanical damage to auxiliary systems of main generator	Category 2	Category 2	Category 3	Category 4

- **Steps 2 and 3:** Selection of an accident scenario and identification of the initiating event of the scenario and evaluation of its frequency.

The accident scenario is made by a single cause-consequence pair only. The scenarios for this study are presented in Tab. 3. The initiating event frequency data are obtained from ANSI/IEEE (1984), OREDA (2002), CCPS (2001) and Lees (1996).

Table 3: Scenarios for LOPA application and initiating event frequencies

Scenario	Initiating Event	Consequence
1	Failure in hydrogen cooler f = 1.47 / 10^6h = 1.29x10^{-2} / year	Explosion
2	Failure of reduction pressure valve f = 2.11 / 10^6h = 1.85x10^{-2} / year	Rupture / hydrogen leakage
3	Failure of seal oil system f = 6.82x10^{-4} / year	Explosion
4	Failure of pressure control valve f = 30 / 10^6h = 2.63x10^{-1} / year	Hydrogen leakage
5	Vibration causing small cracking in the generator f = 3.33 / 10^6h = 2.92x10^{-2} / year	Hydrogen leakage
6	Failure in generator seals f = 1x10^{-1} / year	Hydrogen leakage
7	Failure in gas drier f = 0.52 / 10^6h = 4.56x10^{-3} / year	High liquid concentration inside generator
8	Failures in drain valves f = 5.09 / 10^6h = 4.46x10^{-2} / year	High liquid concentration inside generator
9	Heat exchanger tube rupture f = 1 / 10^6h = 8.76x10^{-3} / year	High liquid concentration inside generator
10	Small crack in hydrogen line f = 1 / 10^6h = 8.76x10^{-3} / year	Hydrogen leakage
11	Valve in carbon gas line partially opened f = 1x10^{-4} / year	Frozen gas in the line
12	Fire in carbon gas cylinder f = 0.90 / 10^6h = 7.88x10^{-3} / year	Explosion

- **Steps 4, 5 and 6:** Identification of the IPLs and estimation of the probability of failure on demand of each IPL, estimation of the risk of the scenario by combining the consequence, initiating event, and IPL data and evaluation of the risk to reach a decision concerning the scenario.

For these scenarios, the ILPs depend on the operator action through an alarm indication in the operator panel. Only the gas dryer has interlocks that can trip the generator due to high temperature and start the standby seal oil pump automatically. Tab. 4 presents the IPLs for each scenario and their PFDs, taken from CCPS (2001) and IEC (1998). The scenario risk evaluation is performed by using Eq. (1) and Tab. 5 (similar to Tab. 8.1 from CCPS (2001) with some adaptations).

The values of the PFDs for the ILPs of scenario 1 are: 1x10^{-1} for automatic valve of water flow and 1x10^{-1} for operator action in response to high temperature alarm. In this step, the risk must be calculated using Eq. (1) for the scenario frequency, considering that all protection fails. The results are presented in Tab. 6.

Table 4: Individual Layers Protection and its Probability Failure in Demand

Scenario	IPLs	PFD
1	Automatic actuation of water flow valve	1x10^{-1}
	Operator action due to high temperature alarm in the operator panel	1x10^{-1}
2	Operator action due to high pressure alarm in the operator panel	1x10^{-1}
3	Standby seal oil pump starts automatically	1x10^{-1}
	Operator action to start seal oil pump due to a low pressure signal	1x10^{-1}
4	Operator action due to low pressure indication	1x10^{-1}
5	Operator action due to high hydrogen consumption	1x10^{-1}
6	Standby seal oil pump starts automatically	1x10^{-1}
	Operator action to start seal oil pump due to a low pressure signal	1x10^{-1}
7	Operator action due to liquid high level in the liquid detector	1x10^{-1}
8	Operator action due to liquid high level alarm in the liquid detector	1x10^{-1}
9	Operator action due to liquid high level alarm in the liquid detector	1x10^{-1}
10	Operator action due to H_2 low pressure alarm	1x10^{-1}
11	Operator action due to CO_2 low pressure alarm	1x10^{-1}

Table 5: Risk Matrix with Individual Action Zones

Frequency of consequences (per year)	**Category of Consequences**				
	1	**2**	**3**	**4**	**5**
$10^{-1} – 10^{-0}$	Optional (evaluate alternative)	Optional (evaluate alternative)	Action at next opportunity	Immediate action	Immediate action
$10^{-2} – 10^{-1}$	Optional (evaluate alternative)	Optional (evaluate alternative)	Optional (evaluate alternative)	Action at next opportunity	Immediate action
$10^{-3} – 10^{-2}$	No further action	Optional (evaluate alternative)	Optional (evaluate alternative)	Action at next opportunity	Action at next opportunity
$10^{-4} – 10^{-3}$	No further action	No further action	Optional (evaluate alternative)	Optional (evaluate alternative)	Action at next opportunity
$10^{-5} – 10^{-4}$	No further action	No further action	No further action	Optional (evaluate alternative)	Optional (evaluate alternative)
$10^{-6} – 10^{-5}$	No further action	No further action	No further action	No further action	Optional (evaluate alternative)
$10^{-7} – 10^{-6}$	No further action	No further action	No further action	No further action	No further action

Scenario 1 results

Scenario 1 was considered the most significant one among the ten scenarios considered. It comprises the failure of the hydrogen cooler that can cause high hydrogen temperatures inside the main generator and has an explosion as a consequence. Due to this consequence, the system has an interlock that automatically starts a valve to control the hydrogen temperature. The results of LOPA indicate one more IPL. This IPL is a new redundant automatic valve to control the hydrogen cooler temperature. The results are shown in Tab. 6.

Table 6: Scenario 1 – Summary Sheet

Scenario Number **1**	Equipment Number **Generator H_2 Cooling System**	Scenario Title **Failure of hydrogen cooling resulting in explosion of generator**	
Date	Description	PFD	Frequency (/year)
Consequence (Description / Category)	Explosion of generator as a result of high temperature of hydrogen **Category 4**		
Initiating Event	Failure of hydrogen cooling		1.29×10^{-2}
Frequency of mitigated consequence			**1.29×10^{-2}**
Independent Protection Layers			
BPCS			
Human intervention		1×10^{-1}	
SIF	automatic valve	1×10^{-1}	
Total PDF for all IPLs		**1×10^{-2}**	
Frequency of mitigated consequence			**1.29×10^{-4}**
Risk Tolerance Criteria Met? (Y/N): Optional			
Actions Required to Meeting Risk Tolerance Criteria: Additional safety instrumented function, as an example another automatic valve to control the hydrogen cooler temperature.			
Notes			

4 CONCLUSIONS

When a PSA is unavailable, LOPA provides fast results for the fire risk quantification, facilitating the decision making and providing insights of the fire protections impact.

LOPA demonstrated that the hydrogen inner-cooling electric generator system is in compliance with the risk scenarios adopted for this study. In the scenario evaluated, some suggestions were made in order to automate some manual actions to increase the system reliability.

The application of LOPA to a nuclear plant is simple and can be performed in every compartment where safe reactor shutdown equipment is present. This technique is recommended in areas where the complexity of PSA is not applicable. LOPA can still be extended to other situations related to risk-informed decision making, e.g., the evaluation of project modifications, plant emergency response planning, events evaluation and classification, etc.

An updated database is extremely necessary for the performance of probabilistic analyses. The database must take into account specific data from Brazilian nuclear power plants or even similar plants, to replace generic data from other databases and sources, thus reducing the analysis uncertainties.

3. REFERENCES

ABNT (1997), *Brazilian Norm NBR 14009-1997: Machine Safety – Principles for Risk Evaluation (in Portuguese),* Brazilian Association of Technical Standards, Rio de Janeiro, RJ, Brazil.

Alves, C. L. (2007), *An Application of the Layer of Protection Analysis (LOPA) to the Fire Hazard Analysis of Shutdown Cable Routes of a Nuclear Reactor (in Portuguese).* M.S. Dissertation, COPPE/UFRJ, Rio de Janeiro, RJ, Brazil.

ANSI/IEEE (1984), *Standard 500-1984: Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear Power Generating Stations,* Institute of Electrical and Electronic Engineers, Piscataway, NJ, USA.

CCPS (2001), *Layer of Protection Analysis, Simplified Process Risk Assessment,* American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, USA.

IEC (1998), *International Standard IEC 61508-1998: Functional Safety of Electrical / Electronic / Programmable Electronic Safety – Related Systems*. International Eletrotechnical Commission, Zurich, Switzerland.

IEC (2001), *International Standard IEC 61882-2001: Hazard and Operability Studies (HAZOP Studies) – Application Guide*, International Eletrotechnical Commission, Zurich, Switzerland.

Lees, F. P. (1996), *Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control*. 2nd edition, Butterworth-Heinemann, London, UK.

OREDA (2002), *Offshore Reliability Data Handbook*. 4th edition, SINTEF Industrial Management, Trondheim, Norway.

Summers, A. E., (2003), "Introduction to Layers of Protection Analysis", *Journal of Hazardous Materials*, v. 104, pp. 163-168.

Vasconcelos, F. M. (2008), An Application of Layers of Protection Analysis (LOPA) to the Risk Evaluation of the Hydrogen Cooling System of the Main Electric Generator of a Nuclear Power Plant (in Portuguese). M.S. Dissertation, COPPE/UFRJ, Rio de Janeiro, RJ, Brazil.

Westinghouse (1984), *The Westinghouse Pressurized Water Reactor Nuclear Power Plant*, Westinghouse Electric Corporation Water Reactor Division, Pittsburg, Pennsylvania.

4. RESPONSIBILITY NOTICE

The authors are the only responsible for the printed material included in this paper.