CHEMICAL ENGINEERING TRANSACTIONS
VOL. 77, 2019
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Genserik Reniers, Bruno Fabiano

ISBN 978-88-95608-74-7; **ISSN** 2283-9216
DOI: 10.3303/CET1977153

The Benefits of Different Risk Assessment Methods Used for Power Plants

Sari Kojo*, Ville Manninen

Wärtsilä Finland Oy, Puotikuja 1, FI-65101 Vaasa, Finland
sari.kojo@wartsila.com

In power plants delivered by Wärtsilä the risk assessment methods used are Hazid, Hazop, LOPA, FMEA, FTA, FERA and QRA. The methods are chosen e.g. depending on the scope of supply for the project and customer requirements. In addition to these the EU product safety legislation is fulfilled by using EN ISO 12100 for machinery risk assessment. All the methods draw their own pictures of risks identified and ways to mitigate them. Only when all the pictures are united the risk reduction can be seen to be sufficient. Through these risk assessments the biggest risks for health, environment and asset are identified and mitigated with protective measures.
In the power plant delivery projects several stakeholders are involved whose requirements needs to be taken into account. The goal of the risk assessment used as well as its limits has to be clearly defined and streamlined through the process. One of the most important factors is the consistent risk evaluation. Hazop and LOPA has been done for Wärtsilä standard design by using Wärtsilä Risk Matrix. In delivery project the customer often wishes to use their own risk matrix and then project wise Hazop and LOPA´s are done together with customer. The risk evaluation may become difficult, if there is a wish to use different evaluation methods by different parties. The risk assessment methods should be therefore agreed in the contract in detailed enough level.

1. Introduction

Engine driven power plants are very good option as a back-up for wind and solar energy. Because of their fast ramp up capabilities they can quickly recover the system, if wind is not blowing or sun is not shining. Full efficiency can also be reached by using several engine-generator sets and one by one they can be started to produce energy efficiently. Wärtsilä engines provide the means to produce energy with the help of auxiliary systems. The processes in engine driven power plant are relatively simple in their control philosophy. Engine driven power plants are in between machinery industry and process industry in their complexity and functionality. While the Hazid, Hazop and LOPA are focusing the deviations of the process the EN ISO 12100 is focusing on man-machine interface. Risks are more effectively identified and mitigated through good combination of risk assessment methods. It is important to choose right risk assessment method as well as keep the analysis within the limitation of the method. This fact is sometimes forgotten, and risk assessment method is used for analyzing a risk that cannot be identified and mitigated with such a method.
The auxiliary systems have different purposes in power plant, where fuel system is providing fuel to the engine. The fuel characteristics creates their own features to design process and risk scenarios. Methane is lighter than air. However, if fuel consists of heavier hydrocarbons it becomes heavier than air. These aspects need to be considered in layout design. Fuel leakage and their effect to layout design needs to be evaluated during Hazid, which is followed by FERA and QRA. Norani A. A. et al., 2017 have used in their BERA (Basic Event Ranking Approach) quantitative approach in evaluating the probability of scenario happening.
The LFO driven engines are used e.g. nuclear power plants emergency diesels and their ability to have high reliability and availability can be utilized there. The nuclear operators in Finland are using PRA probabilistic risk assessment based on fault tree analysis. As an emergency diesel supplier needs to do FMEA for the design as well as FTA for reliability and availability. Through those analysis the possible weaknesses of the

Paper Received: 28 February 2019; Revised: 17 April 2019; Accepted: 21 June 2019

Please cite this article as: Kojo S., Manninen V., 2019, The Benefits of Different Risk Assessment Methods Used for Power Plants, Chemical Engineering Transactions, 77, 913-918 DOI:10.3303/CET1977153

design can be spotted and redesigned. One of the most important findings is lack of redundancy in vital elements of the system.
There is a clear goal in delivery projects risk assessments to reach level of safety, both in customer and Wärtsilä side. Many customers have their own risk matrix which is used in Hazop analysis to clarify which scenarios are transferred to LOPA. Wärtsilä has made Hazop and LOPA studies for our concept designs, in those analysis Wärtsilä own risk matrix is used. Wärtsilä risk matrix includes risks for the environment, safety and asset. Especially in asset determination customer has their own scale and those vary from project to project. One good example is oil rig emergency power plant. The lost production of oil rig causes huge costs even in short period of time (minutes). IEC 61882 standard is applied to Wärtsilä power plants Hazop studies.

2. Limits of Risk Assessment

When risk assessment method is chosen, then the limits of risk assessment needs to be defined. In Hazop the limits are clearly defined as described in IEC 61882 and if additional limitations are needed they should be documented. Especially difficult is to determine human error and which types of them are included to the risk assessment.
In EN ISO 12100 before starting risk analysis it is important to determine limits for use, space and time. Specific attention needs to be taken to determine reasonably foreseeable misuse. Even the experts have difficulties to determine what is reasonably foreseeable misuse. At least a misuse, that company already has an experience of has to be considered. As important it is to determine intended use in a detail level using EN ISO 12100 limitations for use, space and time. When intended use is clearly defined, then everything else in unintended and can be handled as misuse.

3. Risk evaluation

Risk includes in its determination likelihood/probability and severity of the consequence. Evaluation of probability can be based on quantitative data or qualitative estimations. The reliability quantitative data is not always available for specific installations and therefore qualitative is more often used. However qualitative probability estimation is mainly based on participants experience.
Severity of harm to humans, asset or environment needs to be separately evaluated and the scale needs to be calibrated to suit to industry area and company´s state of the art.
One of the challenges is keeping the risk evaluation systematic. There is a clear need of precise risk evaluation documentation order to have correlative probabilities for similar risk scenarios. Systematic approach is especially difficult in probability evaluation, if the scenario has never happened, but it still seen foreseeable.
Quantified risk estimation consists of the mathematical calculation, as accurately as possible with the data available, of the probability of a specific outcome occurring during a specific duration of time. Risk is often expressed as the annual frequency of the death of an individual. Quantified risk estimation allows the
calculated risk to be compared with criteria that can be related back to an actual number of deaths per year or accident statistics. It allows risk reduction measures to be evaluated in terms of by how much they reduce the risk so that the most cost-effective solution can be chosen. Unlike qualitative methods that estimate the risk from each hazardous situation separately, quantified risk estimation is generally used to estimate the total risk from all sources to an individual. (EN ISO 14121-2)
Quantitative risk evaluation requires resources and data and ability to evaluate how data is used for different scenarios. Understanding the nature of basic events is essential in succeeding to have good outcome. This has been recognized also by Norani et al. 2017.
Quantified risk estimation is very resource-intensive and requires considerable skill to be conducted successfully. It requires a detailed and comprehensive model of the chain of events that lead to the defined outcome and is dependent on the quality of data for base events such as the failure of a piece of equipment or the probability of human error. Quantified risk estimation can be subjective and prone to error.
To reduce some of the burden of starting with a blank sheet of paper, and in order to improve consistency, eliminate some of the subjectivity and to reduce error, guided quantified risk estimation methods are available. An example of a guided quantified tool is given in A.6. (EN ISO 14121-2)

4. Hazard and Operability Analysis (HAZOP)

The HAZOP, which is a process hazard analysis methodology, is based on standard IEC 61882. It is based on a theory that assumes risk events are caused by deviations from design or operating intentions. HAZOP is a brainstorming study where a group of experts gather together and work under a chairman’s, called as a

facilitator, instructions at the HAZOP workshop. After the workshop, the facilitator will prepare a report of the HAZOP study.

At the HAZOP study, the design of the processes is checked systematically by considering deviations from the design intent. The causes and consequences of hazardous events are identified, and the adequacy of existing safeguards is considered. If such safeguards don't exist, actions are considered to remedy the situation.

Hazards under consideration in the study are divided to Health, Asset and Environmental hazards. The valuation of the mentioned aspects is calibrated project vice based on the plant purpose (base load/peaking/emergency).

Parameter	Guideword	Causes	Consequences	Safeguards	Health/Safety			Environment			Asset			Recommendations	Responsibility	Comments
					L	C	Risk	L	C	Risk	L	C	Risk			
Flow	No	1. Isolation valve closed or spurious closure of ESD valve upstream of LFO feeder pump or pilot fuel feeder pump.	No flow, high pressure scenario. Overpressure exceeding 8 barg (due to screw pump). Burst of pipe and loss of containment. Possible fire and potential for fatalities.	Internal relief Relief valve downstream the transfer pump.	3	4	U							8. To evaluate a second barrier for overpressure scenario by blocked outlet from PAF901 LFO Transfer Pump.		

Figure 1: Example of Hazop scenario

ID:		Tag no:	Future SIF	P&ID:		C&E:	
Scenario/ hazardous event:	Overpressure of segment downstream LFO transfer pump unit, based on blocked outlet from LFO transfer pumps. No flow, high pressure scenario. Overpressure exceeding 8 barg (due to screw pump). Burst of pipe and loss of containment. Possible fire and potential for fatalities.						
Event Type:	Safety						
Event Consequence:	Multiple fatalities						
Severity Level (Category):	5	Several fatalities					
Risk Acceptance for Event:	0.00002						

Safety Function Loop:	
Safety Function Trip Action:	

	Type	Tag no.
Initiators:		
Final elements:		

Initiating Causes

Ref.	Description	Freq. (/yr.)	Tag	Comments
A	Safety valves closes spuriously	0.01		Automatic valves upstream feeder pumps closing.
B	Operator well trained with no stress - Routine operation	0.1		Fails to open isolation valve after pump switching.
C	Blocked filter	0		Blocked filter is not a cause, as blockage will damage internals only.
D	BPCS instrument loop failure	0.1		Failure of pump speed control

Independent Protection Layers

Ref.	Description	PFDavg	Tag	Comments
1	Relief valve	0.01		Internal pump relief.
2	Relief valve	0.01		Relief valve downstream automatic filter

Conditional Modifiers

Ref.	Description	PFDavg	Tag	Comments
6	Occupancy	1		Not credited
7	Ignition probability unstabilised oil 1 to 50 kg/s (semi	0.05		Assumed semi-confined and between 1-50 kg/s.

PFDavg calculation

Initiating Cause	Freq. (/yr.)	Independent Protection Layers and Conditional Modifiers										Total
		1	2	3	4	5	6	7	8	9	10	
A	0.01	0.01	0.01				1	0.05				0.00000005
B	0.1	0.01	1				1	0.05				0.00005
C	0	0.01	0.01				1	0.05				0
D	0.1	0.01	0.01				1	0.05				0.0000005
E												0

Total Mitigated Event Frequency, Fe/yr.	0.00005055
Required PFDavg of SIS, Ft/Fe	0.395647873
Required SIL	No SIL requirement, but risk reduction is required
Required risk reduction	2.5275

Figure 2: Example of SIL allocation with LOPA for Hazop example in Figure 1

The focus of the HAZOP study is in the operation and maintenance phases of the plant. All foreseen abnormal disturbances of the plant operation are looked at. Examples are process disturbances and natural forces. On purpose harming or terrorist attacks to plant are not part of the scope of the study since they are security issues and not relevant in HAZOP study. In order to succeed in performing a proper HAZOP study, there should be participants from different disciplines to cover all the areas of expertise.
Hazop scenarios that require risk mitigation, or their probability can be decreased through control system design are transferred to LOPA for further analysis.

5. Layer of Protection Analysis (LOPA)

Layer of protection analysis is one of the methods presented by IEC 61511 for safety integrity level (SIL) assessment. It is semi-quantitative method and commonly used in the process industry where it is originally developed. Its purpose is to analyse, if the existing safeguards are adequate for risk mitigation or if additional safeguards are needed. Other purpose is to allocate safety integrity requirements for the existing safety instrumented functions.
Intention in risk mitigation should be to remove the risks primarily with inherently safe design. Mechanical safeguards and other protective measures should be introduced before the safety control system. The safety control system with a SIL rated protective functions should be the last resort.
LOPA begins with identifying the initiating event(s) / cause(s) with their frequencies for the specific hazard that is analyzed as presented in the following example. Next the safeguards applicable for the risk mitigation are listed which were identified in the Hazop and probabilities of failure on demand set for each. If applicable, also the conditional modifiers, like occupancy or ignition probabilities for different amount of fuel type, can be used but this needs to be carefully considered since this has significant impact on the result. After all the data is applied, calculation of the risk is performed. If there is multiply iniating causes these are combined together and total frequency is shown as result. If the risk is in acceptable level, no further recommendations are necessary but if there is a gap for acceptable risk level, additional risk reduction measures would need to be considered. There is an example of LOPA in Figure 2.
Franco Antonella et al., 2016 has also identified a connection between risk assessment methods and used fault tree analysis as a way to allocate SIL with FMEDA.

6. Risk graph

The requirements of EN ISO 12100 are based on EU machinery directive. The approach in EN ISO 12100 is in its simplicity to clarify the tasks operator has to do during the life-cycle of the machinery and evaluate the risk per task including to the evaluation possibility to avoid or limit the harm, probability of occurrence as well as duration of hazard zone. This approach in combination with EN ISO 13849 will then determine machinery´s PL levels. EN ISO 14121-2 represents several options for risk evaluation, if risk graph method is used it doesn´t allow you to take full credit of your safeguards, especially if the harm for the user is death. Example of risk graph from EN ISO 14121-2 is shown in Figure 3. Therefore choosing between risk graph and risk matrix is a task that requires consideration and knowledge of the nature of the risk itself. However EN ISO 14121-2 also gives you opportunity to use quantitative method similar to LOPA.

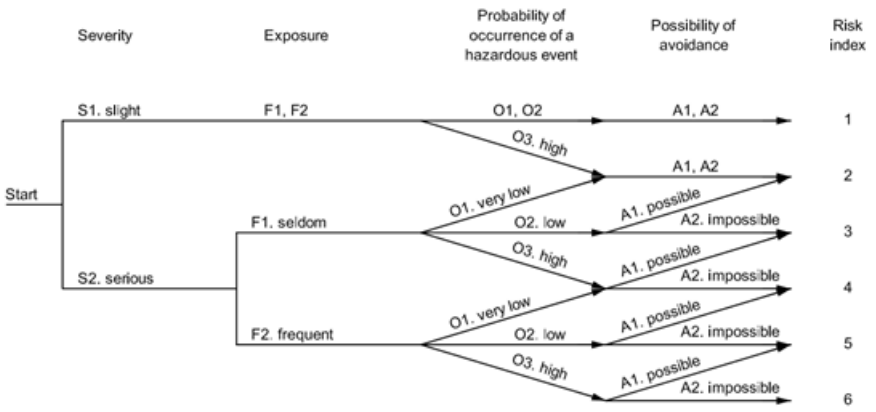

Figure 3: Example of risk graph – (EN ISO 14121-2 Figure A.3)

In machinery safety the “principles of safety integration” is describing the priority order of risk reduction process. The three steps are called as “protective measures implemented by the designer”. Steps are shown in figure 2 of EN ISO 12100. First step is to reduce the risks is by inherently safe design measures, second step by safeguarding and complementary protective measures and third step by information for use (instructions and warnings). Inherently safe design can only be reached, if the risk assessment is the basis of design.

Most challenging in delivery projects risk evaluation is to find the way to suit the company´s own risk categories to customers risk categories. If the approach to evaluate is too different and calibration of risk graph or matrix is not done, it will create contradiction and high risks might be identified even though they don´t exist in practice.

From smaller to middle sized companies there is not necessarily own product safety expert and then it depends the counterparties ability to comprehend risk evaluation process. The focus should be optimized risk reduction and risk evaluation used should support it. When the risk graph is not calibrated correctly, then risks are identified to be relevant even though they are irrelevant. In addition to that it may endanger the risk prioritizing itself.

7. Human error

The way to analyze human error has changed over time. There was earlier an idea that human reliability can be estimated quantitatively, but current understanding is that human behavior is too complicated to get reliable human error probabilities (Rausand M., 2011) However, if a hazardous scenario includes human error possibility it has to be analyzed with methods developed especially for it. One way of mitigating human error is to try to change the design to inherently safe. Human error probability varies a lot in different sources as is shown in Tables 1 and 2.

Table 1: Probability of human error (EN ISO 14121-2 Table A.17)

Error probability	Heading 2
$1{,}0*10^{-4}$	Routine, good feedback with time to make use of it, good appreciation of hazard
$3{,}0*10^{-3}$	Routine, simple
$1{,}0*10^{-2}$	General error of omission
$1{,}0*10^{-1}$	Non-routine, complicated
$1{,}0*10^{-1}$	High stress, time constraint 30 min
$9{,}0*10^{-1}$	High stress, time constraint 5 min
$1{,}0*10^{0}$	High stress, time constraint 1 min
$1{,}0*10^{0}$	Error in second step, having already erred in first

Table 2: Generic guideline data Kirwan B. (1994) Table 11.1

Description	Human-error probability
Operator error – (Non-Routine Task, Low Stress)	$1{,}0*10^{-1}$
Operator error – (Non-Routine Task, High Stress)	$3{,}0*10^{-1}$
Operator failure (to execute routine procedure, assuming well trained, unstressed, non fatigued)	$1{,}0*10^{-2}$
Well trained operator, no stress, independent verification (e.g. LOTO procedure)	$1{,}0*10^{-3}$
Operator well trained with stress – Routine operation performed at least once per month	$1{,}0*10^{0}$
Operator well trained with no stress – Routine operation performed at least once per month	$1{,}0*10^{-1}$

Human error can be further analyzed with e.g. Action Error Analysis. Understanding the human error is its own field of study and one should not underestimate the importance of human error.

8. Conclusions

Every risk assessment method gives their own view of analyzing and mitigating risks. When several methods are used the risk mitigation covers not only one but several ways. If only one method is used some of the risks remain uncovered because the analysis method itself is restricting of finding it. Hazop used alone is giving answers to process deviations, but is not good method of analyzing e.g. man-machine interface. FTA is analyzing the chain reaction behind the risk and leads the way to root cause. In addition to Hazop or FTA an FMEA could be used if a more detailed analysis of fault finding is needed. Regardless of chosen risk

assessment method, it is vitally important to limit the analysis. Limiting will ensure that the method actually fits to its purpose and focuses to risks that can be identified with the method.
It is important to use international standards as basis of risk assessment, which enables to have more standardized solutions that fit to different market areas and their accepted level of safety. ALARP (as low as reasonably practicable) is a determination which is not easy to implement in practice. There has to be clear limitations and acceptance criteria to claim ALARP.
In power plant delivery project there are several stakeholders involved. Notified bodies, external consultants also participate to most of the projects. They have different roles per country even in Europe. In Finland it is possible to ask also authority´s interpretation of sufficient risk reduction and get official statement of acceptable solution. When the contact to authority level is not so straightforward a consultant can help to adjust the design to meet local requirements.
Risk evaluation method can be challenged by customer and an additional iteration of evaluation loop needs to be done. In the best case the risk evaluation can be adjusted and recalibrated to include both energy sector specific risks as well as the additional risks arising from customers field of industry or location of site.

References

Antonello F. et al. Reliability Analysis and Risk Analysis: Integration between Hazop, FMEDA and Fault Tree Analysis for SIL Assessment. Aidic. Chemical Engineering Transactions, Vol 48, 2016
Kirwan Barry, 1994, A Guide to Practical Human Reliability Assessment. Taylor &Francis Ltd, 4 John St, London WC1N 2ET, UK, 379
Norani A.A., Ahmad A., Khalil M.A.R., Al-Shanini A., 2017, Risk-based interventions for safer operation of a hydrogen station, Chemical Engineering Transactions, 56, 1387-1392
EN ISO 12100:2010. Safety of machinery. General principles for design – Risk assessment and risk reduction.
IEC 61511-3: Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels. Annex F.
IEC 61882. Hazard and operability studies (HAZOP studies) – Application guide
ISO/TR 14121-2:2007. Safety of machinery – Risk assessment. Part 2: Practical guidance and examples of methods.
Rausand M., 2011, Risk Assessment. Theory, Methods, and Applications. John Wiley & Sons, Inc., Hoboken, New Jersey.