What is Risk and What is Safety?

Per Hellström[a]
[a] Swedish Radiation Safety Authority, Stockholm, Sweden

Abstract: IAEA tells us that safety analyses shall be performed and that they shall use both deterministic and probabilistic methods. However, already the deterministic safety analyses use probabilistic information, i.e. the frequencies of events that challenges the Defense-in-Depth and that the plant need to survive, of course for availability reasons, but also for safety. So the analysis identifies impacts from disturbances and scenarios to come up with the basic functional requirements and the related success criteria, and in addition also input to the environmental qualification – we want the SSCs in the functions to survive to do their job. Then of course also we want to have certain availability and reliability of operating as well as safety systems. From a deterministic point of view, we achieve this by meeting requirements like the single failure and diversity criteria. These criteria imposes e.g. the use of redundancy and diversity. A deterministic analysis (logical) can be used to demonstrate redundancy and diversity, however a probabilistic analysis can provide the additional reliability information.

This paper will elaborate on what is safety analysis based on deterministic and probabilistic methods, the difference and sometimes confusion that is created. So what are the relations between the safety analysis (deterministic) and a safety analysis (probabilistic). Does the latter really exist or is it indeed a risk analysis? It is anyway used to risk inform decision making, at least it is expected that risk information is used to support a graded approach, both at the plant, but also regulators supervision activities are expected to use resources in a graded fashion that focus resources where we get the most of the buck.

Some further questions that will be elaborated are the fundamental differences between the requirements to analyze safety (and risk), difference between Probabilistic safety analysis and probabilistic Risk analysis), how we maintain and improve safety using risk information (or safety information)?

Keywords: PSA, PRA, Risk Management, Graded approach.

1. INTRODUCTION

IAEA tells us that safety analyses shall be performed and that they shall use both deterministic and probabilistic methods. However, already the deterministic methods many times use probabilistic information, i.e. the frequencies of events that challenges the Defense-in-Depth and that the plant need to survive, of course for availability reasons, but also for safety. So the analysis identifies impacts from disturbances and scenarios to come up with the basic functional requirements and the related success criteria, and in addition also input to the environmental qualification – we want the SSCs in the operational and safety functions to survive to do their job. Then of course also we want to have certain availability and reliability of operating as well as safety systems. From a deterministic point of view, we achieve this by meeting requirements like the single failure and diversity criteria. These criteria imposes e.g. the use of redundancy, diversity and separation. A deterministic analysis can be used to demonstrate redundancy and diversity, however a probabilistic analysis can provide the additional reliability information.

Safety usually implies some margin in design to be confident that things will go well even in case of rather serious disturbances. Safety is also a term with various interpretation and even more the term "risk" is not always used in a stringent way. We want plants to be safe (enough) and we want to use risk management approaches supported by risk assessment techniques to support a graded approach using limited resources in a cost effective way. In my view, safety and risk are different animals and safety

analysis is not necessarily the same thing as a risk analysis, even if we often say that probabilistic safety analysis and probabilistic risk analysis are expressions that can be used interchangeably. This is what is discussed in this paper.

2. WHAT IS SAFETY AND WHAT IS RISK?

2.1. What is Safety?

Some definitions of Safe and safety from Swedish thesaurus:

Table 1: Definitions of Safe and Safety

	Meaning	**Reference**
Safe	free from risks, not dangerous convinced, certain; skilled; no doubt about it, secured	SAOL 2015 [1]
	Something that does not introduces or mean danger Something you can trust, (true, functionality etc.)	SO 2009 [2]
Safety	Condition that not mean danger, Certainty	SO 2009 [2]

As stated below, requirements are to use deterministic and probabilistic approaches in safety analyses. A safe facility (of any kind) is based on margins. Then the safety analyses results shall provide confidence that margins are met. These margins may be in the environmental qualification and in functional requirements (capacities). When we feel safe, we are rather confident that an equipment has margin, e.g. the RPV will survive a much higher pressure, than is expected during normal operation and also in all expected and also most not expected disturbance scenarios. Any equipment in a plant that is supposed to be used during certain circumstances are also qualified with margin to make sure they have a very good chance to survive and perform their intended function. If the conditional failure probability for a certain scenario can be expected to be unity, then there is no margin. Margin in functional and environmental qualification is achieved by having different analysis conditions (usually conservative assumptions), use of conservative calculation tools etc. Also there may be margins in the design or choice of safety class or environmental qualification class.

The safety margin also mean that events that are less frequent than those designed for also will be taken care of. Also use of some bounding design cases will contribute to a certain margin. There is really no “margin” in the occurrence frequency itself. Events with very wide uncertainty distribution are difficult, especially considering that a nuclear power plant is designed to be safe for events /scenarios with a return frequency of 1 in 100000 years or even 1 in 1000000 years. It is difficult to prove this, especially for external hazards where we many times have difficulties with lack of experience and knowledge.

Of course, equipment may also fail by “random” causes, they have a failure rate or failure probability. These causes are not lack of “deterministic” margin. Usually they have to do with human interactions in design, manufacturing, installation and operation/maintenance.

2.2. What is Risk

The NRC's concept of risk combines the frequency of an accident scenario (disturbance) with the consequences of that accident scenario. In other words, the NRC examines the following questions:

- What can go wrong? (event)
- How likely is it? (frequency)
- What would be the consequences? (consequence)

This is usually referred to as the set of triplets. The NRC uses risk information to reduce the probability of an accident and to mitigate its consequences.

Some examples of risk definitions are given below:

Table 2: Definitions of risk

Meaning	Reference
The possibility of a negative development or negative result	SAOL 2009 [3]
The possibility that something bad (unwanted) happens, someone will experience a damage or loss, danger	SAOB [4]
"effect of uncertainty on objectives" **NOTE 1** An effect is a deviation from the expected — positive and/or negative. **NOTE 2** Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). **NOTE 3** Risk is often characterized by reference to potential events and consequences, or a combination of these. **NOTE 4** Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. **NOTE 5** Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.	ISO 73-2009 Risk management — Vocabulary [5]
Probability and consequences of an event, as expressed by the "risk triplet" that is the answer to the following three questions: (a) What can go wrong? (b) How likely is it? (c) What are the consequences if it occurs?	ASME ANS PRA Standard [6]

It can be noted that there are different risk definitions / opinions on definitions. The ISO 73 [5] vocabulary is the one that the international standards organization provides and that comes together with the other ISO guides in Risk Management (ISO-31000 [7]) and Risk management – risk assessment techniques (ISO-31010 [8]).

There are many examples that risk and its different parts are mixed up. The event itself, the consequence and the likelihood /frequency) may be looked at as the risk, see the examples below:

Event Unidentified risks may occur (event occur)
Consequence There is a large risk (in the meaning consequence)
Probability (frequency) Some car brands show a higher risk of being in an accident than others

The ISO 73 [5] definition can be understood as if we know the outcome with certainty, there is really no risk, or managing that risk is "easy". The more uncertainty, the more risk and maybe the more complex to manage such risk.

2.3. What is Risk Management and Risk Assessment?

The definition provided in ISO 73 [5]:

Risk management is coordinated activities to direct and control an organization with regard to risk.

Risk assessment is defined as the overall process of risk identification, risk analysis and risk evaluation.

Risk analysis is the process to comprehend the nature of risk and to determine the level of risk (risk estimation). Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

ISO 73 [5] also provides a definition of risk aggregation, a popular theme these days: risk aggregation is defined as a combination of a number of risks into one risk to develop a more complete understanding of the overall risk.

The NRC Glossary of Risk-Related Terms in Support of Risk Informed Decision Making" (NUREG/CR-2122 [9] provides the following definitions:

Risk Management	A process used at a nuclear power plant to keep the risk at acceptable levels
Risk Significant	A level of risk associated with a facility's system, structure, component, human action or modelled accident sequence that exceeds a predetermined level
Safety Significant	A qualifying term that indicates if something does not meet some Predetermined criterion, it has the potential to affect safety.

Risk significance is used in a risk informed regulatory framework to determine the safety significance of SSCs.

2.4 What shall we focus on?

From a regulators point of view:

- What are the supervision activities with the most return in safety?
- What supervision activities has the largest potential to reduce risk? (may depend on the interpretation of "risk")

The options to reduce risk are:

- Lower frequency of the consequence
  - Lower initiator frequency
  - Lower conditional probability
- Reduce the consequence

With regard to risk, we seem to focus on dominating contributors. What if those things we rely on (low failure probability, low event frequency) turns up to be less reliable? These things provide safety – they are safety significant (USNRC definition). We can identify these by looking at the risk achievement worth. Do we put enough emphasis on these?

From a safety point of view, and safety margin point of view, maybe we shall be more aware of the things that provide safety since there is a risk that they do not provide the expected safety, maybe especially for events with an expected long return frequency such as very severe natural hazards.

3. WHAT IS SAFETY ANALYSIS

Basically the safety analysis shall show that a facility is safe enough. This can be done in different ways. One approach is to use event classes with associated consequence levels as criteria. The design shall meet the criteria by:

1) Making sure that all necessary functions have the correct capacity (pumping capacity, amounts of water in tanks, amount of fuel for diesel generators, relief valve capacity etc.)
2) Making sure that all SSCs part of the necessary functions have the environmental qualification to do the job, even though they may fail randomly (the equipment shall be designed to work during the expected conditions, e.g. equipment that is expected to be used in LOCA conditions shall have the necessary qualification).
3) By meeting certain "reliability criteria" reflected by the application of single failure criteria, diversity criteria, separation criteria, use of grace time, and quality.

Designing to be safe usually implies some margin (to be sure). This margin should both apply for capacity and for environmental qualification. Such margin in design will also provide some margin for event frequency uncertainty.

Requirement 42 in IAEA SSR-2/1, Safety of Nuclear Power Plants; Design" [10] on Safety analysis of the plant design states that:

"A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed."

SSG-2 [11], table 3 presents options for combination of a computer code and input data in deterministic safety analysis. It can be noted that risk informed Option 4 makes a reference to probabilistic safety analysis where the availability of systems are derived from probabilistic safety analysis.

Table 3: Options for Combination of Computer Code and Input Data [11]

Option	Computer code	Availability of systems	Initial and boundary conditions
1. Conservative	Conservative	Conservative assumptions	Conservative input data
2. Combined	Best estimate	Conservative assumptions	Conservative input data
3. Best estimate	Best estimate	Conservative assumptions	Realistic plus uncertainty; partly most unfavorable conditions
4. Risk informed	Best estimate	Derived from probabilistic safety analysis	Realistic input data with uncertainties

The more realistic deterministic safety analysis is used, one may ask where the margin will be?

Regarding probabilistic safety analysis the following statement is made in GSR Part 4 [12] (para. 4.55):

"*The objectives of a probabilistic safety analysis are to determine all significant contributing factors to the radiation risks arising from a facility or activity, and to evaluate the extent to which the overall design is well balanced and meets probabilistic safety criteria where these have been defined*…."

SSG-3 [13] states that probabilistic safety assessment (PSA) is considered to be an important tool for analysis for ensuring the safety of a nuclear power plant in relation to potential initiating events that can be caused by random component failure and human error, as well as internal and external hazards.

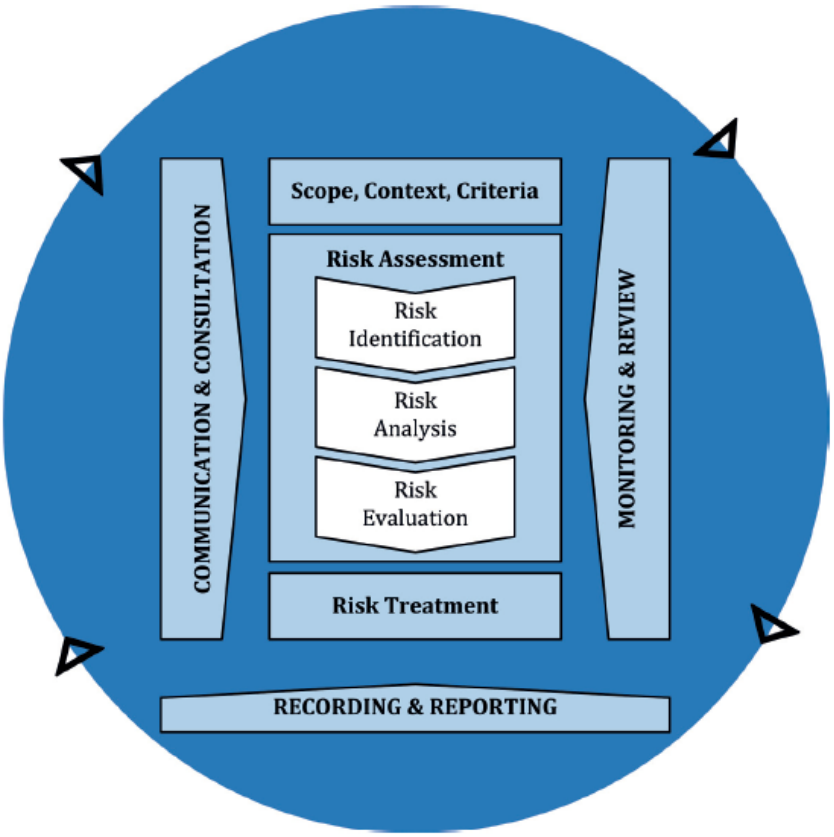
4. RISK MANAGEMENT AND RISK ANALYSIS

Safety analysis has one purpose which essentially is to show and make sure that something is safe enough. As discussed above, safety is also based on the use of margins.

Risk analysis on the other hand is used to support risk management. Risk management is not necessarily to focus on the dominating risk contributors, but also to provide attention to areas where there is uncertainty. Where are the risk drivers? The items that already contribute a lot to risk or those factors that has a potential to have a major influence on risk.

ISI 31000 Risk Management – Guidelines [7] provides a basic framework for Risk Management which is basically in line with the IAEA INSAG-25 [14] and NRC Reg. Guide 1.174 on Risk informed Decision making [15].

Figure 1: Risk Management process [7].



IEC 31010 Risk Management and Risk Assessment Techniques [8] provides more detailed guidance and also describes a number of risk assessment techniques, including event tree and fault tree analysis.

Some areas of probabilistic safety analysis, especially when analysing internal and external hazards seem to find the limit for environmental qualification – providing fragility functions. In these cases, the margin limit is identified or at least attempts are to find this limit and even showing the failure probability as a function of the hazard level. This way, the analysis is really risk informed, but not necessarily safety informed. The margin to safety decreases. Do we want this? How do we show that we have a margin? How do we assess this margin?

From a regulators point of view, it might be important to have an oversight focusing on areas where the margin is small or where the margin is suspect. That might be a risk to go for? And where a higher benefit is achieved compared to go for areas with large margin / small uncertainty.

5. CONCLUSION

One interpretation is that a safety analysis is used to show that something is safe enough, results meet some criteria. This mean that safety analysis can be conservative bounding. Safety analysis also many times uses conservatism in condition and computational tools, and maybe in criteria, to make sure there is some safety margin. The basic safety analysis is therefore not good enough for risk informed purposes where we want to know (realistically) what are the risk drivers, so that we can prioritize risk reduction measures. Usually the term risk analysis is used in such cases (and in most other industries) to support risk management [7].

The safety of a facility or an operation is achieved by identifying hazards, and depending on the potential consequences, making sure that measures are in place to limit those consequences to “acceptable” levels.

The measures are designed with the capacity needed to deal with the hazards and also the environmental qualification, e.g. they shall be designed to function and deliver the needed capacity given the hazards and any secondary impacts that may follow. In order to be safe, usually (always), there is introduced margin with regard to capacity and environmental qualification, and maybe also to reliability. This margin may be the result of assumptions for the analysis and use of conservative calculation tools. We are likely to expect that the margins are different for hazards that occur more frequent than for hazards that occur less frequent. Anyway, with regard to safety we are likely to go for margin to be able to state that something is safe. Whether it is safe enough we may also want to say something about margins both with regard to capacity (we have a cooling water amount or diesel storage that is more than we expect is needed) and with regard to environmental qualification (the equipment is qualified for a much higher temperature / moisture atmosphere than is ever expected).

In risk management / risk informed decision making we really want to know more about (and it is essential) the realistic risk, or safety margin, and not the least the uncertainties.

What contributes to risk and what contributes to safety. Dominating risks in terms of contributing failures is a natural focus for reducing risk. We may overlook the fact that weaknesses in "safety significant" SSCs can be important risk contributors. How do we make sure that expected high reliability is maintained not only for frequent events / conditions, but also for infrequent events / conditions. Do such SSCs maintain their expected high reliability, low failure probability, how sure are we that such SSC will survive (have the correct environmental qualification, and can deliver the expected function such as cooling or pressure relief? What is our trust for very severe impact scenarios that safety systems really will do their job?

The focus maybe shall be shifted towards the expected strengths of a plant? Expected high failure probabilities maybe is something we can live with, or there is improvement potential, on the other hand we may have more to lose if SSC with low failure probability turns up to not meet the expectation?

We need to be aware that risk insights are not necessarily the same as safety insights.

References

[1] SAOL: Swedish Academy Word List (2015).
[2] SO: Swedish Word Book (2009).
[3] SAOL: Swedish Academy Word List (2009).
[4] SAOB: Swedish Academy Word Book.
[5] ISO 73, Risk management - Vocabulary, ISO 2009.
[6] ASME/ANS RA-Sa-2009, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," Addendum A to RA-S-2008, ASME, New York, NY, American Nuclear Society, La Grange Park, IL, February 2009.
[7] ISO 31000, Risk Management – Guidelines, second edition, ISO 2018.
[8] IEC/ISO 31010, Risk Management - Risk Assessment Techniques, Edition 1, IEC 2009.
[9] NUREG-2122, Glossary of Risk-Related Terms in Support of Risk Informed Decision Making, NRC 2013.
[10] SSR-2/1, Safety of Nuclear Power Plants: Design, Specific Safety Requirements, IAEA 2012.
[11] SSG2, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Specific Safety Guide 2009.
[12] GSR Part 4, Safety Assessment for Facilities and Activities, General Safety Requirements Part 4, IAEA 2009.
[13] SSG3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Specific Safety Guide 2010.
[14] INSAG-25 A Framework for an Integrated Risk Informed Decision Making Process, IAEA, 2011.
[15] Reg Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Rev 3, NRC January 2018.