Strål
säkerhets
myndigheten
Swedish Radiation Safety Authority

Paper 317

What is Risk and What is Safety?

Session Th24 – 3.30 PM – September 20 - Risk and Hazard Analysis V

Per Hellström, SSM (Swedish Radiation Safety Authority), Sweden

PSAM14, Int'l Conference on Probabilistic Safety Assessment and Management,
UCLA Luskin Conference Center in Los Angeles, 16-21 September 2018

Outline

- Safety
  - versus
- Risk?

- Probabilistic Safety Analysis
  - versus
- Probabilistic Risk Analysis?

What is safety?

	Meaning
Safe	free from risks, not dangerous convinced, certain; skilled; no doubt about it, secured
	Something that does not introduces or mean danger Something you can trust, (true, functionality etc.)
Safety	Condition that not mean danger, Certainty

- Requirements are to use deterministic and probabilistic approaches in safety analyses.
- A safe facility (of any kind) is based on margins. Safety analyses results shall provide confidence that margins are met.
  - Margins in the environmental qualification
  - Margin in functional requirements (capacities).
- We feel safe, when we are 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.
- If the conditional failure probability for a certain scenario can be expected to be unity, then there is no margin.

Safety (cont´d)

- Then of course, equipment may fail by “random” causes, they have a failure rate or failure probability.
  - These causes should not be lack of “deterministic” margin.
  - Usually they have to do with human interactions in design, manufacturing, installation and operation/maintenance.
- So we need a certain reliability

What is Safety Analysis?

- Basically the safety analysis shall show that a facility is safe enough. 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 quality requirements, application of single failure criteria, diversity criteria, separation criteria, use of grace time etc.

- 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.

Safety Analysis (Cont´d)

- Requirement 42 in IAEA SSR-2/1 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*."
- IAEA SSG-2 options for combination of a computer code and input data in deterministic safety analysis.

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

Safety Analysis (Cont´d)

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

- GSR Part 4 on probabilistic safety analysis (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 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.

What is Risk?

I see the ISO 73 definition as if we know the outcome with certainty, there is really no risk, or at least we can manage that risk. The more uncertainty, the more risk.

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

- These are many times mixed up, the event itself, the consequence and the likelihood /frequency) may be looked at as the risk:
  - Event — Unidentified risks may 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

Definitions of risk
The possibility of a negative development or negative result
The possibility that something bad (unwanted) happens, someone will experience a damage or loss, danger
"effect of uncertainty on objectives" (ISO 73-2009) **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.

Risk Management and Risk Assessment

- The definition provided in ISO 73:
  - *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.

- NRC glossary NUREG/CR-2122
  - 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

What shall we focus on?

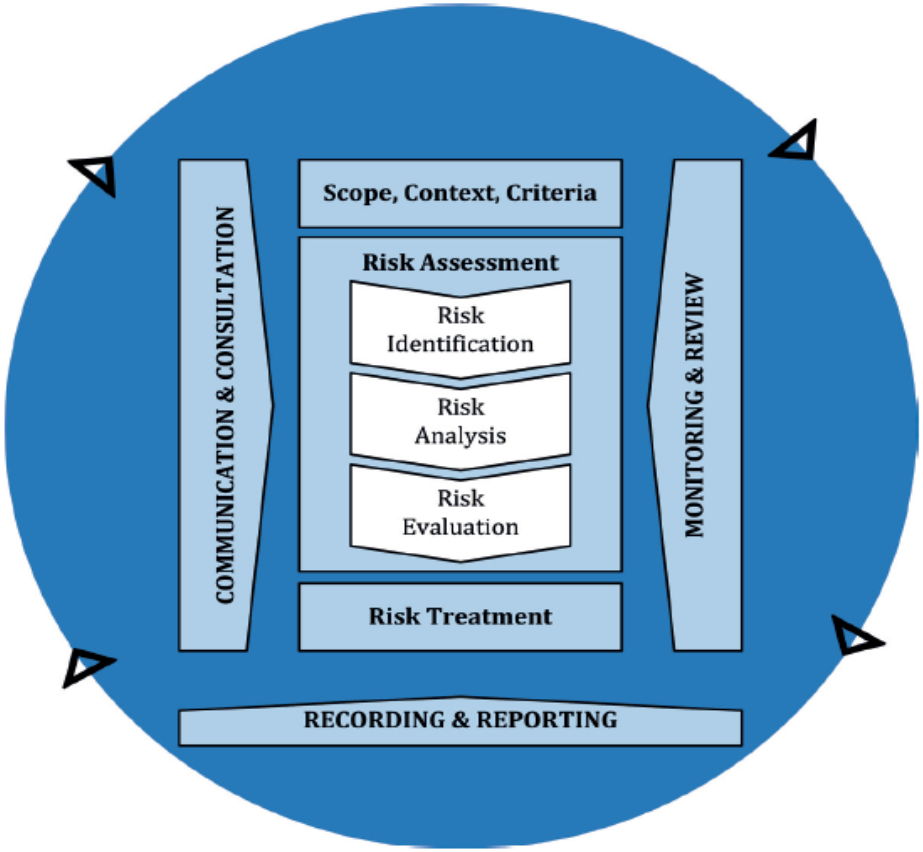
- From a regulators point of view:
  - What are the supervision activities with the most return in safety?
  - What supervision activities has the largest potential to reduce risk?
- The options to reduce risk are:
  - Lower frequency of the consequence
  - Lower event frequency
  - Lower conditional consequence probability
  - Reduce / change 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 and we can identify these e.g. by looking at the risk achievement worth.
  - Do we put enough emphasis on safety significant items?
- 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.

Risk Management and Risk Analysis

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

- Risk analysis is used to support risk management. Risk management is not necessarily to focus on the dominating risk contributors, but maybe more 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: threat, potential source of danger, harm evil etc.

Risk Management Process (ISO 31000)



RISK MANAGEMENT AND RISK ANALYSIS

- IEC 31010 Risk Management and Risk Assessment Techniques 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 analyzing internal and external hazards look for 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.

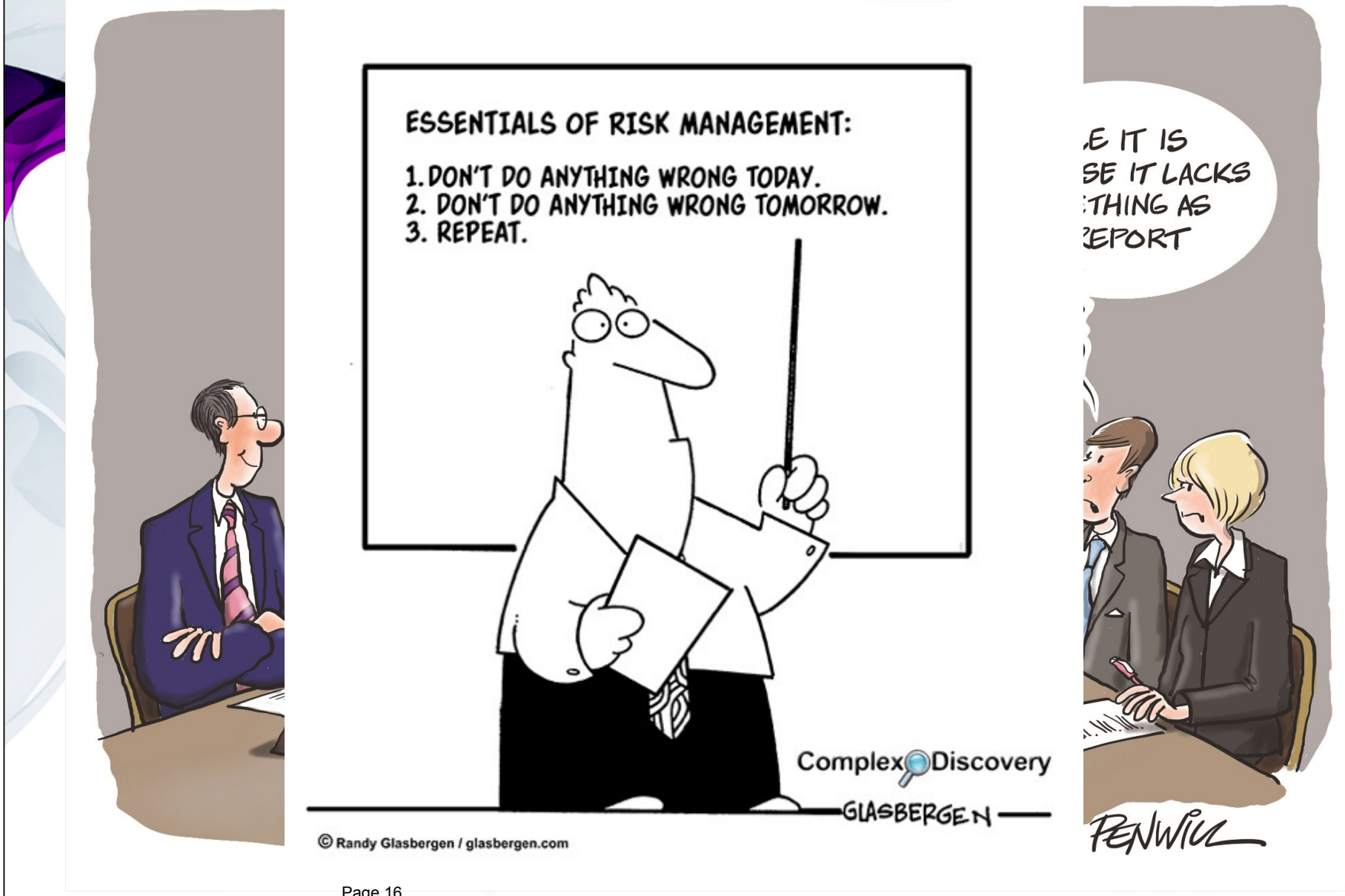
Main Conclusions

- 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 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 “risk” analysis is used in such cases to support risk management.

- 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.
  - To be safe 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 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 and with regard to environmental qualification.

Main Conclusions (Cont´d)

- 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? They have the correct environmental qualification, and can deliver the expected function such as cooling or pressure relief? (we do a lot of work here)
  - 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, on the other hand we may have more to lose if SSC with low failure probability turns up to not meet the expectation?
- Risk insights may not necessarily be the same as safety insights?


ESSENTIALS OF RISK MANAGEMENT:
1. DON'T DO ANYTHING WRONG TODAY.
2. DON'T DO ANYTHING WRONG TOMORROW.
3. REPEAT.
Complex Discovery
GLASBERGEN
© Randy Glasbergen / glasbergen.com
E IT IS
SE IT LACKS
THING AS
EPORT
PENWILL