THE BIGGER PICTURE

Stefan Seidl, ILF Consulting Engineers, Germany, explores the importance of a holistic approach to technical risk management.

Over the past decades, risk management has become increasingly important for the entire lifetime of industrial plants, which includes the design phase, the construction and commissioning phase, the operation phase, and the decommissioning phase. Within the past 50 years, ILF Consulting Engineers has participated in the development from deterministic (simple) towards probabilistic (complex) risk assessment and management methodologies.

In most of ILF's projects, risk management methods are used for technical risk assessments as well as for scheduling or financial risks. Normally these are carried out independently from each other and without an aligned methodology.

This article will explain the typical pitfalls and provide guidance on how to integrate the correlation of risks into a so-called 'holistic approach'. Through this holistic approach, the requirements of legal/normative compliance and technical safety are covered, and at the same time a proper linkage of the identified risks towards the strategic project objectives is ensured.

Methodology

ISO 31000's first edition was published in 2009 and sums up the practice of risk management during the past industrial era. However, in ILF's experience, many projects still have no fully implemented risk management process, or if a risk management was conducted, the following pitfalls occurred:

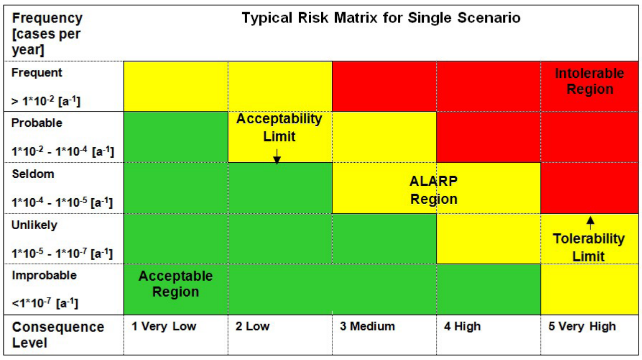

Figure 1. Example of a typical risk matrix for a single scenario.

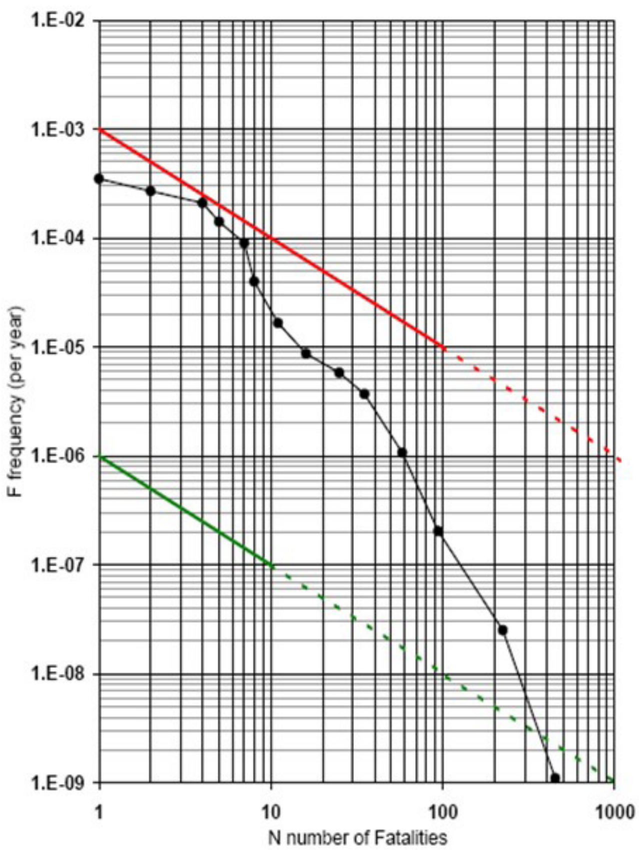

Figure 2. Example of a typical F/N-curve.

Setting up impossible risk acceptance or tolerability criteria

For example, the claim that a project shall have no risk which could kill more than 100 people is honourable, but it does not consider the aspect of probability. In such a case, the project would have to be stopped immediately, because statistically there is a small probability for such a death toll in every project.

Carrying out a risk assessment ex post, in order to justify a decision

This ignores the valuable contributions of risk management to design and engineering decisions.

Using 'Reverse ALARP' arguments

'As low as reasonably practicable' (ALARP) is a value that needs traceable reasons, and not a methodology to attempt to argue that it is acceptable to reduce existing safety standards.

Reducing risk management to mathematical analysis of systems and failure probabilities

Risk management needs the buy-in of all involved disciplines and contractual parties of a project.

Failure to fully consider all possible outcomes

Is the risk of having an asset loss of €200 000 due to the explosion of a piece of equipment at a frequency 10^{-3}/y ALARP? Perhaps yes, if the equipment is located in the field, but not if the equipment is located in the cellar of the office.

Improper alignment on dimensions and definitions

Is the risk of fatality at 1 out of 1000 acceptable? Perhaps yes, if it occurs at the start of a spaceship, but not if it occurs at the start of an airplane.

Risk aggregation was not properly conducted

If risks are just listed without proper aggregation and are consequently missing prioritisation, the organisation will not be able to monitor them continuously.

It is therefore important to involve the right experts with practical knowledge and long-term experience from the very beginning, to properly set up the risk management process.

Definition of required risk level

The client must define tolerability and acceptability criteria of risks. For this set-up, the client can use the following five input parameters:

- Legal requirements (if applicable, e.g. UK, Switzerland, the Netherlands or Russia).
- Lender requirements (if applicable, e.g. World Bank).

- Insurance conditions (if applicable).
- Societal expectations.
- Business criteria of the project owner or operator.

The first four criteria are missing for many projects. The project owner then defines the required risk level in principle based on his individual risk appetite. A risk which is negligible for some owners may be already a critical loss for others, considering their financial strength or reputation.

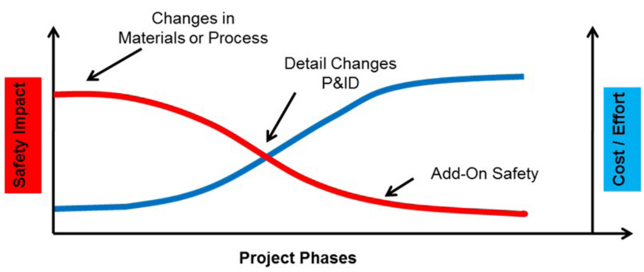

Figure 3. Cost/effort and safety impact over project phases.

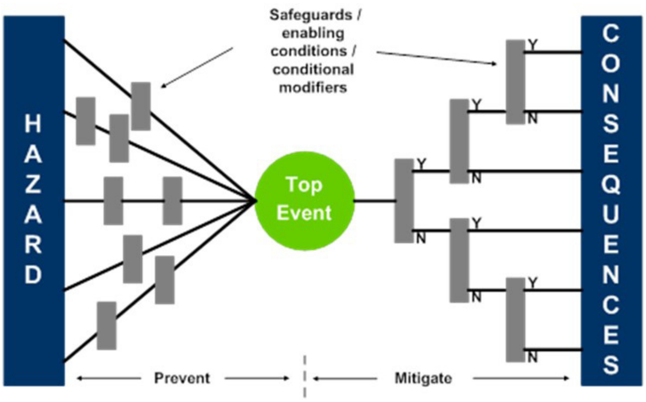

Figure 4. Example of a typical bowtie diagram.

ACTION ITEM CLOSE OUT SHEET				
ACTION NUMBER		SOURCE		
CAUSE				
CONSEQUENCE				
SAFEGUARDS				
RECOMMENDATION				
CONTRACTOR RESPONSE				
CLOSE OUT VERIFICATION				
APPROVAL	DISCIPLINE	NAME	SIGNATURE	DATE
CONTRACTOR				
CLIENT				

Figure 5. Typical example of an action item close-out sheet.

The result of the definition of project specific tolerability and acceptability criteria is typically a risk matrix (Figure 1) and an F/N-curve (Figure 2). Typically, consequence levels are evaluated for their effects on population, environment, reputation and finance.

Focusing on consequences instead of causes, the different risk evaluations use one risk matrix format. This approach allows serving technical risk assessment (e.g. Hazards and Operability Studies and Safety Integrity Level Assessments) as well as assessing risk related to security, legal compliance, schedule, procurement and other factors. The consequences for the project from risks of all sources can be assigned to those four categories.

With the risk matrix and some mathematical modifications, the individual risk, single scenario risk, and impact-related risks can be covered, and the combination of frequency and consequence will define if a risk is acceptable, intolerable or ALARP (Figure 1).

- 'Acceptable' (green region): no further risk reduction required.
- 'Intolerable' (red region): additional measures required to reduce the risk to at least ALARP.
- 'ALARP' (yellow region): risk can be tolerated as long as they fulfill the following criteria:
  - There is a trade-off between the costs of risk reduction and the benefits obtained.
  - The risk controls correspond to good practice.
  - All aspects and safeguards are thoroughly known.
  - The risk is periodically reviewed.

When a risk can have more than one consequence category, the most severe combination of frequency and consequence shall be used to determine which risk region applies.

To fully cover the societal risk, additional criteria for scaling risk with more than one fatality should be applied. This is typically expressed by a double logarithmic graph (Figure 2) showing relation of the number of fatalities (N) and the related accepted (green line) and tolerated (red line) frequency (F). The different risks can then be plotted into the graph (black dotted line) and should hopefully be below the red line.

Impact and cost

Efforts and cost for improving technical safety are lower, the earlier they are applied (Figure 3).

Technical norms, e.g. ISO 17776, IEC 61882 or IEC 61511-3, require implementation of risk assessment and technical risk management already in the engineering phases, mainly during the front-end engineering design (FEED) phase of a project.

Project health, safety, security and environmental reviews (PHSSER) attempt to ensure that the strategic, economic, technical, health, safety, security and environmental components have been properly assessed, and that a well-informed decision can be made at the gates to the next phase.

Level of scrutiny

Inside the oil and gas industry a wide range of technical risk assessment methodologies are used during the design phase. These include: COMAH, EERA, ENVID, ERP, ESSA, FEHA, FMECA; and/or HAZID, LOPA, QRA, RAM, SCE and SIL.

Not all of these assessments, workshops and studies are required for every project in order to demonstrate that the project is safe enough or meets the required risk level. For the appropriate selection, the defined tolerability and acceptability criteria need to be applied to the different types of risks.

Individual risk

The individual risk relates to the likelihood that a person in a particular location will be killed or seriously harmed in the event of an incident. The risk value is independent of the size of the population.

Societal risk

Societal risk relates to the likelihood that a specific number of people in a particular location will be killed or seriously harmed by an incident. The societal risk considers the density and location of population on and around a site.

Single scenario risk

A single scenario risk relates the likelihood that an initiating event develops to its worst reasonably foreseeable outcome. It considers a specific hazard and all possible outcomes related to it.

Impact-related risks

Impact-related risks express the probability that the exposure of a system to a certain impact or condition will yield an undesired outcome over time.

With this holistic overview of the impact of the different risk areas, the proper set-up of assessments, workshops and studies can be aligned to ensure that all areas are addressed, and the tolerability and acceptability criteria are met.

Risk aggregation

Experience shows that in many projects, hazards and related risks are still managed in silos, separating them into discipline units without analysing or even understanding their correlations. However, it is rarely the case that two individual risks are either perfectly correlated, and hence able to be simply added, or perfectly independent, allowing the use of a simple approximate formula to combine them. As a result, it becomes necessary to design a robust general process that enables the aggregation of risks.

One possibility for such a risk aggregation tool is 'bowtie', a method that takes its name from the shape of the diagram (Figure 4). A bowtie gives a visual summary of all plausible hazard scenarios that may result in the top event. Additionally, by identifying control measures (safeguards), enabling conditions as well as conditional modifiers, the bowtie displays what can be done to control those scenarios.

By applying the bowtie or any other aggregation tool, it becomes clear that, for example, an incident during construction is not on the same aggregation level as missing the 'golden weld' milestone in the schedule. Such an incident may be only one of the event paths to the top event of missing the milestone. However, ILF's experience shows that in the risk register of several projects, different aggregation levels are not shown and therefore the dependencies between risks are completely missed.

Only this risk aggregation step transfers a simple list of collected risks into a meaningful risk register, with the possibility of proper risk treatment prioritisation. The involvement of an experienced technical safety expert is essential for that step.

Risk reduction

After the previously described steps have been conducted, there are four options for risk treatment: eliminate, reduce, share, and/or accept.

However, even with the best tools and techniques in place, some risk will always remain unidentified and can therefore not be eliminated or reduced; although if properly done, they can be shared. To be able to ensure the proper treatment of risks, the results of all performed risk assessments need to be collected in a respective risk register.

As a next step, an 'action item close-out sheet' (Figure 5) is created for every recommendation, including an explanation of the implementation of recommendation and documentation of respective evidence for verification.

To avoid double structures in projects, the risk countermeasures should be integrated in the project's general 'list of action points'. This should preferably be linked to the overall 'work breakdown structure'.

Conclusion

Risk management is important. It can save lives, contributes to the objectives and economy of a project, and can support public acceptance of a project. Defining the required risk level for a project is a basic duty of the owner or operator.

Risk management needs engineering experts, operational experience, the right mathematics, and common sense for achieving a correct and practical result. These experts will set up a holistic risk management process and have it completely and correctly documented in a continuously maintained risk register, exceeding the requirements of regulation for the maximum benefit of a project. This ensures that a risk assessment will not end up with a simple list of collected risks, but with a meaningful risk register with proper risk treatment prioritisation.

ILF has been a consulting engineer in the oil and gas industry for more than 50 years, with experience from over 6000 projects worldwide helping operators to avoid the typical pitfalls in risk management.