PRACTICALITY OF RISK ANALYSES
OF ESTABLISHMENTS

HELMUT KÖRBER
APC Angewandte Physik Consulting AG, Switzerland

ABSTRACT

Quantitative risk analyses require high expenditures from a skilled workforce (many person-years), which is mostly unaffordable for an SME industrial establishment. Therefore, a much less workforce-consuming methodology – SQP (Semi-Quantitative Procedure) – was developed. SQP consists of two parts, TRA (Tabular Risk Analysis) and ACCS (Analysis by Conservatively Covering Selection). The risk R is the product of the severity of a damage S of an accident and the probability P of its occurrence. Instead of quantitative numerical values for S and P, SQP is using risk parameters S_n and W_n, similar to VDE/VDI 2180 or SIL. From this, a risk indicator R_n is determined. The method provides a set of differentiated levels of risk. Risk analyses using SQP have been carried out for several industrial establishments being subject to Seveso III Directive upper-tier group. In all cases, it was possible to uncover those (in general very few) installations of the site of operation generating a risk reasonably above the average. The introduction of SQP in the companies has been easy due to the similarity and the experience of the engineers with SIL. Instead of a workload of person-year(s) for a risk analysis of an establishment, only some two person-weeks are required.
Keywords: risk assessment, industrial establishment, upper-tier, probabilistic analysis, Seveso III, semi-quantitative risk analysis, SIL, severe accident, low workload, practicality.

1 INTRODUCTION

Following existing laws, directives, regulations, standards and rules, industrial establishments implement well-defined organizational measures and sophisticated technical systems to guarantee the safe operation of in their plants. The deterministic way of thinking results in the conclusion that, if all is carried out properly and correctly, accidents are and will be prevented. However, experience shows that accidents still occur, nevertheless. This can be evaluated with probabilistic methods, which eventually leads to risk analyses.

The evaluation of complex technical systems and systems under the perspective of risk is not really a new topic. Already since the 1970s, a growing part of the technical and scientific society has become aware of quantitative risk analyses, especially those carried out for nuclear power plants [1], [2]. The labour effort required was huge. In all investigations, it did sum up to many person years of workload of skilled scientists and engineers.

Therefore, quantitative risk analyses were initially carried out for conventional technical installations and plants in exceptional cases only. The reason for risk studies was always a very special boundary condition, for instance if a hazard potential was regarded from the plant operator in contrary to the supervisory authority, or in case of highly controversial projects such as the erection of a hazardous waste incineration plant in a metropolitan area. Another example is the expansion project (additional runway) of Frankfurt/Main airport that led to an extra hazard for a chemical installation as each aircraft in descent and final approach had to cross the site at low altitude [3].

It is understandable that such a big deployment of qualified labour appears to be disproportionately high – at least for small and medium enterprises (SME) operating an installation subject to upper-tier requirements of Seveso III Directive [4]. It is also questioned whether these additional expenditures for skilled staff required to carry out a quantitative risk analysis is not beyond the limit of the reasonableness for a company being exposed to international competition.

2 SKEPTICISM AND BENEFITS

Parts of the population became aware of the risk studies. In particular, in German-speaking countries, it had to be observed that both the calculation with probabilities and the calculatory consideration of dead and injured resulted in mistrust, suspicion and also in full rejection [5]. Even engineers in companies or supervisory authorities who had to deal with the safety of industrial plants did show a reduced confidence. Some are still sceptical today.

2.1 Risk analysis – reasons for scepticism

A one-dimensional explanation for the scepticism cannot be given. In any case, the accumulated experience with regulations, directives and laws plays a key role. This experience has been gained within a period of several generations and covers not only the technical sphere but also the social side of life, after which everything works and nothing goes wrong, if you only follow exactly the given rules. This is almost always true. However, experience shows, too, that despite the best precautions and meticulous compliance with all regulations, incidents can still not be ruled out with absolute certainty.

For most people it is (subjectively) a difference, whether they expose themselves to a risk or whether they are exposed to it from outside, from third party. High risks, for example due to dangerous sports, unhealthy diet, smoking, alcohol and drug consumption are much more likely to be accepted than the possibly low risk that emanates from a neighbouring chemical factory. The risk of participating in road traffic is mentally rated as low, if we drive ourselves. On the other hand, the risk is considered as high, if we are threatened by traffic (from others).

Moreover, it can be observed that the term risk is sometimes not used correctly – in particular in conjunction with negative events such as industrial incidents and accidents. That is why many plant operators avoid the use of the word "risk", because it can be misused from opponents of technical installations. Even if a plant is particularly safe and emanates an extremely low (residual) risk only, the term risk is often unconsciously or consciously, but mistakenly – used as a synonym for "danger", "endangerment", "accident", "hazard" etc. Like this, an impression arises that the installation is very dangerous.

Furthermore, the thinking in terms of probabilities or frequencies of events to be expected is alien to many people, mainly if it is a question of low probabilities. This can be explained by our horizon of experience which covers about 80 to 100 years (three generations). We still can imagine that a major fire occurs in an average of once every 10 years, or that, say, a residential building is destroyed by a gas explosion in the own city approximately every 25 years.

On the other hand, we cannot differentiate with regard to low probabilities. Events being expected at an average frequency of once every 500 years are of the same category as those occurring once in 50,000 years.

2.2 Reasons for conducting risk analyses

There are several reasons for carrying out risk analyses. The most important are:

- Risks are comparable; even if they arise from different potential threats. Thus, the risk to which a resident is exposed from a facility nearby can be compared with natural risks such as earthquakes or floods and also with the risk the resident is responsible for by himself and he decides to take it voluntarily. Unless preconceived opinions oppose it, the comparison of risks can contribute to the acceptance of technical systems.

- By the help of a systematic risk assessment of an entire industrial installation, those (in general few) sub-areas/components can be identified causing an increased risk. This makes it possible to purposefully implement measures of risk-reduction and thus reducing the remaining total (residual) risk the whole establishment.
- Installations being assigned to upper-tier establishments corresponding to Seveso III Directive have to carry out risk evaluations.

Seveso III [4] is a Directive of the European Union (EU) for the control of major-accident hazards with dangerous substances. It is in force in all member states in form of a law or legitimate regulation that represents a transposition of the Directive into the legal framework of each EU state. Seveso III is also relevant for the European Economic Area (EEA).

Corresponding to Seveso III Directive, a determination and analysis of the risks of accidents is required as well as the means to prevent them, with a detailed description of the scenarios of possible major accidents and their probability under which they occur. Additionally, an assessment of the extent and severity of the consequences of major accidents identified is necessary, and all this information has to be documented in the safety report (Seveso III Directive [4], Annex II, 4).

Furthermore, a safety management system (SMS) is required and the organisation of the establishment with a view to the prevention of major accidents. The SMS must take into account the aspects of identifying and evaluating major hazards through adoption and implementation of procedures for systematically identifying major hazards arising from normal and abnormal operation including subcontracted activities and the assessment of the likelihood and severity of such accidents (Seveso III Directive [4], Annex III, b, ii).

As already mentioned, a quantitative risk analysis is very person-power consuming. Therefore, the methodology SQP (Semi-Quantitative Procedure) was developed with the objective of being able to carry out a simplified and nevertheless significant and meaningful systematic risk assessment of industrial establishments. SQP consists of two parts, the TRA (Tabular Risk Analysis) and ACCS (Analysis by Conservatively Covering Selection). First, the two components of SQP will be explained below, and the procedure will be presented. This is followed by an experience report on the introduction of SQP in practice.

3 THE SEMI-QUANTITATIVE PROCEDURE (SQP)

3.1 Tabular risk analysis (TRA)

A systematic safety evaluation must cover the entire industrial establishment. The approach of SQP is to subdivide the establishment into associated section or sub-systems respectively to carry out the TRA. Each sub-system is evaluated with regard to existing potential hazards and the existing preventive measures against possible malfunctions.

In general and mostly, an establishment is composed of several sections which can be defined as subsystems. An example, a chemical plant is shown (Fig. 1). The site has an unloading area (Section 1) where the delivered raw materials are taken and transferred to the entrance storage (Section 2). The manufacturing of products takes place in two steps, in process lines for producing the raw substance (Section 3) and the cleaning system to purify them (Section 4). Finally, the end products are stored in a warehouse or outlet tanks for being shipped to the customer (Section 5). These five sections can be used for TRA.

In the case of a crude oil refinery or a petro-chemical installation like an ethylene plant, there is another option to determine the sub-systems. Most of these facilities are equipped with system to section-wise separate parts of the installation from the rest. This is realized
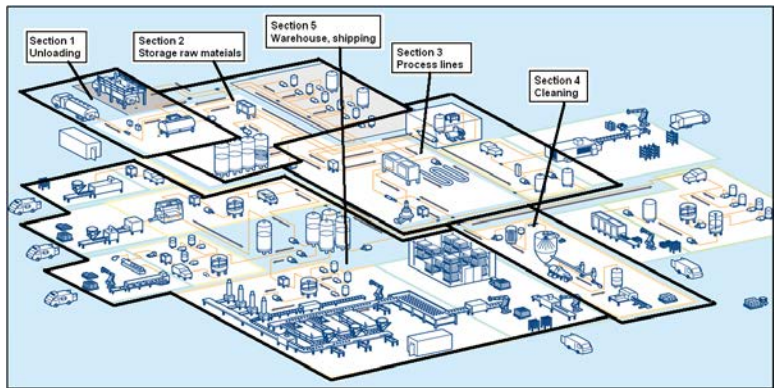
Figure 1: Site of an industrial establishment.

through sealing-off the section in question, containing/locking-in the materials (containment) and taking care for a controlled emergency release or discharge. If so, the sections of such an Emergency Seal-off and Release System (ESRS) can be defined for the tabular risk analysis as sub-systems.

In each sub-system there are numerous technical and organisational measures to ensure a safe operation. Nevertheless, it cannot be ruled out that failures of components or faulty actions of persons occur resulting in a malfunction or in a major accident. It is possible that a vulnerability of an instrument or the weak spot of an apparatus or any other deviation from lay-out and regular operation triggers an accident. This is to find out.

For this purpose, all imaginable chains of events or scenarios must be considered and analysed. A systematic compilation is inevitable. All conceivable root causes must be captured that reasonably can lead an accident. Each event sequence uncovered is listed up in a table (Table 1). Based on this, all these sequences are analysed and evaluated under the aspect of risk. (This investigation is carried out for all sub-systems.) The procedure of carrying out a TRA is given below; Table 1 is to be used as guideline.

Table 1: Working table for carrying out a tabular risk analysis (TRA).

Sub-system	Case and component selected	Potential hazard	Conceivable root cause/ triggering event	Conceivable event sequence/ potential extent of damage	Existing measures to prevent/limit the damage	Risk parameter		Risk indicator	Remark
						S	P	R	

In the sub-system being subject to an analysis (column 1), all components or cases are to be considered (column 2) that might be the reason for triggering an accident. The potential hazards or pessimistic consequences of these disturbances (column 3) and the triggering events (column 4) are compiled and listed. Based on this, each scenario leading to the accident is explained in keywords representing the conceivable chain of events and

the potential extent of the damage (column 5). Columns 2 to 5 briefly illustrate the assumed accident and the possible extent of damage under the assumption that no or only insufficient provision (both technical and organizational) was made against the accident.

For each event sequence the existing measures are listed that shall prevent an accident and, should it occur nevertheless, limit its effects (column 6). These can be technical devices/components but also organizational measures. Examples: the automated addition of an inhibitor into a reactor to stop an excursion, to activate ESRS in case of a problem in the concerned section, an alarm system to indicate the release of hazardous gases or to start emergency response plan, an automated initiation of installed extinguishing devices to fight a fire. These existing measures shall (and, in general, do) take care of an effective prevention that a malfunction or another triggering event cannot initiate an accident.

If, however, the analysis uncovers safety-related weak points, it is quite likely that this results in an accident. Depending on the severity of damage to be expected and the probability of the occurrence, the risk for this accident can then be calculated or assessed (see next section). If necessary, measures have to be taken to reduce the risk.

3.2 Calculating the risk

To assess and the risk of accidents, the severity of the damage is required as well as the likelihood that it will occur. The risk R is defined as the product of the severity of damage S and the probability of the occurrence W (see [1], [2], and Seveso III [4], Article 3, 15):

$$R = S \cdot W.$$

In a quantitative risk analysis, the severity of damage S has to be specified. An approach is to use the expected property loss for S (e.g. in €), or the personal harm (number of injured or deaths). S can also be expressed in an indirect harm like the concentration of a toxic gas at the point of impact (e.g. in mg/m^3 breathing air). Environmental damages can be quantified, too (e.g. in g/m^2 contaminated agricultural land) as well as image damages (e.g. number of negative reports). The user can also define the severity of damage by himself.

The probability is regarded as the average expected frequency of the event per year. For example, if an assumed accident A is expected on average twice a year, the probability for this is $W_A = 2\ a^{-1}$. On the other hand, if accident B is expected to occur once every 10 years on average, this means 1/10 times a year; thus $P_B = 0{,}1\ a^{-1}$.

If statistics show that, say, out of 200 chemical plants sited in the lane of approach of airports, one plant is hit by a plane crash on average every 50 years, then the probability W_C for such an event is for each of these chemical plants $W_C = 10^{-4}\ a^{-1}$. Hence, an impact of an aircraft crashing down on the site can be expected per plant one time every 10,000 years.

In case, this crash will cause a property damage S_C of €80 million (and assumed that no personal or environmental damages are to be expected), the risk R_C can be easily estimated. It amounts to 80 million € times $10^{-4}\ a^{-1}$, i.e. €8,000/a. If the plant operator wants to take out insurance against the consequences of such a crash, the insurance company would set a premium on this basis, i.e. not charge less than €8,000 annually.

3.3 Approximation method SQP for risk assessments

As performing a quantitative risk calculation is possible but very costly, an approximation method has been developed. It results from practical working experience in industrial upper-tier establishments and is safety analysis in Semi-Quantitative Procedure (SQP). SQP does not use accurate quantitative numerical values for severity of damage S and the probability of occurrence W, because each term requires an extended portion of time and is not very precise, nevertheless. Instead of this, SQP is based on risk parameters Sn for the

extent of damage and Wn for the probability. From these, the risk is determined as risk parameter Rn indicating the level of risk.

The parameter Sn for the severity of damage is defined in very close accordance with the widely used standards of VDI/VDE 2180 [6] or SIL [7] considering a graded level of damages S1 to S4 (Fig. 2). However, the severity of damage S0 was added in order to be able to extend the differentiation of damage grades. S0 symbolizes lower values for property damages and reduced or not relevant injuries of persons.
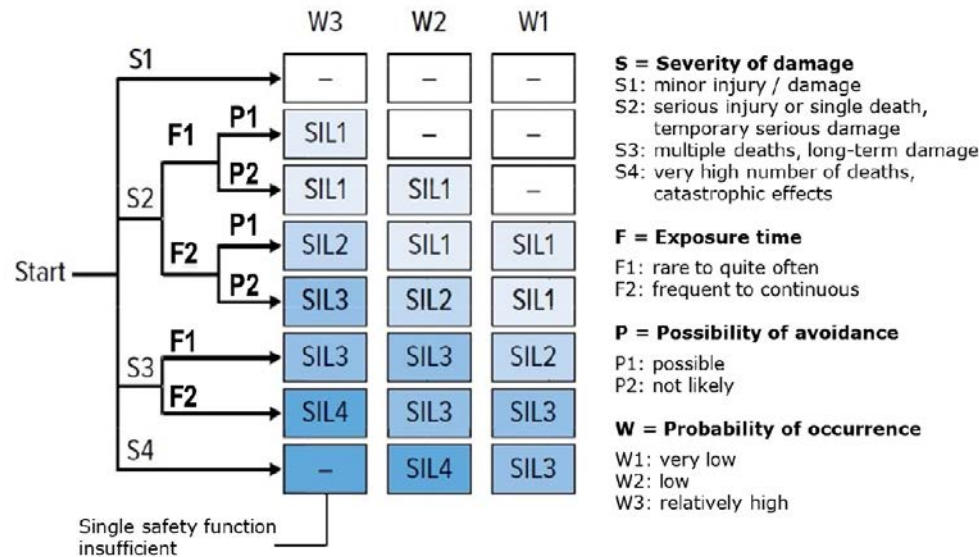

Figure 2: Risk graph corresponding to IEC 61508.

A severe accident in industrial installations can not only result in injuries of persons and lost values of property. It can also have an impact to the ambient. An example for this is the accident in the chemical plant of the company Industrie Chimiche Meda SA (ICMESA) in northern Italy causing an environmental disaster. The accident happened in 1976. Highly hazardous dioxin was spread over into the ambient. Agricultural land was devastated, and several neighbouring towns and villages were hit. Seveso was the community most affected. As another and additional outcome, the image of the company was ruined.

An accident in general casts a bad light on the related operation. Therefore, the extent of the damage does not only include personal injury, environmental damage and property damage, but also expected negative effects on the image. Hence, graded levels for environmental damages are included in SQP as well as expected negative effects on the image of the plant operator. Table 2 summarizes the definitions of the risk parameters Sn and provides the key words for the analysis.

Table 2 also indicates how the parameter Sn is to be applied in investigations according to Seveso III Directive. The extent of damage is relevant for the evaluation of accidents, defined in the Directive as "serious danger to human health or the environment" (Seveso III Directive [4], Article 3, 13). If this criterion is not met, it is not a major accident corresponding to the definition of Seveso III, but an incident. Linking this with the risk parameters Sn for the extent of damage according to Table 2, the result is as follows:

S0 = no relevant injury to persons, negligible environmental damage
    = no accident,

S1 = minor injury, one person, minor harmful environmental damage
    = no accident (as no "serious danger" corresponding to Seveso III),

S2 = serious injuries or single dead, short-term major environmental damage
    = accident (as criterion "serious danger" corresponding to Seveso III),

S3 = seriously injured, several dead, long lasting major environmental damage
    = major accident,

S4 = high number of deaths, irreversible environmental damage
    = very large accident (catastrophe).

Table 2: Definition of risk parameter Sn for severity of damage.

Risk parameter for severity of damage	Extent of damage in case of effects on:			
	Persons	Environment	Image	Property values*
S0	No relevant injury	Negligible small	No effects	< 25 k€
S1	Minor injury, one person	Minor harmful effects	Negligible effects	< 250 k€
S2	Serious injuries, several persons, irreversible injury or single death	Short-term major effect	Short-term negative effects	< 2.5 Mio €
S3	Serious/irreversible injuries, many persons, multiple deaths	Long lasting major damage	Major negative impacts	< 25 Mio €
S4	Very high number of deaths	Long lasting big/irreversible damage	Long lasting negative impacts	≥ 25 Mio €

*k€ = €1,000, Mio € = €1,000,000.

The methodology SQP also uses graded parameters Wn for the probability of occurrence of the undesired event. Consequently, Wn is defined in close accordance with VDI/VDE 2180 [6] and DIN EN 61508 and IEC 61508 [7] (see Fig. 2). However, the grading of W1 to W3 is too crude for the practical application in risk assessment of industrial establishments. In particular, there is no option to also evaluate extremely rare events (that might possibly cause a huge damage). Therefore, the parameter W0 was added. This results in a span of W0 (extremely low) to W3 (relatively high) for the probability parameter Wn. Table 3 summarizes these parameters with a brief explanation of their meaning and typical numerical values for the respective probability.

These probability parameters correspond with quantitative probabilities: If an accident (e.g. large fire) is to be expected at least once in the course of service life of an installation, Table 3 indicates the use of W2 (= low probability of occurrence). Assuming a lifetime of the plant of 20 years (the technical service life is to be considered and not the economic life corresponding to the depreciation period), the probability W_{Fi} for a fire in this plant is $W_{Fi} = 1/20 \ a^{-1}$. Hence, the parameter W2 corresponds to a quantitative probability of

$$W_{Fi} = 5 \cdot 10^{-2} \ a^{-1}.$$

Table 3: Definition of risk parameter Wn for the probability of occurrence.

Risk parameter for probability of occurrence	Probability of occurrence		
	In short formulation	As imaginable frequency	As typical order of magnitude
W0	Extremely low	The incident is not expected in the course of service life of the installation, but is elsewhere in the range of the possible	$2 \cdot 10^{-3}$ a^{-1}
W1	Very low	The incident is to be expected at the most once in the course of service life of the installation, elsewhere it has already taken place	$1 \cdot 10^{-2}$ a^{-1}
W2	Low	The incident has to be expected at least once in the course of service life of the installation or has already taken place	$5 \cdot 10^{-2}$ a^{-1}
W3	Relatively high	The event has to be expected several times in the course of service life of the installation, respectively has already taken place	$2 \cdot 10^{-1}$ a^{-1}

3.4 Determination of the risk indicator

Using the parameters S0 to S4 for the severity of damage and W0 to W3 for the probability of occurrence of the undesired event, a parameter Rn for the risk is determined. For this, a formal production of Sn and Wn is carried out – in close alignment with the quantitative risk calculation (risk = severity of damage multiplied by the probability):

$$Rn = \{ Sn \} \cdot \{ Wn \}.$$

Like this, the risk can be easily "calculated" and expressed in different levels. This is used in the tabular risk analysis (Table 1). The parameters Sn and Wn are determined for each of the conceivable event sequences well as the risk indicators Rn. All is entered into columns 7 to 9 of the table. As numerous event sequences must be considered in the TRA of an industrial establishment, many risk indicators Rn appear in Table 1, correspondingly. In an evaluation of conceivable accidents these levels of risk are used:

    R0 – R1:   extremely low to low risk,
    R2 – R3:   medium risk,
    R4 – R6:   big risk that should be reduced in medium to short term,
    R7 – R12:   very high risk that cannot be tolerated.

This can also be displayed in a risk matrix (Fig. 3).

4 ANALYSIS BY CONSERVATIVELY COVERING SELECTION (ACCS)

Carrying out a TRA (tabular risk analysis) of an industrial establishment with all its sub-systems and components, results in the examination of many conceivable event sequences that might result in a major accident. Even in medium-sized installations of SME, the number of scenarios to be considered can sum up to several hundred. It is possible to reduce this number considerably by using the ACCS method (Analysis by Conservatively Covering Selection). Nevertheless, the safety of the establishment can be systematically checked.
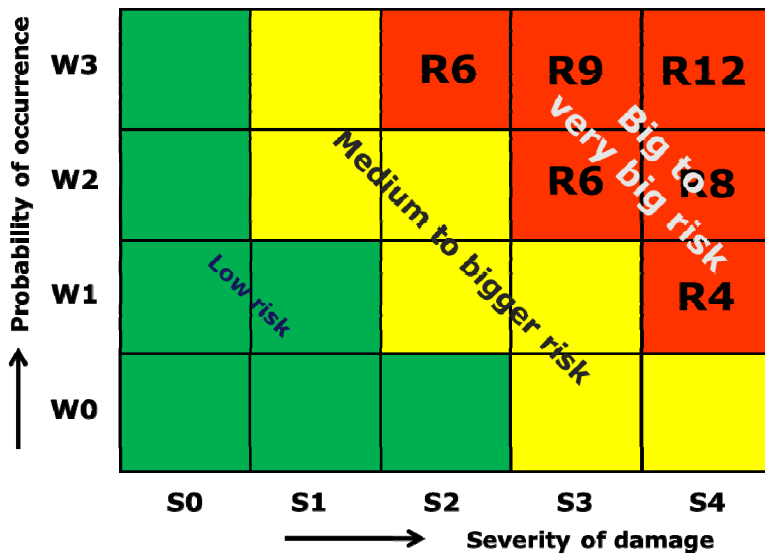
Figure 3: Presentation of the results in a risk matrix.

4.1 The ACCS method

ACCS was developed on the basis of the Failure Mode and Effects Analysis (FMEA) [8], which had been derived from the Failure Effect Analysis (DIN EN 25 448). As ACCS is a systematic safety assessment, it complies with the requirements of Seveso III. Following the ACCS method, those accidents with the most serious negative consequences can be distilled from the entire big spectrum of conceivable accidents. The procedure is as follows.

Starting point is the group of sub-systems of the establishment. In each of these systems, the units and components with the highest potential of accident damages are selected conservatively and listed in Table 1, columns 2 and 3. This is, for instance, the vessel with highest pressure, or the reactor with the more dangerous substances, the tank with the biggest quantity of hazardous materials, the pump with a higher head, the filter with the most toxic dust, the liquid with biggest potential for health hazards, etc. Likewise, from the variety of conceivable triggering events the most conservatives are selected.

All these selections are conservative. Therefore, the sequence resulting from a specified malfunction or a triggering event and the corresponding chain of events (columns 4 to 6) also conservatively cover other comparable cases.

Based on this, the risk indicator is derived for each conceivable accident. At the end of this investigation for the entire industrial establishment covering all sub-systems, a list of the relevant individual risks is displayed that exist in a plant. By comparing the risk indicators and analysing their causes, it is possible to specify and stipulate those components, sub-sections, actions of persons, etc., generating the biggest overall risk.

4.2 Example of a risk analysis

The application of SQP as a TRA together with ACCS is shown below using the example of a chemical plant – at first by considering the sub-system 2 "in-tank farm". Here, there

are various types of materials to be stored in tanks. Ammonia is the substance with by far the most serious danger to human health and the potential for the most serious major accident. Within the tank farm, there several components filled with ammonia (pipes, containers, tanks, etc.). The conservative selection results in taking the NH_3 tanks as components for the further investigation, due to the biggest quantity ammonia.

There are four NH_3 tanks, all of the same size and the same thermo-physical data with regard to operation. All tanks are placed in a collecting tray; however, they differ in age: Two of the tanks went into operation seven years ago, whereas the other two are over 30 years old. Therefore, the latter are conservatively selected for the TRA (see Table 4). These two older ammonia tanks are largely but not completely identical in construction. Both are made of 1.0425 steel (other name: H-II). Today, this material is no longer recommended for the storage of pressure-liquefied NH_3. One of the reasons is that there are more suitable steels which, moreover, have better cold-tough properties, too.

The two old tanks (A and B) are placed directly aside an access road to one of the factory buildings. Therefore, the conceivable event of a fire has to be considered that might arise in the immediate vicinity of the tanks. This can result in a bursting of one or both of the tanks. If so, the massive release of NH_3 conservatively covers other, minor releases (such as leakage through break of a supply pipe, leaking flange, and the like). The risk potential in the wake of a fire and, as well, a brittle fracture affects both old tanks about the same. On the other hand, the risk of stress corrosion cracking is in issue mainly to the older of the two old NH_3 tank because it had not been stress relief annealed.

In summary, three conceivable accidents have to be considered, a "fire in front of the tank", "stress corrosion cracking" and "brittle fracture at low temperature". In any case, the extent of damage corresponds to a major accident with several to many deaths be expected due to the massive release of NH_3. The risk parameters Sn were derived as S3 to S4. The existing measures and provisions for preventing such great damage lead to an evaluation of the risk parameters Wn for the probability of W1 to W2 (Table 4).

This results in the risk indicators of R8 (in the case of a fire next to the tank), R5 (stress corrosion cracking) and R7 (brittle fracture at low temperature), see Table 4.

The risk assessment had not only to be carried out for the sub-system 2 "tank farm" but also for all others, i.e. for the entire establishment. This was also preformed using SQP method with TRA and ACCS. The investigation resulted in a set of risk parameters Rn for some 35 conceivable event sequences and accidents, all of them conservatively covering other event sequences and respective accidents with lower extent of damage. The outcome was that – with the exception of the tank farm – only quite low risks were determined with characteristic parameters of R1 and R2, in some few cases also R3 was found, but nowhere R4 or higher. Thus, the question could be answered as to whether the operation of the plant is connected with a high/very high risk and, if so, which section it emanates from: Yes, there is a considerable risk, and this results from the operation of the NH_3 tanks.

5 EXPERIENCE WITH RISK ASSESSMENTS ACCORDING TO SQP

The introduction of the SQP method for risk analyses in companies is considerably facilitated by the fact that the utilisation of S and W is strongly based on the regulations of VED/VDI 2180 [6] and SIL [7]. All relevant engineers are familiar with this method. That is why they easily can apply the SQP risk approximation method. But there is also a disadvantage: The determination of the risk indicator Rn can also result in R0 – in case of superficial speech, apparently a zero risk. However, this is wrong; this impression must not occur.

There is no zero risk. A risk can be extremely low – but never zero.

Table 4:   Tabular risk analysis according to SQP with ACCS method for the safety evaluation of the sub-system tank farm of a chemical plant.

Sub-system	Case and component selected	Potential hazard	Conceivable root cause/ triggering event	Conceivable event sequence/potential extent of damage	Existing measures to prevent/limit the damage	Risk parameter* S	Risk parameter* P	Risk indicator R	Remark
2 NH₃ tank farm	2.1 Tank A, built in 1981	Bursting of tank, extensive release of NH₃	Fire in front of tank and collecting tray	Tanker catches fire in front of NH₃ tank Heat radiation Bursting of tank Release of NH₃ Dispersion to residential area Many dead	Fire alarm through staff Site fire brigade Alarm and emergency response plan (AERP)	S4	W2	R8	Fire alarm not automated
2 NH₃-tank farm	2.2 Tank A, built in 1981	Bursting of tank, release of NH₃	Stress corrosion cracking	Tank not stress relief annealed Crack formation Leakage Release of NH₃ Several dead High image-damage	Site fire brigade Alarm and emergency response plan (AERP)	S3	W1 to W2	R5	
2 NH₃-tank farm	2.3 Tank B, built in 1987	Bursting of tank, release of NH₃	Brittle fracture at low temperature	Tank material limited cold ductility only No pressure reduction at low temperature Brittle fracture Release and disperse of NH₃ Several, or may be many dead High image-damage	Site fire brigade Alarm and emergency response plan (AERP)	S3 to S4	W2	R7	

*Severity of damage S and probability of occurrence W:
S0 = minor property damage, no injured persons, S1 = moderate damage, S2 = accident, S3 = major accident, S4 = catastrophe,
W0 = extremely low, W1 = very low, W2 = low, W3 = relatively high.

Table 5: Tabular risk analysis of the sub-system tank farm according to SQP method after implementation of measures to improve safety.

Sub-system	Case and component selected	Potential hazard	Conceivable root cause/triggering event	Conceivable event sequence/potential extent of damage	Existing measures to prevent/limit the damage	Risk parameter*		Risk indicator	Remark
						S	W	R	
2 NH₃ tank farm	2.1 Tank A, built in 1981	Bursting of tank, extensive release of NH₃	Fire in front of tank and collecting tray	Tanker catches fire in front of NH₃ tank; Heat radiation; Bursting of tank; Release of NH₃; Dispersion to residential area; Many dead	Road closed; Automated fire alarm; Tank sprinkling; Foam extinguishing system; Site fire brigade; AERP	S4	W0 to W1	R2	
2 NH₃-tank farm	2.2 Tank A, built in 1981	Bursting of tank, release of NH₃	Stress corrosion cracking	Tank not stress relief annealed; Crack formation; Leakage; Release of NH₃; Several dead; High image-damage	Tank is stress relief annealed; Annual material inspection; Q/A of NH₃ purity; Site fire brigade; AERP	S3	W0 to W1	R2	
2 NH₃-tank farm	2.3 Tank B, built in 1987	Bursting of tank, release of NH₃	Brittle fracture at low temperature	Tank material limited cold ductility only; No pressure reduction at low temperature; Brittle fracture; Release and diserse of NH₃; Several, or may be many dead; High image-damage	Automized pressure reductuction; Operating instruction for pressure/temperature monitoring of tank; Periodical checks for possible cracks; Site fire brigade; AERP	S3	W1	R3	

*Severity of damage S and probability of occurrence W:
S0 = minor property damage, no injured persons, S1 = moderate damage, S2 = accident, S3 = major accident, S4 = catastrophe,
W0 = extremely low, W1 = very low, W2 = low, W3 = relatively high.

There are also other risk assessment methods with parameters considering graded levels for the degree of damage and probability of an event – ARAMIS [9] is an example. The main difference is that these methods do not use a similarity to SIL. Therefore, an introduction and efficient application is not as fast as the SQP methodology with TRA and ACCS, and generating results is more time consuming. (That's exactly why SQP was designed similar to SIL.) A quantitative risk analysis is to be compared with SQP under workload aspects: Instead of consuming person year(s) of skilled workforce, SQP enables a medium-sized installation to be risk analysed with limited workload of two to three person weeks only.

Once the spots causing high risk are known, this can be reduced, for instance by retrofitting. Possible variants/alternative solutions for the improvement can already be evaluated in the phase of project planning through SQP method and TRA (tabular risk analysis). This is shown using the example of the chemical plant with NH_3 tank storage (Table 4): Improved measures for fire detection and fire-fighting, the stress-relieving annealing of tank A, various adjustments in metering an control, better monitoring and inspections measures significantly reduced the probability of occurrence of accidents (see Table 5). The risks thus identified are now significantly lower and tolerable.

Risk analyses are powerful tools to prevent severe accidents in industrial installations. There are various approaches to carry out these investigations. Although the basic risk equation is the same, the risk assessment applications are different. A harmonized method, defined as a standard, would help to apply risk analyses more comprehensively and, thus, reducing losses and damages. This is stated as a final recommendation.

REFERENCES

[1] Rasmussen, N.C. et al., Reactor safety study. An assessment of accident risks in US commercial nuclear power plants. *WASH-1400,* NUREG-75/014, 1975.

[2] Bundesministerium für Forschung und Technologie (Herausgeber), Deutsche Risiko-studie Kernkraftwerke, Phase B. Verlag TÜV Rheinland, Köln, 1990. ISBN 3-88585-809-6. (In German.)

[3] Jochum, Chr., Quantitative Risikobewertung für Chemieanlagen bei Land Use Planning – Fallstudie Störfall durch Flugzeugabsturz. Meinungs-und Erfahrungsaustausch für Sachverständige nach §29a BImSchG in Dessau. *Sammlung der Präsentationen,* Warm Engineering (Herausgeber), Freilassing, 23. März 2006. (In German.)

[4] Directive 2012/18/EU of the European Parlament and the Council of 4 July 2012 on the control of major accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EG, (Text with EEA relevance). *Official Journal of the EU* (2012) L 197, pp 1–37.

[5] Rupohl, G., Das misstrauen in der technikdebatte (Mistrust in the technology debate), *KIT Scientific Publishing,* ISBN 9782821894884, 2010. (In German.)

[6] VDI/VDE 2180, Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (P–LT). Beuth Verlag: Berlin, 2007. (In German.)

[7] DIN EN 61508 & IEC 61508, *Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems*, Beuth Verlag: Berlin, 2011.

[8] DIN EN 60812, *Failure Mode and Effects Analysis (FMEA)*, Beuth Verlag: Berlin, 2015.

[9] Debray, B. & Salvi, O., ARAMIS Project: An integrated risk assessment methodology that answers the needs of various stakeholders. *WIT Transactions on The Built Environment*, vol. 82, WIT Press: Southampton and Boston, pp. 265, 2005.