Risk Considerations in the Domains of Protections Against Major Accidents in Comparison with Risk Control for Nuclear Power Plants

Authors	Felix K. Gmünder[1], Patrick Meyer[2]
Affiliation	[1]Basler & Hofmann, Consulting Engineers
	[2]Swiss Federal Nuclear Safety Inspectorate, CH-5232 Villigen-HSK, Switzerland
Address	Forchstrasse 395, 8029 Zurich, Switzerland
Mail	fgmuender@bhz.ch
Web	www.bhz.ch
Fax	+41 1 387 11 00

ABSTRACT

Risk-based decision making in the control of major chemical hazards in Switzerland is presented and compared with new risk-based decision-making framework for Swiss nuclear power plants. The legal framework on which risk control of major chemical hazards is based in Switzerland is provided by article 10 of the "Law Relating to the Protection of the Environment" (LPE, 1983) which deals with protection against disasters. Enforcement is based on the Ordinance on "Protection against Major Accidents" (OMA, 1991) which was put into effect on April 1, 1991. OMA reflects well-established procedures in risk control, in particular those used in the Netherlands in the context of the environmental control policy. At the same time, OMA requires implementation of state-of-the-art safety technology in agreement with the German practice. It is compatible with the corresponding regulations of the European Union (EC Directive 96/82 [1996] and EC Directive 90/219 [1990]). Risk analysis and risk-informed decision-making have a long tradition in the licensing and supervision of nuclear installations. Consequently, the new Swiss nuclear legislation that will come into force in 2005 makes explicit reference to risk. The Nuclear Energy Ordinance, the implementation rules for the Nuclear Energy Act, contains quantitative risk criteria for the safe operation of existing nuclear power plants and for the licensing of new ones. A preliminary outline of the decision-making scheme for risk control, to be published in the Regulatory Guides of the Swiss Nuclear Safety Inspectorate (HSK), is presented. The decision-making approach is then compared to the one used for the control of major chemical hazards. Finally, the paper contains some reflections on the use of risk-based regulatory approaches from the point of view of nuclear waste disposal.

The opinions expressed in this workshop paper are those of the authors.

KEYWORDS

Risk control, decision making, quantitative risk criteria, chemical hazards, nuclear power plant

1 INTRODUCTION

The legal framework on which risk control is based in Switzerland is provided by article 10 of the "Law Relating to the Protection of the Environment" (LPE, 1983) which deals with protection against disasters. In the aftermath of the fire of November 1, 1986 in Schweizerhalle near Basel with the subsequent catastrophic pollution of the Rhine river, political pressure increased to improve provisions on protection against serious damage resulting from major accidents. As a consequence, the Ordinance on "Protection against Major Accidents" (OMA, 1991) came into force on April 1, 1991. The issues of concern are the protection of the population, surface and ground water, soil and property. Other issues of concern may arise in special cases such as the protection of natural parks, livestock, recreational areas or ecosystems of particular value. The most important stakeholders took part in the process of creating the draft version of the OMA (chemicals industry, transportation companies, Swiss railways, future regulators etc.). In addition, before an ordinance becomes law, all affected stakeholders are consulted by the government department in charge.

2 OUTLINE AND SCOPE OF THE OMA

The Ordinance reflects well-established procedures in risk control, in particular those used in the Netherlands in the context of the environmental control policy. At the same time, the OMA requires implementation of state-of-the-art safety technology in agreement with the German practice. The OMA applies to all facilities in which (i) the threshold quantities for a defined set of substances are exceeded (examples of threshold quantities are 200 kg of chlorine, 2'000 kg of ammonia, 20'000 kg of liquefied petroleum gas or 200'000 kg of petrol) or in which (ii) dangerous natural or genetically modified micro-organisms are being contained. Furthermore, OMA applies to (iii) transport routes used for the shipping of dangerous goods (railway lines, roads, and Rhine river).

2.1 Terminology

The OMA provides the following definition for "hazard potential" and "risk":

- Hazard Potential means the sum of all the consequences which substances, products, special wastes, micro-organisms or dangerous goods could have as a result of their quantity and properties.
- Risk shall be determined by the extent of the possible damage to the population or the environment, caused by major accidents and by the probability of the latter occurring.

Note that risk is defined merely as a function of damage extent and probability of occurrence. The mathematical relationship between these two parameters is not specified.

2.2 Procedure

The procedure to control and assess relevant hazard potentials and risks consists of two steps (Figure 1).

In the first mandatory step, the owner of a facility submits a *summary report* containing an assessment of hazards. On the basis of the hazard assessment in the summary report, the enforcement authority decides whether, in a second step, a *quantitative risk assessment* has to be performed.

The summary report with the hazard assessment contains the following main items:
- A list with the maximum amount of any potentially hazardous substance kept at the facility at any given time and for which the threshold value specified by the OMA is exceeded
- A detailed description of existing safety measures
- An estimation of the extent of possible damage to the public and the environment resulting from major accidents at the facility, regardless of the (un-)likelihood of the accident(s) (maximum probable loss, see also section 3.3).

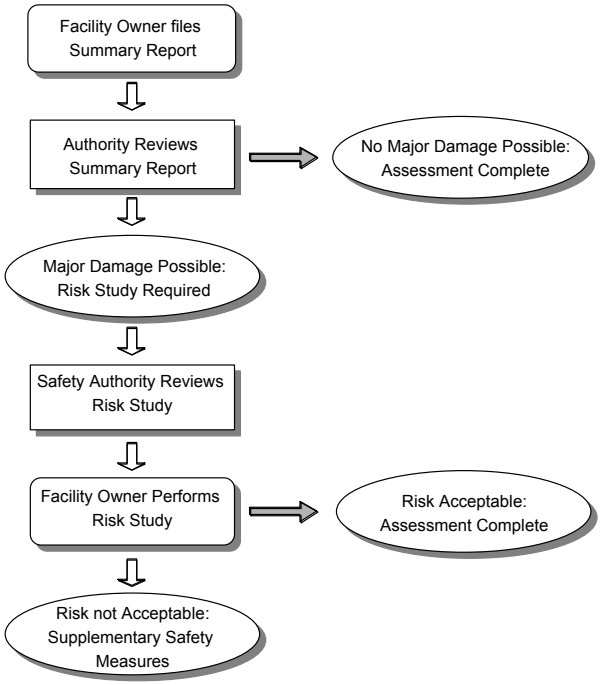


Figure 1.Two-step Procedure for hazard and risk assessment for facilities and installations falling under the OMA (SAEFL, 1996a).

If, in the first assessment step, the enforcement authority concludes that serious damage to the public or to the environment from major accidents must be expected, it orders a *quantitative risk assessment* to be performed. If serious damage is not to be expected, the assessment procedure is completed after the first step. In 1996, when the Swiss Agency for the Environment, Forests and Landscape (SAEFL) began its systematic data collection, some 2'477 facilities in Switzerland were recorded as falling under the OMA. In 40% of all cases, the summary report had been reviewed and classed. For 163 facilities, a risk assessment has been or will be performed (SAEFL, 1996a). The number of about 2’500 installations that fall under the OMA did not change since the first review.

The need for consistency in the application of the OMA throughout the different types of facilities and throughout the different regions of Switzerland was recognized at an early stage. Consequently, the SAEFL published a series of guidance documents for risk analysts and reviewers (i.e. enforcement authorities):
- *Handbooks* with the status of guidelines, explaining the technical hazard and risk assessment process to meet the OMA. In addition, separate guidelines have been published covering the evaluation of the extent of damage and the risk evaluation

(SAEFL, 1996c).

- *Manuals*, which are specific to one type of installation (such as liquid gas storage tanks) and which contain detailed technical information on how to perform hazard and risk assessment for that particular installation. Manuals contain technical background information on the physical phenomena involved in the accidents to be analysed as well as a prototype event-tree/fault-tree risk model for a fictitious facility. So far, manuals have been published for LPG storage (Basler & Hofmann, 1992), high-pressure natural gas pipelines (SNCG, 1997) and large oil storage facilities (Carbura, 1999).
- *Case studies* for fictitious facilities. These are reference studies containing models and data meant to be transferred and/or adapted to a similar case involving the same type of facility. Some case studies contain reference computer codes for solving the event-tree/fault-tree models. So far, a case study for liquid petroleum storage facilities has been published (SAEFL, 1996b) and a case study for ammonia cooling units has been drafted (SAEFL, 1999).

The *manuals* and *case studies* of the guidance documentation accompanying the OMA define the state-of-the-art for hazard and risk assessment for a particular type of facility or installation. The fact that the guidance documents are developed in a joint effort by industry and enforcement authorities guarantees a consensus over what should be considered state-of-the-art. If the state-of-the-art changes because technology evolves, the guidance documents have to be revised. The initiative for such revisions can come from industry or from the enforcement authorities.

The risk assessment is used to (i) control the risk level in facilities where major accidents with severe consequences for the population and/or the environment could occur and to (ii) inform the public about existing risks. It is but one element in a strategy aimed at protecting the population and the environment from the consequences of major accidents.

The hazard and risk assessment studies are reported to the enforcement authorities. A digest of each risk assessment study is available publicly on request. The digest contains the main results and findings of the study. The OMA requires an update of the summary report when significant changes occur at the facility. Examples of significant changes are when the production or storage capacity is raised, new equipment is installed or backfitted or when safety-relevant modifications are made to the production and/or storage processes. Based on the updated summary report, the authority decides whether the risk assessment needs to be updated, following to the two-step process described above.

Considerable effort has been put into making the hazard and risk assessment simple and accessible to the facility owners. Still, it is expected that both risk analysts and reviewers (enforcement authorities) be knowledgeable in the principles of quantitative risk assessment. Usually, the owners of facilities contract a specialized engineering firm to perform the risk assessment. There are no requirements for the risk analyst to formally document his or her competence.

2.3 Legal/Policy Issues

OMA requires the owner of a facility to take all appropriate measures to reduce risk consonant with the state of the art of safety technology and personal experience. Owners must also take all economically viable measures to reduce hazards, to prevent accidents and limit the consequences of possible accidents should they occur. In addition, OMA defines a risk control process described before. The nature of the risk reduction measures (if such measures are necessary) is not prescribed. This is perceived as an advantage, because it allows the owners of facilities to choose between a range of alternative solutions to reduce risk.

2.4 Description of Summary Reports and Risk Studies

2.4.1 Hazard Identification

The *summary report* with the hazard assessment must contain the following main items:

- A list with the maximum amount of any potentially hazardous substance kept at the facility at any given time and for which the threshold value given in the OMA is exceeded (note: the thresholds defined are the same as or lower than those of the Seveso-Directive (EC Directive 96/82 and EC Directive 90/219)).
- A description of safety measures in place at the facility or installation
- An estimation of the extent of possible damage to the public or the environment resulting from major accidents, regardless of the (un-)likelihood of the accident(s) (maximum probable loss)

Appendix I of the OMA (1991) contains a list of potentially hazardous substances and products. Above all, it contains criteria for the identification of potentially hazardous substances. These include toxicity, ecotoxicity, flammability, explosion hazard as well as criteria for dangerous micro-organisms. If the quantities of substances stored at a stationary facility exceed the substance-specific thresholds of OMA (appendix I), they must be included in the summary report discussed above.

Only those damage indicators relevant to the case at hand need to be assessed (Table 1). For instance, for the three examples appearing in this paper (LPG, chlorine and ammonia), the number of fatalities (indicator n_1) proved to be the only relevant damage indicator.

Table 1: OMA damage indicators as given in SAEFL (1996c).

Man	
n_1	Number of fatalities [people]
n_2	Number injured [people]
Natural resources	
n_3	Polluted surface water [m^3 or km^2]
n_4	Polluted ground water [person x months]
n_5	Polluted soil [km^2]
Property	
n_6	Damage to property [SFr]

Figure 2 shows the mapping of damage indicators into the three categories "Accident", "Major Accident" and "Catastrophe". If a disaster value of 0.3 is reached or exceeded for any one of the relevant damage indicators, the authority orders the owner to perform and submit a risk study.

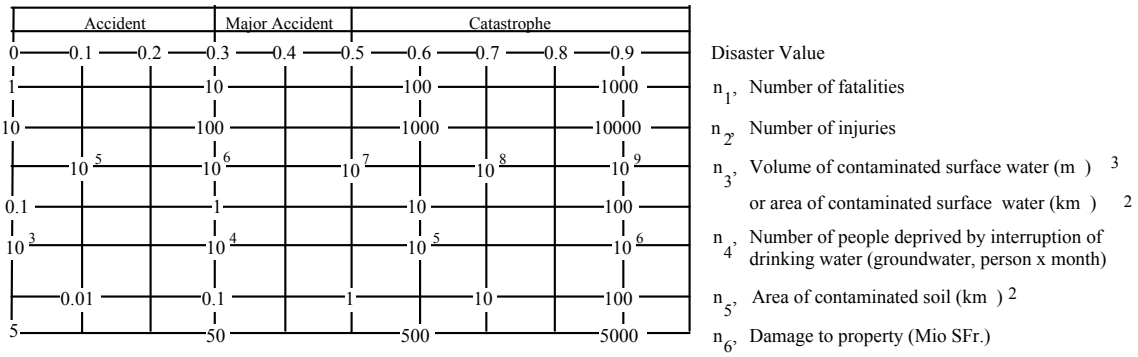


Figure 2: Scale of extent of damage indicators (assignment of disaster values) (SAEFL, 1996c)

2.4.2 Event Scenario Assessment

Event scenario assessment generally consists of the following steps:

- Identification of the *main accident scenarios* to be considered for the type of facility. The main accident scenarios are described at the phenomenological level and represent the link to consequence assessment (example: the occurrence of a BLEVE is a main accident scenario considered for LPG storage).
- Description of the *event sequences* associated with the main accident scenarios. These refer to facility-specific events (starting with the causes or initiating events) which must occur for the main accident scenarios to take place (example: a fire under the tank leads to a catastrophic tank rupture, which leads to a large and rapid release of liquefied gas which can trigger a BLEVE). The event sequences are the basis for the fault-tree/event-tree models.
- Modelling of the event sequences with of fault-trees and event-trees. To reduce the complexity of the event tree model (number of event trees, number of event sequences), *functional events* are sometimes defined (in the LPG example below, they correspond to the release categories; in the chlorine and ammonia examples, the functional events coincide with the main scenarios). The frequency of each functional event is calculated with a fault tree.

Event sequences can be identified in a top-down approach by searching for all possible ways to trigger one of the main accident scenarios. Alternatively, a bottom-up approach can be used in which malfunctions are systematically identified and analysed for their potential to trigger a scenario leading to unwanted consequences (FMEA, HAZOP and similar approaches). In practice, the top-down and bottom-up approaches are often used in combination.

As an example, Table 2 lists the main accident scenarios and the corresponding event sequences for the LPG, ammonia and chlorine examples (SAEFL, 1996b & 1999, Basler & Hofmann, 1999).

Human factors are considered to some extent through the modelling of human actions. Human actions are identified in the accident sequences and the corresponding failure events are quantified using Human Error Probabilities (HEP) found in the literature for similar actions. The risk models included in the *manuals* and *case studies* contain example human actions as well as reference HEPs. Safety culture and organizational factors are among the human factors not explicitly addressed in the risk assessment process.

Table 2. Main accident scenarios and functional events for LPG. For ammonia and chlorine, functional events coincide with main scenarios (SAEFL, 1996b & 1999, Basler & Hofmann, 1999).

LPG		**Ammonia and Chlorine**
Main scenarios	Release categories (functional events)	Main scenarios
BLEVE	Large (catastrophic) leakage	Large (catastrophic) release
Flash fire	Large (catastrophic) leakage; continuous leakage	Large continuous release
		Small continuous release
Vapor cloud explosion	(none identified)	
Fire torch	continuous leakage	
Flying debris	(consequence of BLEVE scenario)	

2.4.3 Consequence Assessment

The methods and models used for consequence assessment depend on the physical processes involved and on the event sequence scenarios considered. However in general, the following items are assessed for each scenario:

1. Quantity of hazardous substance(s) involved
2. (Time dependent) intensity or concentration over the area exposed, taking into account the effect of terrain features and structures
3. Exposure (i.e. number of people exposed, exposure time)
4. Possible consequence mitigation measures

Below, the approach to consequence assessment in each of the three examples (LPG, chlorine and ammonia) is briefly outlined for one representative scenario:

LPG, BLEVE scenario: In a first step, the amount of LPG participating in the BLEVE is determined. From this, the fireball radius (R) can be calculated. Next, mortality rates are derived for people within the fireball radius R and within a three-fold fireball radius (3R). Different mortality rates are applied for people outside (directly exposed to the fireball) and for people inside buildings. Evacuation is usually not considered feasible in the scenario due to the absence of a useful warning time.

Chlorine, large catastrophic release (tank rupture): The propagation of the chlorine gas from the ruptured tank is calculated with the help of a computer model. The time-dependent distribution of the chlorine concentration (Figure 3a and 3b) is obtained including such factors as the surface roughness of the ground and the speed and direction of the prevailing wind at the time of the accident.

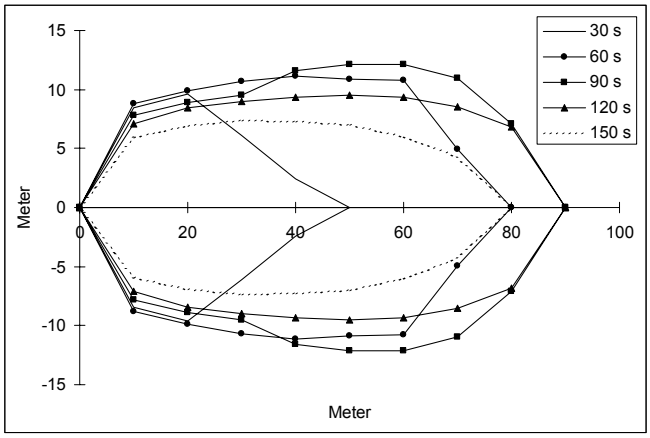


Figure 3a: Chlorine distribution for a 60 kg leakage from a storage tank. Lines of equal concentration (1000 ppm) for different values of surface roughness

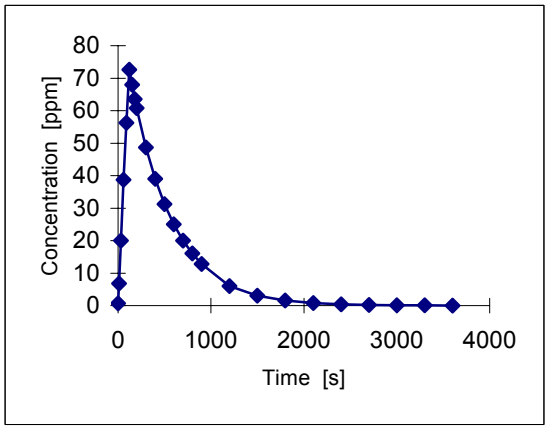


Figure 3b: Time-dependent chlorine concentration in a building as the cloud passes by.

A dose-consequence relationship (probit function) is used to determine mortality as a function of the chlorine concentration and exposure time. For nearby buildings, separate chlorine concentrations are calculated assuming a constant air substitution rate. Evacuation is credited in the assessment of exposure times in scenarios where the warning time is sufficient to allow people to react and escape from the dangerous zone.

Ammonia, large (catastrophic) release: Similarly to the chlorine scenario described above, the time-dependent concentration of ammonia is calculated using a propagation program. A minimum required concentration for lethal exposure is used to delimit the perimeter within which exposure must be considered. Due to the speed with which the scenario develops, no credit is taken for evacuation.

Consequence mitigation measures can be (and should be, if adequate) included. They include the intervention of the fire brigade and evacuation of the population at risk. Credit can be taken for the fire brigade if it can be shown that there is a sufficient warning time for it to deploy. The success of evacuation generally depends on the warning time and on the population density in the exposed area as well as in the emergency evacuation routes (see also the examples of consequence assessment in section 5.1).

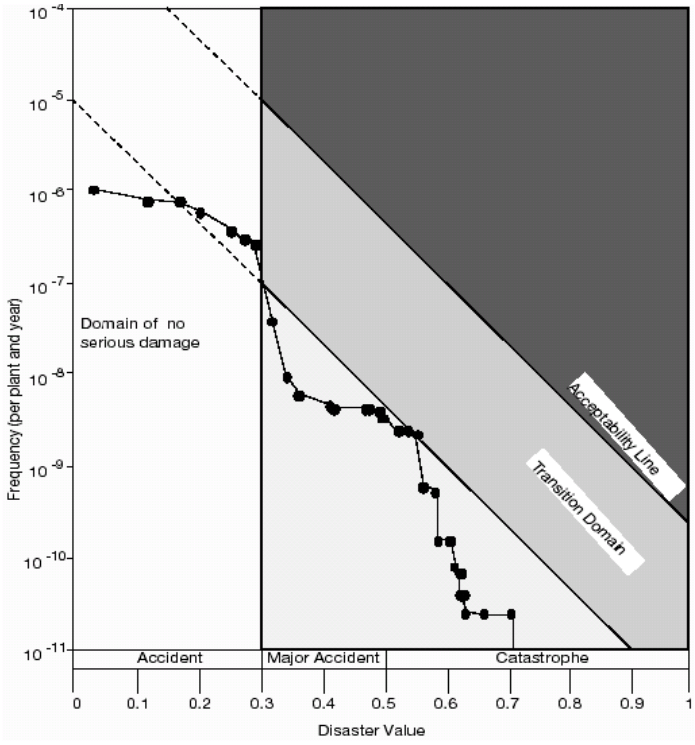
2.5 Risk Estimation and Risk Comparison

The likelihood of effects is expressed quantitatively in terms of the frequencies of the accident scenarios.

The diagram in Figure 4 is divided into four domains:
- no serious damage
- acceptable
- transition
- unacceptable

The slope of the boundary lines separating the three domains 'acceptable', 'transition' and 'unacceptable' is quadratic. This is to account for the risk aversion commonly associated to accidents with large consequences. In risk estimation and risk comparison, the yearly frequencies of the relevant scenarios are plotted against the disaster values in a cumulative frequency distribution (Figure 4). From the cumulative frequency distribution, the acceptability or non-acceptability of the risk can be readily determined. Note that the slope of the boundary lines separating the three domains 'acceptable', 'transition' and 'unacceptable' is quadratic. This is to account for the risk aversion commonly associated to accidents with large consequences.

Figure 4: Societal risk criteria for major accidents (SAEFL, 1996c). Cumulative frequency diagram showing the number of fatalities (n_1) for the LPG storage example. The dots represent individual accident sequences.



The enforcement authority evaluates the risk as follows (Figure 4):

1. If the cumulative frequency curve enters the unacceptable domain the owner of the facility is asked to reduce the risk, else the authority is empowered to take actions including operational restrictions or shutdown.
2. If the cumulative risk curve enters the transition domain, the enforcement authority will measure the interests of the facility owner against the needs of the public and the environment for protection from accidents. Depending on the outcome of these considerations, the risk has to be reduced to a level defined by the authority.
3. If the cumulative risk curve lies in the acceptable domain all through, the risk assessment procedure is complete. However, the owner must still take all appropriate measures to reduce risk (s. below).

To obtain more insights on dominant risk contributors, separate curves can be plotted in the cumulative frequency diagrams grouping scenarios, which take their origin in the same initiator (Figure 5). A risk outlier can be defined as representing a substantial fraction of the total risk, where "substantial" is not further defined. A vulnerability is a risk outlier whose cause can

be attributed to a system, type of component or operational practice of the installation under scrutiny. A vulnerability would further exist if a significant amount of risk were due to one particular type of accident (Figure 6).

Figure 5: Cumulative frequency distribution showing the contribution of the different scenarios to the number of fatalities (n_1) for the LPG storage example.

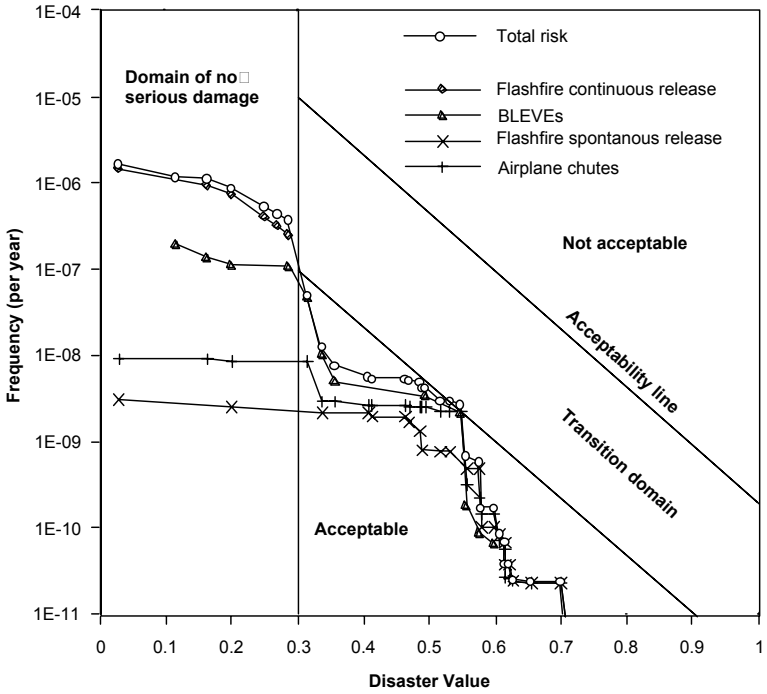
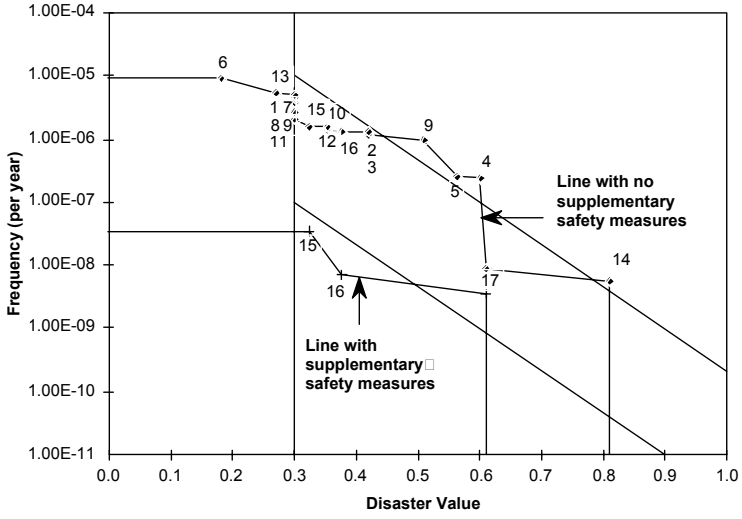


Figure 6: Cumulative frequency distribution showing the number of fatalities (n_1) for the example of the ammonia refrigeration plant in a public ice skating rink. The upper curve shows the risk before, the lower curve the risk after implementation of supplementary safety measures. The numbers correspond to individual accident scenarios.



3 RISK CONTROL IN LICENSING AND SUPERVISION OF NUCLEAR INSTALLATIONS

Since the mid-eighties and the requirement for full-scope probabilistic risk studies (PSA) for nuclear power plant, control of risk from nuclear installations has played an increasingly important role in regulation in Switzerland. In 2005, a new legal framework will be introduced with the coming into force of the Nuclear Energy Act and its implementation rules, the Nuclear Energy Ordinance. The Energy Ordinance contains quantitative targets for the risk from nuclear installations. Furthermore, the Safety Guides issued by the Swiss Nuclear Safety Inspectorate HSK, currently under revision, will include guidelines for regulatory decision making which address both the risk and the uncertainties contained in the quantitative estimation of risk.

3.1 Legal Basis

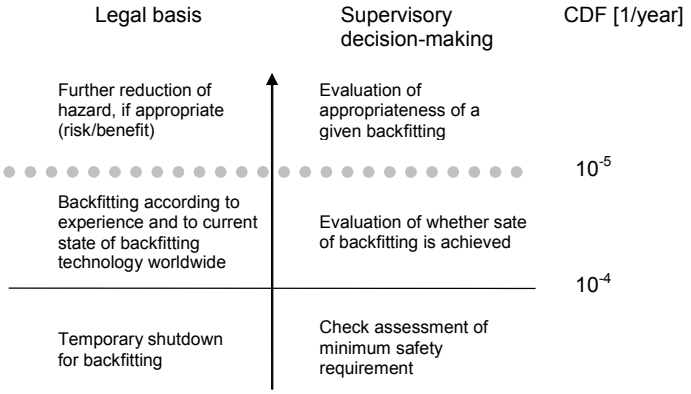
The Nuclear Energy Act requires the license holder to take the nuclear installation temporarily out of service and backfit it when certain criteria are met (article 22/3 of the Nuclear Energy Act). In response to this general rule, the Nuclear Energy Ordinance limits the total core damage frequency (CDF) for nuclear power plants. For new nuclear power plants commissioned after the coming into force of the Nuclear Energy Act, the CDF must be smaller than 10^{-5} per year and plant. For operating nuclear power plants, the CDF must be smaller than 10^{-4} per year and plant or else the plant must be temporarily shut down and

backfitted. In fact, the target values recommended by the International Atomic Energy Agency (IAEA, 1992) are turned into firm shutdown rules by the Swiss regulations. Independently from probabilistic requirements, the Nuclear Safety Act also requires that operating nuclear power plants be "…backfitted to the extent necessary according to experience and the current state of retrofitting technology (worldwide), and beyond, provided this contributes to a further reduction of hazard and is appropriate" (article 22/2/g of the Nuclear Energy Act).

3.2 Supervisory Decision-Making for the Backfitting of Nuclear Power Plants

Figure 7 depicts the proposed probabilistic basis for the future supervisory decision making process concerned with backfitting existing nuclear power plants (i.e. commissioned before the Nuclear Energy Act comes into force)[1]. Starting from the bottom of the picture, the lower safety limit for operating plants required by article 22/3 was set at a CDF of 10^{-4} per year. This corresponds to the value recommended by IAEA for operating nuclear power plants. Figure 7 also sets a target value at a CDF of 10^{-5} per year to discriminate between those backfits necessary to maintain safety with experience and the current state of retrofitting technology and those which further reduce hazard, if appropriate (article 22/2/g of the Nuclear Energy Act). For a well-balanced supervisory decision basis, these probabilistic criteria will have to be supplemented by criteria from design-basis and from operational experience.

Figure 7: Core damage frequency (CDF) per year and legal basis and supervisory decision making.



The somewhat fuzzier delimiter used for the "state-of-the-art" line means that the value is a target (recommended) value whereas the "minimum safe operations" line is considered a "hard" threshold. Note also that neither delimiter is frozen for all times: expected progress in safety technology is likely to move both delimiters towards lower values of CDF representing higher safety levels.

3.3 Supervisory Decision-Making for additional Measures against Severe Accidents

Note that the decision-making framework proposed in Figure 7 is based on point-estimate (mean) values for the CDF. Figures 8a and 8b depict a somewhat more elaborate decision-making process where the uncertainty on the estimates is explicitly taken into account (Schmocker 1997). The decision diagram in Figure 8b illustrates the steps of the decision-making procedure: if the 95%-fractile curve for the candidate nuclear power plant is smaller than the limiting curve for the mean ("limit mean"), then no further measures against severe accidents need to be considered. This would be the situation where the likelihood of core damage being lower than 10^{-5} per year could be demonstrated with 95% confidence (or conversely, that there is only a 5% chance that core damage is greater or equal to 10^{-5} per year). Next, the mean and 95%-fractile curves of the candidate nuclear power plant are checked against their respective limiting curves ("limit 95%" and "limit mean" respectively). If either of these criteria is violated, potential backfits against severe accidents need to be implemented regardless of costs involved ("Yes" path). If both criteria are met, potential improvements or backfits need to be implemented only if they are cost-effective ("No" path).

[1] Although legally possible, the commissioning of new nuclear units in Switzerland within the next decade is not believed to be politically feasible. Consequently, as far as nuclear power plants are concerned, the Nuclear Energy Act and its ordinances will apply to existing units only.

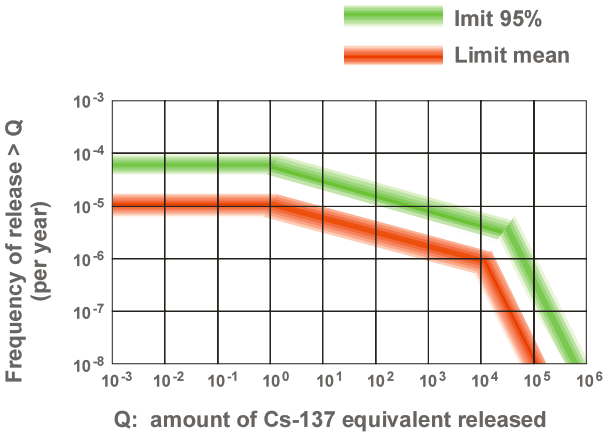


Figure 8a

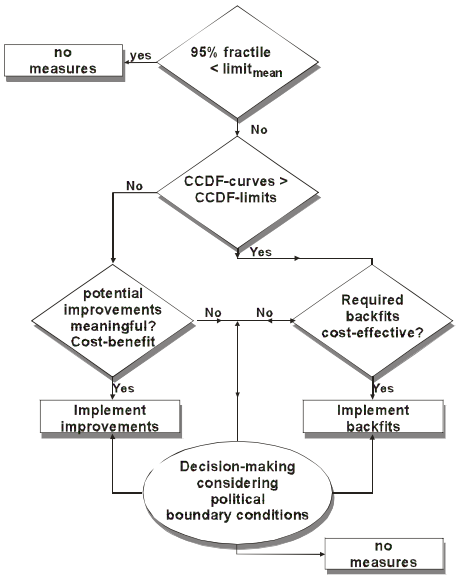


Figure 8b

This framework has been used by HSK to evaluate the appropriateness of additional measures to mitigate consequences of severe accidents in Swiss nuclear power plants. The frequency of release of radioactive aerosols (measured in terms of the amount of Caesium equivalent released) was chosen to evaluate the impact of severe accident measures. In contrast to the decision diagram depicted in Figure 7, which relies on a single point-estimate value, two percentiles (the mean value and the 95-percentile) from the release frequency distribution are independently controlled, effectively and explicitly involving the uncertainty of the estimate in the decision-making process. Note that uncertainty represented here as the difference between the mean and the 95-percentile of the distribution represents the sum total of epistemic and aleatory uncertainties which are quantified in the probabilistic model used to estimate release frequencies.

4 DECISION-MAKING IN THE PROTECTION AGAINST MAJOR ACCIDENTS VS. DECISION-MAKING IN THE CONTROL OF NUCLEAR RISK

It is interesting to point out the differences in the two decision-making approaches described above. Although both of them are risk based, significant differences exist in system characteristics, in the approach and in the underlying methodology to quantify risk and uncertainty (Table 3).

Table 3: Differences between two approaches

	Chemical hazards (OMA)	NPP Risk (Nuclear Safety Act)
System characteristics	Low to medium hazard potential. Hazard potential can be reduced	Large hazard potential. Hazard potential difficult to reduce
Decision-making approach	Hazard control through risk reduction	Risk control through safety improvements
Risk analysis methodology	Probabilistic, point estimate estimation	Probabilistic, distributed input- and output parameters
Treatment of uncertainty	Implicit, through reduction of risk	Explicit. Risk criteria take into account uncertainty.
Backfitting rule	State of the art technology determines appropriate measures to reduce risk. Probabilistic target to determine supplementary safety measures to be implemented.	Probabilistic target for minimum safe operations. State of the art of backfitting technology must be implemented regardless of probabilistic target.

4.1 System characteristics

The OMA applies to installations with small to medium hazard potentials. Often, technological alternatives exist that allow more hazardous installations to be replaced by less hazardous ones (reduction in the amount of hazardous substances involved; changeover to a less risky technology altogether). The same is difficult to achieve for today's nuclear power plants: their radioactive inventory (hazard potential) is intimately linked to the power they produce. A reduction in hazard potential by a nuclear alternative would require a substantial technological step.

4.2 Decision-making Approach

The decision-making approaches chosen are commensurate to system characteristics. Where risk reduction can be achieved by

hazard control, the uncertainties on the remaining risks are minimized too. Where hazard control is not feasible, risk control is the (necessary) alternative.

4.3 Risk analysis methodology and treatment of uncertainties

There are only minor differences in the analysis and quantification of risks between the two approaches. Working with distributed parameters is a prerequisite to the explicit use of uncertainty in the decision-making process. One could argue that the treatment of uncertainties is implicit in the case of the OMA decision-making scheme: reducing risk to a residual level also reduces the uncertainties associated with those risks. In fact, this is the approach chosen by deterministic safety assessment, where safety substantial safety margins are used in design to rule out certain undesirable outcomes.

4.4 Backfitting Rule

Backfitting is usually what drives the regulatory costs for existing installations. Consequently, backfitting rules are often important elements of regulation that reveal the true face of a decision-making approach. The most striking feature of both approaches is that they do not solely rely on risk criteria. Regardless of whether the risk criteria are met, the state of the art in safety technology must be implemented by the owner/the license holder.

5 CONCLUSIONS

- In Switzerland the Ordinance on Protection against Major Accidents (OMA, 1991) has been in force since 1 April 1991.
- Accompanying handbooks and guidelines published by the Swiss Agency for the Environment, Forests, and Landscape (SAEFL) which include an example of a summary report and a risk study as well as risk evaluation criteria have enhanced substantially the enforcement delegated to the Cantons.
- Hazard potentials have been reduced by many establishments with dangerous substances, products or special wastes below the quantity thresholds set by the to evade coming under the OMA.
- Safety measures in the great majority of establishments are now more thoroughly checked and updated if necessary.
- The OMA has initiated education and development of knowledge with regard to risk and safety. In particular, the Federal Institute of Technology at Lausanne and Zurich and at the University of St. Gall started postgraduate education in 1994 and many companies are keen to improve expertise.
- Information of the public is one of the main goals. However, the intention of the OMA is to disclose just the summary of the risk study on request. This rather restrictive information policy results from public indifference on the one hand and new regulations on privacy on the other.
- For many years, risk criteria have been a valuable tool for the targeted continuous improvement of the safety of nuclear power plants. In the future, risk-based decision making will receive a legal basis when the Nuclear Energy Act and the Nuclear Energy Ordinance become effective in the year 2005.
- In risk-control for nuclear power plants, decision-making is moving from the use of point-estimate values towards the explicit consideration of epistemic and aleatory uncertainties.

Some Thoughts from the perspective of Safety Assessment for Nuclear Waste Repositories

The assessment of the hazards of nuclear waste repositories is specified in the Swiss regulatory guide HSK-R-21. The more likely scenarios for the release of radioactive substances are assessed deterministically using conservative assumptions to control uncertainties. The less likely scenarios have to meet a risk target, where the risk measure is the product of probability and consequences. A safety report is required that contains elements in analogy to the summary report for installations that fall under the OMA. But unlike in the case of the OMA, the elements are evaluated quantitatively. An important difference to both OMA and NPP safety is that nuclear waste repositories cannot rely on mitigation to prevent inadmissible releases, since such releases would take place in the far future. The repository has to be designed based on passive safety. While dose or dose risk is the primary measure, additional indicators such as the release of radionuclides across defined system boundaries or concentrations of radionuclides in defined system parts are used to characterize the safety of nuclear waste repositories. This could be compared to the choice of damage indicators of the OMA. As for scenario analysis, the main observation is that in the repository safety analyses, the description of the baseline case itself (the reference or "null" scenario) is very labour-intensive, since this first step is by no means trivial and requires challenging predictions into the future. In safety analyses performed so far, the possible risk target has not been used, but probabilistic calculations have been used to assess the effects of multiple uncertain parameters in particular scenarios. The results of these calculations were shown as cumulative damage frequency curves similar to the one in Figure 8a.

6 REFERENCES

- Basler & Hofmann (1992). *Manual for LPG Storage Vessels regarding the Summary Report and the Risk Study in Relation to Protection Against Major Accidents* (in French and German). Basler & Hofmann Consulting Engineers, Forchstrasse 395, CH-8029 Zürich, Switzerland.
- Basler & Hofmann (1999). *Case Study of a Risk Study for a Chlorine-Based Cleansing Plant in a Public Swimming Pool*

(in German). Basler & Hofmann Consulting Engineers, Forchstrasse 395, CH-8029 Zürich, Switzerland.
- Carbura (1999). *Manual for the Safety of Large Mineral Oil Storage Facilities.* CARBURA and Swiss Agency for the Environment, Forests and Landscape (SAEFL), (revision 11), Zurich, Switzerland.
- EC Directive 90/219 (1990) on the Contained Use of Genetically Modified Micro-organisms.
- EC Directive 96/82 (1996). Seveso II Directive on the Control of Major Accidents Hazards Involving Dangerous Substances.
- IAEA (1992). IAEA Safety Series No. 106, "The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety", 1998.
- LPE (1983). *Law Relating to the Protection of the Environment. Bundesgesetz vom 7. Oktober 1983 über den Umweltschutz (USG).* SR 814.01, Berne, Switzerland.
- OMA (1991). *Swiss Ordinance on Protection against Major Accidents* (Ordinance on Major Accidents, OMA), SR 814.012, (in English, French or German) February 27, 1991 (Updated July 1994), Berne, Switzerland.
- SAEFL (1991). *Handbook I for the Ordinance on Major Accidents, OMA, Guidelines for Establishments with Substances, Products or Special Wastes* (in French or German), Swiss Agency for the Environment, Forests and Landscape, SAEFL, Berne, Switzerland.
- SAEFL (1996a). *Umweltschutz*, monthly publication of the Swiss Agency for the Environment, Landscape and Forests, SAEFL, Nr. 3/96, March 1996 (in German), Berne, Switzerland.
- SAEFL (1996b). *Case Study of a Risk Study for a LPG Storage Vessel, Ordinance on Major Accidents* (in French or German), Swiss Agency for the Environment, Forests and Landscape (SAEFL), Berne, Switzerland.
- SAEFL (1996c). *Evaluation Criteria for the Ordinance on Major Accidents, OMA, Evaluation of the Extent of Damage, Evaluation of the Acceptability of Risk, Guidelines for Establishments with Substances, Products or Special Wastes* (in French or German), Swiss Agency for the Environment, Forests and Landscape (SAEFL), Berne, Switzerland.
- SAEFL (1999). *Case Study of a Risk Study for an Ammonia-Based Cooling Process in a Public Ice Rink* (in French or German, draft edition). Basler & Hofmann Consulting Engineers, Forchstrasse 395, CH-8029 Zürich, Switzerland.
- Schmocker, U. (1997) *Technische Massnahmen zur Begrenzung der Folgen schwerer Unfälle*. SVA-Vertiefungskurs "Notfallmanagement innerhalb und ausserhalb des KKW", Winterthur, 15.-17. Oktober, 1997.SNGC (1997). *Manual for the Safety of High Pressure Natural Gas Installations.* Swiss Natural Gas Company (revised edition), Zürich, Switzerland.