
Learning From Experience in Safety Engineering and Development of Safety Philosophy

H. Liemersdorf*, J.-C. Niel**

* *Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, D-50667 Köln*

** *Nuclear Safety and Radioprotection Institute, F-92265 Fontenay-aux-Roses*

1 INTRODUCTION

The technical development starting with the use of fire to produce metallic materials up to the time being with a high level of technology has been determined by a process of learning from experience. Let us look back on the development of steam engines and railways as an example. A view to the historical research refers to a long process of learning with numerous accidents. Burst of the steam vessel was the main reason described by history books. Learning from experience was a principle of the technical development. Step by step the quality of material and manufacturing improved and preventive technical devices to limit high pressure such as safety valves have been developed. As a result of this process of learning, the need for design and assessment criteria has also been identified with respect to the specification of materials or rules for design and construction. To harmonize this knowledge, specific design codes have been developed (e. g. the steam boiler ordinance), first in Great Britain and later on in other countries with an industrial technical progress. The goals and objectives of these codes contained both, quality assurance with respect to the availability and performance of the steam engines and railways as well as safety engineering to avoid a steam vessel burst or other dangerous impacts to the people. Concerning safety engineering another important step in the historic development was the installation of a state supervision with independent inspectorates. However, in parallel to learning from experience the scientific basis for the design of technical equipment and components has been built up by a development of technical calculation methods.

Different to the example “steam engines and railways”, in the field of use of nuclear energy the need of an anticipatory safety assessment was in fact recognized in an early stage. That need led to the principle of incorporating safety in the design phase of a nuclear power plant (NPP). Based on this principle, the following is a good question:

Do we really need experience feedback for NPP safety?

2 HISTORY OF DEVELOPMENTS IN REACTOR SAFETY

Evaluating the history of using nuclear energy, the safety philosophy of a NPP is mainly based on three aspects:

- Multiple barriers for the retention of fission products with stringent quality requirements,
- Anticipatory analyses of possible events and the implementation of effective and reliable engineered safeguard systems for their control, and

- Specific research to gain insight to phenomena, effects, event sequences, and influences as a basis of the safety related design,

Thus the initial assumption was: **Safety = Technical Safety**

However, real events such as TMI and Chernobyl revealed the significance of operator actions and of the cultural and organizational environment for reactor safety. Safety reviews with regard to the state-of-the-art in science and technology have shown a need for upgrading safety measures and preventive maintenance. Furthermore, probabilistic safety analyses (PSA) became a more widespread tool for the quantitative assessment of the safety level as well as for finding gaps in the deterministic safety concept including the human factor.

That development leads to the actual definition: **Safety = Technical Safety
+ Safety Management**

In this definition, safety management includes all influences related to human factor, organizational aspects, the interaction of man, technology and organization (MTO), and measures to optimize the nuclear safety culture.

Taking into account this development and asking for the contribution of experience feedback, one will find the following insights:

- The investigation of incidents in NPP worldwide is the main basis for technical and human factor improvements.
- The use of operating experience feedback is a major aspect of safety management.
- PSA relies on operating experience in analyzing event sequences.
- PSA requires data from operating experience to quantify the reliability of systems and components.
- PSA reveals precursor events which can be observed during NPP operation worldwide before the occurrence of severe core damage (example: events prior to TMI).

Likewise, the experiences in other highly technical non-nuclear fields show the importance of the operating experience. As an example: The analysis of severe accidents in space technology also revealed precursor events in the operating experience.

The conclusion takes into account that besides all anticipatory safety measures and analyses the experience feedback from the operating plants is needed to ensure the NPP safety on a high level.

3 INSTRUMENTS FOR THE USE OF EXPERIENCE FEEDBACK

The use of experience feedback from NPPs requires:

- A suitable method for processing each NPP's own findings, events and their causes for internal use as well as for the transfer of appropriate information to external authorities,
- Information paths (systems) for the exchange of the findings,
- An adequate method for evaluating the findings from other NPPs to clarify their applicability to other plants and to implement improvements.

For an effective use of experience feedback the following prerequisites have to be fulfilled:

- Covering all incidents worldwide occurred is necessary, as relevant events do not occur very often,
- Performance of in-depth accident analyses and not just of remedial actions,
- Willingness to report openly and adequately about all relevant findings,
- Willingness to learn from the experience of others and to make one's own improvements.

3.1 Current systems for the reporting of incidents and for exchange of information in the international frame

In principle, in all countries with operating NPPs, the licensees as well as the regulatory authorities dispose of national evaluation and reporting systems which may be quite different in kind, depending on national conditions.

For the international exchange among NPP licensees, the WANO system was installed. This system contains several activities, amongst other things external plant safety reviews, the determination of performance indicators and, last not least, the exchange of information on important incidents.

For the international exchange on the authority and TSO level, the Incident Reporting System (IRS) of the IAEA/OECD-NEA was set up. It is the major technical tool for the use of feedback in the international frame. The IRS reports contain in depth information with respect to causes of incidents, the plant behavior, and the technical systems involved.

The IAEA furthermore developed and established an information and classification system for the information of the general public. That is the “International Nuclear Event Scale (INES)”. In the case of incidents or accidents with a classification of INES ≥ 2 short reports will be distributed by the IAEA. In that sense, INES is a communication instrument not being suitable for a technical feedback.

It has to be noted that all these systems follow different objectives (not just safety).

From the IRSN and GRS point of view, the following insights and suggestions should be pointed out:

- Involving NPP licensees in the comprehensive and in-depth evaluation of operating experience does not follow a standardized pattern and should be improved. That does not mean a call for a more strict official regulation. It is a part of responsibility and self-interest and last not least a part of an actively practiced safety culture.
- The official national reporting systems in Europe should be harmonized and assimilated. Germany, in particular, is not a good example for realizing an adequate reporting system:
 - Two different evaluation concepts with respect to the safety significance of incidents exist side by side (national reporting criteria and INES scale).
 - Reporting criteria are sometimes not sufficiently differentiated and precise and therefore open to interpretation; they are oriented too much to formal criteria such as the time between the occurrence of an incident and the required report.

- There are no regulations for a generic evaluation of events below the reporting threshold.
 - A review is planned, but GRS is concerned that necessary developments may be handicapped by conflicting interests of the Federal Ministry for the Environment, Nature Conservation and Reactor Safety (BMU) and the Federal States authorities ("Länder"). From GRS expert point of view, it is absolutely necessary for an improved use of the German operating experience that rules will be established for the generic analysis of findings and events below the reporting threshold in a way that
 - ⇒ Experts can make use of these investigations when developing safety related improvements.
 - ⇒ At the same time, the licensees' interest in the confidential treatment of operational processes remains protected.
- In the case of the licensees' international "WANO" reporting system, for many years the activities focused on the identification and representation of "Performance Indicators". However, the necessary transparency is not yet noticeable. We believe that an increased exchange of information on safety related operation experience would be more important.
- Regarding the official international reporting systems, the following can be stated:
- The "INES" scale has proven its worth both with regard to its objective and its methodological approach; it is now applied all over the world. Recent developments aim at a more precise differentiation of radiological events with little consequences (operating personnel and environment in the close vicinity) (background: these events outnumber those reported according to INES criteria).
 - With its detailed descriptions of the causes and sequences of events, the "IRS" provides a technically qualified basis for the feedback of experiences to authorities and TSOs. However, preparing the individual reports requires quite a considerable effort. As a matter of fact, the number of reports issued by almost all participating countries has noticeably decreased as a result of budgetary cuts. As a result, the authorities in charge, e. g. OECD, have recommended to all member countries to fulfill their obligations. From the TSO point of view, we strongly support this recommendation.

4 FINDINGS AND CONCLUSIONS

As already indicated in the introduction, the feedback of experience also influenced the development of safety philosophy. Examples are:

- The continuous development of the technical systems and procedures for the control of LOCAs, differentiating between leak size and leak location (e. g. for breaks in the area of the pressurizers in PWR plants after the TMI event),
- The development and establishment of safety management systems with regard to the preservation of technical qualification, safety-directed operator actions during plant operation, and MTO interaction,
- The importance of being able to control radiolysis gas accumulations in BWR plants (application of the defense-in-depth concept by providing successive measures),
- The development of an ageing management system for the timely detection of ageing mechanisms with a view to preventive maintenance.

Ageing management in particular requires continuous analysis of operating experience. However, care should be taken in this context – as in all other evaluations of operating experience – that these investigations are not restricted to a simple (rough) identification of indicators and trends. By no means we want to question the usefulness of such statistical analyses. They are an important tool for the experts.

Nevertheless, the practice of daily evaluation has shown that in principle safety-relevant events are complex processes which may affect different technical systems as well as the behavior of the personnel.

Therefore, there is a general need for a thorough interdisciplinary engineering approach in order to correctly identify the various coherences. As an example, two types of actual incidents should be described briefly:

- During fuel loading from the fuel storage tank to the reactor vessel of a French NPP an error in the loading occurred in 2001. A great number of fuel elements has been found in a wrong position. Analyses showed that a significant influence on the control of reactivity could result from unfavorable conditions. The cause of the incident was a systematically error of the operators and deficiencies in the organization of the staff.
- Failures in the barriers for containing radioactive material have been identified by two incidents in German NPPs, which occurred in 2002 and in 2004. In both cases the release of radioactivity to the environment and the radiation dose to the workers inside the plants was very small. However, there is a safety significance due to the fact that more than one level of defense in the defense-in-depth concept failed. Despite this, it has to be clearly stated that the experience feedback from similar events in the past was not effective. From GRS point of view the reason could be a lack in the analysis depth of the external operating experience by the operator.

Particular diligence in these activities is always required whenever findings from other plants have to be checked for their applicability. Practical experience has shown that it is mostly the licensee who often sets too high standards and then breaks off any further observations, if e. g. materials, components affected or the location of installation do not correspond to the specifications. However, if the observed causes or damage mechanisms may also have safety-relevant effects on other components, the evaluations have to be continued.

It is also inappropriate to discount any findings on operational systems that have no safety significance, if comparable safety related systems exist, which might potentially be affected. Especially the upgrading of I&C systems to modern digital I&C also for the safety system calls for wide-ranging feedback of experiences so that unknown design deficiencies can be detected in time.

The importance of probabilistic precursor analyses was underestimated for a long time. This was mainly due to methodological shortcomings. Today's advanced probabilistic analysis methods, however, are useful tools allowing to show up quantitatively the safety relevance of relevant events. A recent trilateral study by IRSN, GRS and NUPEC has shown that the procedures in the respective countries differ and that the results can therefore not always be compared one to one. Related to the underlying analyses and data, however, it is possible to make reliable statements on the safety margins that still exist in the events that occurred regarding the probability of damage to the reactor core. This provides both licensees as well as regulatory authorities with a basis for the assessment of the adequacy of upgrades and technical improvements. Therefore, this analytical tool should in future be used more systematically. The most important prerequisite, namely the availability of a plant specific PSA, has by meanwhile been largely fulfilled for all European plants.

Finally, we would like to say a few words about the role of deterministic and probabilistic approaches in reactor safety assessment. Whatever the strength of probabilistic approaches, the deterministic approach remain the base. An effective feedback of safety related operating experience is needed in both approaches.