SAFETY OF NUCLEAR POWER; WHO LEARNS FROM WHOM?

B. WAHLSTRÖM, P. HAAPANEN, K. LAAKSO and U. PULKKINEN

Technical Research Centre of Finland, VTT Automation, P.O.Box 1300, FIN-02044 VTT, Finland

Abstract: The safety of hazardous installations is a common concern for many industrial areas. The story of nuclear power safety is considered with a special emphasis on the transfer of experience between nuclear power and other industrial areas. There should be several benefits of an exchanging of experience and safety methodologies, but it seems that such exchange has not been very efficient. Incidents and accidents seem to have had a very large influence on how safety practices have developed. Different mechanisms and organizations promoting an exchange of experience between and within industrial areas are discussed. It is argued that a systems approach to safety is beneficial especially when experiences from neighboring industrial fields are interpreted. The inherent dilemma for management of safety is the incongruity between safety and efficiency. Improvements in efficiency can make an installation less safe. Accidents can accordingly be seen as unsuccessful experiments aiming at improving efficiency. Education and training in the systems aspects of safety should make it easier to exchange experience in the design, construction, operation and maintenance of hazardous installations.

Key Words. Safety; reliability; nuclear power; social and behavioral sciences; human factors; man-machine systems; system analysis; system failure and recovery

1. INTRODUCTION

Nuclear power for electricity production was, when introduced, seen as a technology with many expectations. Today an increasing public opposition, strengthened by the accidents at Three Mile Island (TMI) and Chernobyl, has caused this picture to fade. The opposition points to failures of communication, because from an objective point of view the nuclear industry has been able to achieve a remarkable safety record.

Safety has been a continuing concern for the nuclear industry. It has fostered an environment for the development and application of many new methodologies of safety engineering. Some twenty years of technological development have brought many of the early ideas for assessing and improving the safety of the plants almost to a regular use. The nuclear industry has, in developing these methodologies, been able to draw experience from other industrial fields. Similarly there has been a transfer of knowledge from the nuclear field to other industrial areas. In spite of this it seems that incidents and accidents have provided the most intense learning periods. This would suggest that each industrial area has to go through its own hard lessons, because accidents have seldom revealed something new.

Safety is important not only for nuclear power, but also for the chemical industry, off-shore, transportation, aerospace applications, etc. These industries have developed and utilized their own approaches, by which a remarkable safety record has been reached. Different industries have different needs, but safety is on a generic level similar. A continued safety relies both on efficient safety assurance methodologies and on an efficient utilization of experience. The utilization of the methodologies and experience applies not only to technical solutions, but also to the approaches by which the technical processes are managed. Regulators and standardization organizations have an important role in enforcing a transfer of good safety management practices. Research organizations, consultants and vendors working in several industrial fields have also important roles in transfering experience between industrial fields.

If there is only little interaction between different industrial areas it is likely that they will diverge with respect to details of their safety solutions. This would lead to an accumulation of less operational experience and therefore perhaps to less mature solutions and a degraded safety. It is also more difficult to introduce new technical solutions if the practices in different industries are very diversified. Clearly conservatism and cautionness has to be applied for hazardous installations, but it should not lead to postponing the introduction of improved technologies. The introduction of programmable systems for safety systems in nuclear applications has raised these kinds of concern.

The paper addresses cross-industrial learning processes especially from the view of the nuclear industry. Safety practices such as deterministic safety requirements, probabilistic safety analyses, control room reviews, incident analysis methods, safety communication, etc. are discussed as examples. A systems approach for safety management which is based on a safety analysis and a collection of experience is proposed and discussed. As a conclusion it is proposed that generic principles of safety management should be made as explicit as possible to facilitate cross-industrial exchange of experience.

2. SAFETY IN THE NUCLEAR INDUSTRY

The nuclear industry in all countries is regulated which means that there is an independent authority taking stand on safety related matters. The authority has also the responsibility to create regulations. Slightly different approaches have been used in different countries. All approaches are relying more or less on international standards and regulations. The support of international organizations such as the International Atomic Energy Agency and OECD Nuclear Energy Agency has been instrumental in developing standardized approaches to regulation. The system created in Finland is similar to the systems used in Western industrialized countries, but is selfstanding based on Finnish legislation.

Present practices in the nuclear industry are a result of a long development. One of the early questions "what is safe enough" (Starr, 1969) has had both a direct and indirect influence on the development efforts. The early discussions set the directions and many people and organizations were involved. The principle of an independent regulatory body was implemented by splitting up the early atomic energy commissions. This general principle is now applied everywhere. The industry is responsible for the safety of the installation and for proving that to the regulatory body. The regulatory body is granting an operating license when enough evidence for the safety of the installation has been presented. The operating license does not release the licensee from the responsibility of operating the installation safely. The safety of nuclear power has thus developed through an interaction by two independent activities where the regulatory body sets up requirements to which the industry creates solutions.

The nuclear power industry has adopted a number of general principles of design to ensure an acceptable safety of the installations. A plant should comply to a number of deterministic safety principles. The most important of them is the *single failure criterion* which requires that no single failure should be able to cause an accident. This principle leads to the use of *redundancy*. The possibility of common cause failures again has introduced the principles of *diversity* and *separation*. These principles are often referred to as the *defence in depth* where different forms of *prevention* and *mitigation* provide a framework of erecting multiple barriers towards unwanted events (IAEA, 1988a). In the nuclear power plants *technical specifications* define limits and conditions for safe operation.

One of the standard tools applied by the nuclear industry uses *probabilistic safety assessment* (PSA). A PSA embodies a description of the plant and how it is operated in an accident model built using *fault* and *event trees*. The results of a PSA include quantitative estimates of plant risk in terms of core melt frequency (PSA level 1), amount of radioactive materials released (PSA level 2) or health effects of the accident (PSA level 3). The necessity of covering also human errors in the safety analysis was recognized early. The problem is to create a reliable and valid modelling framework for human actions. The prediction of human errors, such as errors of omission, commission or timing to be based on situational characteristics and performance shaping factors is still in its infancy. An early approach to the treatment of human errors was introduced with the THERP-methodology (Swain, Guttman, 1983). The problem of including human errors in the PSA framework is connected to the difficulty of modelling the complexity of human behavior by the probability of a certain action.

Human factors consideration in nuclear power plants has introduced a requirement to use standardized procedures for assessing the quality of the control room. Some of the US guidelines (USNRC 1981) are giving rather concrete guidelines on how certain functions should be implemented. The guidelines have been challenged as mechanistic and not providing the deep understanding of real critical issues of man-machine interactions. The requirement to implement *symptom based* instead of *event based procedures* has got a widespread support. The use of training simulators for the training of operators is almost a regular practice for most of the nuclear power plants in the world. A special consideration is the so called *30 minutes rule* which ensures that enough time is available before critical actions are required by the operators during accidents. Another requirement is to have a *shift technical advisor* available for the case of an accident. An accident would also call for the establishment of a *technical support center* manned with reactor experts. The possibility of an evacuation of the control room has to be taken into account by establishing an *emergency operation facility*.

Incident reporting systems were built up early within the nuclear industry. In USA the nuclear power plants are supposed to report all significant events to the US Nuclear Regulatory Commission. These Licensee Event Reports (LER) provide an eminent source of information for a safety analyst. Similar reporting requirements are set up by the regulatory body in most countries. The International Atomic Energy Agency (IAEA) is together with the OECD Nuclear Energy Agency (OECD/NEA) operating an international reporting system (IAEA, 1990a).

Policy level commitment
statement of safety policy
management structures
resources
self regulation
Managers commitment
definition of responsibilities
definition and control of safety practices
qualifications & training
rewards & sanctions
audit review & comparisons
Individuals commitment
questioning attitude
rigorous and prudent approach
communications

Fig.1. An approach towards a safety culture.

Safety culture has been proposed as a concept with a bearing on many safety issues of nuclear power (IAEA, 1991a). It places an emphasis on organization and management which can have important influences on many of the performance shaping factors of human errors (see Fig.1). The safety culture concept is stressing the importance of a general commitment to safety matters on all levels of involved organizations. These considerations have a more general relevance in which the transfer of good operational practices are stimulated. The IAEA has initiated programs for independent assessments of safety by international teams. These programmes of which the OSART programme (IAEA, 1988b, 1988c, 1989) is well established and have been successful and valuable for the power plants as a mechanism for distributing good operational practices. The analysis practices for feedback of experience are handled by the ASSET programme (IAEA, 1991b). The concept of a safety culture has also been brought into checklists for assessing the efficiency of organizations (IAEA, 1993). These programmes for an international safety review have got an important function in distributing good operational practices.

3. SAFETY IN OTHER INDUSTRIAL AREAS

The approach of an independent authority with the power to shut down the installations or to keep systems on ground is common to many industrial sectors. The organization and the power of the authority may however vary considerably. There are international bodies ensuring common approaches and a transparency of national systems, but their charter and authority may vary considerably. New safety requirements or procedures are typically initiated by an identification of generic problems. International bodies provide a forum for a rapid distribution of such new knowledge. The peer review procedures ensure that standard quality control procedures are implemented before new scientific results are allowed to enter the process.

The safety precautions in the aerospace industry were formed in the pioneering days. The need for considering the human in the loop was recognized early as certain aircraft dynamics proved difficult to control (Allen, McRuer, 1979). A projection of the growth of the civilian part of the industry in passenger miles concluded that flight safety of the early fifties had to be improved by an order of magnitude. Early accidents draw the attention of the authorities to generic problems such as the materials fatigue experienced in multiple loadings. These problems were resolved in tight schedules for inspections and exchange of crucial parts. Present systems of type acceptance together with a continuous monitoring of components and experience has been able to meet the challenge of an acceptable safety. The systems do not make accidents impossible, but the remaining problems are well under control and are in balance with a willingness to pay for improvements. Airworthiness certification has been mandatory for aircrafts since the creation of the International Civil Aviation Organization (ICAO) in the late forties and the Chicago Convention. The problem of having to certify flight-critical functions for software arose for the first time at the beginning of the eighties with the Airbus A310 and Boeing 757 and 767 programmes. No specific regulations existed when the aircraft programmes began. The problem had been identified in the middle of seventies and groups of experts in Europe (EUROCAE) and USA (RTCA) had begun working on these questions. The work lead to RTCA Do 178 (or EUROCAE Ed. 12) standard, which sets rather strict requirements for software-based functions (JAR, 1986). The strong points of Do 178 are its "system" approach to the problem, and the use of different certification levels. The airworthiness certification works on the following principles:

- main input elements are potential consequences on total aircraft airworthiness of system failures,
- these consequences are classified (minor, major, hazardous, catastrophic),
- according to these classes, quantitative probability requirements for the occurrence of the failure conditions are set,
- certification is to demonstrate that the probability figures are lower than the objectives.

The chemical industry uses as its most important safety assurance method the hazard analysis and operability analysis (HAZOP). The method is using structured brain storming sessions where possible deviations from normal process conditions are catalogued. Deviations are amended with backward causes and forward consequences to identify possible needs of changes in the design. The development of the methodology goes back to the aftermath of the Flixborough accident (Parker, 1975) where the cause of the accident was attributed to poor design. The HAZOP methodology has been put almost into a regular use in the chemical and the petrochemical industries. The offshore industry is using methods from the petrochemical industry which on its part has close connections to the chemical industry. The severe conditions especially in the North Sea has however introduced also own traditions and practices. In spite of the similarities there seems to be differences in the national practices.

The transportation sector has developed its own safety requirements which are different depending on the mode of transportation. Road transportation is governed by national bodies which vary considerably. There seems also to be a wide acceptance of loss of life and material in the prevailing level of road accidents. Sea transportation is in principle very safe under ideal conditions, but heavy traffic or difficult passages combined with fog and other extreme weather conditions increase the possibility for accidents. Convenience flags gives a possibility to maintain inferior levels of safety precautions which seems to demonstrate in a higher rate of accidents. Signalling systems for train dispatching have been developing according to their own safety standards. Rail transportation has been more prone to rely on programmable safety systems than the nuclear power industry.

Utilities such as electricity, communication and water supply have become increasingly important in maintaining functions of a modern society. The systems are, as any complex system, increasingly vulnerable to failures and break downs. The two major blackouts in New York City in 1965 (Friedlander, 1966) and 1977 (Wilson and Zarkas, 1978; Sugarman, 1978) are examples illustrating the dependence of a major city on a continuous supply of utilities. These two events also illustrate the difficulty of applying the lessons of one incident for improving the systems to avoid further similar incidents. Break downs of the telephone systems in major population areas show similar problems of vulnerability.

Biotechnology is an emerging technology and certain comparisons with nuclear power can be made. The possibility that a genetically engineered organism is running amuck in some biotope is a real danger against which systematic barriers should be erected. The industry itself has proposed certain precautions which should make it possible to achieve a reasonable safety. There is a growing public concern on these issues which may have repercussions on the success of the industry.

4. LESSONS LEARNED FROM ACCIDENTS

Encountered accidents have initiated periods of intense learning by the affected industry. A common response to accidents in neighboring fields is to disparage their importance and attribute them to simplistic causes. Another reaction is also to point to technical differences which would make exactly the same development of events impossible. A thorough analysis usually reveals a large number of interacting causes. Similar causes can often be present in other hazardous installations. A common conclusion is that there seldom are completely unexpected causes, but rather an unlucky combination of well known problems. An observation by Perrow (1984) is that accidents tend to occur in tightly coupled systems with unexpected interactions between subsystems. The accidents occur often as an interaction between the technical, organizational and personnel systems (Bowonder, Linstone, 1987).

The collection of experiences from incidents or accidents relies on a thorough analysis (Laakso, 1984). In the analysis deviations from acceptable operational practices and deficiencies in the plant design are sought. A second line of question is to ask what the causes for these deviations were, why they were allowed to persist in the system and what corrective actions should be introduced. It is important to note that there are no objective stopping criterion for investigating the next level causes for some observed deviation.

Incidents and accidents in the nuclear field have steered the development towards certain solutions. The Browns Ferry incident brought the requirement for separation between redundant systems into the regulations. The Three Mile Island (TMI) accident brought for the first time the possibility of radioactive release tangibly to the attention of the public. During the accident the importance of an emergency response plan was demonstrated. Many contributing causes to the accident were identified (Mason, 1979). The official report (Kemeny, 1979) attributed the accident, in addition to deficiencies in technical solutions, to three major human factors related issues, ie. control room design, operational procedures and operator training. These findings where not unexpected, because already two years earlier the issues hade been thoroughly considered in an EPRI report (Seminara *et al*, 1976).

The accidents in the chemical industry have led to similar systems improvements. The Flixborough accident identified important design deficiencies and was the driving force in taking the HAZOP procedure into a regular use. The Seveso accident initiated several improvements of the chemical industry especially within the European Community (CEC, 1989). The perhaps most important changes in the views were associated with a requirement that the potentially hazardous industries should inform local authorities about potential dangers. The Bhopal accident is the worst technological disaster ever occurred (Shrivastava, 1987). An analysis of the accident revealed several of the usual safety problems. A special cause was the transfer of a hazardous industrial installation to a country with a poor infrastructure. In spite of this finding relatively little has been done to establish standards for technology transfer projects to developing countries. In the off-shore industry one of the more spectacular accidents was the

Piper Alfa fire (Paté-Cornell, 1993).

The Chernobyl accident is the only accident at a commercial nuclear power plant which has caused immediate radiation related deaths of people (IAEA, 1986). In addition it is expected to cause a number of delayed cancers. One lesson from the accident is that distress of the exposed population has to be handled very diplomatically. The response of the authorities is of utmost importance. Any problems in communicating can bring the full impact of insecurity and distrust into the relations between the public and the authorities. The ultimate cause of the accident was the possibility of a runaway reaction at low power of the reactor. Runaway reactions, although regularly used in the chemical industry, are always representing a very specific danger (Gustin, 1992). The contributing factors were unawareness by the operators of very basic facts of the dynamics of the reactor they operated together with an almost complete fixation with the experiment they were performing. The bravery of the firefighting brigades was indicating that they were almost unaware of the dangers of their task. Officials were conditioned by their old reflex of hiding and denying. Information on the consequences of the accident was sometimes delayed and even labeled as secret. The first weeks after the Chernobyl accident these responses resulted in tens of thousands of people receiving unnecessary high thyroid doses (Belayev, 1991).

The Challenger accident demonstrated the importance of communication problems within large organizations (Bell, Esch, 1987). Before the accident the safety reviews had been rather qualitative, but after the accident PSA practices more similar to procedures in the nuclear field were brought in (Garrick, 1989). The Herald of Free Enterprise accident illustrated similar problems of communication, but also brought into the open a setup almost waiting for something to happen.

Accidents tend to release a post-accident crisis. There is a strong temptation to ignore problems of emergency planning, but there is also the danger that in the absence of any plan disproportionate measures to some small incident are taken. In setting the balance between not doing anything and doing too much we must be careful not to jump from one briar patch into another. Several prejudices are prevailing e.g. that accident provokes panic and irresponsibility. A proper dealing with an outbreak of a crisis implies that a complex and sensitive system has to be set up in beforehand and triggered into operation at the crisis. Remedies go through public communication, training efforts, responsiveness to different kinds of crisis situations (Lagadec, 1990).

5. SAFETY AND THE SOCIETY

Nuclear power, but also other fields of industry, have been forced to take due consideration to public opinion. Industrial responses to media interest in hazardous installations has over a period of some twenty years changed from being closed and denying. The reason for this change has been media disasters, where some minor incident has been blown up in local and international headlines. The authority responses to the Chernobyl accident were also in many countries viewed as disastrous from a communication point of view. Risk communication is today at least in the scientific community viewed as extremely important as a component in promoting trust and confidence (Jungermann *et al*, 1988). One important part in the communication is to set the baseline of the accident according to an agreed scale of severity (Figure 3.).

ACCI-	7. major accident
DENT	6. serious accident
	5. accident with off-site risks
	4. accident mainly in installation
INCI-	3. serious incident
DENT	2. incident
	1. anomaly
Below scale, no safety significance	

Fig.2. The international nuclear event scale (IAEA, 1990b).

Nuclear power was created as a solution to an increased demand on electricity. The industry itself views risks as minor and stresses that other energy options actually carry more risks (Cohen, 1990). In spite of the scientific argumentation these studies have done little in influencing the public acceptability of nuclear power. The public fear of nuclear power has been claimed to be coupled to hidden images (Weart, (1988). These may be relevant and a common view among technicians is that the public behaves irrationally in reacting to risks (Zeckhauser, Viscusi, 1990). The society seems to react stronger on some risks than others (Kasperson et al, 1988). If these findings are not taken into account in the political decision making processes it is likely that technological development will be stalled. A number of studies have been conducted to identify the value judgement of responses to different risks. Results suggest that two components, dread and unfamiliarity, govern the perception of risks (Slovic, 1987). A third component is the perceptions of individuals own reference group which seems to be the best explanation of views held (Wildavsky, Dake, 1990). It is evident from the debate that a basic lack of trust and confidence has emerged. It has been argued that a cultural dimension has to be given proper consideration in deciding about risks (Douglas, 1985). To what extent the nuclear establishment can regain the required trust and confidence remains to be seen. The importance of providing rapid, correct and understandable information will anyhow be an important component in this process.

Societal concerns have in many countries initiated a defacto moratorium for nuclear power. This in spite of the fact that other energy options are contributing to a global climatological change through the emissions of greenhouse gases. Nuclear waste is introducing another dimension of waste handling, but the problems are connected to the very long term confinement needs. Available technologies and present amounts of high level waste, however, give time for developing viable solutions. The controversy on nuclear waste seems therefore somewhat out of proportion as compared with other contemporary dangers (Karplus, 1992). The nuclear waste issue provides an important lesson for other industrial areas. The image of highly toxic and undestroyable waste together with negligent or even fraudulent handlers is extremely frightening taking into account the impacts on coming generations. The industry also carries the burden of horror stories of early radiological experiments which have been kept secret (Smolove, 1994). Before the nuclear industry can regain trust and confidence in the eyes of the laypublic it is necessary to clear out those shadows from the past. Public confidence and trust has to be gained on a continued basis, because a loss can be very difficult to compensate. The nuclear debate has actually demonstrated that societal concerns can override all other arguments.

One additional argument against nuclear power generation has been its imagined connections to military use although more direct routes to nuclear weapons can be found. It is evident that many countries saw the introduction of a civilian programme of nuclear power as a possibility to get access to important military technology. The military connections have brought aspects of the technology outside normal societal influence. This has been seen in USA as a difference between regulations for military and civilian nuclear installations, which however now seem to dilute (Blush, Sturdivant, 1992). The Nuclear Proliferation Treaty was established as an institutional solution to prevent the dual use of technologies. The problem has not been solved because there always is the possibility that some country will not obey the internationally agreed procedures. From a societal point of view it can be argued that the plurality of disagreement provides an important insurance function in helping the society avoiding costly mistakes (Schwarz, Thompson, 1990). This can actually be seen as an example of a feedback on the societal level ensuring quality control of important decisions.

6. TRANSFER OF SAFETY EXPERIENCE

The extent to which ideas and solutions can be transferred between industrial sectors can always be disputed. Much of the industry specific routines are coupled to the specfic properties of substances and materials used. The confinement of various materials will all require their own procedures, but they are on a generic level very similar. Incident reports are providing generic findings citing problems with seals and welds, contamination, separation, fire fighting, safety systems, control and instrumentation, inspection, control room solutions, operating procedures, etc. With a proper frame of generality it should be possible to use generic methods for ensuring the safety of design, construction, inspection and maintenance.

Risk analysis is used in different forms in many industrial sectors. Still it is almost only nuclear power which to a larger extent is using quantification of risks. Licencing decisions are however difficult to base on exact quantitative requirements, because of uncertainties in methods and models. There is however a tendency to move the quantification into the requirements as the ongoing discussion on *safety goals* indicates (OECD/NEA, 1990). A quantification on a goal level is beneficial, because it forces the analyst to rigidity and accuracy in the analysis. One exception to the sparsity of quantitative estimates in the conventional industry has been the Dutch requirements for hazardous installations (VROM, 1989).

Training simulators were introduced early in the aerospace industry. In the introduction there was probably more enthusiasm than a true concern for safety. The very close interaction between the pilot and the system under different conditions provides a very natural ground for the use and benefit of training simulators. Training simulators in the nuclear industry were taken into a more regular use during the seventies. Training simulators are to some extent used in the chemical and petrochemical industry otherwise very sparingly.

Digital control and instrumentation (C&I) systems have been introduced at a rapid pace within the process industries all over the world. The reason for the rapid break-through has been the many benefits of the new systems as compared with the old analog systems. Important agents in this rapid technology transfer are the C&I-vendors which have an interest in promoting a rapid shift to new technologies.

The burden of proof in the licensing process is laid on the industry. If some solution has been possible to bring through the licensing process there is an incentive to stick to this solution. This brings in an inherent conservatism into the industry. This conservatism of using proved solution is natural in the prospects of potential damages with a major release of radioactivity. Public fears also tend to make the impact of an accident larger than an objective evaluation would propose. The conservatism and the burden of proof introduces a danger of not utilizing technological possibilities which even can lead to the use of obsolete solutions because of the difficulty of licensing new solutions. This might lead to a separation between nuclear and non-nuclear applications which is in nobody's interest. These difficulties have been seen in attempts to introduce digital control and instrumentation systems for the protective functions.

Environmental protection is a concern for all industrial areas. A number of methods for the assessment of environmental and human health risks have been suggested (Paustenbach, 1989). Similarly it has been proposed that product life cycle analysis studies and environmental impact assessments should be carried out before major industrial investments are undertaken. Again it would be important that enough transfer of ideas and methods between industrial areas are undertaken. The whole industry initiatives such as the *Environmental Auditing* concept proposed the International Chamber of Commerce (ICC, 1989) gives an impetus of taking a systems look at the problems.

When new technologies are introduced there will always be new lessons learned. In accuiring these lessons a certain prudence has to be shown. Biotechnology and genetic engineering is on the edge to be introduced in a larger scale. The transfer from a laboratory to an industrial environment gives a qualitative change which may introduce unknown threats. Biotechnology has similarly to the nuclear industry a dual use in the military sector. Discussions on ensuring the safety of biotechnical installations have been started. There is also a beginning public debate of emerging concerns. Drawing on the experience from nuclear power it would be important to establish internationally agreed safety precautions applicable to all installations. These safety precautions should also be communicated to the public. An international body entrusted with the distribution of good safety practices would also have an important role. Activities to ensure that trust and confidence can be maintained between the laypublic and the industry is very important.

7. A SYSTEMS APPROACH FOR SAFETY

The safety of technical systems can be approached with systems analytic methods. The three problems of systems analysis *modelling*, *simulation* and *control* should all be combined to provide a general structure of safety management. Safety management is ultimately a control problem where the systems should be designed and operated to provide an acceptable safety. The system has therefore to be modelled to identify the influence of crucial control variables. By simulating the system with different control structures and control parameters the safety of the system can be optimized.

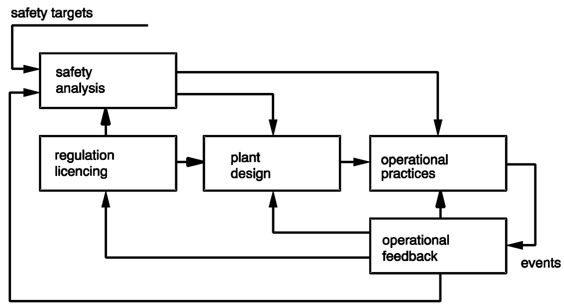

Fig.3. The feed forward paths of safety analysis and the experience feedback paths.

A safety analysis is a model of the system predicting the resulting safety level. The safety analysis part can be seen as a feedforward control loop setting the predicted safety to an acceptable level. The feedforward control has to be amended with a feedback control correcting possible modelling errors. The feedback path is intended to provide information necessary to update the risk analysis model based on obtained experience. The resulting control structure is given in Figure 4.

Another systems oriented requirement for reaching an acceptable safety is connected to internal feedbacks in the systems. Feedbacks ensuring acceptable quality controls have to be included on all levels of the involved organizations. The feedback should be as immediate as possible to ensure a reliable detection and a rapid correction of failures in all work processes.

People, such as designers, safety analysts, operators and maintainers, have an important contribution to safety. The technical safety of installations has been improved to a point where it is expected that it will be dominated by "people factors" (Freudenborg, 1988). A combination of all these components of human behavior into a safety model provides a real challenge for systems analysis (Wahlström, 1994b). All systems should be designed to take human abilities and limitations into account. It may still be difficult to model the human component in safety. An important component in ensuring human reliability is to promote the understanding of the systems and their dynamics (Hukki, Norros 1993). Only if the persons involved have a true understanding of the inherent dynamics of the systems they are designing or operating they will have the possibility to avoid disastrous decision errors. An understanding of how people are reasoning and how they are forming their internal models are important components in ensuring safety (Wahlström, 1994a). The complexity of the systems and the interactions between system components provide a very large challenge for ensuring this understanding (Wahlström, 1992).

There is an inherent conflict between safety and economy which has to be understood by safety analysts. When an acceptable safety is reached the next consideration is how the efficiency of the system can be improved. Improvements can be concerned with materials saving, larger throughputs, speed of production, etc. Changes in process design, operation or maintenance can have an influence on the safety. The influences can be assessed in a safety analysis, but sometimes the impacts of changes are difficult to quantify. A change can decrease the safety, but if the change is marginal the decreased safety can be observed only through a tedious collection of experience. People and organizations are actually performing experiments with the systems to explore the borders of a safe operational envelope. An accident occurs when these borders are crossed (Starbuck, Milliken, 1988).

8. CONCLUSIONS

Nuclear power provides an interesting story for history of technology. The emergence of the new era was brought to the attention of the world by two devastating bombs. The image of nuclear power as a doomsday technology was promoted by the cold war and nuclear tests during the fifties. Opening up the technology for a peaceful use created a lot of enthusiasm. It is therefore only natural that early predictions of the new technology were overoptimistic. The new field attracted many talented scientists and engineers. Their enthusiasm obscured the fact that nuclear power is qualitatively different as compared with other energy sources (Collinridge, 1983). An unproven technology will always carry along new kinds of problems which have to be solved before the technology can be put into a regular use.

In retrospect it is evident that the success of the nuclear industry from the safety point of view has a large credit to the international exchange of experience. IAEA has played a crucial role in this spread of safety excellency. In the nuclear industry there has always been voices stressing the danger of overregulation. It is clear that the regulation has brought in additional expenses for the industry. These expenses should be seen as insurance fees for decreasing the likelihood that some operators will make a mistake with influences on the whole industry. It should actually be in the interest of the serious operator to keep less serious operators out of business.

To what extent other fields can draw on these experiences? Most of the industry is conventional in that respect that operational experience has been gathered over decades of operation. There have not been many similar cases of a qualitative change in the processes. The really hard lesson for nuclear power has been to understand that the industry is truly global. An error anywhere is an error everywhere. The assurance by the industry that problems in one country do not apply to another has never been accepted by the public. The only viable response is to ensure openness in communication and high quality routines on all levels of operation. In the conventional industry there still seems to be remnants of a secrecy policy especially with respect to environmental matters. Such a policy can have serious repercussions for the industry as a whole.

Ensuring high safety standards in any hazardous process is a task which is relatively independent of the process. The processes have to be designed with clearly defined safety objectives. The design should reflect the needs of the people operating the plants. Routines for quality control should be introduced and maintained during design and construction. The operational organization should be adapted to special safety requirements. There is a benefit in exchanging experience between industrial areas. This exchange of experience requires very talented people. The extraction of generic findings from industry specific experience requires a very specific skill. A training towards such skills might be included in courses of *Systems design for safety* to be given in the curricula at the technical universities.

The exchange of experience between industrial sectors has been more a matter of chance than systematic efforts. A systematic search seems to take place only where major new installations are built. An optimistic view is that the experience is transferring although rather slowly. The initiation of a whole industrial initiative in safety management should help in providing an intensified transfer of experience on the design and operation of hazardous installations. Such a high level fresh look on old traditions within an industry can help in resolving urgent problems before they make themselves explicit in an accident.

7.1.2006

9. REFERENCES

Allen, R.W., D. McRuer (1979). The man/machine control interface-pursuit control, *Automatica*, Vol.15, 683-686.

Belayev, S. (1991). A concept of living conditions for people in the regions affected by the Chernobyl accident, presented at the IAEA conference on "International Chernobyl Project", 21-24 May.

Bell, Trudy E., Karl Esch (1987). The fatal flaw in flight 51-L, *IEEE Spectrum*, February, 36-51.

Blush, Steven M., M.H. Sturdivant (1992). Lessons to be learned from a tritium release, IEEE Fifth Conference on Human Factors and Power Plants, June 7-11, Monterey, California.

Bowonder, B., H.A. Linstone (1987). Notes on the Bhopal accident: Risk analysis and multiple perspectives, *Technological Forecasting and Social Change*, **32**, 183-202.

CEC (1989). Council directive of 24 June 1982 on the major accident hazards of certain industrial activities. Official journal of the European communities, 1989, No L230, 5 August 1982.

Cohen, Bernard L. (1990). *The nuclear energy option: An alternative for the 90s*, Plenum Press, New York.

Collinridge, David (1983). *Technology in the policy process; controlling nuclear power*, France Pinter Publishers, London.

CISHC (1981). A guide to hazaed and operability studies. Chemical industry safety and health council of the chemical industries association, London, 42p.

Dougherty E.M. (1990). Human reliability analysis - Where shouldst thou turn? *Reliability Engineering & System Safety*, **29:**3.

Douglas, Mary (1985). *Risk acceptability according to social sciences*, Russell Sage Foundation, New York.

Drogaris, G. (1991). Community documentation centre on industrial risk; major accident reporting system; lessons learned from accidents notified, Joint Research Centre, Institute for Systems Engineering and Informatics, EUR 13385 EN, ECSC-EEC-EAEC, Brussels-Luxembourg.

Friedlander, Gordon D. (1966). The Northeast power failure - a blanket, *IEEE Spectrum*, February, 54-73.

Freudenborg, William R. (1988). Perceived risk, real risk: Social science and the art of probabilistic risk assessment, *Science*, Vol.242, 44-49.

Frola, F.R., Miller, C.O. (1984). System safety in aircraft management, Logistics Management Institute, Washington.

Garrick, John B. (1989). Risk assessment practices in the space industry: The move toward quantification, *Risk Analysis*, **9**, No.1, pp.1-7.

Gustin, Jean Luis (1992). Runaway reactions, their causes, and the methods to establish safe process conditions, *Risk Analysis*, Vol.12, No.4, 475-481.

Hukki, Kristiina, Leena Norros (1993). Diagnostic orientation in control of disturbance situations. *Ergonomics*, **36**, No.11, pp.1317-1327.

IAEA (1986). Summary report on the post-accident review meeting on the Chernobyl accident, IAEA-75-INSAG-1, Vienna.

IAEA (1988a). Basic safety principles for nuclear power plants. A report by the international nuclear safety advisory board. IAEA-75-INSAG-3. Vienna. 74p.

IAEA (1988b). OSART guidelines, reference document for IAEA operational safety review teams, IAEA-TECDOC-449, Vienna.

IAEA (1988c). OSART results, a summary of the results of operational safety review team missions during the period August 1983 to May 1987, IAEA-TECDOC-458, Vienna.

IAEA (1989). OSART results II; a summary of the results of operational safety review team missions during the period June 1988 to May 1989, IAEA-TECDOC-497, Vienna.

IAEA (1990a). Incident reporting system. Report on the technical committee/workshop on new guidelines for preparation and analysis of IRS reports. 10-14 December 1990, Vienna. 34 p.

IAEA (1990b). INES: The international nuclear event scale, IAEA-INES-90/1, Vienna. 38p.

IAEA (1991a). Safety culture, IAEA-75-INSAG-4, Vienna.

IAEA (1991b). ASSET guidelines, revised 1991 edition. Reference material prepared by the International Atomic Energy Agency for assessment of safety significant events teams, IAEA-TECDOC-632, Vienna. 149p.

IAEA (1993). ASCOT guidelines, Guidelines for the organizational self-assessment of safety culture and for reviews by the assessment of safety culture in organizations team, draft report, 1-2 April, Helsinki, Finland.

ICC (1989). Environmental auditing, Publication 468, ICC Publishing SA, Paris, March.

JAR (1986). Joint Airworthiness regulation. Advisory document providing guidance for understanding the intent of JAR 25.1309 (a) through (d). ACJ 25.1309, 3rd draft, January 1986.

Jungermann, H., R.E. Kasperson, P.M. Wiedemann (1988). Risk communication, Proceedings of the International Workshop on Risk Communication, October 17-21, KFA Kernforschungsanalage Jülich GmbH, Germany.

Karplus, Walter J. (1992). *The heavens are falling; the scientific prediction of catastrophes in our time*, Plenum Press, New York.

Kasperson, Roger E., Ortwin Renn, Paul Slovic, Halina S. Brown, Jacque Emel, Robert Goble, Jeanne, X. Kasperson, Samule Ratick (1988). The social amplification of risk: A conceptual framework, *Risk Analysis*, Vol.8, No.2, pp.177-187.

Kemeny. J.G. (Chairman). (1979). Report of the presidents commission on the accident at Three Mile Island, US government printing office. Washington DC, October 1979.

Laakso, Kari (1984). A systematic feedback of plant disturbance experience in nuclear power plants. Thesis. Helsinki university of technology.

Lagadec, Patrick (1990). *States of emergency, technological failures and social destabilization*, Butterworth-Heinemann, London.

Mason, J.F. (1979). The accident that shouldn't have happened, *IEEE Spectrum*, 32-42, November.

OECD/NEA (1990). Consideration of quantitative safety guidelines in member countries, Committee on the Safety of Nuclear Installations, OECD Nuclear Energy Agency, October.

Parker, R.J.(chairman). (1975). The Flixborough disaster: Report of the court of enquiry: Her majesty`s stationary office. London.

Paté-Cornell, M. Elisabeth (1993). Learning from the Piper Alpha Accident: A postmortem analysis of technical and organizational factors, *Risk Analysis*, Vol.13, No.2, pp.215-232.

Paustenbach, Dennis J. (1989), *The risk assessment of environmental and human health studies: A textbook of case studies*, John Wiley&Sons, New York.

Perrow, C. (1984). *Normal accidents; living with high-risk technologies*, Basic Books, New York.

Seminara, J.L., W.R. Gonzalez, S.O. Parsons (1976). Human factors review of nuclear power plant control room design, Report EPRI-NP-309, Electric Power Research Institute, Palo Alto, CA.

Shrivastava, Paul (1987). *Bhopal; anatomy of a crisis*,

Ballinger Publishing Company, Cambridge, Mass.
Slovic, Paul (1987). Perception of risk, *Science*, Vol.230, 280-285.
Starbuck, William H., Frances J. Milliken (1988). Challenger: Fine-tuning the odds until something breaks, *Journal of Management Studies*, **25**:4, pp.319-340.
Starr, Chauncey (1969). Social benefits versus technological risk; What is our society willing to pay for safety, *Science*, **165**, 1232-1238.
Sugarman, Robert (1978). New York City's blackout: a $350 million drain, *IEEE Spectrum*, November, pp.44-46.
Swain, A.D., H.E. Guttman (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications, NUREG/CR-1287, US Nuclear Regulatory Commission.
Schwarz, M., M. Thompson (1990). *Divided We Stand: Redefining Politics, Technology and Social Choice*, University of Pennsylvania Press.
Smolove, Jill (1994). The widening fallout, *Time*, January 17, No.3, pp.30-31.
USNRC (1981).Guidelines for control room design reviews, US Nuclear Regulatory Commission, NUREG-0700.
VROM (1989). National Environmental Policy Plan (NEPP); to choose or to lose, Letter of the Minister of Housing, Physical Planning and Environment, Second Chamber Session 1988-1989, 21 137, nos 1-2, The Netherlands.
Wahlström, Björn (1992). Avoiding technological risks; The dilemma of complexity, *Technological Forecasting and Social Change*, **42**:3, 351-365.
Wahlström, Björn (1994a). Models, modelling and modelers; an application to risk analysis, *European Journal of Operations Research (EJOR)*, **75**:2.
Wahlström, Björn (1994b). Modeling of man-machine systems; a challenge for systems analysis, in Beroggi, G. *Computer Supported Risk Management* (accepted for publication).
Weart, Spencer R. (1988). *Nuclear fear: A history of images*, Harvard University Press, Cambridge, Mass.
Wildavsky, Aaron, Karl Dake (1990). Theories of risk perception: Who fears what and why? *Daedalus*, **119**:4, 41-60.
Wilson, G.L. P. Zarkas (1978). Anatomy of a blackout, *IEEE Spectrum*, February, 38-46.
Zeckhauser, Richard J., W. Kip Viscusi (1990). Risk within reason, *Science*, Vol.248, 559-564.