Systems safety in the high-tech industrial environments; technology and human reliability[1]

Björn Wahlström
Technical Research Centre of Finland
VTT Automation, POB 13002
FIN-02044 VTT, Finland

Abstract: The paper gives a brief account of safety precautions in nuclear power with an emphasis of human and organisational issues. Lessons from accidents as experienced by high-risk industries provide a consistent picture that human errors and organisational deficiencies are important causes of accidents. A simultaneous combination of seemingly minor problems can add up to cause a major accident. The importance of these contributors to incidents have been recognised by the nuclear industry and have led to additional investments in safety. These involve among others self-assessments and organisational reviews. In fostering a safety culture, the integration of work and information technology can provide new solutions. A short reference to nuclear safety research in the Nordic countries is given. The development of a continuing safety relies on an efficient cooperation between process engineers, information technology specialists and work researchers.

Introduction

Systems safety has got an increased attention within the high-tech industry of today. One important reason is the recognition of the importance to consider public opinions. High-tech industry is moving on frontiers of human knowledge and has been characterised by a rapid adoption of information technology. Information technology has made many new solutions possible. It has allowed a scaling up of production systems together with their efficient control. Order of magnitude improvements have been achieved in safety and reliability, but increased size of the systems and the use of more hazardous materials provide to increased accident potentials.

Nuclear power took off with an image of high-tech and promises for cheap and abundant energy. That image has now faded due to several reasons. One is certainly connected to public concerns in response to the accidents at Three Mile Island and Chernobyl. Both accidents demonstrated the globality of nuclear power and they were followed by very strong reactions of distrust by the public.

The history of nuclear power[1] can provide lessons for other high-tech industries which ponder a globalisation and a scale up of potentially hazardous production processes. Lessons from the nuclear industry stress efficient regulation, a prudent approaches to safety and a consideration for the man in the loop. Safety control is a necessity for the high-risk industries in achieving initial and continued acceptability.

[1] Key note presentation at the International Symposium Work in the Information Society, 20-22 May 1996, Helsinki, Finland

Measures to avoid large accidents which may jeopardise the future of a whole industry should always be given the highest priority.

The main argument of the paper is that safety measures to be efficient should be properly anchored in the work organisations. This paper describes briefly safety measures in the nuclear industry of today and tries to put them into a context of continued organisational learning and safety culture.[2]

High risk technologies

High risk technologies have many things in common. The potential for disastrous accidents place extreme demands on reliability and quality on equipment and work. The systems are complex and paths of influence between subsystems are not restricted in time and space.[3] Human errors and organizational deficiencies can through minor triggering incidents cause a chain of events spiralling towards a major accident.[4] Accidents such as Three Mile Island,[5] Chernobyl,[6] the Tenerife airplane crash,[7] Bhopal,[8] Challenger[9] and Piper Alpha[10] also show that earlier warnings have not been responded to properly.

Lessons from accidents provide a consistent picture. An interaction of several technical failures, human errors, organisational deficiencies and societal oversights can together bring the systems to a state where a single triggering event is disastrous.[11] Accidents demonstrate a simultaneous break down of several safety controls where the absence of only one failure might have prevented it. Major accidents have had an important influence on the safety precautions in respective industries, but there seems to be difficulties in learning from each other.[12]

One generic lesson from the high risk technologies has been the identification of human errors as one major cause of incidents and accidents. Responses has been to stress the need for well designed man-machine interfaces. Guidelines and standards have been developed for interface design, but the rapid development in the information technology seems to bring in new generations of equipment where many standard problems appear in a new form.

A recent lesson is that also organisational deficiencies can be an important contributing factor for human errors. Findings from accidents indicate that organisations sometimes only pay lip services to concerns for safety. This points to one important managerial problem in the control of safety which is concerned with the difficulty of getting a proper feedback from all the subtle influences on safety that even straightforward decisions may have.

High risk technologies are regulated. This typically means that a regulator is defining preconditions for using the technology. The acceptability of the installations are controlled in a licensing process and regular inspections are performed to ensure that requirements are complied to. Accidents demonstrate that this controlling functions has not always been efficient and that there even are obvious shortcomings that have not been reacted to.

These problems of ensuring that the human and organisational part of the systems is able to live up to the quality requirements is aggravated by two development trends. An increasing demand for higher efficiency is responded to by increasing unit sizes and decreasing operational margins. Units are becoming more

complex and are supposed to be operated by smaller crews. It is therefore easy to understand that the optimization may go on until something breaks. The risk homeostasis theory asserts that safety improvements are offset by efficiency improvements to set the resulting risk level on a level implicitely considered as acceptable.[13]

Safety precautions in the nuclear industry

The safety precautions applied in the nuclear industry have been developed over many years. In that process the influence of the international organisations such as IAEA and OECD/NEA has been instrumental. Several international working groups, meetings and conferences have been challenged with the task of defining precursors for safety. The work has been documented in a large number of safety standards and guides. Proposed safety practices have rapidly been transfered to safety regulations in the nuclear countries.

An independent safety authority and the licensing process carried out before a nuclear power plant is allowed to be operated are two corner stones in building safety of nuclear power. The safety authority has the task as a representative for the public ensure that all necessary safety precaution are taken and that they are efficient. In the licensing process design solutions are reviewed, constructions are analyzed, installations are inspected and personnel is examined to ensure that no operational conditions can provide a threat to people nor to the environment. The licensing process is governed by safety goals set for the plants eg. that a major accident at a plant shall not occur with a frequency larger than once in 100000 years.

Safety requirements and applied safety principles build a protection against unwanted sequences of events. The most important is the defense in depth principle according to which multiple physical barriers and levels of protection guard against release of radioactive materials. Other important safety principles are the single failure criterion, the principle of separation and the principle of giving operators respite time in accident situations. Safety requirements also include a thorough analysis of accident sequences with both deterministic and probabilistic criteria. A certain conservativity is required to be used in interpreting results from the safety analyses.

In spite of the detailed safety requirements and the licensing process the operator of a nuclear installation is always responsible for all aspects of its safety. This responsibility has been defined as fostering a safety culture[14], with a clear commitment to safety from the policy level, from managers and from all individuals involved in work at the plants. This involves organising safety reviews, establishing quality assurance processes and taking human factors into account. Simulators are used regularly in the training of control room operators and the validation of operational procedures. Emergency exercises are carried out at regular intervals to ensure a preparedness both for on-site and off-site organisations.

The forward control path of planning and analysing is closed by a feedback loop of collection and utilisation of operational experience. Plant events and incidents are collected through formalised reporting procedures at the plants and are further reported to safety authorities. All events are analyzed in detail to provide an understanding of their causes and possible needs for safety improvements. Reports

on the incidents are further distributed through international channels to give the whole industry rapid access to information which might be relevant for improving safety. Plants and safety authorities have specialised groups for analysing relevant of international experience.

Organisational reviews are used both by nuclear power plants themselves and by the safety authorities to assess the adequacy of safety precautions.[15] These reviews can be carried out as self-assessments or peer reviews. IAEA can as a service for national governments provide international review teams specialised in certain aspects of the safety activities.[16]

Human errors and organisational deficiencies

An understanding of the importance of human errors and organizational deficiencies for nuclear safety is well established today. This has implied a shift from placing the blame on single humans, to a more mediated view of designing technical systems and their organizations in an integrated fashion. The organization should be seen as providing an important safety net for the people in the system, to catch and correct human errors before they have had any effects on system safety.

The underlying cause for a human error can be seen as a resource and demand conflict in a specific decision making situation. Resources of the human decision maker in terms of abilities, training, procedures, available information, available time, etc. are not enough as compared with demands of the situation as characterised by operational goals, conflicting information, influence of actions, etc. Such conflicts of resources and demands should ideally be detected in a task analysis and corrected by changes in plant and control room design, procedures, training, staffing, etc.

Present human factors practices in the nuclear power industry include a thorough review of control room solutions to remove deficiencies in earlier designs. Safety parameter display systems are commonly employed to give the operators an easy access to the most important safety control features of the plant. Symptom based procedures have been created to support the diagnosing of complex plant transients. Simulators are used to familiarise the operators with details of plant transients. Probabilistic safety analysis is used to identify phases in the transients which are prone to operator errors.

The analysis of operational experience goes into details also with respect to human errors and organisational deficiencies. Fostering a non-blaming view towards such errors and recognising that they are caused by system deficiencies, it is possible to create an atmosphere of openness enabling minor problems to be reported and corrected. Identified development needs such as communication, safety attitudes, commitment and orientation can be addressed in training programmes.

Nuclear organisations, like many other organisations, rely on a well structured approach towards planning and operation. These approaches are documented in organisation and quality handbooks. Regular reviews are carried out to ensure that actual practices confirm with the handbooks. Indicators of efficiency and safety are used to provide early warnings of emerging problems. Involving the whole organisation in the definition of goals at various levels provides a mechanism of making partly conflicting goals explicit and easier to respond to.

Organisations designed according to these lines and which additionally are using various reviews to approach a path of continuous improvements should be both rewarding for the its people and fulfil demands for high reliability. This can be obtained with an organisational culture that is promoting communication and commitment. If all individuals are actively oriented with a questioning attitude it should be possible to detect and correct possible deficiencies in time.

Integration of work and information technology

The nuclear industry has only been partly influenced by the rapid development in information technology over the last twenty years. The main reason is that very few new nuclear plants have been ordered during that period. Another reason is the explicit requirement that nuclear plants should rely on proven technology which has brought a certain reluctance towards introducing new solutions. Major nuclear vendors have however developed and also licensed their own approaches in which modern information technology has been given a major role. Plant modernisations have brought in new systems in the control rooms, but many of those have not been considered safety critical.

The use of information technology has been more profound in supporting activities. The analysis of various accident sequences can today be carried out far deeper into the phenomena than was possible earlier. The calculations of a probabilistic safety analysis can be executed in a personal computer on the table of the safety analyst. Efficient databases are used to keep track of preventive and corrective maintenance together with failure frequencies and the utilisation of spare parts. Plant documentation is far easier to keep up to date using the new systems. Computer systems are also used to convey contacts between organisations during emergencies. Data bases support the collection and distribution of operational experience.

Information technology has had a large impact on control rooms. Efficient computerised systems provide intelligent alarms and early fault detection. Artificial intelligence methods can provide support for the diagnosing of plant transients and for selecting proper control actions. Interfaces to plant documentation and plant simulators can provide both support during transients and provisions for training when the plant is at steady power. Interfaces to maintenance and work planning systems can support communication between operation and maintenance. The possibility to transfer plant data to various off-line systems can support the analysis of transients.

It has been proposed that information technology can be used to promote cooperation and teamwork. Various prototype systems for computerised cooperation have been built. These technologies will find their way also into the high-risk technologies, but it is likely that the systems will be tailored only to restricted tasks. It is also likely that functions will be implemented in the systems used, rather than to be installed as specific one purpose systems. Those very few plants built during the last ten years have been realised with a massive support of information technology for the communication between members of the design teams.

Intelligent autonomous agents have been proposed as a new concept in software engineering. This concept can have interesting applications also in high-

reliability organisations. Present organisational designs are hierarchical which at least in principle implies that higher organisational levels should have a full description and understanding of control task at lower organisational levels. This requirement will introduce overlaps in the organisation and a decreased efficiency. One can argue that the overlap has the benefit of introducing redundancy, but it may in some cases obstruct a division of responsibilities.

The intelligent autonomous agents are not likely to be introduced as an organisational model for nuclear power plants, but they can provide insights for how to organise cooperation between various groups at the plants. Intelligent autonomous agents are assumed to have their own goals and tools for achieving them. They have mechanisms of self-reflection and learning to make it possible for them to improve their own behaviour over time. The agents interact with each other on interaction places, each with their own rules for the interactions. The agents and the interaction places are supported by communication networks and archives.

Intelligent autonomous agents provide a model of people and their work processes. It may be possible to use this model as a description of interactions and their relationships. Such a model may also be used to ask questions on the availability of important information in certain situations. Conditions for improvement and learning can also be elucidated by this models. Ultimately it may be possible to use the descriptions as computer models to make predictions for how certain conditions and transients can be handled at the plants.

Nuclear safety research in the Nordic countries

Research cooperation in nuclear safety was initiated in the Nordic countries already twenty years ago. The cooperation included human factors related issues from the beginning. Early projects were addressing control room design, human reliability and operator training. Later projects also included issues such as organisation and management, control room design, advanced information technology and emergency management. Main contributors to the research have over the years been the Risø National Laboratory in Denmark, the OECD Halden Reactor Project in Norway and the Technical Research Centre of Finland (VTT). The Swedish Nuclear Power Inspectorate (SKI) and the Finnish Centre for Radiation and Nuclear Safety (STUK) have been involved in funding and giving directions for the research. The nuclear utility companies in Finland and Sweden have been actively involved both in providing an environment for the research and in applying the results obtained.

Experience from several research programmes has shown the benefit of the cooperation. Nordic funds has made it possible to extend scarce national resources. Experts have been able to find colleagues to communicate with. Projects have had an impact which has extended far beyond Denmark, Finland, Norway and Sweden. A long term view has been adopted and several research issues were investigated before the Three Mile Island and Chernobyl accidents demonstrated their importance. The present research programme is running in the period 1994-97 and contains several projects with a relation to human factors and organisations. A review of the content and efficiency of safety related activities has an application on management issues, an investigation of sequences involving human errors and organisational

deficiencies is a part of the safety analysis and an investigation of maintenance practices provides insights in organisational response to aging.

In addition to the long term research oriented projects various studies has been carried out by VTT together with STUK and the power companies in Finland. The expertise of the operating personnel has been investigated in a row of projects carried out at VTT. A common theme has been the task of the operating personnel of complex automated systems and how people cope with unpredictable problems and technical failures. Some of the studies have been methodological and other more application oriented. A starting point has been the understanding that disturbances in the system also include possibilities for development. The disturbances set critical demands on the operators, but also give opportunities in creating expertise.

In one study the work culture of maintenance personnel was analyzed in interviews concerning daily work. The analysis included an identification of various needs in the work, an evaluation of potentials for people to meet requirements and the existence of supportive organisational mechanisms. An orientation-based approach to expertise was utilized in this study.[17] A second study investigated decision making of control-room operators in simulated disturbance situations. In that study the difficulty of interpretation of information as compared with the demands on the operators to take operative actions become evident.[18] Results also indicated differences between the crews' utilization of informativeness of available process information. One practical aim of the simulator study was to develop a method to be used in operator training for evaluating the cooperative decision making of crews.[19] Such a method can also enhance feedback to the trainees.

Conclusions

In high-risk industrial environments there has been an increased recognition of the importance to consider the human part of the system. Present solutions to ensure safety and reliability solutions have been created in a cooperation between engineers and behavioral scientists. The challenge is to develop better models of the human and organisational systems to make design processes more efficient.[20] A systems engineering approach can provide an important key in this endeavour.[21]

The main dilemma of the high-risk industries is to balance between needs to use proven technologies and needs for applying the best available technology. Also the nuclear industry should be able to make use of innovations in hardware, software and netware. This problem can be approached only from multiple angles where evidence from other industries is used together with detailed procedures for verifying and validating proposed solutions.

A continuous quest for higher safety and efficiency introduces the need for new tools, new systems and new organisational solutions. Information technology has been able to take up the challenge of providing cheap, efficient and reliable solutions. These solutions should be adapted to specific needs in each application area. In that adaptation process one should be aware of that the new systems may introduce the need for new organisational solutions. In a period of rapid technological development a special care should be put on understanding both the demands of the industrial processes and the opportunities as provided by the new technology. If the

consideration of the new solutions are carried out in a too restricted framework it is not likely that optimal solutions can be created. The integration of various views as seen by managers, operators, maintainers, safety analysts, etc. will provide one important key to a continuing success.

Only a prudent approach towards safety and a continued trust of the public can make high-risk technologies a viable alternative of production.[22] This can be built only through the people at the plants and their supporting organisations. Their tasks also involve informing the public on choices and communicating the associated risks in an honest manner.[23]

13.5.1996

References

1. Weart, Spencer R. (1988). Nuclear fear: A history of images, Harvard University Press, Cambridge, Mass.

2.Carroll, J.S. (1995). Sustaining improvements through safety culture: Problem identification and organizational learning processes, ANS-meeting on Safety Culture in Nuclear Installations,Vienna, 24-28 April.

3.Björn Wahlström (1992). Avoiding technological risks; the dilemma of complexity, Technological Forecasting and Social Change 42/3, pp.351-365.

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

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

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

7.K. E. Weick (1990). The vulnerable systems: An analysis of the Tenerife air disaster, Journal of Management, 16:3, pp.571-593.

8.Shrivastava, Paul (1987). Bhopal; anatomy of a crisis, Ballinger Publishing Company, Cambridge, Mass.

9.Starbuck, William H., Frances J. Milliken (1988). Challenger: Fine-tuning the odds until something breaks, Journal of Management Studies, **25**:4, pp.319-340.

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

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

12.B. Wahlström, P. Haapanen, K. Laakso, U. Pulkkinen: Safety of nuclear power; who learns from whom?, International Federation of Automatic Control, SAFE-PROCESS'94, 13-15 June, Espoo, Finland.

13.Wilde, G., J., S. (1988). Risk homeosrtasis theory and traffic accidents: Propositions, deductions and discussion of dissention in recent reactions, Ergonomics, **31** pp.441-468.

14.IAEA (1991). Safety culture, INSAG-4, International Atomic Energy Agency, Vienna.

15.Rick Jacobs, Sonja Haber (1994). Organizational processes and nuclear power plant safety, Reliability Engineering and System Safety **45**, pp.75-83.

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

17. Norros, L. (1995). An orientation-based approach to expertise. In: Hoc, J.H., Cacciabue, C., Hollnagel, E. (eds.): Expertise and technology: Cognition and human-computer communication. Hillsdale, New Jersey: Lawrence Erlbaum.

18. Hukki, K., Norros, L. (1993). Diagnostic orientation in control of disturbance situations. Ergonomics, 36, 11, November, 1317-1328.

19. Norros, L., Hukki, K. (in preparation). Dynamics of process operators' decision making in a disturbance situation: A contextual analysis, International Journal of Cognitive Ergonomics.

20.Björn Wahlström (1995). Modeling of man-machine systems; a challenge for systems analysis, pp.61-76, in Giampiero E.G. Beroggi, William A. Wallace: Computer Supported Risk Management, Kluwer Academic Publishers, Dordrecht.

21.Björn Wahlström: Models, modelling and modellers; an application to risk analysis, European Journal of Operations Research, Vol.75, Issue 2.

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

23.Baruch Fischoff (1995). Risk perception and communication unplugged: Twenty years of process, Risk Analysis, Vol.15, No.2, pp.137-145.