Differences between Human Reliability Approaches in Nuclear- and Aviation-Safety

Oliver Straeter and Barry Kirwan

Abstract: **Any industry has its own constraints which led to certain approaches for running the business and for dealing with safety issues. However serious events and accidents are showing that industries can learn a lot from each other, in particular in the field of human factors and human errors. This paper is a contribution to a cross-industry discussion of human factor issues. It will outline an approach to learn from decisions taken in an industry and the dynamic development of human factor issues rather than a comparison of differences in the state of a technology regarding human factor issues.**

The paper presents the opinion of the authors and not necessarily the ones of Eurocontrol. It is based on the authors' experience in both Nuclear Power Plant (NPP) Industry and Air Traffic Management (ATM) since several years.

Index Terms: **Human Performance, Human Reliability Analysis, Scenario Analysis, Interdisciplinary Analysis, Integrated Human Performance Modeling, Safety Management, Knowledge Management**

INTRODUCTION

Different industries start under different constraints for their technical developments and in interrelation with certain industrial partnership. Air Traffic Management (ATM) for instance was (and is) naturally linked to the developments of Aviation whereas the nuclear industry is naturally linked to the developments in process industry.

However, both are process-controlling environments with dynamic processes. Experiences in both fields show that human factor issues would considerably gain from a cross industry perspective. The paper will demonstrate in two examples how to mutually learn from human factor issues. The paper shows how cross industry perspectives can be generated using the event tree and scenario technique.

This paper will compare ATM (Air Traffic Management) and NPP (Nuclear Power Plants). The reasons for comparing ATM and NPP is that both authors have experiences in these fields and because both industries are very similar regarding the human performance issues. Certainly there are also many differences and similarities of ATM to other industries as the transport area (car, flight deck train for instance). These are not addressed here.

Some of the observations made may not be valid in general. They are based on the experiences made by the authors. It is intended to stimulate further discussion with this paper; it does not strive for general validity.

PHASES OF HUMAN FACTOR DEVELOPMENT

In many industries, if not in all, the technical developments are driving the human factor issues that an industry is faced with. Automation results in various human factor problems, which usually are not considered seriously till severe incidents or accidents happen (the Human Factor issue in NPP was founded more or less after the TMI accident).

It therefore seems that the lack in awareness of human factor problems is a major contributor to incidents and risk of the technical systems. This lack in awareness usually leads to a considerable sluggishness of the organizational part of an industrial system to include new human factor problems that rise during the phases of the industry. As an example, the problem of the decrease of knowledge in nuclear industry was first discovered in ~1990, however, 1990 there was no actual demand of addressing this problem, because it has not yet had an impact on the operation of nuclear plants. In the year ~2000 consequently considerable events happened showing that the loss of knowledge was a considerable contributing factor (Sträter, 2002; IAEA, 2001).

The sluggishness to incorporate Human Factor issues is surely an organizational one. An appropriate representation of human factors experts throughout the organization would mitigate this problem of dead-times from recognition of human factor issues until they are realized in the safety relevant industry.

From the human factor point of view, the following phases of Human Factor (HF) developments in respect to safety issues are relevant to be supported:

1. Problem discovery (e.g., ageing, knowledge-management, safety culture, errors of commission)
2. Concept generation (raising attention within the

organization, preparation of the organization for dealing with the problem, literature research)
3. Concept definition
4. Design of methods from concepts and development of methods
5. Method application (trial applications, validation studies)
6. Implementation of method (throughout implementation in all parts of organization)
7. Concept monitoring (is the concept covering the aspects it was designed for, e.g., using operational feedback)

It takes time till the phases are realized in an operational setting. Therefore (as in the technical development of a product or an industry), human factor issues may cautiously be considered in the problem discovery phase. Errors of commission are an example of how long the development of this issue may take. The incident in TMI for instance included errors of commission. Up to now, the EOC-methodology has reached phase 5 (Method application). Some of the methods for EOC had trial applications, validation studies as shown in OECD (2002).

TMI is also a hint that the phase 7 (Concept monitoring) was never reached for the issue of HRA methodological development within the safety regulation of nuclear industry.

HUMAN FACTOR ISSUES

Table 1 represents those Human Factor Issues that were observed as being worthwhile to be compared between ATM and NPP. They mean the following:

- Establishment of explicit safety assessment including related organizational processes: NPP developed over the years a very explicit safety assessment procedure, namely probabilistic safety assessment. Such an explicit assessment procedure is not yet present in ATM.
- Analysis and assessment of hybrid system: NPP recognized the problems of Hybrid systems about ~10 years ago and performed investigations on the impact of technologies from several development stages in control rooms.
- Risk Informed Decision-making (RID) and Regulation: RID has been discussed for several years in the nuclear industry to face the changes the industry due to the free energy-market, phasing out of the industry, and aging of the plants. Unfortunately RID is as yet only realized to some extent and in some countries.

Table 1: Comparison of ATM and NPP based on personal guesses about the development state regarding human factors

Human Factor Issues	***Current phase in ATM***	***Current phase in NPP***	***Stage of Development related to time-scale year 0 (rough estimates)***
Establishment of explicit safety assessment including related organizational processes	Problem discovery	Concept generation	NPP 10 years ahead
Analysis and assessment of hybrid system	Concept generation	Method application	NPP 10 years ahead
Risk Informed Decision-making (RID) and Regulation; RID only realized in some countries	Concept generation	Design of methods	NPP 5 years ahead
Safety Culture including organizational aspects in Human Reliability Assessment	Design of methods	Method application	NPP 5 years ahead
Human Reliability Assessment (HRA) methodology including integration of prediction and assessment of human error	Design of methods	Implementation of method	NPP 2 years ahead
Event evaluation and operational feedback programmes	Implementation of method	Concept monitoring	NPP 2 years ahead
Mirrored organization and Mirrored regulation	-	-	No one ahead
Inclusion of human error into the design process of automated Systems	Method application	Design of methods	ATM 2 years ahead
Human factor centered Automation	Method application	Concept generation	ATM 2 years ahead
Human Factor integration in Design and development phases of technical systems (HF-case)	Concept definition	Concept generation	ATM 5 years ahead
Information flow between parties (including regulatory body and ATM)	Concept monitoring	Design of methods	ATM 5 years ahead
Crew Resource Management (CRM)	Implementation of method	Problem discovery?	ATM 5 years ahead
Monitoring of concepts including processes for improvement and for looking into new safety issues	Concept monitoring	Problem discovery?	ATM 5 years ahead

- Safety Culture including organizational aspects in Human Reliability Assessment: The inclusion of organizational aspects in operation, operational feedback programmes and HRA (Human Reliability Assessment) would be essential since many incidents are showing the importance of the organizational impacts.
- Human Reliability Assessment (HRA) methodology including integration of prediction and assessment of human error: HRA is an essential part of including human issues in the safety regulation process in NPP.
- Event evaluation and operational feedback programmes: In NPP several initiatives for integrating operational feedback into an international exchange of information are in place (IRS – Incident Reporting System; IAEA 2001).
- Mirrored organization and Mirrored regulation: These concepts specify that industry and regulator should have human factor issues represented according to the importance of human factor issues. Mirrored organization means the mismatch of human factor staffing and human factor issues present in the industry. E.g., depending on the industry, at least about 50% of all in operational events are due to human errors. However, the regulation units usually represent human factors with less that 5% staffing. Mirrored regulation represents that human factor experts should be equally represented in regulation and industry.
- Inclusion of human error into the design process of automated systems: Often human factors is the 'dead end' of system development, though most of the human factor problems could have been avoided if human factors were included already in the design phase of a technical system.
- Human Centered Automation: History shows that technical departments usually drive technical developments. Human issues are usually recognized in late development phases. Problems that usually can only be changed with a high effort of restructuring, reorganization and further technical development at these stages. Complaints of Human Factor experts at this stage also lead to a bad image of Human Factors (i.e., as a sourpuss). Human factor centered automation attempts to avoid this lack of cooperation of technical developments and human factors.
- Human Factor integration in Design and development phases of technical systems (HF-case): Related to the problems described in the last point is the early inclusion of human factors issues in the design of technical systems. Eurocontrol has recently established such a process called 'HF-case'.
- Information flow between parties (including regulatory body and ATM): Safety is a collaborative task of regulator and licensee (Balfanz et al., 2002). Collaboration requires an open information flow between regulator and licensee.
- Crew Resource Management (CRM): According to the approach of Crew Resource Management of Aviation, ATM uses the concept of Team Resource Management (TRM). Both are techniques introduced into the working system to enhance the team communication and team processes. Errors in team behaviour are important to look at in the nuclear industry since they lead to the safety relevant event initiators (Sträter, 2002).
- Monitoring of concepts including processes for improvement and for looking into new safety issues: Any technique or process is relying on the continuous further development of the concepts included in the technique. Human Reliability Assessment was for instance for many years concerned with errors of omission. However, errors of commission were meanwhile modeled in recent developments (OECD, 2002). However, the time from the first problem observation (the TMI Accident, 1979) till the concept was in the modeling stage needed roughly 15 to 20 years – an example for the failure of the efficient monitoring regarding errors of commission in nuclear. Safety relevant problems should be addressed much faster.

SCENARIOS OF FUTURE DEVELOPMENTS

The comparison of ATM and NPP regarding the development-state of human factors reveals issues that are interesting. However, it is to be understood why they are in a particular state, what the constrains were at a certain point in time, how historical decisions impacted safety, and finally in which time frame the impact led to safety problems. Based on these considerations, the reasons why the industries are in the state they are can be investigated by performing a scenario analysis of the developments. Scenario analysis can be represented in the well-known event tree approach.

Two example-scenarios are provided in the following. They show how to learn form experience. The history of the NPP area may provide lessons for a good future of ATM, and vice versa.

The outcome of the scenario analysis will be to see possible dangers and possibilities for future developments in the „other" industry. The analysis will also provide key decision requirements to achieve a good future in either of both industries.

The two examples given below are the knowledge management scenario in NPP and the Safety management scenario in ATM.

THE KNOWLEDGE MANAGEMENT SCENARIO IN NPP

The operator age distribution in the nuclear industry is in a considerable condition. In German NPPs for example, aging was first seen as a problem in 1990. However no considerable actions were introduced to resolve the situation.

Meanwhile, in ~2000, the first incidents happened due to loss of corporate knowledge and memory. The issues have many reasons on various levels involved in regulation and operation leading to the confidence that everything is OK

Similar knowledge management issues were observed in several other states as well (IAEA, 2001). One contributor to these issues seems to be that the industry is in a phase-out state (events occurred for instance during the opening and breakdown of the energy market in Russia, and after the German decision to cancel nuclear power).

Figure 1 shows the scenario comparing knowledge management in NPP and ATM. It demonstrates that ATM is in a very similar state to NPP 10 years ago. In principle, ATM has too options to deal with the expected loss of corporate knowledge due to retirements: wait and see, or else start a knowledge management initiative. From the experiences in NPP it can be concluded that an active approach is much more favorable that the 'wait and see' option.

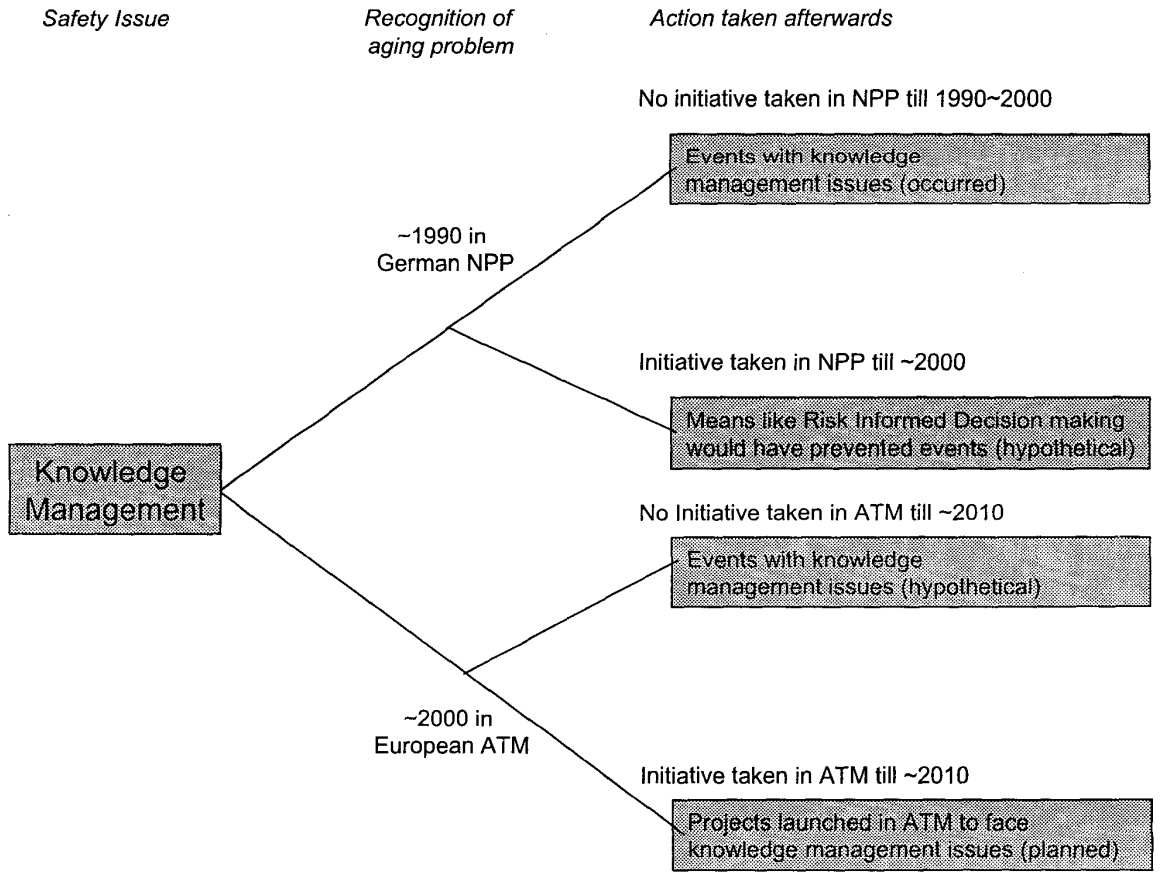

Figure 1. A scenario for Knowledge Management

NPP can learn from this scenario that it must go into RID (Risk Informed Decision-Making) in order to face

the changes in the industry. ATM can learn that it has to take care about knowledge management issues to maintain safety in future.

THE SAFETY MANAGEMENT SCENARIO IN ATM

Figure 2 outlines the second scenario of human factor aspects in safety management. Safety assessments in NPP are very explicitly formulated using PSA (Probabilistic Safety Assessments) and HRA (Human Reliability Assessments) for Human issues respectively. Explicit safety assessments have advantages and disadvantages. The main advantage is that the safety of the industry can be measured and any party (licensee and regulator) is informed about the safety level of a particular plant. However, this advantage is also its disadvantage since the measurement methods have to be prescribed. As a result, many safety assessments are overruled and do not reflect the real safety issues that the plant is faced with (Straeter & Zander, 1998). IAEA (2001) also showed that questioning attitude and a certain level of openness towards safety issues that are non-compliant to prescribed safety procedures would lead to considerable improvements of the safety level.

A certain level of flexibility and open discussion would improve the safety in such problems of over-ruled situations. ATM does have such an attitude to be open towards missing safety aspects. However, the explicit safety assessment is not yet present (though systems are being developed and are beginning to be implemented in some areas). In order to maintain the safety level in the industry under the condition of the growing traffic density it has to be approached without giving up the advantages of the implicit safety approach. Optimal safety can be achieved if implicit and explicit safety aspects are mixed in an optimal matter.

NPP can learn from this scenario that it must go into an open collaborative safety approach in order to get implicit safety aspects covered. ATM can learn that it has to make an effort to get explicit safety informed assessments to cope with the future demands in ATM (due to traffic increase). This effort should not abandon the implicit safety approach but should complement it. Means like knowledge management and integrated human modeling are options for a co-operative implicit and explicit safety approach.

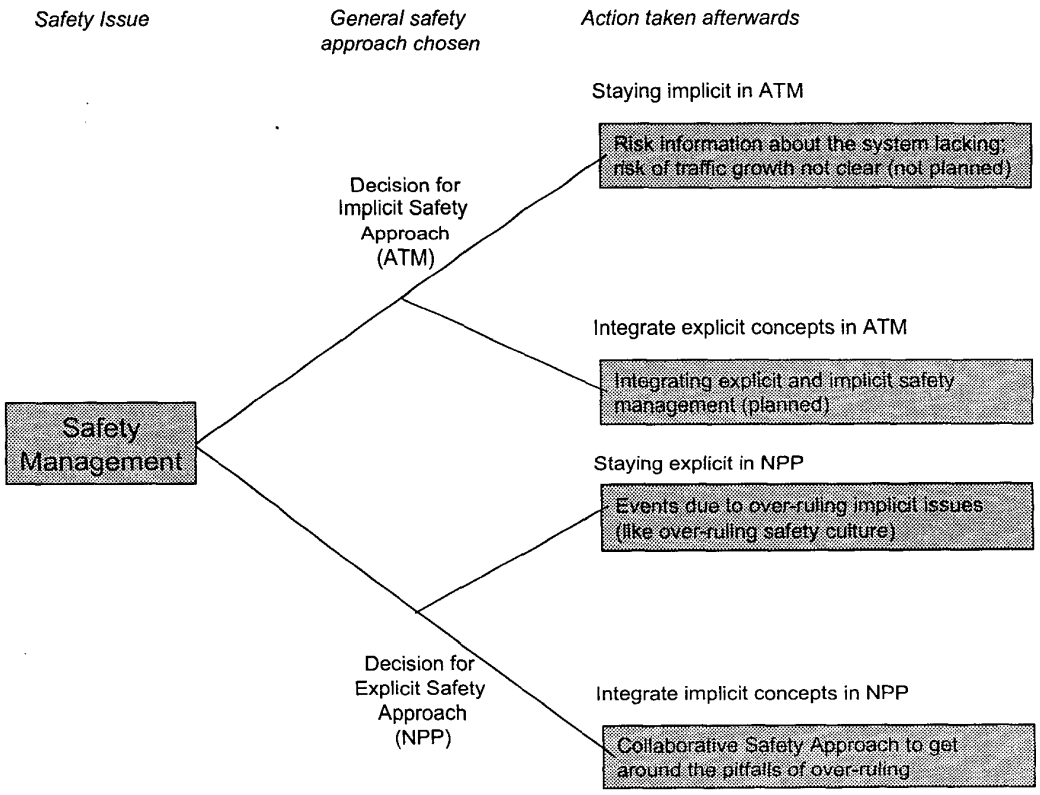

Figure 2. A scenario for Safety Management

COMMON PROBLEMS AND COLLABORATIVE LEARNING

The paper has outlined some bright and some not so bright scenarios of safety and human factors. It has provided two scenarios that showed how different

industries can learn from each other, what the technical aspects to be considered are, what may have went better, and where current problems in one industry can be used to avoid similar problems in another industry.

- NPP can learn from the first scenario that it must go into RID (Risk Informed Decision-Making) in order to face the changes in the industry. ATM can learn that it has to take care about knowledge management issues to maintain safety in future.
- NPP can learn from the second scenario that it must go into an open collaborative safety approach in order to get implicit safety aspects covered. ATM can learn that it has to make an effort to get explicit safety informed assessments to cope with the future demands in ATM (due to traffic increase).

The scenarios showed a commonality in that respect that human factor aspects (as well as others) require monitoring of the concepts in developments of existing concepts. Additionally, the awareness that no concept can be complete and efficient is an essential element of safety.

It was shown in the paper that the incidents discussed are mainly due to failures in monitoring the safety relevant concepts.

Monitoring needs collaboration of all parties involved in the safety regulation and operation of the industry. Collaboration in turn needs a frame of reference that establishes and maintains the communication between the parties.

REFERENCES

Balfanz, H.-P-, Linsenmaier, B. & Straeter, O. (2002) Development of Practical Criteria for Safety Culture Assessment in German nuclear power plants. PSA '02. Detroit.

IAEA (2000) IRS Study on Incidents Caused by Loss Of Corporate Knowledge And Memory (Phase I - Selection of events for in depth analysis). IAEA. Vienna (IAEA-J4-CS-10/00).

IAEA (2001) Guidelines for describing of Human Factors in the IRS (Human actions and related causal factors and root causes) IAEA. Vienna (IAEA-J4-CS-10).

OECD (2001) Errors of Commission in Probabilistic Safety Assessment. Workshop of the OECD/NEA. NRC. Washington.

Sträter, O & Zander, R.M. (1998) Approaches to more Realistic Risk Assessment of Shutdown States. Paper for the OECD-Workshop "Reliability Data Collection for Living PSA" in Budapest, Hungary from 21.4. to 23.4.1998. NEA / CSNI / R (98) 10. OECD NEA. Paris. p. 236 ff.

Sträter, O. (2000) Evaluation of Human Reliability on the Basis of Operational Experience. GRS-170. GRS. Köln/Germany. (ISBN 3-931995-37-2)

Sträter, O. (2002, in press) Building the new HRA. OECD Workshops on strengthening the link between HRA and data. Reisebericht. GRS. Cologne.

Sträter, O. (2002, in press) Considerations on the Elements of the Quantification of Human Reliability. OECD Workshop on strengthening the link between HRA and data. OECD. Paris.