Presented at the International Conference on Operational Safety Experience and Performance of NPPs and Fuel Cycle Facilities, IAEA, 21-25 June 2010, Vienna, Austria

Models, methods and tools for safety management

Experience from Vattenfall

Björn Wahlström[1], Carl Rollenhagen
Vattenfall NSMI
Jämtlandsgatan 99
SE-162 87 Stockholm
Sweden

Abstract. Efficient safety management relies on both formal and informal systems. The formal system can be seen as written into the management system consisting of policies, mission statements, value declarations, organisational structure, job descriptions, instructions, etc. The informal system relies on people and their attitudes, beliefs, knowledge, skills, orientations, habits, practices, values, etc. This informal part is often associated with the safety culture of the organisation. Considerable efforts have been spent in understanding these formal and informal parts of safety management. One approach in a search for models, methods and tools for safety management was selected by Vattenfall in the year 2005 when the Nordic Generation Safety Management Institute (NSMI) was founded. The institute was given the task to support safety management within Vattenfall through research, development and training activities. The paper reflects on experience from Vattenfall NSMI during the first four years of operation.

1 Introduction

Vattenfall decided in the year 2005 to establish an internal institute NSMI, with the task of supporting the company with training and R&D in the area of safety management. This decision was initiated in the aftermath of an EU project called LearnSafe [1]. An important part of the decision was to integrate Vattenfall Hydro Power as a stakeholder in NSMI. The activities started in April 2006 and the first major task of NSMI was to initiate a training course in safety management addressing the nuclear plants as a part in the qualification process for managers with an operational responsibility. A pilot course was given in November 2006 at the Ringhals nuclear power plant and it served as providing a conceptual frame for later courses.

The second task of NSMI, to initiate, carry out and supervise R&D activities, was in the beginning put on a hold. During that time NSMI participated in several discussions with the Vattenfall plants on various safety management issues, which the plants had to resolve on a medium term and which could be approached in R&D projects.

The NSMI activities have so far illustrated the benefit of amending practical safety related activities at the plants with more theoretical approaches, such as utilising results from academic research. The combination of training and R&D activities has been beneficial. For example, the discussions during training sessions have generated issues to be scrutinized in more detail and the results from the research activities have been fed back to later training courses. The focus on R&D also includes a proxy and an obligation to monitor and evaluate national and international activities within safety science. One specific goal of the activities has been to build an understanding of how various parts of safety management interact and how this understanding should be packaged into training courses.

The discussion below describes some experiences from NSMI. One part of this experience has already been collected and analysed in an evaluation of the NSMI activities, which according to the original inauguration decision of the institute was made after three years of operation. The result of this review was very favourable and took a clear positive stand for a continuation and institutionalisation of NSMI as an organisational entity within Business Unit Nuclear of Vattenfall.

2 A set of training courses

NSMI has over the years offered several courses in safety management at different organisational levels in Vattenfall. Two courses in strategic safety management have been given to senior managers and board members at the corporate level. Six courses in basic safety management have been directed

[1] Corresponding author, contact information, bjorn@bewas.fi, Djurholmsvägen 2, AX-22920, Brändö, Finland

to senior managers at the Vattenfall production plants and two courses for shift supervisor at one of the Vattenfall nuclear power plants in Sweden. The courses have deliberately been made to cover a broad scope to support an understanding of safety activities that goes beyond standard prescriptive formal approaches. The course evaluations that have been collected over the years indicate a large satisfaction with both content of and lecturers at the courses.

2.1 A basic course in safety management

The first course in safety management was considered as a pilot course and it was developed based on the assumption that managers should have a broad understanding of issues related to safety. Such an understanding is considered necessary, because simple prescriptions cannot cope with all possible situations that may occur. In addition the broader understanding gives explanations for why certain safety provisions are in place, which can help in situations that have not been foreseen.

Lecturers with a background safety science have been selected for the courses. One important component in the planning was to make the basic course compulsory for persons, who have an operational line responsibility. The basic course has now got an established form and it is given as two plus two days. The course has attracted senior managers also from the safety, maintenance, technical support and human resources departments at the plants.

2.2 A course in strategic safety management

The success with the basic course in safety management opened up for a discussion of the need for increased insights in safety matters at the corporate level within Vattenfall. The first course was given in February 2009 in Swedish and was repeated in English in May 2009 to allow for participation from the Vattenfall units in Germany. The course is two days long and it is intended for senior managers at the corporate level, board members in the Vattenfall companies, asset managers, etc. Especially the separation between the *sharp* and the *blunt end* [2] has been important for illustrating the difference between an operational and a strategic focus in decision-making.

2.3 A course for shift supervisors

The incident at the Forsmark plant in July 2006 initiated among other actions also a safety culture enhancement programme. As a part of this programme a one-day refresher course in safety management was provided to all shift supervisors in Forsmark. This course was focused on a repetition of basic safety thinking within nuclear power together with historical glimpses from the nuclear power programme in Sweden. Further development of this course has been transferred to KSU, the organisation in Sweden, which carries out operator training using simulators.

3 Research activities

The development of the basic course in safety management took the major part of the resources during the first financial year of NSMI. Discussion within the steering group of NSMI and the plants however provided ample inputs for in depth considerations of how to target research activities. The concepts of safety culture and safety indicators rapidly became obvious issues for further investigations. Furthermore the extensive modernisation programmes at the Swedish nuclear power plants also illustrated the need for a better understanding of how technical, organisational and people components interact in plant modifications. Principles and practices of regulatory oversight has been a third component of many discussions.

3.1 Safety culture and safety indicators

The concept of safety culture was born in the aftermath of the Chernobyl accident. It has been very important in illustrating the people and organisational components of safety. However, the concept has sometimes got quite mechanistic interpretations, which may interfere with established principles in ensuring safety [3]. In Sweden a yearly safety climate survey has become a practice at the nuclear power plants. There seems however to be a need for more thinking, before the collected information can be used more effectively in improvement programmes [4]. Event investigations are an important

safety activity from which many lessons can be learned [5]. The methods and tools used for event analysis have an influence on the results obtained [6]. A practical difficulty seems to be to close the loop from lessons learned to persistent improvements [7]. The commonly voiced recommendations that the nuclear power plants should become learning organisations should however be made more concrete before such goals can be reached [8].

3.2 The review process of plant modifications

Plant modifications are important for safety, because they close the loop from the feedback of operational experience to safety improvements. On the other hand, experience has also shown that plant modifications may introduce problems if not carried out in a prudent way [9]. The review processes during the planning, design and installation of plant modifications are intended to ensure that the intended benefits will be reached and no new safety challenges will be introduced. However, this does not seem to be the case for many plant modifications. A PhD project was initiated to investigate this issue in more detail [10]. A similar project was carried out for Vattenfall Hydro Power.

3.3 Regulatory oversight

The regulatory oversight is an important component in safety activities [11]. The regulatory model in Sweden builds on openness and confidence, where the licensees maintain a strong independent safety review function. This model has shown its strength in spite of a few cases where misunderstandings on behalf of both parties seem to have created unnecessary confrontations. A conclusion has been that it would be interesting to study more in detail how this model works in practice. One could for example investigate how the regulator and how the licensees perceive daily interactions and which types of issues are easy respective difficult to approach. A hypothesis is that an effective regulatory oversight builds on clear and explicit roles both for the regulator and the licensees. A proposal has been written for a project that takes a look on how a few typical questions have been initiated, carried out and closed. It is expected that such a project could provide important information for improving regulatory oversight.

4 Models, methods and tools

The training courses and the research activities of NSMI have provided many topics for discussions, where pros and cons of various practices connected to safety management have been put on the table. These discussions have sometimes been rather philosophical and sometimes very "down to earth", but they have always circled around issues related to safety, how safety is constructed and what methods and tools can be used to control safety. The discussions have showed a real concern for safety issues and an urge for understanding a large variety of contributing factors. The discussions have provided inspiration for us to search for better models that can be used to illustrate and explain some of the more fundamental issues behind nuclear safety. A list of interesting issues for research in safety management is maintained as a part of the annual planning of NSMI activities. The sections below illustrate some of them, which we think would warrant more attention in the future.

4.1 Risk analysis and safety engineering

It often helpful to separate between risk analysis and safety engineering, because these activities involve different views and approaches. The risk analysis activity is focused on identifying various threats and assessing their consequences, whereas safety engineering is focused on removing, controlling and mitigating those threats. Risk analysis could therefore be said to focus on problem identification and safety engineering on problem solving. There is also a difference between the two activities in terms of specialisation, where the risk analysis part typically is carried out by specialists and the engineering solutions for acting on the safety threats are decided on by generalists.

Risk analysis and safety engineering activities are nevertheless tightly interwoven. This is for example demonstrated in the concept of design basis accidents, which in the nuclear field is used as a major design principle. According to the principle a suitable set of challenging accident scenarios are postulated as the basis for safety engineering efforts. Suggested engineering solutions are analysed under varying conditions to check if they can ensure that the plant can be kept within safe operational

boundaries. If not, then different or additional safety provisions have to be introduced. The risk analysis can also be seen as suggesting event sequences to protect against and the safety engineering to point at systems and components that are crucial in that task.

4.2 How safety is constructed

One of the most important points of departure in explaining how safety is constructed is to use the notion of three different systems sometimes called *man*, *technology* and *organisations* (MTO). It is important to understand that these three systems are fundamentally different, which means that different models have to be used to understand their characteristics. This also implies that they should be monitored and controlled in different ways. When this is understood more thorough discussions of necessary models, methods and tools can be initiated.

A second point of departure is to discuss necessary conditions for a successful control of these three systems. From systems engineering we can learn that at least four conditions have to be fulfilled. There has to be a goal for the control, the system should be observable and controllable and finally one should have a model of the system. The observability and controllability conditions have been discussed in depth within systems theory, but the concepts are easy to understand, one should be able to observe the behaviour of the system and one should be able to influence it in desired directions. The need for a model implies that one should have an idea how different control actions will influence system behaviour.

From this very general discussion the concepts of feedback and feed forward loops can be introduced. Successful control of safety should start with risk analysis, i.e. a feed forward model based effort that is comprehensive enough to reveal possible threats that have to be reacted on. Because no model can depict the reality in all its detail, it is important to introduce a feedback loop of operational experience. Finally the regulatory oversight provides a societal control loop, which forces safety activities in the plants to spend a second thought in their task to convince a third party that the operation can be considered safe.

4.3 To control safety

From this very general discussion of necessary conditions for control of safety, one can move to their implications for the MTO-systems. For the M-system it is for example important for managers to set goals in terms of people needed to operate the plant, their skills and number. The managers should furthermore be aware of the strengths and weaknesses of their staff and their actions should drive the M-system towards identified goals. Finally managers should have a kind of mind model of what they have to do in order to move the system in the right direction. A similar kind of reasoning can be applied to the T- and O-systems.

In the management of organisations there are two additional conditions that should be given appropriate consideration. The first has to do with the fact that all control actions causes a burden on resources. This means that the original problem of controlling safety has to be amended with the additional problem of managing resources over time. The second additional condition has to do with system dynamics. If one has to meet some time targets, it may be necessary to invest more resources into applied control actions. Inherent dynamics in the system may also imply that controls have to be exercised in a certain time window to be efficient.

The difficulty of applying system models for the control of nuclear safety lies in the complexity of the nuclear power plants, their staff and the organisation. The complexity is due to a multitude of interactions within and between subsystems. Some of the interactions are linear, but many of them are non-linear and contain time dependent and stochastic components. That means that accurate predictions of their behaviour are impossible, which means that the models used for control have to be simplifications [12]. However, it is still necessary to have a reasonably accurate model that is refined enough to convey the essence of actual situations in the support of decisions by responsible managers.

4.4 The safety management system

The safety management system can be seen as the combination of formal and informal parts that describe the MTO-systems and that give guidance on how they can be controlled. The formal part of the safety management system is composed of written mission and value statements, instructions and other documentation that describes how and when various activities are carried out and by whom. The informal part is embodied in values, norms, attitudes and beliefs and it is often associated with organisational culture. The formal part of the safety management system is typically designed and written down as a conscious effort, where the informal system to a large extent is emerging over time without conscious actions. The management system has sometimes metaphorically been called the "software of an organisation".

One interesting property of software that is supposed to control a system is that it should have the same complexity as the system that it is placed to control. This principle was formulated in the 1950ies as the principle of requisite variety [13]. The principle implies that managers should have an understanding of not only the MTO-systems, but also of how the formal and the informal parts of the management system interact in producing safety.

This frame, which is based on general systems engineering principles, has important lessons to give. It is for example clear that one has to assess all three components of the MTO-systems and one has to assess both the formal and the informal parts of the management system. The assessment has to be based on an understanding of how safety is constructed within the MTO-systems. In this context it also important to realise that a proper control may imply finding a balance between competing goals. Finally, it is also important to understand that that the assessment itself, depending on the methods and tools used, may influence safety either for the good or for the bad [14].

4.5 Closing the feedback and the feed forward loops

The discussion above has been carried out and refined in several occasions within the NSMI activities. The perhaps most important benefit of the discussion is that the frame it provides, gives an opportunity to assess if the safety activities at the plants can be considered to sufficient. This question is crucial, because it provides a check that all important issues have been considered. If important safety activities are in place, the next question to ask is whether or not they are executed to a high enough standard. This quality issue should also be placed in relation to the influence on safety that various activities have.

This quality question can be addressed for example by benchmarking with other organisations, which also has the immediate benefit that it may point out concrete issues to improve [15]. Another line of approaching the quality issue could be to create behaviourally anchored rating scales for the activities in question. This approach may open up a possibility to create leading indicators for assessing safety, by selecting a set of necessary conditions for safety and making such quality assessments for activities contributing to them.

In trying to pinpoint important safety activities at the plants, the feedback and the feed forward loops are essential. Models could be used in a planning mode to create candidate designs for the MTO-systems, which are assessed with predictive models. If predictions point to problems, the candidate designs can be refined in a new round. The planning can be associated with a feed forward path, which together with a feedback path of operational experience can be used to update the planning models. These simultaneous feed forward and feedback loops should be functional on all levels within the organisation and used to identify possible safety deficiencies to be corrected.

5 Conclusions

One conclusion of the NSMI activities is that there is no grand model that can be used to control safety at the nuclear power plants. Instead there has to be a common frame into which different situational models can be placed. These models should be transferred into the thinking of the managers responsible for safety related activities at the plant. This task may actually call for creative dialogues between managers having practical problems and safety theorists in a search for models that are

simple enough to illustrate the essence of various problems, but still refined enough not to be trivial. If such dialogues are exercised they may also help in making tacit knowledge from the plants explicit enough to be collected and documented.

Another pronounced finding from the activities is also that safety should be the concern for a larger group of managers than those directly responsible for plant operation. One may even suggest that one constructive approach would be to launch mapping activities, where organisational units are asked to illustrate how they may influence safety both for the good and for the bad. Such maps can then serve as simple mind models for how various activities within the organisation can influence safety.

Modelling approaches such as indicated above are in our opinion important in a continuous search for approaches that can ensure a safety of the nuclear power plants. They can support the need for setting standards for various safety activities at the nuclear power plants and thus the can also serve as a reference for safety assessments to be made. This may help in providing answers to the old question "What is safe enough?", which still is as relevant as it was when it was asked the first time some fifty years ago.

Disclaimer: The opinions expressed in this paper are given by the two authors and do not necessarily reflect opinions held by Vattenfall.

REFERENCES

[1] WAHLSTRÖM, B. et al, LearnSafe – Learning organisations for nuclear safety, VTT Research Notes 2287, Technical Research Centre of Finland, Espoo.

[2] REASON, J., Managing the risk of organizational accidents, Ashgate, Aldershot (1997).

[3] ROLLENHAGEN, C., Can focus on safety culture become an excuse for not rethinking design of technology?, Safety Science 48 (2010) 268–278.

[4] ROLLENHAGEN, C. et al, Development of a Safety Climate Questionnaire for Nuclear Power Plants, Joint 8th Annual IEEE Conference on Human Factors and Power Plants and 13th Annual Workshop on Human Performance. Monterey, California, August 26-31, 2007.

[5] ROLLENHAGEN, C., Event investigations at nuclear power plants in Sweden: Reflections about a method and some associated practices, Safety Sci. (2010), doi:10.1016/j.ssci.2009. 12.012

[6] ROLLENHAGEN, C. et al, The context and habits of accident investigation practices: A study of 108 Swedish investigators, Safety Science 48 (2010) 859–867.

[7] LINDBERG, A.-K., et al, Learning from accidents – What more do we need to know?, Safety Sci. (2010), doi:10.1016/j.ssci.2010.02.004.

[8] WAHLSTRÖM, B., Organisational learning – Reflections from the nuclear industry, Safety Sci. (2009), doi:10.1016/j.ssci.2009.11.010.

[9] NEA, Safety of modifications at nuclear power plants – the role of minor modifications and human and organisational factors, CSNI/R(2005)10.

[10] FALK, T. et al, Technical reviews of plant modifications; challenges in performing safety reviews (submitted for publication).

[11] WAHLSTRÖM, B., Reflections on regulatory oversight of nuclear power plants, Int. J. Nuclear Law, Vol. 1, No. 4, 2007.

[12] WAHLSTRÖM, B., Decisions in complex systems; finding a balance between competing forces, 26th NeTWork Workshop on "Resolving Multiple Criteria in Decision Making Involving Risk of Accidental Loss", Schloss Steinhöfel, Germany, 27-29 September 2007.

[13] ROSS ASHBY, W., An Introduction to Cybernetics, Chapman & Hall, 1956.

[14] WAHLSTRÖM, B., et al, Assessments of safety culture – to measure or not?, 14th European Congress of Work and Organizational Psychology, 13-16 May, 2009, Santiago de Compostela, Spain.

[15] WAHLSTRÖM, B. et al, An international benchmark on safety review practices at nuclear power plants, VTT Research Notes 2015, Technical Research Centre of Finland, Espoo.