nks

Nordisk kernesikkerhedsforskning
Norrænar kjarnöryggisrannsóknir
Pohjoismainen ydinturvallisuustutkimus
Nordisk kjernesikkerhetsforskning
Nordisk kärnsäkerhetsforskning
Nordic nuclear safety research

NKS-88
ISBN 87-7893-146-0

Safety Management: A Frame of Reference for Studies of Nuclear Power Safety Management and Case Studies from Non-Nuclear Contexts

Ola Svenson[1)] and Ilkka Salo[1,2)]

[1)] Stockholm University, Sweden
[2)] Lund University, Sweden

September 2003

Abstract

A systems perspective on safety management is introduced followed by two briefly presented case studies of safety management. The first study concerns a car manufacturer and the second study a road traffic tunnel system. The risks of a car accident in the first case study are evident. The great exposure generates many incidents and accidents. In the second study, the rather low traffic intensity through the tunnel produces few incidents and accidents and only a few fatal accidents over the years. Yet, the risk of the individual traveller is much greater in the tunnel than on the average road. The case studies are presented in a systems perspective with emphasis on information feedback about the risks of the systems. The first case study illustrates high quality safety management, while the second case study shows many weaknesses of the safety management in the tunnel system. Some differences in safety management between the case studies are noted. The last part of the study presents an organizational perspective on safety management and offers alternative theoretical perspectives on the concept of safety management. The report shows that further studies are needed both (1) to develop a frame of reference for describing safety management across industries and activities and (2) to collect data illustrating of good and poor safety management. Then, the results can be used to strengthen and/or improving safety management in the nuclear power industry and its regulators.

Key words

Safety management, case studies, systems perspective, information feedback

NKS-88
ISBN 87-7893-146-0

Electronic report, September 2003

Published by
NKS Secretariat
P.O. Box 30
DK – 4000 Roskilde, Denmark

Phone +45 4677 4045
Fax +45 4677 4046
www.nks.org
e-mail nks@catscience.dk

NKS

SAFETY MANAGEMENT: A FRAME OF REFERENCE FOR STUDIES OF NUCLEAR POWER SAFETY MANAGEMENT AND CASE STUDIES FROM NON-NUCLEAR CONTEXTS

Ola Svenson (1) and Ilkka Salo (1,2)

(1) Risk Analysis, Social and Decision Research Unit
Department of Psychology, Stockholm University
(2) Department of Psychology, Lund University

September 2003

CONTENTS

1. Introduction

The purpose of the present study is to provide a perspective on the management of nuclear power safety through reference to safety management in non-nuclear systems. The report will start with a general systems perspective of safety management. This will be followed by two case studies and the report will finish with an organizational perspective applied to safety management. The material will be covered in a summary fashion to fit the perspectives chosen here and the interested reader will be referred to the original source material in the text if s/he wants more information about the specific cases.

A nuclear power plant or any other industry/human technology activity can be modeled as a suprasystem with two subsystems interacting to keep that suprasystem in a steady state when it performs what it is intended to produce, e.g., electricity. But also when it enters outage, stays in outage and when the system starts production again.

The physical plant is a subsystem, which is a concrete constructed, technical non-living system and the other subsystem is the organization of people constituting a concrete living system (Miller, 1978). The purpose of the organization is to keep the suprasystem, including the technical and the organizational systems and their subsystem, within the limits of a steady state when producing electricity at a rate determined by other suprasystems (e.g., economic and political systems). That is, managing the suprasystem so that it is kept in a steady state with the all the variables within the range of stability prescribed by that steady state. If this is not done, the system's structures and processes change and the system itself moves towards another steady state. In this change the system may even have difficulties to survive, but ideally it should adapt to the new environmental requirements.

When one of the variables moves towards the limit of stability, the system strives to counteract the movement through negative feedback. This is normal regulation of the system. Both the plant technical subsystem and the organization subsystem have lower level subsystems and some of these have the purpose of keeping variables within their ranges of stability.

When the system is exposed to stresses that threaten to move variables outside the range of stability and the system out of its steady state, adjustment processes keep variables within their ranges of stability despite stresses. In this situation, special subsystems (e.g., barrier function systems, Svenson, 1991, 2001) are activated to preserve the steady state of the system. Barrier function systems, a kind of subsystems, perform processes with the purpose of retaining a system within a steady state even under stress. If one barrier function system cannot handle the situation there are usually other backup systems. In a nuclear power plant, the organization and the plant are designed so that for most threats, other barrier function systems are activated to keep the suprasystem in a stable steady state. In living systems, such as humans there are normally so many coupled adjustment processes that the system is ultrastable (Miller, 1978, p. 36).

Adjustment processes rely on negative feedback with the purpose of decreasing the deviation of a variable from the steady state of a particular variable and there are different kinds of negative feedback used to keep a system in a stable steady state. Among these one finds (1) internal feedback with a feedback loop that never crosses the boundary of the system and (2) external feedback, which goes outside the boundaries of the system receiving input from other

systems. Some feedback relates to (3) the output and regulates the output at a steady state level (4) Input signal feedback uses the input to regulate the input, for example, if too much information reaches the system the information may be buffered or slowed down. There is also (5) passive adaptation feedback, which reaches a steady state through altering environmental variables (e.g., the system of a heater controlled by a thermostat that cuts off power when the environment has reached a certain temperature.

Loose feedback is a feedback that permits errors or marked deviations from the steady state before corrections are initiated. For example, delaying feedback in time creates such a feedback if a deviation develops quickly. The opposite is tight feedback with a feedback loop that is quick and immediately corrects a deviation. People have problems with delayed feedback when controlling dynamic systems in an intuitive mode.

Power represents one system's ability to control another system at the same or at another level. Power and control is initiated, carried out and terminated through a sequence of information exchange. A system transmits a message or command signal to another system and there are a number of specific characteristics of such messages. The message has an address (receiver), a signature, contains evidence that the transmitter is legitimate, expects compliance and the message specifies an action the receiver is expected to carry out. The relationships between a regulatory body and a regulated industry illustrates such a relationship, but almost all communication within an organization can be seen in a perspective of formally defined and informal power.

As mentioned above the purpose of a nuclear power plant system is to remain in a preferred steady state that is partly defined by external rewards and punishments and partly by internal factors. One goal of a nuclear power plant system is to produce electricity as cheaply as possible during specified time intervals. Another goal is to operate the plant under complete safety without any risks to people, the environment or the plant itself.

"A system is adjusted to its suprasystem only if it has an internal purpose or external goal which is consistent with the norm established by the suprasystem " (Miller, 1978, p.40) and therefore it is interesting to know to what extent the subsystems making up a nuclear power plant or any industry comply with the suprasystem and how. All adjustment processes have their costs. The costs can be in terms of sending information, energy, material, money, time etc and scarcity may affect how close to the goals the system can operate. Optimal resource allocation processes are essential in all system management including safety management., Living systems have adapted resource allocation admiringly well in their normal natural environments. However, when the environment changes drastically and the systems are not prepared for this, the systems may become exposed to serious threats and have trouble with, for example, information overload, system resource scarcities and improper output. This perspective may apply to the individual operator or group of operators as subsystems in safety management of an industry.

Adaptation and feedback are essential in any system. Adequate management in the system and its subsystems implies that adaptation and feedback functions are kept so that the plant remains in a steady state during its life time, even under conditions of threat and stress.

2. Safety Management

On the suprasystem level, management is a process in which a producer, societal representatives and the public interact in finding a balance between the benefits, costs and risks of an activity or a product (Svenson, 1984). The activities can be those of a nuclear power plant or of a car manufacturer producing a car. Safety management is part of management devoted to management of potential risks to people and the environment. It includes determining maximum levels of risks for those exposed to a risk and to keeping exposures within these limits.

The case studies that will be presented below illustrate some important aspects of safety management and they concern a car manufacturer and a road tunnel system. Following this, we shall present some important perspectives from an organizational point of view.

Management is a multifaceted process and therefore it is impossible to cover all aspects of safety management. Therefore, the case studies below will give the reader a summary focused on (1) strategic safety philosophy, (2) internal and external feed back processes, (3) adaptative changes in interactions with the environment and (4) interaction with regulators of the risks.

3. Case Study: Volvo Car Corporation

3.1 The system

The present case study is based on Volvo Car Corporation as it was in 1980 (Svenson, 1984). Since then, two decades have passed and the owners of the company have changed. Volvo Car Corporation is now controlled by Ford in USA. To the present author's knowledge, there is no recent review of the changes, for example, in safety policy as a result of this change of ownership. Although, the case study is old it is presented here because it represents a very successful example of industrial safety management of the industry's product – the car. In addition, a lot of other activities were going on in the company, led by the general manager Per Gyllenhammar, including safety management to protect those working in the industry. But that is another case study, except for the effects of these activities in terms of reinforcing the trust in and proud of the company including the safety of its cars. The planning horizon for the company was 5 to 7 years or more into the future. The company had dominating owners with a long time perspective who did not consider short-term profit the major success indicator.

Within the Volvo organization, no specific body was devoted exclusively to hazard management. The coordinating unit for safety and environment (of about 15 people), the Safety and Environment Unit formally belonged to the Department of Quality but acted quite independently. The Crash-worthiness and crash-avoidance investigations were performed in the Volvo Safety Center belonging to the Department of Product Development and Design. Below, we will present other means, agents and processes used to provide safety feedback to the company.

3.2 Strategic safety policy

In 1980, the Volvo Car Corporation produced some 300 000 cars in different countries. The company had safety as its explicit top management policy during almost all the time up to 1980 (for a short period, high reliability of the cars was the top priority goal). The company was sufficiently profitable for the owners through the years with a small loss only during one year.

Volvo applied a systems approach to safety management: “Today we consider normally three causative elements, in the road safety system, the driver, the vehicle and the road itself with its environment such as signs and signals, More generally, we speak of a man-milieu system and can treat each element’s involvement in transportation in a rational way” Larsen, 1975, p 42-43).

The general safety strategy was implemented early in the company’s history. The general manger (Engellau), had a wife who worked actively as an occupational therapist and could learn about traffic accident victims, a fact which could reinforce a policy of safety.

In terms of work force, there was a certain “Volvo spirit” among those working in the company being proud of the quality and the safety of its products.

The company’s safety strategy was not a general unspecific mantra. Instead, it was interpreted in concrete goal states to increase safety (seat belts, split brake systems, windshield wiping/washing etc). As a concrete goal for the company a safety vehicle was created to show what an example of an ideally safe car would be. This made the safety goals of the company very concrete. Of course, this vehicle was much too costly to put into mass production but it was designed with safety and other technical features that in the future perhaps could be included in the regular cars. In this way a distant goal was erected towards which the company could strive.

The company also had a policy to adapt the production process so that those who worked in the company would not be worn out by their work and suffer from physical or mental fatigue. This aspect of the company as caring for their line workers will not be commented further here as it is the risks of the car that are in focus. However, the attitude towards and treatment of the workers is an indication of company policy and culture possibly affecting safety and quality. Therefore, these issues should not be left out in more full-blown analyses of safety management.

The safety strategy goal of Volvo was not driven by external regulation but self imposed. It was not synonymous with the goal of quality and seen as partly competing with the high quality goal. The safety of Volvo cars was used in advertising and in creating a brand image of Volvo.

3.3 Internal feedback including subcontractors

The Volvo cars were followed from the design stage to scrapping some 15 to 20 years later and the internal system variable feedbacks were secured through the planning and production phases.

The work with a new car model moved into more intensive planning about 5 years ahead of the start of mass production of that car model. During this process, safety functional property specifications preceded the first technical description. The functional safety was then assessed based on the technical blueprint descriptions of the car. Following this, a test car was produced and tested in terms of safety (e.g., crashworthiness and crash-avoidance). Changes were made when these planning stages were recycled. After this, a final prototype was constructed and after this on-line production was started.

Changing limits of system: Outsourcing and insourcing - At the time outsourcing was not a goal in itself as it would be during the late nineties in Sweden**.**

Feedback to subcontractors about their products - A number of subcontractors delivered the parts of a car that was mounted in Göteborg and elsewhere. To decrease vulnerability to delivery disturbances, more than one subcontractor produced a component or a system.

The Volvo Company itself had the full personal expertise within the company and all necessary knowledge about the components and subsystems that they ordered from subcontractors. Safety related components and systems were marked with a special symbol and were subject to very strict quality tests before they were allowed to proceed to the mounting stage. Manufacturers who produced a component or system also had to document all critical steps in manufacturing the items they delivered (e.g., inspection planning, production planning and material handling).

The quality and safety of subcontractor products was assessed in a detailed quality assurance process based on statistical sampling techniques and decision criteria and particularly strict criteria for safety related components. Safety related components were not inspected through statistical sampling and were marked with a special symbol. The quality control routines for non-safety related items had more statistical power (the probability of detection a deviation with statistical significance if there is a deviation), than the Swedish tests for testing seat belts at the time (Svenson, 1984). The criteria for the subcontractors were set so that they would benefit from having a significantly higher average quality rather than just approaching the quality pass limit, because a single quality deviation of one unit would reject all planned or delivered units of the component or subsystem rejected.

3.4 External feedback

The quality assurance program was effective during the initial production phase and as long as a car model was in production. Then the manufacturing process was kept constant and there were almost no changes. All changes were made at preplanned times, usually once a year, to avoid the introduction of unwanted side effects and errors. The only exception to this was in case of a recall (when the manufacturer takes responsibility for repairing a manufacturing weakness or error).

Volvo Designed External Safety Feedback - After the car had entered the market, Volvo designed a number of output system feedback loops.

(1) One of these was *complete follow up of cars in use*. Some kinds of cars, e.g., all police cars, were followed through special service contracts and all the data fed back to the company.

(2) The company also had (and has) its own *insurance company for* Volvo cars only, through which essential information about the cars in use is collected and integrated.
(3) Furthermore, Volvo analyzed all accidents in Sweden of a particular kind, namely, *all fatal accidents* with a Volvo car involved.
(4) *On the spot accident investigations* were performed in the Göteborg region by a team on call and the results reported back to the company.
(5) The company also controlled, followed up and kept record of the *spare part market* for original Volvo parts.

Non-Volvo Designed External Safety Feedback – There were a number of external safety feedbacks providing information to the car manufacturer. We start with information related to commercial success and continue with safety related feedback.

(1) *Number of cars sold* is an important measure for a car manufacturer.
(2) The *profit* made is another important economic variable, enabling allocation of resources for safety (which in turn affects safety of later models and the sale of these).
(3) *Motor journalism* and in particular in Sweden and the US with their important markets.
(4) *Product liability claims* derive predominantly form markets with an emphasis on legal solutions as in Britain and the USA.
(5) *Recalls* of cars with failures for repair. The recall can be detected by Volvo or anybody else and can be legally demanded or not. There had not been any legally demanded recalls of Volvo cars.
(6) *Annual vehicle inspections* are carried out in many countries. The Swedish statistics was detailed and important at the time in providing external feedback to the company including the safety of the Volvo cars.

3.5 Adaptation through changing environment

The system environment of the Volvo Company that is of importance for safety management consists of society, owners, financial markets, customers, road systems, drivers etc.

As mentioned above, the owners allowed Volvo to prioritize a long-term advanced safety policy needing financial and other resources. Volvo was active in suggesting transportation system policies and solutions in addition to taking an active role in discussing, exploring and predicting societal conditions on many levels (e.g., a specific and highly competent group of advisers to the group of leaders of the company). The company played an important economic and political role in the Swedish society, later extended to the European scene. Presently, the Volvo car company belongs to Ford, but Volvo trucks, motors etc remain in the old Volvo company.

3.6 Interaction with regulatory bodies

Volvo had a goal that the company should present a safety feature before it was regulated in Swedish law. This had the effect that Volvo improved the safety of their own cars thereby showing that an improvement was feasible also for others, which in turn was a support for legislators wanting to improve safety.

Thus, in order to increase or keep a certain safety level of the cars produced by Volvo, legislation often followed after the introduction of the company's own safety measures. In

addition, the contacts between the authorities and Volvo could make it possible to recommend postponing of a specific for law some time with reference to production or other problems.

The regulatory strategies (Durbin & Melber, 2000) applied by the regulators could be described as partly descriptive and partly based on self-assessments.

3.7 Concluding remarks

The Volvo Car Company is an example of a company with quite advanced safety management routines to secure safety of the cars. Great flexibility when designing a car was coupled with strict rigidity when assembling the car. These activities were both in-company processes. The staff of the company was highly competent in dealing with subcontractors. The staff designed control systems that were cost effective and very strict on safety. Not only the internal feed back loops, but a majority of the external feedback loops were also created by the company itself. Most of these external feedback loops were not imposed by societal regulations.

To summarize, among the factors who made The Volvo Car Company a successful safety manager one finds the following: (1) Explicit, concrete and implemented safety goals, (2) Volvo constructed their own technology with adequate documentation, (3) The technology was modern, adaptive and interesting for those working with it, (4) Volvo itself designed feedback loops to systematically secure information about system parameters, (5) Sufficient expert competence was available when placing orders among subcontractors, (6) Staff was sufficiently numerous so that most staff could work without serious stress, (7) Perceived and real risks of the product, the car, are high and prominent in comparison to many other risks (8) Owners prioritized long time perspective, stability and gains and allowed safety to be a significant goal of the company.

4. Case Study: The Muskö Tunnel

There are great differences between a road tunnel system and an auto manufacturer. The road tunnel produces a traffic flow while the auto manufacturer produces cars, the tunnel is an old existing hard to revise technical system while the cars manufactured are subject to greater changes etc. And yet, the risks concern the same negative consequences associated with traffic accidents.

4.1 The system

The island of Muskö in the archipelago south of Stockholm is connected to the mainland through a tunnel, which is 3 km long and goes down deep to reach a low point of about 70 m below see level. It is a narrow two-way road tunnel open for traffic including regular busses. The traffic is rather limited during most of the year and increases during the summer because there are a number of summerhouses on the island. The tunnel is dangerous for a number of reasons among which risks of collisions, fire and flooding are prominent. The Swedish National Road Administration Office in the Stockholm region manages it. The Administration Office is located some 50 km from the tunnel. Another branch of the National Road Administration separate from the Road Office was responsible for maintenance and repair at

the time (this branch was exposed to economic competition from companies with less experience with the tunnel).

In addition, about 10 different organizations carried out the activities needed to run the tunnel. Only one person in the Road Office had a reasonably complete overview of the tunnel system. Unfortunately, he was ill at the time of investigation (Svenson, Sjöström &Thyni, 2003) and worked only part time after having become overworked and ordered partial sickness leave. There is a central control room in the Office and the control room personnel had limited knowledge about the tunnel even though there was a technical connection from the tunnel via a printer to the control room.

4.2 Strategic safety policy

There seemed to be no overall safety strategy for the tunnel except those of all roads in Sweden (the roads should carry traffic efficiently, be safe and be distributed all over Sweden). A specific general safety goal is expressed in "the zero vision", which means that there should always be the goal of reducing the total number of fatalities on the roads (the ultimate goal is zero deaths).

4.3 Internal feedback

As mentioned above, on the strategic and tactical levels, there was only one person in the Road Office responsible for the information from the tunnel and its outsourced management organizations. This was a very weak link. The every day operational feedback from the tunnel was designed to arrive electronically to the Office, but the information about this feedback link (a printer) was not well known by the personal working in a central information and control room in the Road Office building. There were weak links to directly control the tunnel (e.g., closing the tunnel in case of a fire alarm).

Adaptation through changing input- There are several restrictions on the traffic through the tunnel. For example, when explosives to the navy base on the island are transported through the tunnel, other traffic is not allowed to use the tunnel. A computer system has been installed to keep track of the number of cars in the tunnel at the same time, but it did not work as expected when the investigation of the tunnel system was made (Svenson, Sjöström & Thyni , 2003). The tunnel had an automatic system giving a red “do not enter” signal if there was too much traffic in the tunnel linked to this system, but that system was not working at the time of the investigation. There is also a speed limit of 50 km per hour. Unfortunately, the drivers violate the speed limit and the average speed is much above the permitted speed (the mean speed is 67 km/h).

Adaptation through changing system- There have been several changes of the tunnel through new and revised systems. To exemplify, the heavy leakage of water into the tunnel (it was earlier flooded so that it was impossible to drive through it in the past) has been reduced through different attempts to seal the walls. Signs to show the way to the nearest exit (there are no emergency exits) were mounted on the tunnel wall high above the road surface and flat to the wall. In case of a fire, the smoke would hide the signs, and if there were no fire their mounting would need special attention. In the winter the leaking water freezes and therefore a heating system was added to the system.

Adaptation through changing environment - One alternative way of handling the traffic is to build a bridge, but this has been considered too costly. Warnings have been mounted on the way to the tunnel, but it is not so easy to change the environments of the tunnel in other ways to increase safety. However, designing the road before entering the tunnel so that traffic would have to come to an almost complete stop is quite possible.

4.4 Changing limits of system: Outsourcing and subcontractors

The tunnel project is an example of almost complete outsourcing and subcontractor support. The branch of the Swedish Road administration responsible for road maintenance in the tunnel was outsourced and worked as a subcontractor on a competitive market. Some of the organizations (e.g., the firm responsible for the electricity of the system including heating to avoid ice) have long experience of the tunnel but were at the time exposed to competition from other companies without this knowledge. Decisions based on subcontractor bids only would have been very negative to the safety of the system. On the other hand, tacit knowledge about safety relevant features is hard to evaluate in economic terms.

4.5 Subcontractors and Tunnel System

Figure 1 show the different subcontractors on top of the figure. The bottom shows different subsystems in the tunnel and the different kinds of traffic and travellers through the tunnel. The original paper provides detail about the different subsystems and their interactions (Svenson, Sjöström & Thyni, 2003).

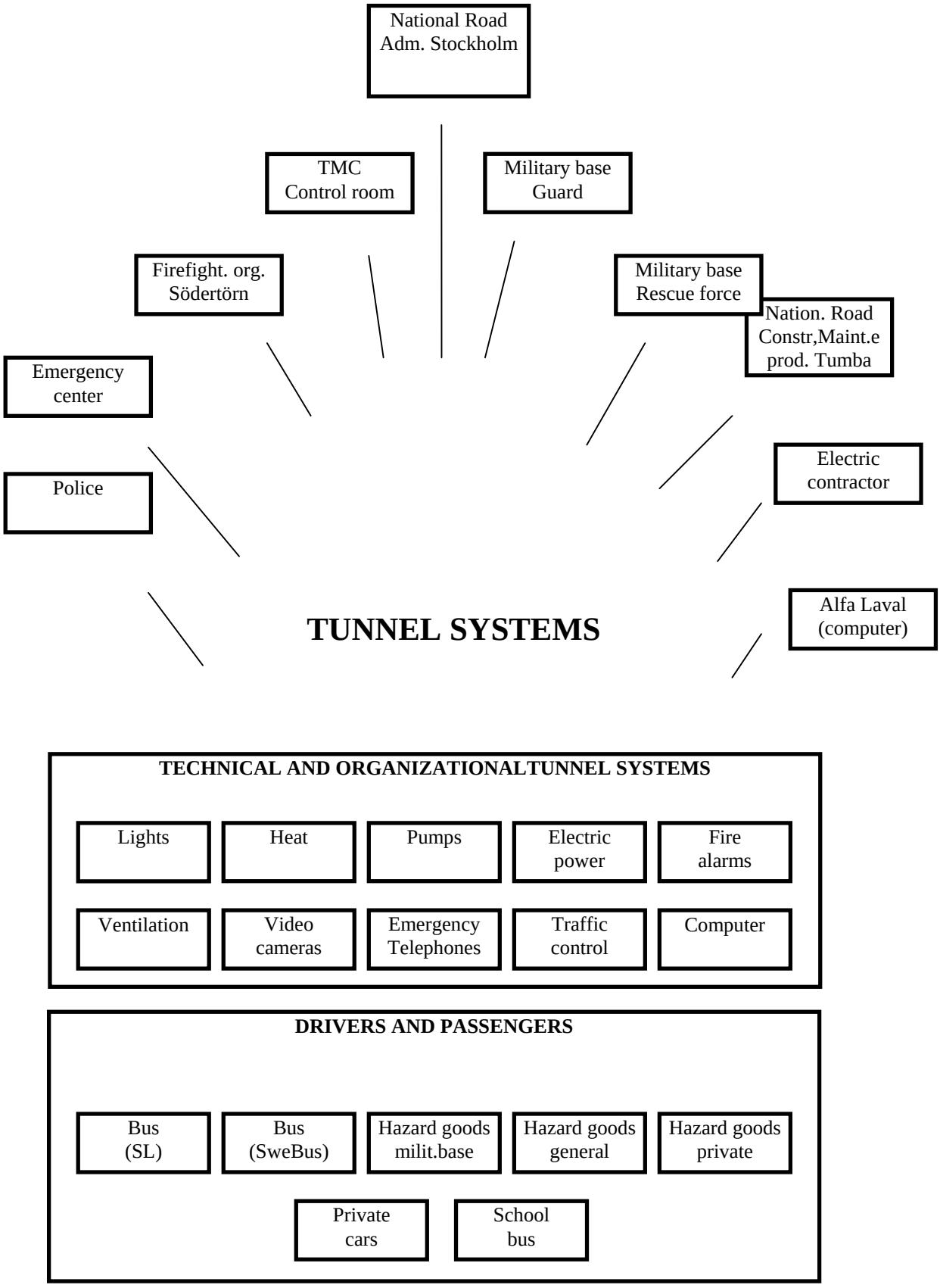

Figure 1 Organizations active in management of the Muskö road tunnel, the subsystems of the tunnel and elements of transportation.

4.6 Feedback to Subcontractors

There were no formalized feedback routines ensuring that the office received information about how the subcontractors managed the tunnel. There were no formalized routines for feedback about the quality of the subcontractor work to the Office. There was a responsible person (unfortunately sick without an equally competent replacement) at the Office who was informed continually about what was going on in the tunnel. Much of the responsibility for the tunnel safety seemed to have been taken over by the electricity subcontractor and the local branch of the office, both responsible for implementing maintenance and repair of the tunnel system.

4.7 External Feedback

Road Office Designed Safety Feedback - As mentioned above, information about how well the system worked was not continually fed back to the organization in a formal way indicating a loose feedback. There were informal and formal contacts to the office from subcontractors and organizations active in management of the tunnel. A few people at the Road Office took part in the interaction

Non-Road Office Designed Safety Feedback - Accidents and information about disturbances in the traffic are examples of non-system controlled feedbacks. The Road Office normally analyses all fatal accidents and keeps record of all police reported accidents. This provides important information about the safety of a road segment including the tunnel. In comparison to many roads, the risk of an accident per year is rather small in the Muskö tunnel depending on limited traffic. However, the potential consequences of an accident involving a bus and/or fire in the tunnel are catastrophic.

The local fire fighting organization responsible for evacuation and fire fighting in case of an accident in the tunnel, “blew the whistle” telling the Road Office that they would not risk their fire fighters’ lives in the tunnel in case of a fire, that a risk analysis had to be performed and that the safety of the tunnel system had to be improved. Therefore, a risk analysis of the tunnel was performed by Svenson, Sjöström and Thyni (2003).

4.8 Concluding remarks

At the time the Muskötunnel was a striking example of a poorly managed system in comparison with Volvo Car. Some of the reasons for this was (1) no specific safety goals for the tunnel, (2) the technology (tunnel) was given to the Road Office and was not ordered or constructed by the Office, (3) the technology was old fashioned, unsafe and did not live up to modern safety standards, (4) the Office had unreliable feedback about system parameters, (5) the Office had competence for ordering from subcontractors, but (6) the number of staff was quite insufficient for controlling too many subcontractors and this put stress on the personal so that they became sick, (7) the expected number of negative consequences (e.g., deaths) was small compared with the overall negative consequences of road traffic in Sweden reported to the Office and made the tunnel a low safety priority system, (8) the organizational goal of outsourcing maintenance and production and Office resource allocations left the responsibility with a few people at the remaining subcontractors who had formal and informal knowledge about the tunnel because they had worked with it during several years. Such informal

knowledge is of great value form a safety perspective, but it is likely to be ignored or difficult to defend in economic bids by new subcontractors who wish to enter the market.

5. An Organizational Perspective on Safety Management

In the following, we shall return to a theoretical perspective and select the organization as focus of our account. The present study should apply to Nordic conditions and management in Sweden and the Nordic societies. It should be noted that there is an abundance of material in the organizational and safety culture literature referring to organizations in USA and in the UK. However, many of the findings of those studies are not directly relevant in a Swedish context.

One main difference between Sweden and USA/UK concerns the laws protecting the employee against unfair treatment by the employer. To exemplify, in the USA an employer can fire an employee in a manner that would be impossible in Sweden of 2002. In Sweden, the employer would have to present good reasons to let off an employee and most of the time a union is involved protecting the employed and checking out that the laws are followed. Less hierarchical organizations with more power at the lower echelons can facilitate negative feedback in the form of, e.g., “whistle blowers”.

5.1 A Swedish perspective: Safety Management with Relevance for the Nuclear Power Industry

Modelling the concept of safety management - Safety is of great importance to risk technologies. Previous Swedish studies concerning safety have often had their focus on quite specific activities or areas (e.g., operators, maintenance personnel, organizations). A study of safety on a more *general* level (e.g., the interaction between different organizations and their relevance for safety at large) may fall short because of its relatively greater complexity, which in turn makes it difficult to use the results directly for concrete safety improvements without further considerations. If safety thinking is something that should be integrated in every managerial activity it may result in an established policy of safety management that will have repercussions on other managerial activities.

In a bottom-up perspective, the efficacy with respect to safety of the prevailing management policy could be traced back from the consequences of specific activities up to the management of those activities. In a top-down perspective, the effects of an adopted safety policy can be followed through several stages, for example: objectives, planning, orders, implementations, benchmarking, feedback etc. Thus, the study of safety management may be a way of moving safety research to a more general level.

Studies of safety management in the Swedish nuclear power safety area are quite few to the best of the present authors' knowledge. The U.S. Department of Energy (DoE) recently paid attention to so called *Integrated Safety Management* (ISM) and implemented it in most of its offices (DoE, 2000). DoE’s policy for *safety management* (DoE, 1996) follows 7 so called *guiding principles* and 5 so called *Core Functions* (how the actions shall be carried out). According to this approach safety management should be integrated in the activities as a whole (see Table 1 for details).

But what is in fact safety management? In nuclear operations we are quite familiar with the concept of safety. Even if the definitions of the safety concept differ between contexts, there is an assumption of a mutual understanding between the regulator and licensee that safety is a most important issue. All nuclear power activities are assumed to be carried out using safe operations. Management, on the other hand, is a less welldefined concept (perhaps not if we ask the managers). On one hand, management has to do with all operations carried out in a plant. In this sense the concept has to do with “how to handle” or “how to cope” with different situations and demands. This definition applies to all personnel at the plant, and the technical measures applied.

A more traditional view is that the managers or the managerial staff carries out management. From this point of view some argue that management is made up by two components: (I) organizational skill, and (II) entrepreneurial sense. The first component includes principles and techniques of management such as the ability to delegate. The second component includes principles such as recognizing and making use of opportunities, predicting market needs and trends, achieving one's goals by sustained drive, skilful negotiation, and articulate advocacy (Dictionary of business, 1996). In the safety management context, some of the terms above, such as “market”, can be changed to or complemented with “safety”. Management is often (traditionally) described on different levels of management (see Figure 2).

Table 1 DOE principles for safety management.

7 Guiding Principles

1. *Line Management Responsibility for Safety*
Line management is directly responsible for the protection of the public, the workers, and the environment. As a complement to line management, the Department's Office of Environment, Safety and Health provides safety policy, enforcement, and independent oversight functions.

2. *Clear Roles and Responsibilities*
Clear and unambiguous lines of authority and responsibility for ensuring safety shall be established and maintained at all organized levels within the Department and its contractors.

3. *Competence Commensurate with Responsibilities*
Personnel shall possess the experience, knowledge, skills, and abilities that are necessary to discharge their responsibilities.

4. *Balanced Priorities*
Resources shall be effectively allocated to address safety, programmatic, and operational considerations. Protecting the public, the workers, and the environment shall be a priority whenever activities are planned and performed.

5. *Identification of Safety Standards and Requirements*
Before work is performed, the associated hazards shall be evaluated and an agreed-upon set of safety standards and requirements shall be established which, if properly implemented, will provide adequate assurance that the public, the workers, and the environment are protected from adverse consequences.

6. *Hazard Controls Tailored to Work Being Performed*
Administrative and engineering controls to prevent and mitigate hazards shall be tailored to the work being performed and associated hazards.

7. *Operations Authorization*
The conditions and requirements to be satisfied for operations to be initiated and conducted shall be clearly established and agreed-upon.

5 Core Functions

1. *Define the Scope of Work*
Missions are translated into work, expectations are set, tasks are identified and prioritized, and resources are allocated.

2. *Analyze the Hazards*
Hazards are associated with the work identified, analyzed, and categorized.

3. *Develop and Implement Hazard Controls*
Applicable standards and requirements are identified and agreed-upon, controls to prevent/mitigate hazards are identified, the safety envelope is established, and controls are implemented.

4. *Perform Work Within Controls*
Readiness is confirmed and work is performed safely.

5. *Provide Feedback and Continuous Improvement*
Feedback information on the adequacy of controls is gathered, opportunities for improving the definition and planning of work are identified and implemented, line and independent oversight is conducted, and, if necessary, regulatory enforcement actions occur.

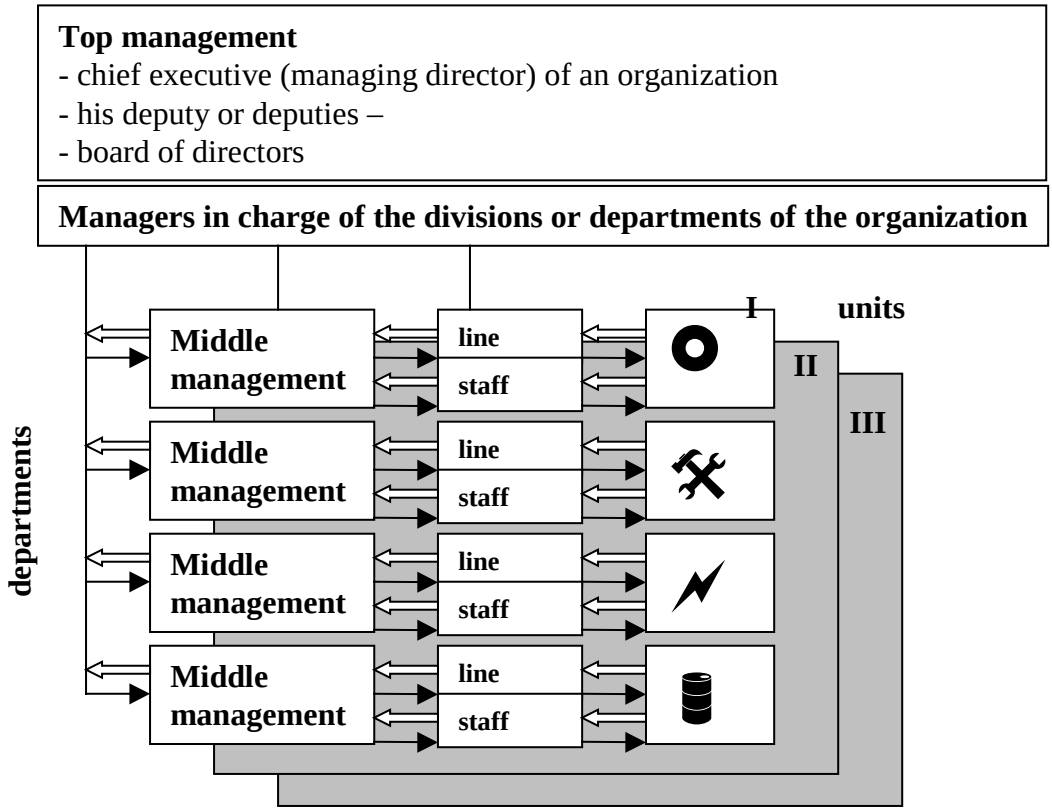

Figure 2. The figure shows a schematic example of how management can de described on different levels (top-, middle-, line/staff-management). The black arrows symbolize how information such as decisions, orders, or policies, are communicated, manifested, and delegated downward from higher to lower levels of management. The black arrows symbolize the feedback flow backward to higher levels

One could argue that such views as the above might indicate different managerial foundations within an organization, one related to technological/engineering management and one related to economic management. On the other hand, one could also argue that it is an absolute necessity to have shared or common views on the management of safety, whatever economical or technical.

Safety management can be modeled in different domains in the organization - A concept is partly defined in relation to the context where it is applied. In this section we are attempting to model safety management in relation to traditional concepts of organization, including a selection of other related concepts such as *organizational learning, organizational and safety culture, organizational and environmental change, and management control systems.*

The conditions for safety management are not static - Demands on safety can rise rapidly from various causes, not only following incidents. Structural changes in an organization, changes in safety rules and policies, changing demands from society are such examples. The flexibility of the organization is important here.

Some authors argue that one prerequisite for successful safety management is the organizations ability to adapt to a changing environment. Organizations that are unable to re-engineer or adapt themselves to shifting demands and situations will failure (Kloot, 1997, see review in Salo & Svenson, 2002, pp. 28-37). There is often an intrinsic resistance to change the operating paradigm in organizations (Levinthal, 1991; Miller, 1993; Hames, 1994, reviewed in Kloot, 1997; Salo & Svenson, 2002). Organizations should be designed to ensure that the organization adapts to changes in its environment (Lowe, 1971, reviewed in Kloot, 1997; Salo & Svenson, 2002).

One important key to organizational change is the organization's ability to learn. According to Argyris (e.g., 1999) and Senge (1990) ***organizational learning*** is often recognized as an organizationaladjustment to environmental change. Organizational learning is viewed as a process whereby members of the organization respond to changes in the internal and external environments of the organization by detecting errors that they then correct so as to maintain the central features of the organization. Change follows error detection and a questioning of underlying policies and goals as in "generative-" or so called "double loop-learning" (Argyris, 1977; Kloot, 1997; Salo & Svenson, 2002). Psychological processes are important here. Organizational learning is then a fundamental shift or movement of mind, enabling the environment to be perceived differently and to see the organization actions as creating problems and solutions (Senge, 1990 reviewed in Kloot, 1997; Salo & Svenson, 2002). One way of modelling safety management is to put it in relation to what extent it will facilitate learning about safety in organizations.

In nuclear power plants, safety management could for example actively encourage not only individual workers and organizations to engage in activities to promote learning, but also incorporate a self-criticism that incorporates mechanisms of learning in the management itself. Various technical and organizational innovations can also be utilized to achieve this purpose, as for example, improved feedback systems for reporting incidents.

Management control systems for safety - But which are the means to achieve successful safety management? One answer to this is high quality management control systems. As with several safety related concepts, management control systems are viewed differently, either as a concept covering a control function beside other functions, or as a concept that must be treated in a holistic manner. For example, in Anthony's (1965, reviewed in Kloot, 1997; Salo & Svenson, 2002) hierarchy of planning and control, strategic planning, management control, and operational control are viewed as separate entities, all taking place at different levels and at different points of time along the process (see Figure 3).

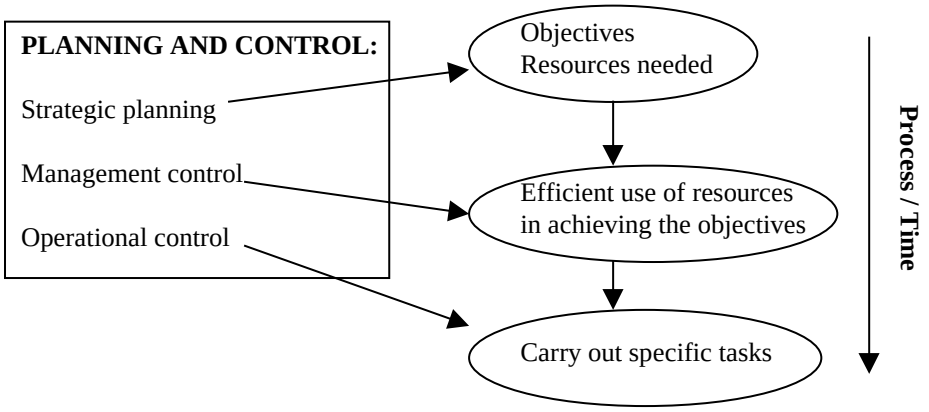

Figure 3. Hierarchy of planning and control according to Anthony (1965).

A more holistic approach was chosen by Lowe (1970, 1971, reviewed in Kloot 1997; Salo & Svenson, 2002) who describes management control as

> *a system of organizational information seeking and gathering, accountability and feedback designed to ensure that the enterprise adapts to changes in its substantive environment and that the work behaviour of its employees is measured by reference to a set of operational subgoals (which conform to overall objectives) so that the discrepancy between the two can be reconciled and corrected for*

Models of the former type may be appropriate for control during stabile conditions, but not during change, while models of the later type seems more suited to an ever changing world.

Different types and amounts of organizational learning may result from different management control systems. Both are concerned with adapting or changing an organization so it fit into its environment (Kloot 1997; Salo & Svenson, 2002).

Some authors (e.g., Argyris, 1990; Dent, 1990; Kloot 1997; Salo & Svenson, 2002) argue that management control systems can both promote or impede the possibilities for generative learning. The clarity and comfort experienced with such systems can fool you to reinforce conservative rationales (they are sometimes designed to do so) that in turn will inhibit change. On the other hand, the control systems can be designed to open up new possibilities and creating new images of the organization and the way it interacts with its environment. Therefore, in the area of nuclear power as in other activities it is essential to know the advantages and possible pitfalls of improvements of old systems and in design of new control systems. When organizations restructure, for example, from a hierarchical (vertical) to a flat (horizontal) organizational structure it is important to reevaluate the control system and take necessary steps to adapt it to the new organization. This may require a development of a completely new control system. Of course, one should take advantage of opportunities, of whatever kind, to design or improve management control systems so they can cope with changes in a positive way and promote generative learning in the organization.

The following management control system characteristics are required for generative or double loop learning (Kloot, 1997; in Salo & Svenson, 2002): (a) appropriate accounting

information; (b) performance measurement systems; (c) true participative decision making: (d) strategic planning; and (e) high quality emphasis.

Finally, the management control system is a mirror of the management ideals of the organization. The features are of such ideals become materialized in various ways in the organization. When a person is new in an organization, it does not take a long time for him or her to identify these features, and when identified they are used as an image for categorization of the organization as one of that type or one of another. The image of the organization is in turn closely related to the climate at work, to efficacy, and perhaps also to safety.

It is clear that individuals or organizations not only learn from themselves but also from each other. It is therefore obvious that knowledge transfer between individuals and organizations is an important issue in learning. In the process of knowledge transfer one unit is affected by the experience of another (Argote & Epple, 1990; Huber, 1991; Lewitt & March, 1988; Argote et al., 2000; Salo & Svenson, 2002).

Organizational and safety culture vs. safety management: who carries whom? - One popular concept used as one indicator of safe operations is *safety culture*. There are several definitions found in the literature, as the two examples below related to the nuclear poere field:

"Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance." (INSAG-4 [3])

or

"Safety culture refers to the characteristics of the work environment, such as the norms, rules, and common understandings, that influence plant personnel's perceptions of the importance that the organization places on safety. It includes the degree to which a critical, questioning attitude exists that is directed toward plant improvement." (Jacobs & Haber, 1994)

But let us go one step beyond this seemingly artefactual façade and take a closer look at the concept of safety culture. According to the safety culture concept it seems as if people in the same culture have both ideas and behavior in common (Kopelman et al., 1990; Druckman et al., 1997; Salo & Svenson, 2002). New management principles and the difference in performance they produce can be said to constitute a change of culture. Culture can be identified at both the hypothetical construct level and at observable levels (i.e., Ott, 1989; Rosseau, 1990; Hunt, 1991, reviewed in Druckman et al., 1997, ch. 3; Salo & Svenson, 2002, p. 6). Schein (1992), illustrates culture as existing at three different awareness levels with subsequently lowered levels of appearance: (1) *artifacts*, that are visual organizational structures and processes; (2) *espoused values*, that are strategies, goals and philosophies expressed by managers and other members of the organizational culture; and (3) *basic underlying assumptions*, the unconscious and taken-for-granted beliefs, perceptions, thoughts, and feelings. The basic underlying assumptions can be considered as primary origins for values and action.

In one sense it may be possible to view safety management as a "carrier of safety culture". For example, if management identifies the prevailing culture as related to safe operations and

actively supports the development of a safety culture. But the opposite relation, that safety management is viewed as one of many possible aspects of the safety culture, may also be true.

In one attempt to answer the question “can culture be viewed as the manager or the managed”, it can, from one perspective, be claimed that culture manages the cultural uncertainties and create order in the social world. This includes shared identity and commitment among the members of the organization over time. Culture creates continuity (Trice and Beyer, 1993, reviewed in Druckman et al., 1997, ch. 3; Salo & Svenson, 2002, p. 6). But also more negative aspects, such as ethnocentrism and polarization (we-them) can be fostered by the culture (Druckman, 1994; Druckman et al., 1997; Salo & Svenson).

From another perspective, culture can also be considered as created during a complex process of learning among groups of people (e.g., Schein, 1992). There are two major problems for learning. First, survival, growth and adaptation in the environment, and second, internal integration that allow groups to adapt and function. Culture is formed along with peoples strive for stability, consistency, and meaning. Learning can occur on both a behavioral and a more abstract-level.

Salo and Svenson (2002) presented a selective review of organizational culture and safety culture. There, were no claims were made concerning which view of the concepts that is the most appropriate. As with concepts in general their meanings are constructed and reconstructed in different contexts and times.

Epilogue on organizational and system concepts - For safety reasons, is important to model safety management from a systems point of view. From a nuclear safety perspective, safe operations are usually described according to the technological system structures and/or system components existing in the particular industry where the safe operations in question shall be carried out. This approach is fundamental for several reasons. For example, in ideal systems a systems perspective allows identification of deviations from a steady state related to known safety standards of different subsystems and/or components of the systems, through feedback channels, giving opportunity to a prerequisite of countermeasures to correct the deviation. From this perspective it is also possible to trace and identify consequences to various alerts, both individual human, organizational and/or technological. By applying a system approach we can link different measurable units of consequences to actions.

At this time we have not fully integrated the traditional organizational concepts into a full-blown systems perspective. But, there is a striking similarity between traditional organizational concepts and system theoretical concepts that is not incidental. For example, an organization can be described as a living suprasystem. It sometimes includes different subsystems, both living and/or non living (individuals, departments, units, technology, etc). The organization as a system, as we have seen above, is not a stable entity. It is affected by various forces that move the organization-system away from a steady state (change). So, it has to be controlled by various means in order to maintain a defined stable state or to adapt to changing demands (management control systems, learning, adaptation, etc).

When we are dealing with safety, and particularly nuclear safety, communications between the different actors (e.g., industry, regulator, subcontractors, etc) are of fundamental importance. The different actors often have quite different secondary purposes (if we agree about safety as the primary purpose) as a foundation for their activities, and we often find

differences between sublevels within an organization. In nuclear activities the frame of reference for safe operations is mainly technical and, hence, traditionally oriented toward a system perspective. If we adopt the system approach we have the opportunity of utilizing the least common denominator, namely concepts for communication known among different actors on different levels concerned with nuclear power plants.

6. Remarks

The case studies in this report were presented in a systems perspective with emphasis on information feedback about the risks of the systems. The first case study illustrated a high level of safety management, while the second case study shows many weaknesses of the safety management process. Some differences in safety management between the case studies were noted. The organizational perspective on management in the last section focused on a central area of safety management. To conclude, further studies are needed both (1) to further develop a frame of reference for describing safety management across industries and activities including organizational aspects and (2) to collect data from different industries and activities, which can illustrate high quality and perhaps poor safety management and how safety management can be improved. The results from these studies will be of value in the choice of strategies to strengthen and/or improve safety management in the nuclear power industry and its regulators as well as in other industries and activities with their corresponding regulators.

7. References

Argote, L., & Epple, D. (1990). Learning curves in manufacturing. Science, February 23, 247, 920-924.

Argote, L., Ingram, P., Levine, M. L., & Moreland, R. L. (2000). Knowledge transfer in organizations: learning from the experience from others. Organizational Behavior and Human Decision Processes, vol 82, no 1, 1-8.

Argyris, C. (1977). Double loop learning in organizations. Harward Business Review, Sept-Oct, 59-72.

Argyris, C. (1999). On organizational learning, 2nd ed. Blackwell Publishers Inc, Malden, MA, USA.

Bloomsbury Thesaurus (1997), Bloomsbury, England.

Dictionary of business (1996), Oxford: Oxford University Press and Market House Books.

Druckman, D. (1994). Nationalism, patriotism, and group loyalty: A social-psychological perspective. Mershon International Studies Review, 38, 43-68.

Druckman, D., Singer, J. E., & Van Cott, H. (1997). Enhancing organizational performance. Washington, D.C.: National Academy Press.

Durbin, N, & Melber, B. (2002) Alternative regulatory strategies: Commercial nuclear power discussions of issues and comments. Unpublished (Stockholm: SKI 14.13 Dnr 011133 January 28, 2002).

Hames, R. D. (1994). The management myth. Sydney: Business and Professional Publishing.

Huber, G. P. (1991). Organizational learning: the contributing processes and the literatures. Organization Science, 2, 88-115.

Internationa Nuclear Safety Advisory Goup, (1988). Basic Safety Principles for Nuclear Power Plants, Safety Series No. 75-INSAG-3, IAEA, Vienna (1988).

Internationa Nuclear Safety Advisory Goup, (1991). Safety Culture, Safety Series No. 75-INSAG-4, IAEA, Vienna (1991).

Jacobs, R., & Haber, S. (1994). Organizational processes and nuclear power plant safety. Reliability Engineering and System Safety, 45, 75-83.

Kloot, L. (1997). Organizational learning and management control systems: responding to environmental change. Management Accounting Research, 8, 47-73.

Kopelman, R. E., Brief, A. P., & Guzzo, R. A. (1990). The role of climate and culture in productivity. In B. Schneider (Ed.), Organizational climate and culture, pp. 282-318. San Francisco: Jossey-Bass.

Larsen, L. S. (1975) Systems technology in support of road safety legislation. Road Safety Symposium, Cape Town, September 8- 10 1975.

Lewinthal, D. A. (1991). Organizational adaption and environmental selection – interrelated processes of change. Organizational Science, 2, 140-145.

Lewitt, B., & March, J. G. (1988). Organizational learning. Annual Review of Sociology, 14, 319-340.

Lowe, E. A. (1971). The idea of a management control system. Journal of Management Studies, Feb, 1-12

Miller, D. (1993).The architecture of simplicity. Academy of Management Review, 8, 116-138.

Salo, I., Svenson, O. (2002). Organizational and safety culture: a selective review.

Senge, P. (1990). The fifth discipline. Sydney: Random House.

Svenson, O. (1984) Managing the risks of the automobile: A study of a Swedish car manufacturer. Managent Science, 30, 486 –502.

Svenson, O., Sjöström, P. & Thyni, G. (2003) Risk management of a human technology system: A dangerous road traffic tunnel. Submitted for publication.

Trice, H. M., & Beyer, J. M. (1993). The cultures of work organizations. Englewood Cliffs, NJ: Prentice-Hall.

U.S. Department of Energy (2000) Integrated Safety Management (ISM) Implementation, Memorandum for the deputy secretary, Washington, DC 20585, October 4 2000.

U.S. Department of Energy (1996) Safety management system policy, POLICY DOE P 450.4, 10-15-96.

Bibliographic Data Sheet **NKS-88**

Title	Safety Management: A Frame of Reference for Studies of Nuclear Power Safety Management and Case Studies from Non-Nuclear Contexts
Author(s)	Ola Svenson[1)] and Ilkka Salo[1,2)]
Affiliation(s)	[1)] Stockholm University, Sweden [2)] Lund University, Sweden
ISBN	87-7893-146-0
Date	September 2003
Project	NKS-R-04
No. of pages	24
No. of tables	1
No. of illustrations	3
No. of references	28
Abstract	A systems perspective on safety management is introduced followed by two briefly presented case studies of safety management. The first study concerns a car manufacturer and the second study a road traffic tunnel system. The risks of a car accident in the first case study are evident. The great exposure generates many incidents and accidents. In the second study, the rather low traffic intensity through the tunnel produces few incidents and accidents and only a few fatal accidents over the years. Yet, the risk of the individual traveller is much greater in the tunnel than on the average road. The case studies are presented in a systems perspective with emphasis on information feedback about the risks of the systems. The first case study illustrates high quality safety management, while the second case study shows many weaknesses of the safety management in the tunnel system. Some differences in safety management between the case studies are noted. The last part of the study presents an organizational perspective on safety management and offers alternative theoretical perspectives on the concept of safety management. The report shows that further studies are needed both (1) to develop a frame of reference for describing safety management across industries and activities and (2) to collect data illustrating of good and poor safety management. Then, the results can be used to strengthen and/or improving safety management in the nuclear power industry and its regulators.
Key words	Safety management, case studies, systems perspective, information feedback

Available on request from the NKS Secretariat, P.O.Box 30, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4045, fax (+45) 4677 4046, e-mail nks@catscience.dk, www.nks.org