Strål
säkerhets
myndigheten
Swedish Radiation Safety Authority

Authors: Erik Hollnagel

Research

2013:09

An Application of the Functional Resonance Analysis Method (FRAM) to Risk Assessment of Organisational Change

Report number: 2013:09 ISSN: 2000-0456
Available at www.stralsakerhetsmyndigheten.se

SSM perspective

Background

An analysis model has the purpose to make a specific phenomenon under investigation understandable. Traditional safety models assume that events can be represented as chains or sequences of causes and effects - either as simple linear progressions or as combinations of paths. Accident investigations and risk assessments therefore typically proceed in a step-by-step fashion and propagating gradually either backwards or forwards from a chosen starting point. Experience shows that events can be due to performance variability rather than malfunctions and that the relationship between events and consequences is non-linear in the sense that the nature or magnitude of the consequences may be disproportionate to and unpredictable from the preceding events. In such cases, the events are better explained by coincidences rather than by causal relations. The Functional Resonance Accident Model (FRAM) describes system failure and adverse events as the result of a functional resonance arising from normal performance variability.

Objectives

The objective of this study was to demonstrate an alternative approach to risk assessment of organisational changes, based on the principles of resilience engineering. The approach in question was the Functional Resonance Analysis Method (FRAM). Whereas established approaches focus on risks coming from failure or malfunctioning of components, alone or in combination, resilience engineering focuses on the common functions and processes that provide the basis for both successes and failures. Resilience engineering more precisely proposes that failures represent the flip side of the adaptations necessary to cope with the real world complexity rather than a failure of normal system functions and that a safety assessment therefore should focus on how functions are carried out rather than on how they may fail.

The objective of this study was not to evaluate the current approach to risk assessment used by the organisation in question. The current approach has nevertheless been used as a frame of reference, but in a non-evaluative manner.

Results

While it is clear that the two approaches are different, the choice of which to use in a given case cannot simply be made from the
The author has demonstrated through the selected case that FRAM can be used as an alternative approach to organizational changes. The report provides the reader with details to consider when making a decision on what analysis approach to use. The choice of which approach to use must reflect priorities and concerns of the organisation and the author makes no statement about which approach is better. It is clear that the choice of an analysis approach is not so simple to make and there are many things to take into account such as the larger working environment, organisational culture, regulatory requirements, etc.

Need for further research

SSM does not see a need for further research at this time.

Project information

Contact person SSM: Lars Axelsson
Reference: SSM 2008/348 and SKI 2008/669/200803006

There are some passages in the text where specific analysed documents have been quoted. The author has chosen not to translate these parts.

Strål
säkerhets
myndigheten
Swedish Radiation Safety Authority

Authors: Erik Hollnagel
MINES ParisTech Crisis and Risk Research Centre (CRC),
Sophia Antipolis Cedex - France

2013:09

An Application of the Functional Resonance Analysis Method (FRAM) to Risk Assessment of Organisational Change

Date: November 2012
Report number: 2013:09 **ISSN:** 2000-0456
Available at www.stralsakerhetsmyndigheten.se

This report concerns a study which has been conducted for the Swedish Radiation Safety Authority, SSM. The conclusions and viewpoints presented in the report are those of the author/authors and do not necessarily coincide with those of the SSM.

SSM 2013:09

Table of Contents

1. Background – The Development of Risk Analysis and Safety Assessment

The realisation that things can go wrong is as old as civilisation itself. Probably the first written evidence is found in the Code of Hammurabi, created circa 1760 BC, which even includes the notion of insurance against risk ('bottomry'). It was nevertheless not until the late 19th Century that industrial risk and safety became a more common concern. Hale & Hovden (1998) argued that there are three distinct ages in the scientific study of safety, which they named the age of technology, the age of human factors, and the age of safety management.

The First Age

In the first age, the main concern was to develop technical measures to guard machinery, to stop explosions, and to prevent structures from collapsing. This period was introduced by the industrial revolution (usually dated to 1769) and lasted throughout the 19th Century until after the Second World War. The focus on technology is underlined by the observation made by Hale (1978), that investigators in the late 19th Century were only interested in having accidents with technical causes reported, since other accidents could not reasonably be prevented.

One of the earliest examples of a discussion of a systematic risk assessment was the *Railroad Safety Appliance Act*, from 1893, which argued for the need to combine safety technology and government policy control. But despite prominent examples of safety concerns, such as Heinrich's book on *Industrial Accident Prevention* from 1931, the need for reliable equipment, hence the need for reliability analysis only became commonly recognised towards the end of the Second World War. There were two main reasons for this. First, that the problems of maintenance, repair, and field failures had become severe for the military equipment used during the Second World War. Second, that new scientific and technological developments made it possible to build larger and more complex technical systems that included more extensive automation. Prime among these developments were digital computers, control theory, information theory, and the inventions of the transistor and the integrated circuit.

In the civilian domain, the fields of communication and transportation were the first to witness rapid growth in complexity as equipment manufacturers adapted advances in electronics and control systems. In the military domain, the development of missile defence systems, as well as the beginning of space programme, relied on equally complex technological systems. This created a need

for methods by which risk and safety issues could be addressed. Fault tree analysis was, for instance, originally developed in 1961 to evaluate the Minuteman Launch Control System for the possibility of an unauthorized missile launch. Other methods such as FMEA and HAZOP were developed not just to analyse possible causes of hazards (and later on, causes of accidents), but also to identify hazards and risks.

By the late 1940s and early 1950s, reliability engineering had become established as a new engineering field. Reliability engineering combined the powerful techniques of probability theory with reliability theory. This combination became known as probabilistic risk assessment (PRA), later also called probabilistic safety assessment (PSA). PRA was successfully applied to the field of nuclear power generation with the WASH-1400 'Reactor Safety Study.' This report was produced by a committee of specialists under Professor Norman Rasmussen in 1975 for the USNRC, and is therefore often referred to as the Rasmussen Report (Atomic Energy Commission, 1975). It considered the course of events which might arise during a serious accident at a large modern Light Water Reactor, using a fault tree/event tree approach. The WASH-1400 study established PRA as the standard approach in the safety-assessment of modern nuclear power plants.

The Second Age

The second age was rather abruptly introduced by the accident at the Three Mile Island (TMI) nuclear power plant on March 28 1979. Before that date, the established methods such as HAZOP, FMEA, Fault Trees, and Event Trees had been considered as sufficient to establish the safety of nuclear installations. After TMI it became clear that something was missing, namely the human factor. The human factor had already been considered in system design and operation through the discipline of human factors engineering, which had started in the U.S. as a speciality of industrial psychology in the mid 1940s. Human factors engineering had, however, focused mainly on the efficiency (productivity) side of system design and had paid little attention to safety issues. That changed completely after 1979.

Since PRA by that time had become established as the industry standard for how to deal with the questions of safety and reliability of technical systems, it was also the natural starting point when the human factor needed to be addressed. The incorporation of human factors concerns in PRA led to the development of human reliability assessment (HRA), which at first was an extension of existing methods to consider 'human errors' in the same way as technical failures and malfunctions, soon to be followed by the development of more specialised approaches. The

details of this development have been described in several places, e.g., Hollnagel (1998) and Kirwan (1994), but the essence was that human reliability became a necessary complement to system reliability – or rather that reliability engineering was extended to cover both the technological and human factors. The use of HRA quickly became established as the standard analysis for NPP safety, although there has never been any fully standardised methods (e.g., Dougherty, 1990) – or even a reasonable agreement among the results produced by different methods (Poucet, 1989).

The Third Age

The third age came about for two reasons. The first was an increasing dissatisfaction with the idea that health and safety could be ensured by a normative approach, simply by matching the individual to the technology (HMI design). The other was that several accidents made clear that the established approaches, including PRA-HRA, had their limits. Although the change was less dramatic than the aftermath of TMI, accidents such as Challenger and Chernobyl, which both happened in 1986, and in retrospect also Tenerife (1977), made it clear that the organisation had to be considered in addition to the human factor (Reason, 1997). One consequence was that safety management systems became a focus of development and research.

The extension of the established basis for thinking about risk and safety, i.e., reliability engineering and PRA, to cover also organisational issues was, however, less straightforward than in the case of human factors. It was initially hoped that the impact of organisational factors on nuclear power plant safety could be determined by accounting for the dependence that these factors introduced among probabilistic safety assessment parameters (Davoudian, Wu & Apostolakis, 1994). It was, however, soon realised that other ways of thinking were required. Pidgeon (1997), pointed out that organisational culture had a significant impact on the possibilities for organisational safety and learning, and that limits to safety might come from political processes as much as from technology and human factors. In a different context, the school of High Reliability Organisations (HRO), made clear that it was necessary to understand the organisational processes needed to operate complex, technological organisations (Roberts, 1990).

At present, the practice of risk assessment and safety management still finds itself in the transition from the second to the third age. On the one hand it is realised by many, but not yet by all, that risk assessment and safety management must consider the organisation as specific organisational factors (Van Schaardenburgh-Verhoeve, Corver & Groeneweg, 2007), as safety culture, as ‘blunt end’ factors, etc. If accidents sometimes can be caused by organisational factors, it follows that any changes to these factors must be the subject of a risk assessment. On the other hand

it is still widely assumed that the established approaches either can be adopted directly or somehow extended to include organisational factors and organisational issues in risk assessment and safety management. In other words, organisational 'accidents' and organisational failures are seen as analogous to technical failures. Since HRA has 'proved' that the human factor could be addressed by a relatively simple extension of existing approaches, it seems reasonable to assume that the same will be the case for organisational factors. This optimism is unfortunately based on hopes rather than facts, hence completely unwarranted. It is becoming increasingly clear that neither human factors nor organisational factors can be adequately addressed by methods that rely on the principles on which technical safety methods are based. There is therefore a need to revise or abandon the easily held assumptions and instead take a fresh look at what risk and safety mean in relation to organisations.

The Challenge: Organisations as a Risk Issue

The starting point for doing so must be the realisation that the organisation, what(ever) it *is* and what(ever) it *does*, is essential for safety as well as for productivity. The organisation should, of course, not be considered as an entity by itself, but be seen together with the physical processes (the technology) and the people who carry out the work (the human factor). This viewpoint has been expressed in various ways, for instance as the MTO-perspective, as the SHEL (Software, Hardware, Environment, Liveware) model, as socio-technical systems theory, as safety culture, etc. From the practical point of view, the new role and the importance of the organisation *qua* organisation points to two significant and interrelated issues.

- The first issue is how the organisation can be *controlled* or managed so that it will produce an intended outcome or set of outcomes. The control problem refers both to how the day-to-day performance of the organisation can be brought about, and to how specific organisational changes should be planned and effectuated.
- The second issue is which *risks* may arise from the organisation and how these risks should be described, analysed, and managed. The risk problem also refers both the day-to-day performance and to the potential consequences (side-effects) of organisational changes.

This study has focused on the risk problem rather than the control problem, although it has been necessary to consider the latter problem as well, as an organisational change necessarily relates to both, cf., Figure 1. An organisational change is in many ways a control issue, i.e., a question of how a specific change can be brought about in an effective manner. Once the change has been made, the

risk issue is whether the consequences will be as intended, i.e., as imagined when the change was planned, or whether the consequences will differ from what was intended and whether that difference will constitute a safety – or productivity – risk. A third issue, that will not be addressed here, is the risk that the implementation of the change will fail.

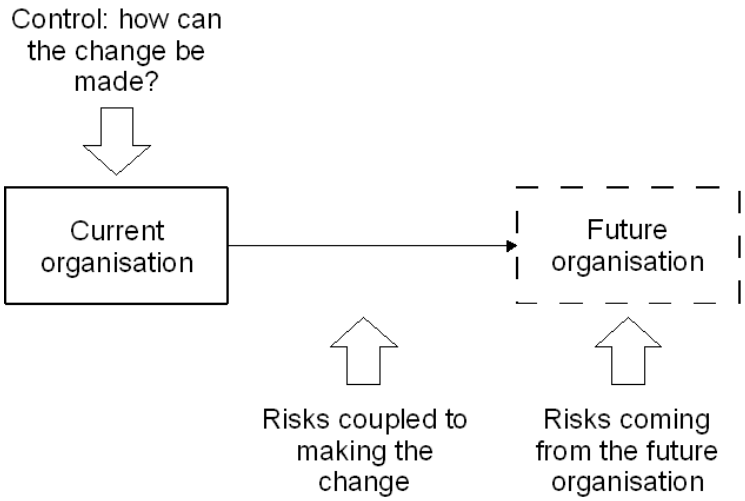

Figure 1: Risks of changing versus risks of change

2. The Socio-Technical System

As described above, the third age of safety brought the socio-technical system into focus. The term itself was used already in the 1960s by researchers from the Tavistock Institute of Human Relations in London. The idea of a socio-technical system is that the conditions for successful organisational performance – and conversely also for unsuccessful performance – are created by the interaction between social and technical factors. (Notice the emphasis on *social*, rather than *human* factors.) This interaction comprises both linear (or trivial) 'cause and effect' relationships and 'non-linear' (or non-trivial) emergent relationships, and has two important consequences.

- The optimisation of system performance cannot be achieved by the optimisation of either aspect, social or technical, alone. Attempts to do so will increase the number of unpredictable or 'un-designed' relationships, some of which may be injurious to the system's performance.
- The safety of socio-technical systems can be neither analysed nor managed only by considering the system components and their failure probabilities. In other words, safety assessment of socio-technical systems and organisations cannot be achieved by extrapolating the principles of reliability engineering and PRA.

2.1. The Concept of Normal Accidents

The special relations between socio-technical systems, risk, and safety were described by the American sociologist Charles Perrow in his book *Normal Accidents* (Perrow, 1984). The fundamental thesis of the book was that the industrialised societies, and in particular the socio-technical environments that provided their foundation, by the beginning of the 1980s had become so complex that accidents were bound to occur. Accidents were thus an inevitable part of using and working with complex systems, hence normal rather than rare occurrences. Perrow wrote about the state of affairs in the beginning of the 1980s, but neither the socio-technical systems, nor the problems they create, have become any simpler since then.

Perrow built his case by going through a massive set of evidence from various types of accidents and disasters. The areas included were Nuclear Power Plants, Petrochemical Plants, Aircraft and Airways, Marine Accidents, Earthbound Systems (such as dams, quakes, mines, and lakes), and finally Exotic Systems (such as space, weapons and DNA). The list was quite formidable, even in the absence of major accidents that occurred soon after, such as Challenger, Chernobyl, and Zebrügge.

Perrow proposed two dimensions to characterise different types of accidents: *interactions* and *coupling*. With regard to the interactions, a complex system – in contrast to a linear system – was characterised by the following:

- Indirect or inferential information sources.
- Limited isolation of failed components.
- Limited substitution of supplies and materials.
- Limited understanding of some processes (associated with transformation processes).
- Many control parameters with potential interaction.
- Many common-mode connections of components not in production sequence.
- Personnel specialization limits awareness of interdependencies.
- Proximate production steps.
- Tight spacing of equipment.
- Unfamiliar or unintended feedback loops.

According to Perrow, complex systems are difficult to understand and comprehend and are furthermore unstable in the sense that the limits for safe operation (the normal performance envelope) are quite narrow. (Perrow also contended that we have complex systems basically because we do not know how to produce the same output by means of linear ones. And once built, we keep them because we have made ourselves dependent upon their products!)
Systems can also be described with respect to their coupling, which can vary between being loose or tight. The meaning of *coupling* is that subsystems and/or components are connected or depend upon each other in a functional sense. Thus, tightly coupled systems are characterised by the following:

- Buffers and redundancies are part of the design, hence deliberate.
- Delays in processing not possible.
- Sequences are invariant.
- Substitutions of supplies, equipment, personnel is limited and anticipated in the design.
- There is little slack possible in supplies, equipment, and personnel.
- There is only one method to reach the goal.

Tightly coupled systems are difficult to control because an event in one part of the system quickly will spread to other parts. Systems with complex interactions are difficult to control because the outcome of specific interventions can be uncertain and/or difficult to anticipate. Systems that are both tightly coupled and have complex interactions are consequently even harder to control, and also harder to analyse.

Perrow used the two dimensions of *interactions* and *coupling* to illustrate differences among various types of systems, cf. Figure 2.

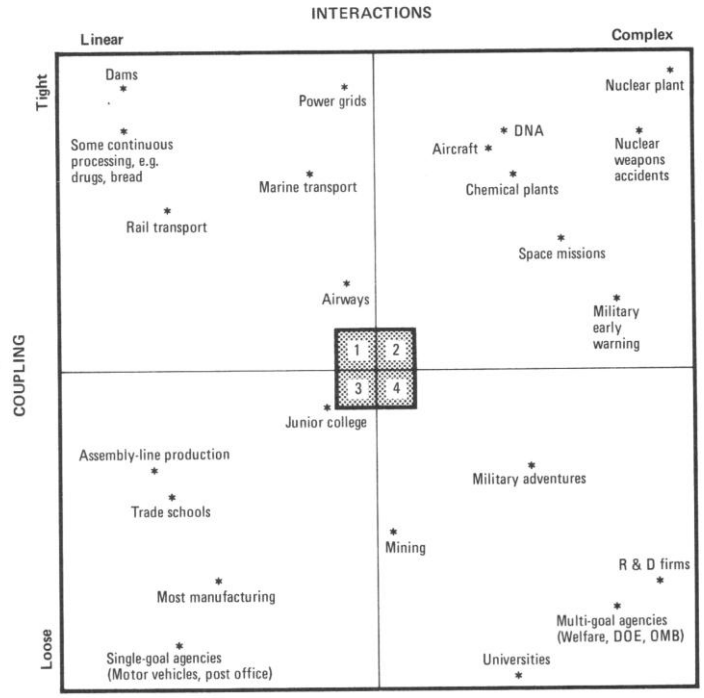

Figure 2: The Perrow diagram (from Perrow, 1984)

According to this way of thinking, the worst possible combination with regard to accident potential was, of course, a complex and tightly coupled system. Perrow's prime example of that was the nuclear power plant, with Three Mile Island accident as a case in point. Other systems that belonged to the same category were, e.g., aircraft and chemical plants. It was characteristic, and probably not a coincidence, that all the systems Perrow described in the book were tightly coupled and only differed with respect to their complexity, i.e., they were mostly in the second quadrant.

3. From Socio-Technical Systems to Resilience Engineering

A recent study (Hollnagel & Speziali, 2008) looked at developments in accident investigation methods. It was found that although the socio-technical systems that are the fabric of society continue to develop and to become more tightly coupled and complex, accident investigation methods do not change or develop correspondingly. This means first of all that the methods we have and use today may be partly inappropriate because the world around us changes and with that the nature of the problems. But it also means that even new methods after some time will become underpowered, even though they may have been perfectly adequate for the problems for which they were developed in the first place. The same obviously goes for risk and safety assessment methods. Indeed, in both fields the predominant models, and therefore also the mindsets, date from the 1970s, if not earlier.

The purpose of a model is to make the phenomenon under investigation understandable, hence amenable to analysis. The traditional safety models assume that events can be represented as chains or sequences of causes and effects, either as simple linear progressions or as combinations of paths (e.g., Benner, 1975). Accident investigations and risk assessments both typically proceed in a step-by-step fashion, gradually following links either backwards or forwards from the chosen starting point. In accident investigation, prominent examples are the Domino model (simple linear), the Swiss cheese model (complex linear), and the MTO model (also complex linear). In risk assessment, examples are event trees (simple linear), fault trees (complex linear), and Petri nets (also complex linear).

Accidents and incidents, whether understood as the unexpected and unwanted outcomes or the events that lead to them, can however occur in the absence of malfunctions and failures and be due, e.g., to performance variability or other transient phenomena. It is also common that the relationship between events and consequences is non-linear in the sense that the nature or magnitude of the consequences may be disproportionate to and unpredictable from the preceding events. In such cases, the events are better explained as a result of coincidences than as a result of causal relations. Such events are commonly called *emergent*. The reason why this happens is the increasing intractability of socio-technical systems. These systems tend to become larger and to have tighter coupling among subsystems, often due to external demands to efficiency and productivity.

In order for a system to be controllable, it is necessary to know what goes on ‘inside’ it to have a sufficiently clear description or specification of the system and its functions. The same requirements must be met in order for a system to be

analysed, in order for its risks to be assessed. That this must be so is obvious if we consider the opposite. If we do not have a clear description or specification of a system, and/or if we do not know what goes on 'inside' it, then it is clearly impossible effectively to control it as well as to make risk assessment. We can capture these qualities by making a distinction between tractable and intractable systems, cf., Table 2 below.

Table 2: Tractable and intractable systems

	Tractable system	Intractable system
Number of details	Description are simple with few details	Description are elaborate with many details
Comprehensibility	Principles of functioning are known	Principles of functioning are partly unknown
Stability	System does not change while being described	System changes before description is completed
Relation to other systems	Independence	Interdependence
Metaphor	Clockwork	Teamwork

The established approaches to risk assessment all require that it is possible to describe the system in detail, for instance by referring to a set of scenarios and a corresponding required functionality. In other words, the system must be tractable. As pointed out above, socio-technical systems, including nuclear power plants, are generally intractable. This means that the established methods are not suitable. Neither is it realistically possible to simplify the system descriptions so much that they become tractable in practice. It is therefore necessary to look for approaches that can be used for intractable systems, i.e., for systems that are incompletely described or underspecified.

Resilience Engineering represents such an approach. Traditional approaches to risk and safety depend on detailed descriptions of how systems are composed and how their processes work in order to count 'errors' and calculate failure probabilities. Resilience Engineering instead starts from a description of characteristic functions, and looks for ways to enhance an organisation's ability to create processes that are robust yet flexible, to monitor and revise risk models, and to use resources proactively in the face of unexpected developments or ongoing production and economic pressures. Socio-technical systems are always underspecified, which

means that individuals and organisations must adjust their performance to the current conditions. Because resources and time are finite, it is inevitable that such adjustments are approximate. In resilience engineering, accidents and failures are no longer seen as representing a breakdown or malfunctioning of normal system functions, but rather represent the converse of the adaptations necessary to cope with the real world complexity.

3.1. The Safety of Socio-Technical Systems

In order safely to manage such systems, it is necessary that models and methods are developed with a recognition of the following facts:

- *Performance conditions are always underspecified*. Since it is impossible to specify work in every detail, individuals and organisations must always adjust their performance to match the current conditions. Since resources and time are finite, such adjustments will inevitably be approximate. Performance variability is unavoidable, but is a source of success as well as of failure.
- *Many adverse events can be attributed to a breakdown or malfunctioning of components and normal system functions, but many cannot*. Such intractable events are best understood as the result of unexpected combinations of the variability of normal performance. Adverse events are therefore seen as representing the converse of the adaptations necessary to cope with real-world complexity.
- *Effective safety management cannot be based on hindsight, nor rely on error tabulation and the calculation of failure probabilities*. It is a general thesis of control theory that effective control cannot rely exclusively on feedback, except for very simple systems. Effective control requires that responses are prepared and sometimes executed ahead of time, i.e., feedforward. Neither is it sufficient to base safety managements on a count of adverse outcomes, since these are discrete events that exclude the dynamics of the system.
- *Safety cannot be isolated from the core (business) process, nor vice versa*. Safety is the prerequisite for productivity, and productivity is the prerequisite for safety. Safety is achieved by improvements rather than by constraints.

In Resilience engineering (Hollnagel, Woods & Leveson, 2006) the safety of complex socio-technical systems, such as nuclear power production, depends

critically on an organisation having the following four qualities (cf., Hollnagel, 2009, see also Figure 3).

- It can *respond* to regular and irregular threats in a robust, yet flexible, manner. No system can survive without being able somehow to respond when something goes wrong. It is, indeed, at the core of reactive safety management. Many systems, however, have a limited range of responses or are unable fully to adjust their responses to meet unexpected demands.
- It can flexibly *monitor* what is going on, including its own performance. This quality is necessary for all systems that exists in dynamic and unpredictable environments. The monitoring itself should furthermore be open to critical assessment, so that the system does not come to rely on established practices that may no longer be adequate.
- It can *anticipate* risks and opportunities in the longer term. Anticipating what may happen must go beyond the classical risk assessment, and consider not only individual events but also how they may combine and affect each other. Whereas many systems practice some kind of monitoring, few put a significant effort into anticipating, at least as far as safety is concerned.
- It can, finally, *learn* from experience. Learning requires more than collecting data from accidents, incidents, and near-misses or building up a company-wide database. Whereas data are relatively easy to amass and can be collected more or less as a routine or procedure, experience requires the investment of considerable effort and time in a more or less continuous fashion.

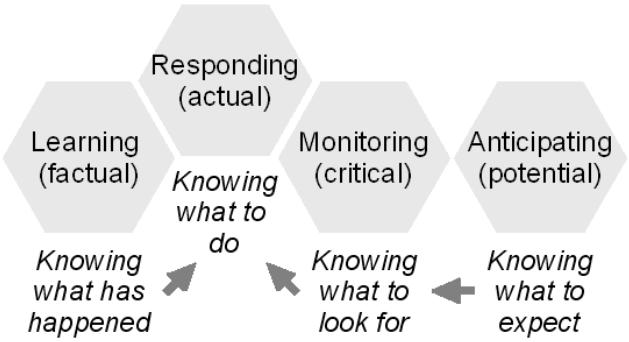

Figure 3: The four qualities of resilience

All four qualities depend critically on what kind of model the organisation has about itself, i.e., what it is and what it does, and about the environment in which it exists. The model is more precisely the assumptions about the nature of the processes that take place in and around the organisation, specifically the causal relations. This model, or these assumptions, are especially important for accident investigation and risk assessment, since they basically determine what is taken into consideration and what is not, and how relations among system components can be described.

4. Assessing the Risk of Organisational Change

As stated in the beginning of this report, the purpose of this study was to show how the principles of resilience engineering, and more specifically the functional resonance analysis method, could be used to make a risk assessment of an organisational change. The study used an organisational change that recently was carried out by the Ringhals NPP as a reference case. (In the following, the organisation will be referred to as Ringhals AB or RAB.) In order to provide sufficient background for the use of the FRAM, it was necessary to go into some detail with the reorganisation at Ringhals, as described in the provided documentation. It is, however, important to make clear that the study did not intend to analyse or evaluate the organisational change in its own right, but only to characterise it as a basis for applying the FRAM. The comparison that is presented at the end serves only to compare the principles of two approaches, the approach used by RAB and the FRAM. The comparison should not be construed as an evaluation of the organisational change at RAB, nor of the quality of the risk analysis done by RAB.

As mentioned earlier, a distinction can be made between the risk of making a change, or the risks associated with the implementation, and the risks that may be an outcome of the change once it has been made (Figure 1). The intention of this study was to consider only the latter.
The reference case was an organisational change at RAB. The change comprised a common organisation of the two units, Ringhals 3 and Ringhals 4, since this was seen as very advantageous from safety, quality, and economical points of view. The change was argued as follows:

Ringhals 3 och 4 tillhör samma generation anläggningar och är i grunden identiska konstruktioner. Det finns därför en rad samordningsfördelar (säkerhetsmässigt, kvalitetsmässigt och ekonomiskt) med att ha en samlad organisation.

VD har därför tagit beslut om att utreda lämplig struktur för gemensam organisation Ringhals 3 och 4. Den totala verksamhets-, ansvars-, och arbetsomfattningen för R34 skall vara oförändrad.

Syftet med förändringen av R34 är att likrikta ledning och styrning samt öka effektiviteten, bibehålla ett tydligt driftledningsansvar samt ge förbättrade förutsättningar för genomförande av anläggningsutveckling avseende förnyelse och säkerhetsuppgradering.

(1978311)

A large number of documents were made available for the study. Table 3 provides a complete list of these documents. The list is in chronological order.

Table 3: List of documents related to the reorganisation

Dokument ID / Version	*30/12/99*	*Namn*
1740550/18.0	*30/12/99*	*RVS förvaltning och utveckling*
1723490/8.0	*30/12/99*	*VD-direktiv - Reaktorsäkerhet*
1723954 I 22.0	*30/12/99*	*Befogenhetsdelegering inom Ringhals AB*
990714068 / 9.0	*30/12/99*	*Fackområdesdirektiv Reaktorsäkerhet*
990706003 I 5.0	*28/02/05*	*Ringhals primär säkerhetsgranskning*
990702051 /7.0	*30/12/99*	*Ringhals fristående säkerhetsgranskning*
1722338/5.0	*30/12/99*	*Delegering av arbetsuppgifter rörande företagaransvar vari ingår arbetsmiljö och kärnkraftssäkerhet inom Ringhals AB från Bertil Dihne till Göran Molin*
1975451 /2.0	*30/12/99*	*MTO 01/08 Förebyggande MTO-utredning med anledning av R34 organisationsöversyn.*
1977926 13.0	*30/12/99*	*R3 R4 Fristående säkerhetsgranskning av gemensam organisation för Ringhals 3 och 4*
1978311	*30/12/99*	*Anmälan - organisatorisk förändring Ringhals i enlighet med SKIFS 2004: 1 kap 4 5§*
1972964/2.0	*30/12/99*	*Ringhals 3 och 4. Planering och genomförande av organisationsförändring*
1977629/3.0	*30/12/99*	*PSG av Planering och genomförande av omorganisation och sammanslagning av Ringhals 3 och Ringhals 4*
901213024/15.0	*30/12/99*	*Instruktion för myndighetskontakter*
1973885/2.0	*30/12/99*	*Intresseanmälan till befattningar inom den nya organisationen på R34*
1973584/2.0	*30/12/99*	*R34 organisationsöversyn - Kontroll av organisationsalternativ*
1971991 /2.0	*30/12/99*	*Uppdrag organisationsjustering Ringhals 3 och 4*
1706456/17.0	*30/12/99*	*Ringhals Ledningshandbok*
990319080/9.0	*30/12/99*	*Ringhalsgruppens hantering av ansökan om undantag, tillståndsansökan och anmälan till SKI*
1746427/4.0	*30/12/99*	*Ringhalsgruppens övergripande instruktion för säkerhetsbehandling*
1734863/7.0	*25/06/07*	*Rutin för organisations- och verksamhetsförändringar*
1844193 (QPD - 1060)	*01/04/07*	*Vattenfalls Standard för Säkerhetsledning och Struktur för Säkerhetsgranskning*

Dokument ID / Version	*30/12/99*	*Namn*
1976916/2.0	*19/02/08*	*Riskbedömning av omorganisation och sammanslagning av Ringhals 3 och Ringhals 4*

The documents are clearly not all equally relevant for the study. Some deal with matters related to the organisation in general, such as *1722338/5.0 'Delegering av arbetsuppgifter rörande företagaransvar vari ingår arbetsmiljö och kärnkraftssäkerhet inom Ringhals AB från Bertil Dihne till Göran Molin.'* Some provide background information and general instructions that apply to organisation changes as a whole, such as *1746427/4.0 'Ringhalsgruppens övergripande instruktion för säkerhetsbehandling.'* But many directly address either the proposed organisational change, its implementation, and/or the safety assessment. The following documents constitute the more specific basis for this study.

Dokument ID / Version	*Datum*	*Namn / Sammanfattning*
1976916/2.0	*2008-02-19*	*Riskbedömning av omorganisation och sammanslagning av Ringhals 3 och Ringhals 4*
		Detta är en bedömning av de risker som har identifierats i samband med omorganisation och sammanslagning av Ringhals 3 och Ringhals 4. *Riskbedömningen har utförts av Huvud- och Avdelningsskyddsombuden i samverkan med arbetsgivaren.* *Identifierade riskbedömningarna har bedömts i nivåerna Liten, Medel och Stor.* *Ingen av riskerna har identifierats eller bedömts som stor.* *Åtgärder mot de identifierade riskerna kommer att genomföras successivt under året. Vissa av de identifierade riskerna måste bevakas i inledningsskedet av organisationens idrifttagning.* *Efterhand som planerade och genomförda åtgärder vidtas kommer denna rapport att revideras och nya versioner skapas.*
1734863/7.0	*2007-06-25*	*Rutin för organisations- och verksamhetsförändringar*
		Både förändringar i omvärlden och förändringar av givna förutsättningar fordrar ständig fokus på hur vi på bästa sätt skall använda tillgängliga resurser. För att möta nya/ändrade krav kan behov uppstå att genomföra förändringar i organisation eller i verksamhet. *Denna instruktion syftar till att säkerställa att begränsningskrav och lönsamhetskrav uppfylls, såväl under som efter genomförandet av organisations och verksamhetsförändringar.*

Dokument ID / Version	*Datum*	*Namn / Sammanfattning*
		Instruktionen innefattar tillvägagångssätt för såväl "större" som "mindre" förändring. Definition av mindre och större förändring finns i ordlistan på Insidan. De förändringar som inte faller in under denna definition betraktas som utveckling i linjen och genomförs löpande under linjechefens ansvar. *Denna Instruktion ersätter Anvisning "Rutin för organisations- och verksamhetsförändringar" med samma ID-nummer.*
1977629/3.0	*30/12/99*	*PSG av Planering och genomförande av omorganisation och sammanslagning av Ringhals 3 och Ringhals 4*
		Granskningen ger att tillämpliga säkerhetsaspekter är beaktade. Före idrifttagning föreslås att funktionsbeskrivning för R34S och delegeringshandlingar tas fram samt påverkan på SAR klarställes. *Kommentarerna är omhändertagna och åtgärdade på ett acceptabelt sätt.* *Bedömningen är att organisationsförändringen ger förutsättningar för en effektivare och starkare organisation och att reaktorsäkerheten och säkerhetskulturen minst kommer att behållas.*
1973584/2.0	*30/12/99*	*R34 organisationsöversyn - Kontroll av organisationsalternativ*
		Vid arbetet med organisationsöversynen för Ringhals 3 och 4 togs några organisationsförslag fram. Dessa remissades och kommenterades av hela ledningsgruppen. Slutligen fanns fyra förslag. *Arbetsgruppen kontrollerade hur bra de olika organisationsalternativen uppfyller kraven i uppdragsbrev och SWOT. Kontrollen gjordes enligt en framtagen mall, se bilaga l .* *Resultatet visar på stor likhet mellan alternativens uppfyllnad av kraven.* *I bilaga 1 framgår hur kontrollen gjordes och resultatet.* *Det fortsatta arbetet med organisationsförändringen ledde till att ett alternativ togs fram som slutligt, för att ligga till grund för rapport om "Ringhals 3 och 4 - Planering och genomförande av organisationsförändring", Darwin 1972964.* *Arbetsgruppen kontrollerade även hur bra det slutliga organisationsalternativet uppfyller kraven i uppdragsbrev och SWOT.* *Kontrollen gjordes enligt en framtagen mall, se bilaga 2. Varje område gavs omdömet "2 uppfylls väl" eller "1 uppfylls". För de områden som bara fick en 1:a gjordes en kommentar om hur vi avser att bevaka området. Dessa punkter skall också vara med i den utvärdering av organisationsförändringen som R34 avser göra i*

Dokument ID / Version	*Datum*	*Namn / Sammanfattning*
		slutet på året.
1971991 /2.0	*30/12/99*	*Uppdrag organisationsjustering Ringhals 3 och 4*
		VD ger Göran Molin i uppdrag att utreda lämplig struktur för gemensam organisation Ringhals 3 och 4, samt efter separat beslut implementera och leda den nya organisationen.
1972964/2.0	*30/12/99*	*Ringhals 3 och 4. Planering och genomförande av organisationsförändring*
		Göran Molin har av VD fått i uppdrag att utreda lämplig struktur för gemensam organisation Ringhals 3 och 4, samt implementera och leda den nya organisationen. Den totala verksamhets-, ansvars-, och arbetsomfattningen för R34 skall vara oförändrad En mindre grupp med stöd från hela R34ledning har, bl.a. via SWOT analys, arbetat fram en ny organisationsstruktur och föreliggande rapport som stöder planeringen och genomförandet av organisationsförändringen. *Kommunikationen följer en uppgjord kommunikationsplan och sker med personalorganisationerna, liksom med medarbetarna. Arbetsmiljöfrågor har hanterats bl.a. genom involverande av Huvudskyddsombudet. MTO-frågorna beaktas genom stöd från RQH.* *Med vald organisation uppnås en boskillnad mellan operativt och strategiskt arbete. Den ger en tydlig adressering av analys och anläggningsdokumentation, samt förbättrade förutsättningar för driftcheferna att fokusera mot den operativa driften. Driftledningsstrukturen är fortsatt tydlig. Ökat fokus på uppföljning av systemprestanda och provdrift av nya anläggningsdelar adresseras i enheten Anläggningsstöd, den ger också ökat utrymme för planering. I Anläggningsteknik har Analys och dokumentation tydliggjorts i en egen grupp. Gruppen Anläggning hanteras blockens underhåll och utveckling.* *Påverkan på verksamhetsstyrande dokumentation har identifierats.* *Remiss och säkerhetsgranskning har planerats och resurser för detta är vidtalade.*
1975451 /2.0	*30/12/99*	*MTO 01/08 Förebyggande MTO-utredning med anledning av R34 organisationsöversyn.*
		Medarbetarna är överlag mycket positiva till den föreslagna organisationsförändringen. Många fördelar finns med att slå samman organisationerna och flera av fördelarna handlar om ledarskap. Gemensam ledningsgrupp, entydig information och gemensam kultur är positiva följder. *Vidare hoppas många att med den nya organisationen ska det*

Dokument ID / Version	*Datum*	*Namn / Sammanfattning*
		skapas utrymme för cheferna att vara goda ledare för sina underställda. *Det återstår dock att klarställa "rutornas" (de organisatoriska enheternas) funktion. Vad ska medarbetarna ha för arbetsuppgifter, vilka olika roller ska de axla och vilket ansvar innebär det.* *Hand i hand med ansvaret som åläggs respektive roll måste befogenheterna gå. Ingen kan ta ansvar för något som han/hon inte kan påverka.* *Den nya organisation som är föreslagen för Ringhals 3 och 4 kommer att skilja sig från strukturerna på block 1 och 2. Det innebär i praktiken att i den händelse verksamhetsledningssystemet inte är organisationsoberoende så kan problem uppstå.* *Många frågor och förbättringsområden handlar om samarbete och kommunikation mellan de organisatoriska enheterna.* *Redan idag finns ett antal vakanser inom de båda organisationerna och med stor sannolikhet kommer de behöva tillsättas även i den nya organisationen.* *Dessutom har farhågor framkommit som säger att ett par av de föreslagna enheterna/grupperna bör vara betydligt större än vad som är dimensionerat i dagsläget.* *Rekommenderade åtgärder finns beskrivna i punkt 8. Åtgärdsansvariga skall lämna ställningstagande till rekommendationerna till MTO-samordnare RQH senast 4 veckor efter utgiven rapport*
1978311	*30/12/99*	*ANMÄLAN - ORGANISATORISK FÖRÄNDRING RINGHALS i enlighet med SKIFS 2004: 1 kap 4 5§*
1977926 13.0	*30/12/99*	*R3 R4 Fristående säkerhetsgranskning av gemensam organisation för Ringhals 3 och 4*
990706003 I 5.0	*30/12/99*	*Ringhals primär säkerhetsgranskning*
		Kraven på SÄKERHETSGRANSKNING av händelser, åtgärder och förhållanden med påverkan på BARRIÄRER och DJUPFÖRSVAR anges i [1] samt i [7]. *Denna instruktion beskriver formerna får hur den primära säkerhetsgranskningen vid Ringhals ska genomfåras. Detaljanvisningar återfinns i vissa underliggande dokument.*
990702051 /7.0	*30/12/99*	*Ringhals fristående säkerhetsgranskning*
		Enligt Statens kärnkraftinspektions författningssamling finns krav på säkerhetsgranskning av förhållanden, utpekade händelser och

Dokument ID / Version	*Datum*	*Namn / Sammanfattning*
		tekniska och administrativa åtgärder med påverkan på barriärer och djupförsvar. *Säkerhetsgranskningen genomförs i två steg; först den primära säkerhetsgranskningen, som görs i linjen, därefter den fristående säkerhetsgranskningen som görs inom staben säkerhet och miljö, RQ.* *Denna instruktion beskriver hur den fristående säkerhetsgranskningen skall genomföras.*

4.1. Purpose of the organisational change

The purpose of the proposed change was to develop a common organisation for Ringhals 3 and Ringhals 4, as described above.[1] The intention was that this change should affect only some parts of the two units, and that the overall functioning of the two units should remain the same (*'Den totala verksamhets-, ansvars-, och arbetsomfattningen för R34 skall vara oförändrad,' 1978311*). The change was furthermore limited to some of the departments at the two units*:* '*Förändringen av organisationen berör i huvudsak driftstödsgrupperna och teknikenheterna på Ringhals 3 och 4. Övriga enheters verksamhet påverkas marginellt, med undantag för att kemienheten får resurser för hela miljöområdet.*'
The expected benefits of the change were described as follows in document 1971991/2.0 '*Uppdrag organisationsjustering Ringhals 3 och 4'*:

- *Likriktad ledning och styrning och ökad effektivitet*
- *Tydligt driftledningsansvar*
- *Förbättrade förutsättningar for ansvarstagande for och genomförande av anläggningsutveckling avseende förnyelse och säkerhetsuppgradering*
- *Förbättrade förutsättningar for systemansvar genom utökad systemanalys / prestandauppföljning*
- *Tydligt gränssnitt mot övriga RAB*
- *Förbättrade förutsättningar for varaktig saker drift (PLM, 50+)*
- *Förbättrad operativ, medel och långsiktig planering, inkl. RA-planer på kort och lång sikt*
- *Förutsättningar for kommande kompetensväxling*
- *Att R3 och R4 varaktigt:*

1 A minor comment is that this change in some documents was called *organisatorisk förändring*, and in other documents *organisationsjustering*. Strictly speaking the two terms are, however, not synonymous.

- *Kan köras (drift-kompetens/bemanning)*
- *Går att köra (Anläggningarna ar bra underhållna och utvecklade)*
- *Får köras (Tillstånd från myndigheter, t.ex. SKIFS)*

While the purpose of the proposed organisational change was not primarily to improve safety, it was clearly important that the current level of safety was not jeopardised. The importance of safety is clear from the following statement:

"En fullgod säkerhet i Vattenfalls kärnkraftverk ar en grundförutsättning for verksamheten och for tillgänglighet, hög effektivitet och god lönsamhet. Säkerhet skall alltid ha högsta prioritet och vid eventuell målkonflikt mellan kärnkraftssäkerhet och andra verksamhetsmal skall säkerhetsmässigt konservativa bedömningar göras. Säkerhet står inte i motsatsförhållande till produktion och ekonomi."

(1844193/3.0)

In order to ensure a high standard of safety, the Vattenfall company has developed a detailed '*Standard for Säkerhetsledning och Struktur for Säkerhetsgranskning.'* This specifies, among other things, that organisational changes shall be subject to both a primary safety examination (PSG) and an independent safety examination (FSG):

Tekniska eller organisatoriska ändringar i anläggningarna, vilka kan påverka de förhållanden som angivits i säkerhetsredovisningen (SAR) eller som ar av annan principiell säkerhetsmässig betydelse ska genomgå primär och fristående säkerhetsgranskning.

(1844193/3.0)

The details of these examinations will be described below.

4.2. Details of the organisational change

The decision about the new organisation was based on an evaluation of four alternatives. The four alternatives are shown in Figure 4.

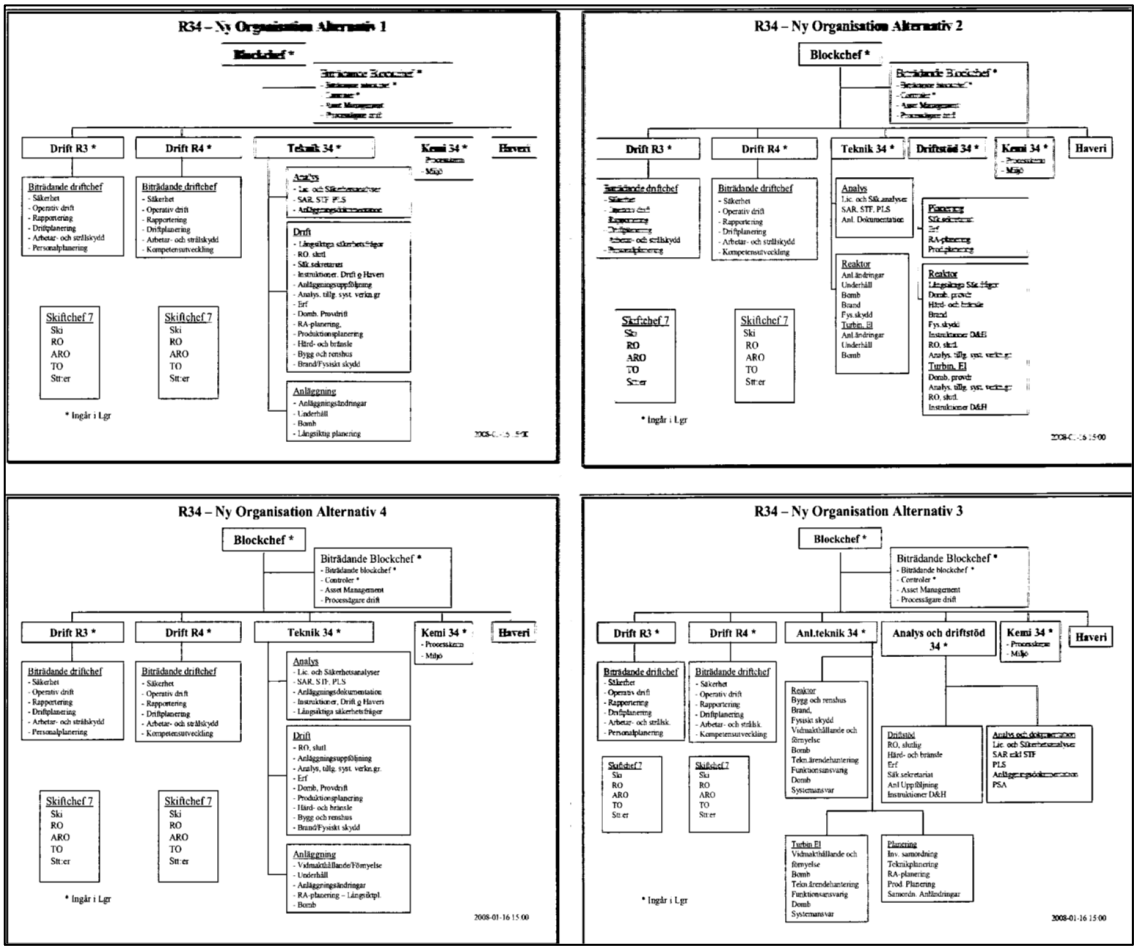

Figure 4: Alternatives for the organizational change

The evaluation of the four alternatives has been described in document *1973584*, *R34 organisationsöversyn – Kontroll av organisationsalternativ*. The evaluation was based on a checklist of items from the following main categories: demands (11 items, taken from *1971991*), demarcations (5 items, also taken from *1971991*), strengths (4 items), weaknesses (4 items), possibilities (4 items), and threats (4 items). (The four last categories are derived from the so-called SWOT principle, cf., Figure 5.)

Figure 5: The SWOT diagram

Each item was assigned one of the following values:

- '2' – meaning that the requirement was fully met,
- '1' – meaning that the requirement was met, and
- '-' - meaning that the requirement was not applicable.[2]

The evaluation showed that the four alternatives were quite equal in how well they met the requirements, and that they all met them rather well. The proposed new organisation, which was not among the alternatives, was also evaluated and received a satisfactory score. In cases where an item was scored as a '1', a note was made about how this should be followed-up during the change. These items were also to be included in the evaluation of the effects of the change that was planned for the end of 2008.

The details of the change were described as follows:

I den nya organisationen fokuserar Driftenheterna på anläggningens driftklarhet. Det vill säga att kraven på anläggning, bemanning/kompetens i kontrollrummen uppfylls. Driftsenheterna kommer att ha en stab bemannade med en biträdande driftschef. R3DL har personalplanerare medan R4DL har kompetensutvecklare. Skiftlagen påverkas ej av omorganisationen.

2 There was apparently no assignment corresponding to a requirement not being met.

Två nya enheter skapas, Anläggningsstöd och Anläggningsteknik. Anläggningsstöd kommer att bistå både Driftsenheterna och Anläggningsteknik med kompetens och resurser.

Anläggningsteknik kommer framförallt att arbeta med anläggningens vidmakthållande, förnyelse och expansion.

Anläggningsstöd består av grupperna Drift och Planering. Driftgruppen stödjer driftsenheterna med anläggningsuppföljning, RO-hantering, driftdokumentation mm. Driftgruppen stödjer även Anläggningsteknik med driftombud och behövd driftskompetens. Planeringsgruppen hanterar blockens planering på kort och lång sikt inklusive driftplanering. I ansvaret ingår att även utveckla och hantera ABH-funktionen.

Anläggningsteknik består av grupperna Analys och dokumentation samt Anläggning. Gruppen Analys och dokumentation ansvarar för säkerhetsanalyser, SAR, STF, PLS, anläggningsdokumentation, PSA samt långsiktiga säkerhetsfrågor. Anläggningsgruppen huvudsakliga verksamhet är anläggningsvård (Underhållsdimensionering) och anläggningsutveckling.

Förutom de nya enheterna kommer en biträdande blockchef att tillsättas med operativ inriktning och en specialist med inriktning strategisk anläggningsutveckling. Skälet till att utse dessa är den just nu mycket omfattande anläggningsutvecklingen av blocken.

Biträdande blockchef är också stf och avlastar blockchefen i operativa frågor, möjliggör fokusering på utveckling av säkerhetskultur, driftledning och driftmannaskap.

Specialist med strategisk inriktning skapar förutsättningar för ökat ansvarstagande och förvaltning i långtidsperspektivet för strategiska investeringar, effekthöjningsprojekten, övergångsplanerna samt strategisk planering.

(1978311)

The proposed organisational change is shown in Figure 6. The grey boxes contain the functions that are new to this organisation, i.e., *anläggningsstöd, anläggningsteknik, biträdande blockchef*, and s*pecialist*.

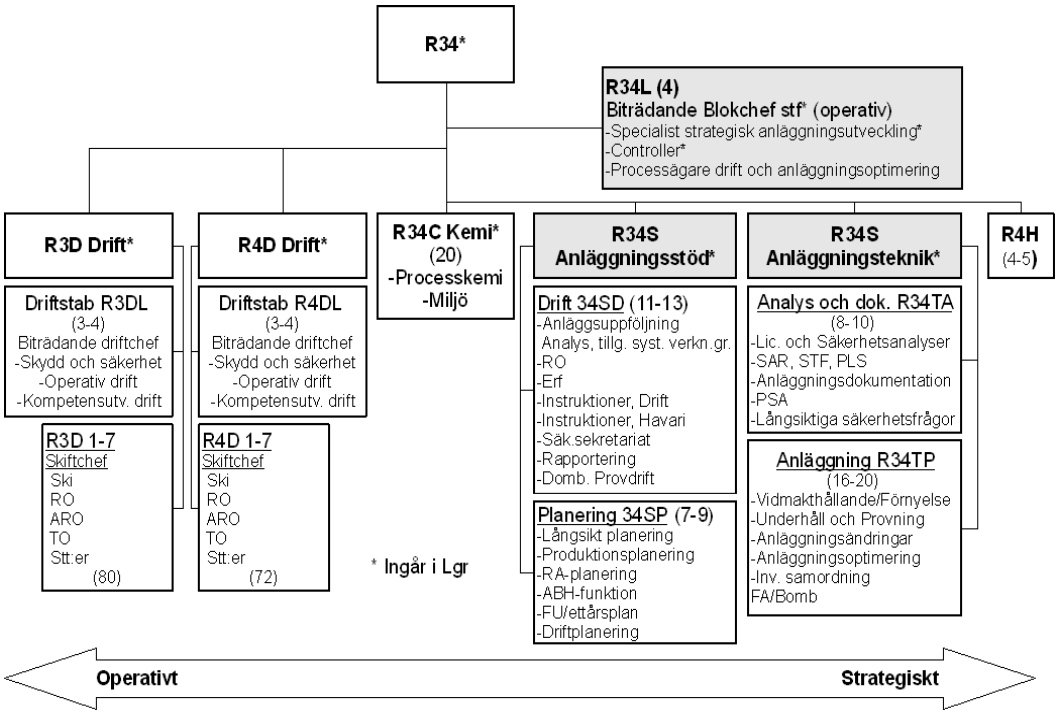

Figure 6: Diagram of proposed organisational change

It is clear from the figure that direct changes were not made to the operation of the two units (*driftstab*), but only to the support functions. Because of this, the RAB risk assessment did not include a PRA.

4.3. Risk assessment of the organisational change

The guidelines for risk assessment of organisational change are provided by the document *1746427, Ringhalsgruppens övergripande instruktion för säkerhetsbehandling*. This document defines what a risk assessment is, namely:

Säkerhetsgranskning definieras i SKIFS 2004:1 som "en kontroll av att tillämpliga säkerhetsaspekter är beaktade, och att tillämpliga säkerhetskrav på en anläggnings konstruktion, funktion, organisation eller verksamhet är uppfyllda". Vidare anges att granskningen skall genomföras systematiskt och vara dokumenterad.

The document also defines that a risk assessment always has two parts or stages, a primary risk assessment (*primär säkerhetsgranskning* or *PSG*) and an independent risk assessment (*fristående säkerhetsgranskning* or *FSG*).[3] Additional details are provided by the document *1734863, Rutin for organisations- och verksamhetsförändringar*. In accordance with this document, the conditions for these assessments are defined as follows:

Primär säkerhetsgranskning (PSG) genomfors i förekommande fall efter planeringsfasen. PSG baseras pa specifikation "Planering och genomförande av större resp. mindre förändring" enligt bilaga 2 och 4. PSG följer for instruktionen "Ringhals primär säkerhetsgranskning" (9907060037).

Efter avslutad PSG genomfors fristående säkerhetsgranskning (FSG) enligt fastlagd rutin i "Ringhals fristående säkerhetsgranskning" (990702051).

The relation between the PSG and FSG is shown in Figure 7.

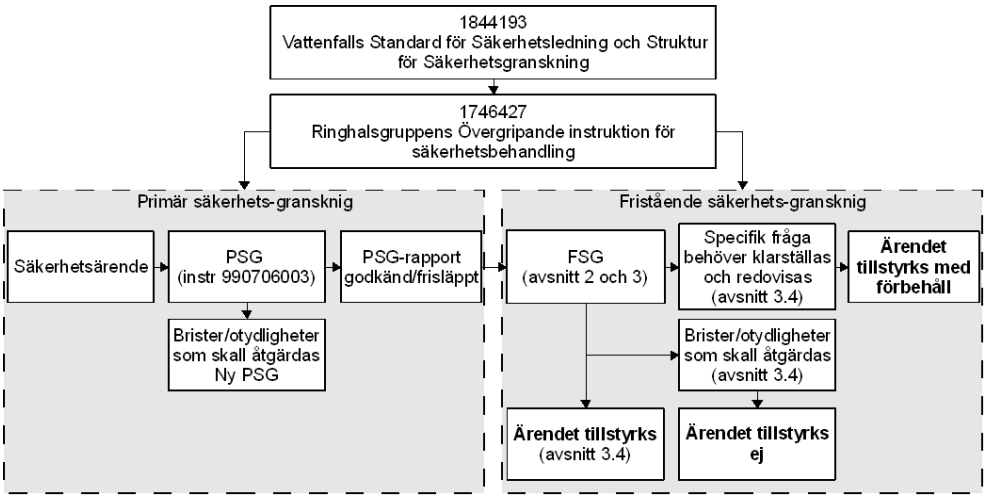

Figure 7: Guidelines for PSG and FSG

The document *9907060037* defines the principles for a PSG. It stipulates that a PSG must be carried out for events (*händelser*), documentation (*dokumentation*), and changes and analyses (*ändringar och analyser*). Only the latter is considered here. In the case of organisational changes, the document makes the following clarification:

3 The RAB documents variously refer to safety examination (*säkerhetsgranskning*) and risk assessment (*riskbedömning*). This report will use the term risk assessment.

Här avses ändringar vilka på principiell nivå påverkar de organisatoriska krav som anges i säkerhetsredovisningen avseende organisationen och styrningen:

- *av driftarbetet*
- *av kontrollrumsarbetet*
- *av underhållsarbetet*
- *av hanteringen av kärnämne och kärnavfall*
- *av reaktorsäkerhetsarbetet*
- *av kvalitetssäkringsarbetet*
- *av haveriberedskapen*
- *av det fysiska skyddet*

The document *1734863* defines that the following areas must be considered by the risk assessment.

- Reactor safety (*Reaktorsäkerhet*)
- Organisation and performance (*Organisation och verksamhet*)
- Work environment (*Arbetsmiljö*)
- MTO aspects (*MTO-aspekter*)
- The management system (*Verksamhetsstyrsystemet RVS*)

For the second item, organisation and performance, a set of more detail issues were defined. These were:

- Ability to achieve targets (*Förmåga att uppnå satta mål*).
- Risk for loss of competence during the change (*Risk för kompetensglapp vid genomförandet*).
- Risk that requried resources are not established (*Risk för att erforderliga resurser inte kan tillskapas*).
- Risk that requirements to competence are not met (*Risk för att kompetenskrav inte kan tillgodoses*).
- Risk for long-term loss of competence (*Risk för kompetensflykt i ett långtidsperspektiv*).
- Consequences of failure to complete training as planned or in time (*Konsekvens av om utbildning inte kan genomföras planenligt eller måste utföras i fel skede*).
- (Increasing) demands to own staff (work load) (*Belastning på egen personal*).
- Ability to complete work assigments (*Förmåga att fullfölja arbetsuppgifter*).

- Risk that roles become unclear (*Risk för att roller blir otydliga*).
- Risk of an impoverished work environment (*Risk för arbetsmiljöförsämringar*).
- Risk that attitude changes may affect efficiency and safety in a negative manner (*Risk för attitydförändringar som kan påverka effektivitet och säkerhet negativt*).
- Risk that estrablished practice is not properly replaced or that established work routines are lost (*Risk för att etablerad praxis inte ersatts eller att etablerade rutiner tappas bort*).
- Risk that formal and informal channels of communication are lost or become less effective (*Risk för att formella såväl som informella kontaktvägar förloras eller blir mindre effektiva*).

4.3.1. Primary Risk Assessment (PSG)

The primary risk assessment (PSG) is described in document *1977629, PSG av planering och genomförande av omorganisation och sammanslagning av Ringhals 3 och Ringhals 4*. The assessment was based on a checklist containing 17+1 items.

1. ***Syfte och mål***. *Finns tydlig beskrivning av syfte och mål med organisationsförändringen?*
2. ***Instr 1734863, Rutin för organisations- och verksamhetsförändringar***. *Är instruktionen rätt tillämpad?*
3. ***Konsekvensanalys***. *Finns analys som syftar till att identifiera potentiella svagheter och styrkor i den nya organisationen?*
4. ***STF och SAR/FSAR***. *Beskrivs ev. påverkan på STF och/eller SAR/FSAR?*
5. ***Principer för säkerhetsarbete***. *Finns tydlig beskrivning av principerna för säkerhetsarbete och säkerhetsledning?*
6. ***Ansvarsfördelning***. *Finns tydliga funktions- och befattningsbeskrivningar som beskriver rapporteringsvägar och ansvarsfördelning?*
7. ***Förändringar i ansvar***. *Beskrivs förändringar i ansvars- och uppgiftsfördelning mellan organisationsenheter?*
8. ***Kompetens***. *Beskrivs förändringar i kompetens- och resursbehov?*
9. ***Arbetsmiljö***. *Påverkar ändringen fysisk och/eller psykosocial arbetsmiljö?*
10. ***Simulator***. *Finns behov av att träna personalen i simulator?*
11. ***MTO-analys***. *Finns behov av förebyggande MTO-analys?*
12. ***Styrande dokument***. *Finns lista över styrande dokument som skall uppdateras prioriterings- ordning för dessa?*

13. ***Tidplan***. *Finns tidplan för de åtgärder som krävs för en kvalitets-säkrad implementering av organisationsförändringen, med utbildningsinsatser angivna?*
14. ***Utvärderingsplan***. *Finns plan för uppföljning och utvärdering av organisations förändringen där det anges tidpunkt, samt vad som skall följas upp, och vem som är ansvarig?*
15. ***Genomrörda bedömningar***. *Är genomförda bedömningar med avseende på reaktorsäkerheten invändningsfria?*
16. *Behöver ärendet granskas av* ***annan kompetens*** *än din?*
17. ***Övergripande säkerhets bedömning***. *Leder organisations-förändringen till bibehållen eller ökad säkerhet för anläggningen som helhet?*
18. ***Övrigt***.

The PSG clearly reflects the definition given in document *1746427*. If we try to categorise the 17 items, leaving out 'other,' the result is the following:

- Items that mainly deal with risk as the consequences of the change: 3, 15, 17.
- Items that mainly deal with the implementation of the change: 1, 2, 4, 7, 8, 9, 10, 12, 13, 14, 16.
- Items of a general nature: 5, 6, 13.

The conclusion of the PSG was that applicable safety issues had been considered in the organisational change. It was further concluded that the organisational change would create the conditions for a more efficient and stronger organisation, and that reactor safety and safety culture at least would be maintained at the current level.

4.3.2. Independent Risk Assessment (FSG)

The guidelines for the independent risk assessment (FSG) are described in document *990702051, Ringhals fristående säkerhetsgranskning*. They specify the FSG as such:

Den fristående säkerhetsgranskningen, FSG, skall genomföras på en anpassad nivå, med hänsyn till ärendets säkerhetsmässiga betydelse/påverkan, principiella betydelse, komplexitet och omfattning

- *bedöma att tillräckliga säkerhetsmarginaler finns, baserat på principiella och grundläggande krav beträffande barriärer och djupförsvar*

- *beakta MTO-aspekter (samspelet Människa- Teknik- Organisation)*
- *beakta CCF-aspekter (Common Cause Failure)*
- *genomföras systematiskt, med hjälp av checklista och dokumenteras*
- *beakta riktlinjerna avseende ständiga förbättringar av reaktorsäkerheten i Ringhals enligt Instruktion 1839723 (Övergripande mål och förhållningssätt för reaktorsäkerhet).*

The FSG is clearly more directed at the risks of the organisational change in a classical sense.

The overall outcome of the FSG was reported in document *1977926, R3 R4 Fristående säkerhetsgranskning av gemensam organisation för Ringhals 3 och 4*. The conclusion from the FSG was that the organisational change had been managed in a satisfactory way from both a quality and a reactor safety point of view. The FSG also made some specific comments about how to deal with outstanding issues.

The details of the FSG were reported in document *1976916, Riskbedömning av omorganisation och sammanslagning av Ringhals 3 och Ringhals 4*. This evaluated a number of risks that had been found during the organisational change. Each risk was scored using the categories of small, medium, or large. However, none of the risks were in fact scored as large. The document also described the action to be taken for each risk, but this part of the analysis is not addressed in this study. Table 4 provides a summary of the identified risks and the score they were given.

Table 4: Summary of identified risks

Risk nr.	*Identifierad risk*	*Bedömd potentiell risk (liten/med el/stor)*
1	*Risk for att ansvar, resurser, befogenheter och kompetens inte följs åt eller svarar mot varandra i den nya organisationen. Kan på sikt ge en degraderad säkerhetskultur.* *Delegeringar kan inte mottagas om man inte råder över läget.*	*Liten*
2	*Risk for att rutiner, instruktioner och säkerhetsföreskrifter inte revideras utifrån ändrade arbetssatt och organisation.*	*Liten*

Risk nr.	*Identifierad risk*	*Bedömd potentiell risk (liten/med el/stor)*
3	*Oklara gränser (vem skall göra vad) leder till att risk for att arbetsuppgifter "ramlar" mellan stolarna och inte utförs eller dubbelarbete.* • *Medarbetarna får svårt att veta vem man skall vända sig till om det inte blir tydligt.* • *Om arbetsuppgifter överförs till någon annan genererar det i en inkörningsperiod ökad initial arbetsbelastning.* • *Viktigt med information och kommunikation mellan chefer och medarbetare samt mellan medarbetarna.* • *Olika "informella" kontaktvägar kan tappas bort.*	*Liten* *Finns med i viss utsträckning i rapporten under punkt 8.2. Bedöms därmed som liten risk.*
4	*I samband med omorganisationen kan nyckelpersoner byta jobb vilket leder till risk att arbetsuppgifterna inte utförs i förväntad omfattning.*	*Liten*
5	*Risk for försämrad gruppbildning och samarbete kan forsvåras om inte avdelningar och enheter sitter tillsammans.*	*Liten* *Finns med i rapporten under punkt 8.3. Bedöms därmed som liten risk.*
6	*Målen riskerar att bli oklara och otydliga när verksamhetsplaner slås samman.*	*Liten*
7	*Risk att förlora åtgärder i omorganisationen om man inte fortsätter att följa instruktionen for organisationsförändring.*	*Liten*
8	*Otydligt hur ERF-funktioner på blocken skall fungera och sammanhållas. Avser både intern och extern ERF, bevakning av AvÄrS osv.* • *Hur blir kopplingen och samarbete med den nya avdelningen RQH? En ny roll "Säkerhetscontroller" skall införas på Ringhals. Hur kommer den in i omorganisationen?* • *Erfarenhetsåterföring är med i SWOT-analysen och är upptagen som en svaghet i den gamla organisationen. Utmärkt tillfälle att i samband med omorganisationen förbättra denna svaghet.* • *Fyra avdelningar har detta upptaget som arbetsområde. Driftstab R3DL och R4DL, 7.3.2.1, Anläggningsstöd Drift R34SD, 7.3.3.1 Anläggningsstöd Planering R34SP, 7.3.3.2.*	*Medel*

Risk nr.	*Identifierad risk*	*Bedömd potentiell risk (liten/med el/stor)*
9	*Övergång till ny organisation leder till en stor arbetsinsats och redan idag har flera medarbetarna mycket att göra.* • *Arbetsbelastning och prioriteringar ar viktiga faktorer att beakta vid förändringen.* • *Nyanställningar ger att utbildningsresurser kravs och avlastning behovs for handledare.*	*Liten*
10	*Arbetsbelastningsskillnad mellan R3 och R4 kontrollrum kvarstår.* • *R3 operatorernas arbetsbelastning ar högre (renshus och totalavsaltning).* • *R3 bemanning blir ibland tvungen till rockad internt vid ersättare från R4.*	*Liten*
11	*Numerären for den nya organisationen beskrivs inte tydligt. Antalet medarbetare beskrivs i organisationsförslaget endast i övergripande siffror. Det definitiva antalet ar inte preciserat.*	*Medel*
12	*Arbetsbelastning på individ nivå kan bli for hög.* • *Risk for att anställda kan gå i väggen om inte förberedelser och kartläggning av vilka arbetsuppgifter som skall utföras och fördelas ar klara före genomförandet.* • *Kan även innebära att fördelningen av arbetsuppgifter kan bli tydligare och lättare att fördela på flera medarbetare.*	*Liten*
13	*Risk att nuvarande chefernas arbetsbelastning ökar inför övergången till ny organisation.* *De "nya" cheferna kommer också få en hög arbetsbelastning i formandet av avdelningarna.*	*Medel*
14	*Svårighet att upprätthålla kompetensnivån med manga medarbetare på nya positioner.* • *Vidareutveckling av kompetens ar också svart utan parallell tjänstgöring.* • *En generationsväxling ar förestående.*	*Liten*
15	*Risk att attityder och kulturskillnader kan påverka effektivitet och säkerhet negativt.* • *Kommunikations- och förståelsebrist (kulturskillnader) mellan blocken.* • *Kan uppträda i inledningsskedet av omorganisationen.*	*Liten*
16	*Förlorad känsla av ägande, "Lost ownership", när man jobbar mot två block. Lojalitetskonflikter kan uppstå om vilket block som skall prioriteras.*	*Liten*

Risk nr.	*Identifierad risk*	*Bedömd potentiell risk (liten/med el/stor)*
17	*När man delar upp driftkontoret och driften (kontrollrum) finns risk att "murar" skapas mellan drift, anläggningsstöd och anläggningsteknik.* • *Prestigekamp kan uppstå.* • *Kommunikation mellan drift (kontrollrum) och anläggningsstöd samt anläggningsteknik*	*Liten*
18	*Risk att etablerad praxis inte ersatts eller att etablerade rutiner tappas bort.* • *Degraderad sammanlagrad kompetens ("lost or degraded organisational memory")*	*Liten*
19	*Risk att den enskildes förändringssituation inte säkerställs i samband med omorganisationen* *Tajt tidplan:* • *Risk att alla inte hänger med eller att man inte når ut till alla medarbetare. Vi hinner inte säkerställa den enskilde individens förändringssituation (mognad) då tidplanen ar tajt.* • *Medarbetarna hinner inte med att ta till sig all information inför förändringen for att göra ratt val vid intresseanmälan till ny tjänst m.m.?*	*Medel*
20	*Kontrollrumspersonal:* *Risk finns att medarbetare förlorar tillhörighet om man lånas ut eller flyttas runt i for stor utsträckning. Ger försämrad trivsel m.m.* *Oro finns redan i dag for skillnader på R3 och R4 med avseende på anläggningskompetens.* *Kompetensprofiler kräver att man kan kora "ratt" anläggning. Detta med avseende på att anläggningarna "växer" ifrån varandra de närmaste aren.* *Dagtid och kontrollrumspersonal:* *Risk att omorganisationen genererar en ökad förväntning att man skall genomfora två revisioner per år. Alla medarbetare kanske inte klarar av eller orkar med det.*	*Medel*
21	*Risk for att oroskänslor uppträder i samband med omorganisationen. Eftersom intresseanmälan skall ske till tjänster och cheftjänster utannonseras.* • *Risk for ökad lång- och/eller korttidssjukfrånvaro*	*Medel*
22	*Risk for att blanda ihop blocktillhörighet ökar.*	*Liten*
23	*Risk att faktiska skillnader i anläggningarna inte omhändertas på rätt sätt eller hanteras korrekt, kan ge försämrad säkerhet och säkerhetskultur.*	*Liten*

As noted earlier in this report, a risk assessment can in principle focus on the risks of making a change, the risks associated with the implementation, or the risks that may be a result of a change. The two first can be called for implementation risks and the latter for outcome risks. A simple tally shows that the majority of risks listed in Table 4 were of the type outcome risks.

- Implementation risks: 4, 6, 7, 9, 13, 19, 21.
- Outcome risks: 1, 2, 3, 5, 8, 10, 11, 12, 14, 15, 16, 17, 18, 20, 22, 23.

All of the outcome risks were of what one could call a generic type, i.e., they addressed general issues. The FSG did not consider specific tasks or activities, perhaps because the change was to the support branch of the organisation rather than to the operational branch.
In summary, the risk assessment of the organisational change can be described as shown in Figure 8 below.

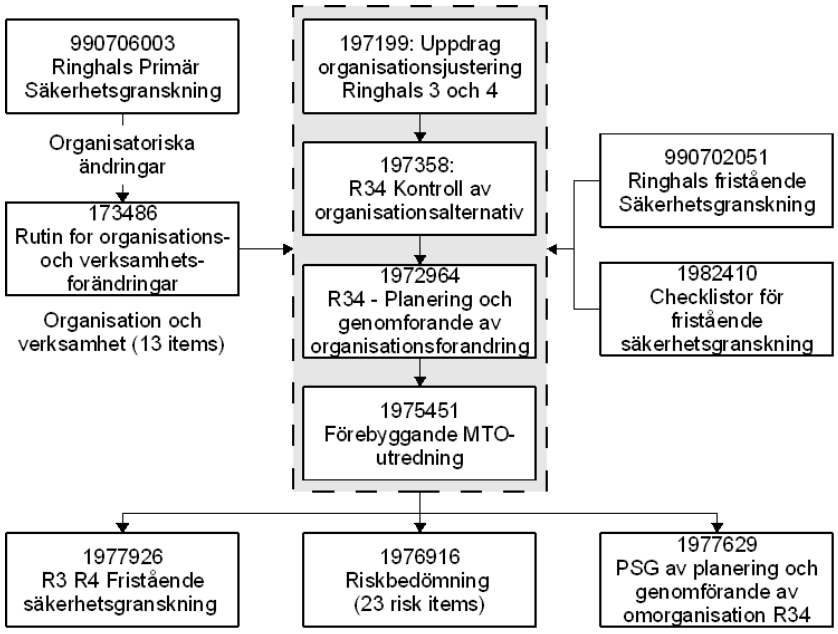

Figure 8: Risk assessment of organisational change (R34)

5. A Resilience Engineering Approach to Risk Assessment

As described in the *Background* section of this report, risk assessment of both human factors and organisations grew out of the risk assessment of technical systems. The optimistic hope that new sources of risk could be addressed by traditional methods has, however, turned out to be futile. Although the use of linear models and cause-effect thinking is still firmly entrenched in practice, numerous real-life cases have shown that neither human factors nor organisational factors can be adequately addressed by relying on the principles developed to deal with technical problems. The main reason is that risks in socio-technical systems cannot be assigned to identifiable parts of the systems' structure (people or social groups). Instead, the risks must be seen in relation to the systems' functions. The systemic perspective acknowledges that risks are not always *resultant*, i.e., ascribable to component failures – where components may be human and organisational as well as technical. Instead, risks may be *emergent*, i.e., due to coincidences or unintended couplings among events and activities that are not in themselves wrong.

An organisation can quite generally be defined as is a social arrangement of people that pursues collective goals, that controls its own performance, and that has a boundary separating it from its environment. The collective goals may in some cases be the same as individual goals, but the individuals often have to accept collective goals that are not originally their own. The organisation can control its own performance in the traditional sense of being anti-entropic. This means an organisation is able to maintain order in the face of disruptive influences, specifically that it can respond in an appropriate manner to what happens, as well as prepare itself to respond before something happens. Organisations have traditionally been described in terms of their 'components,' and in term of the roles of the people who effectively make up the organisation. The traditional organisational 'components' are divisions, departments, groups, offices, etc., and represent a hierarchical structure. The boundaries are therefore defined in terms of how people are grouped together, often with reference to the organisational chart or diagram. An example of that is the new organisation for Ringhals 3 and Ringhals 4, which in Figure 9 is shown in a way that emphasises the hierarchical structure.

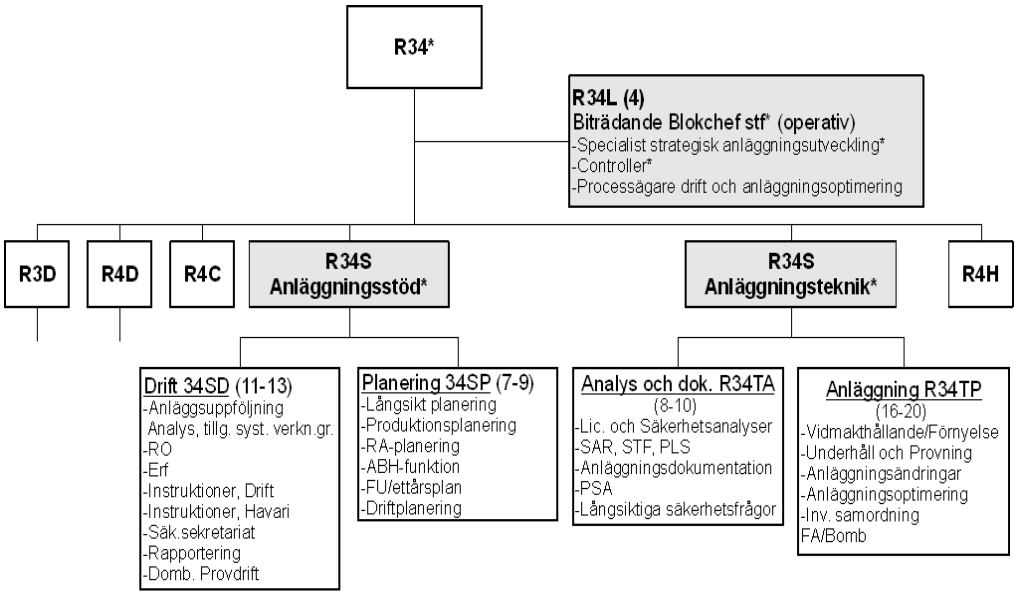

Figure 9: Details of the new organisation for R3 & R4

Consider, for instance, *R34S Anläggningsstöd*, which is divided into *Drift 34SD* and *Planering 34SP*. Both *Drift* and *Planering* are further described in terms of a number of competence areas or types of functioning, e.g., *långsikt planering*, *produktionsplanering*, etc., and are also characterised by how many people they require.

It is, however, also possible to describe an organisation in terms of the functions it requires in order to achieve its goals. This is in good agreement with the definition of an organisation, which emphasises the ability to pursue (collective) goals and to control (its) own performance. The view of functions starts from what an organisation *does* rather than from what it *is*, hence pays little attention to the organisation's structure. The arrangement is therefore one of how functions relate to each other rather than of how organisational 'components' are configured. From this perspective an organisational change affects how functions are *carried out*, rather than where functions are *allocated*. Risk assessment similarly becomes a question of whether it is possible to carry out the required functions in an adequate manner, rather than a question of whether a function may fail or go wrong.

5.1. The Functional Resonance Analysis Method

The Functional Resonance Analysis Method (FRAM; Hollnagel, 2004) describes system failures (adverse events) as the outcome of a functional resonance arising from the variability of normal performance. The method refers to a model or a representation of individual and/or organisational functions, where the characteristics of each function provide the basis for describing its potential variability.[4] The resonance principle is invoked to explain how disproportionately large effects may arise from small or even insignificant variations, and the emphasis is on dynamic dependencies rather than failure probabilities. The couplings among functions are described in terms of six dependency relations (input, output, time, control, pre-conditions, and resources) and are potential rather than actual, i.e., there are no pre-defined cause-effect relations. The dependency relations can be used to determine whether it is possible for two functions to become coupled, depending on the performance conditions. In this way it is possible to identify both intended and unintended couplings. In the case of accident investigation this can be used to find where coincidences may have arisen (e.g., Nouvel et al., 2007; Sawaragi et al., 2006); in the case of risk assessment this can be used to explain how coincidences may arise from performance variability, hence to identify the potential risks in a given situation.

Since it was first proposed (Hollnagel, 2004), the FRAM has been applied in several domains, such as healthcare, air traffic management, aviation, and off-shore operations. An illustrative example from the nuclear domain was provided by Hollnagel & Nygren (2006). The procedure for using the model has been clearly described (Woltjer & Hollnagel, 2007) and some of the initial steps of the method can be facilitated by software tools.

5.2. Principles of FRAM

Resilience Engineering provides a practical basis for the development of systemic models in order to describe the characteristic performance of a system as a whole, rather than either the cause-effect mechanisms of the simple linear models or the epidemiological factors of the complex linear models (Hollnagel, 2004). The purpose of a systemic model is to describe the dynamic and non-linear nature of interactions within a system. This represents a necessary development of the traditional view where accidents are described either as sequences or as concatenations of latent conditions. The Functional Resonance Analysis Method

[4] Although the descriptions often focus on humans and human behaviour, it is equally relevant for organisations, cf., the definition of an organisation as an aggregation of people.

has a clearly articulated theoretical basis, which can be explained in terms of the following four principles.

First principle: The equivalence of success and failures

Resilience Engineering represents a way of thinking about safety that emphasises a system perspective. Whereas established risk management approaches are based on hindsight and emphasise error tabulation and calculation of failure probabilities, Resilience Engineering looks for ways to enhance the ability of organisations to create processes that are robust yet flexible, to monitor and revise risk models, and to use resources proactively in the face of disruptions or ongoing production and economic pressures. In Resilience Engineering failures do not stand for a breakdown or malfunctioning of normal system functions, but rather represent the converse of the adaptations necessary to cope with the underspecification that is a consequence of real world complexity. Individuals and organisations must always adjust their performance to the current conditions; and because resources and time are finite it is inevitable that such adjustments are approximate. Success is a consequence of the ability of groups, individuals, and organisations to anticipate the changing shape of risk before damage occurs; failure is simply the temporary or permanent absence of that.

Resilience is defined as the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions. In all of these the contribution of the human is crucial. By recognising the human as an asset rather than as a liability, Resilience Engineering advocates a proactive approach to safety that is well suited to overcome the problems associated with complex systems. The Resilience Engineering view of performance variability can be summarised by the following four points:

1. Both normal performance and failures are emergent phenomena and have a common source (variability of normal performance).
2. The outcomes of actions may sometimes differ from what was intended, expected or required. The difference can either be beneficial or harmful.
3. The adaptability and flexibility of human work is the reason for its efficiency.
4. The adaptability and flexibility of human work can, however, also be the reason for the failures that occur, although it is rarely the cause of such failures.

Adopting this view means that there is a need for models that can represent the variability of normal performance and methods that can use this both to provide more comprehensive explanations of accidents and to identify the possible risks.

Second principle: The inevitability of approximate adjustments

In a systemic perspective, the variability of a system's normal functioning is due to two basic facts.

- First, that the operating conditions usually are underspecified, hence rarely, if ever, as imagined or as prescribed. This is a consequence of the intractability of socio-technical systems. It means that it is practically impossible to prepare instructions in advance that are so detailed that they can be followed to the letter. The solution is instead to provide guidelines and procedures that can be used as a basis for concrete actions. Guidelines and procedures are usually supported by extensive professional training.
- Second, that the operating conditions are dynamically changing in a more or less orderly manner. The changing conditions mean that it is practically impossible to have precise procedures prepared in advance. It also means that people who are supposed to act in a situation, be they managers or operators, only can plan with certainty for the short-term. They must constantly be ready to revise their plans and to adjust the implementation of plans to match the current conditions.

This variability is not just something that characterises the actual operation of the system, but something that exists throughout its lifetime – from the beginning of the life cycle to the very end. To get anything done humans must always adjust their performance to the current conditions. Humans are fortunately extremely adept at finding effective ways of overcoming problems at work, and this capability is crucial for safety. Indeed, if humans always resorted to follow rules and procedures rigidly in cases of unexpected events, the number of accidents and incidents would be much larger. Human performance can therefore at the same time both enhance and detract from system safety. Assessment methods must be able to address this duality.

Performance adjustments are always necessary, and because resources and time are finite it is inevitable that such human adjustments are approximate. Approximate adjustments that coincide and combine to create an overall instability can become the reason why things sometimes go wrong. To the extent that performance variability has been considered by safety assessments, it has primarily been used to understand operations that have gone wrong (operational failures). But it can

equally well be applied to design, construction, testing, maintenance, modification, and decommissioning. Design failures and latent conditions, for instance, can be seen as an outcome of performance variability at the respective stages of the system's life.

Third principle: Consequences are emergent

The variability of normal performance is rarely large enough in itself to be the cause of an accident or even to constitute a malfunction.[5] But the variability of multiple functions may combine in unexpected ways, leading to consequences that are disproportionally large, hence produce non-linear effects. Both failures and normal performance are emergent rather than resultant phenomena, because neither can be attributed to or explained by referring only to the functions or malfunctions of specific components or parts. Socio-technical systems are intractable because they change and develop in response to conditions and demands. It is therefore impossible to describe all the couplings in the system, hence impossible to anticipate more than the most regular events.

Referring to the definitions of tractable and intractable systems given above, we can see that tractable systems usually are associated with resultant outcomes, while intractable systems are associated with emergent outcomes. An outcome is classified as resultant if it can be explained by referring to the properties of the components of the systems that produce it. That is tantamount to saying that the system is tractable, i.e., that descriptions are simple with few details and that the principles of functioning are known. An outcome is likewise classified as emergent if it is not predictable from knowledge of the system's components, and if it is not decomposable into those components. That is tantamount to saying that the system is intractable, i.e., that descriptions are exceedingly detailed and that the principles of functioning are partly unknown.

Fourth principle: Functional resonance

As a systemic approach, FRAM overcomes the intrinsic limitations of established methods by focusing on the relationships between system functions. FRAM also replaces the traditional cause-effect relation by the principle of resonance. This means that the variability of a number of functions every now and then may resonate, in the sense that they may reinforce each other and thereby cause the variability of one function to exceed normal limits. (The outcome may, of course,

5 That there is a variability of normal does not mean that there is a normal performance variability. The criteria for how much variability is acceptable depends on the nature of the activity and the work conditions.

be advantageous as well as detrimental, although the study of safety for natural reasons has focused on the latter.) The consequences may spread through tight couplings rather than via identifiable and enumerable cause-effect links, e.g., as described by the Small World Phenomenon (Travers & Milgram, 1969). The resonance analogy emphasises that this is a dynamic phenomenon, hence not attributable to a simple combination of causal links. This principle makes it possible to capture the characteristic dynamics of the system's functioning (Woltjer & Hollnagel, 2007), hence to identify emergent system properties that cannot be understood if the system is decomposed into isolated components.

6. Description of the Functional Resonance Analysis Method

In its present form, the method comprises the following five steps.

1. The first step is the definition of the purpose of the analysis since FRAM has been developed to be used for both accident investigation (looking at past events) and safety assessment (looking at future events).
2. The second step is the identification and description of system functions. A function, in FRAM terms, constitutes an activity which has important or necessary consequences for the state or properties of another action.
3. The third step is the assessment and evaluation of the potential variability for each singular function. The proposed methodology uses an *a priori* assessment of a set of Common Conditions (CCs) that have an influence on the function's performance variability. The Common Conditions are derived from the Common Performance Conditions (CPC) described by Hollnagel (1998). This evaluation should be integrated with the retrospective information extracted from accident database to the extent that data are available.
4. Step four is the identification of functional resonance. The aim of this step is to determine the possible ways in which the variability from one function could spread in the system and how it may combine with the variability of other functions. In case of functional resonance, the combinations of variability may result in situations where the system loses its capability safely to manage variability. The propagation may be both direct via the output from a function, and indirect via the effects that the variability may have on the CCs.
5. The fifth and last step in a FRAM analysis is the identification of effective countermeasures to be introduced in the system. In FRAM prospective, countermeasures aim at dampening performance variability in order to maintain the system in a safe state. But it is consistent with the principle of Resilience Engineering to consider also measures that can sustain or amplify functional resonance that leads to desired or improved outcomes.

The following sections provides an outline of how FRAM can be used to make a risk assessment of an organisational change. As the presentation will show, FRAM requires information that is not available in the chosen case. The reason for that is simply that FRAM highlights issues that are not covered by established approaches, hence lead to other questions. Because of this it is not possible in this report to be very concrete about the actual organisational change. To compensate

for that, more emphasis will be put on describing in detail the steps required to model and to evaluate performance variability using the FRAM.

6.1. Step 1: Define the Purpose of the Analysis

The first step is the definition of the purpose of the analysis. As already mentioned, FRAM can be used both as an accident investigation method and as safety assessment method. Although the major steps of the method are the same, some details needed for accident investigation will differ from the details needed for a risk assessment. For example, for something that has happened, the performance conditions will be known. Whereas for future events, the likely performance conditions must be estimated. It is therefore necessary clearly to state which of the two aspects of safety management the method is going to be used for. In the present description, the focus is on risk assessment of an organisational change, i.e., looking into possible future events. Once this objective has been established the following steps should be performed in order to identify and evaluate the risks.

6.2. Step 2: Identification and Description of Relevant System Functions

The system identification and description of the relevant system functions takes place through the following substeps.

- The first substep is the choice of the overall functionality or performance that will be the focus of the analysis. Since this study refers to an organisational change where the outcome was a common organisation of Ringhals 3 and Ringhals 4, the focus is nominally the functioning of this new organisational unit. The study case did, however, not specify any organisational functions in detail. But from a general point of view, *planning* is clearly an important function, and it was therefore chosen as the focus for the FRAM risk assessment.
- The second substep of the system identification is the determination of the system's boundaries. Since the FRAM considers functions rather than structures (or objects), there are not 'natural' boundaries, such as those resulting from the physical characteristics of humans and machines or the physical delineation of an industrial plant. The boundaries must reflect the focus of the study, in particular the scope of the analysis. The FRAM allows the analyst to expand the boundary as needed, by including additional functions in the description at a later point in time. (The boundary can obviously also be retracted by removing functions from consideration.) An analysis will usually begin by a set of functions that from a common sense

perspective is relevant for the focus. This set will typically be modified during the initial stages of the analysis, for instance by using task analysis or by interviewing the people who do the work, but will sooner or later converge on the set of functions that, for the parties involved in the analysis, represents the overall functionality that is the focus of the analysis.

Even though one of the new organisational units resulting from the change is dedicated to planning (*Planering 34SP*) it does not mean that the boundary for the analysis is the same as the organisational boundary for this unit, i.e., the 'box' in Figure 9. Planning is something that happens in several places in the organisation, and which cuts across the formal organisational boundaries. Planning is, for instance, also included in the job description for both for the *Specialist strategisk anläggningsutveckling* and the *Verksamhetscontroller* who part of R34L (4) (cf. Figure 9).

- The third substep of the system identification is to choose a level of detail, or degree of resolution, for the function description. The rough guideline is also here to begin with a level of detail that makes sense vis-a-vis the activity or performance being considered. In principle, this should be the level at which the variability of a function has an impact – for instance that the possible failure modes, should something go wrong, are meaningful in terms of the actual performance. In the current study, the descriptions in the documents provided by RAB were on a rather high level, and the initial analysis will therefore remain on that level. It is, however, something that can be revised if a more detailed analysis is carried out at a later time.

6.2.1. Function identification

Once the focus and level of the modelling have been determined, the system functions have to be identified. The principle that guides this is the need to achieve a description of the normal activities performed by the socio-technical system being analysed. It is therefore necessary that the functions are described without any judgement about the possible quality or correctness of their outputs, e.g., whether they represent a possible risk. For the identification of the functions it is often useful to start from a task analysis or from the official documents of the interested organisation, e.g., procedures. The information gathered in this way needs to be integrated with the contribution of the domain experts. Only the personnel actually involved in the daily work activity, from managers to operators, have the appropriate knowledge about how they perform their tasks in a specific situation. The process of function identification is essential to assure the quality of the resulting system modelling. Several iterations may be needed until a clear and common understanding of the functioning of the socio-technical system has been reached.

After the initial function identification has been made, it is possible to go on with the next step, the characterisation of each function. This does not preclude that the set of functions is modified at a later point in time. The FRAM is a modular approach where it is easy to make modifications to the model. The FRAM is used to produce a model description of a case, rather than a structured representation such as a diagram. The difference between the FRAM model and the instantiations of the model will be discussed below.

In the study case, the planning functions is not described in detail. While several types of planning are mentioned (e.g., *Långsikt planering, Produktionsplanering, RA-planering, ABH-funktion, FU/ettårsplan, Driftplanering*), the more precise contents of this planning is not mentioned. This is probably because the planning as such is not meant to change, only the allocation of planning to an organisational unit. In the document *1972964* it is simply mentioned that:

En separat grupp i enheten Anläggningsstöd bildas med fokus på planering på kort och lång sikt.
Planeringsgruppen hanterar blockens planering på kort och lång sikt inklusive driftplanering. I ansvaret ingår att aven utveckla och hantera ABH-funktionen.

The study therefore simply started by considering the single, but high-level, function of planning.

6.2.2. Function description

Following the function identification the safety assessment proceeds by characterising each function in terms of six aspects or parameters, namely Input, Output, Preconditions, Control, Time and Resources. Hollnagel (2004) defines the six parameters in the following terms:

1. Input (I): that which the function processes or transforms or that which starts the function,
2. Output (O): that which is the result of the function, either a specific output or product, or a state change,
3. Preconditions (P): conditions that must be exist before a function can be executed,
4. Resources (R): that which the function needs or consumes to produce the output,
5. Time (T): temporal constraints affecting the function (with regard to starting time, finishing time, or duration), and
6. Control (C): how the function is monitored or controlled.

The description of each function is made by using a simple table format, which then becomes the basis for the further analysis. It is also this description, rather than the graphical representation, that constitutes the FRAM model. It is indeed very important not to confuse the FRAM model with the graphical representation of FRAM. The representation is typically in the form of a diagram showing functions as hexagons and the connections between them as lines. However, unlike fault trees and event trees, the analysis is not made on the basis of the diagrams but on the basis of the descriptions of the functions. The characterisation of the functions, in terms of the six aspects, contains the potential couplings among functions. The following steps in the analysis can show which of these potential couplings may become actual couplings, i.e., become realised or instantiated under given conditions. If we take the (initially) single function of planning, the analysis can begin by considering possible descriptors for the six parameters.

Table 5: Description of the 'planning' function

Function	**Planning**
Input (I)	A request for a plan. This can be a regular request, as in the case of an *ettårsplan*, and in principle this request can be generated internally in the planning function. It can also be an external request, e.g., for an outage, unexpected maintenance work, etc.
Output (O)	The output is generically speaking a plan. There may, however, be several types of output, corresponding to, e.g., *Långsikt planering, Produktionsplanering, RA-planering, ABH-funktion, FU/ettårsplan,* or *Driftplanering.* It may well be that a continued analysis finds it necessary to define several different planning functions.
Preconditions (P)	The most important pre-conditions is probably that there is sufficient information available about the situation for which the plan is needed.
Resources (R)	There are several resources needed for the planning function, and some of these may be unique to the type of plan being produced. Some obvious resources are manpower, ***competence***, computer support, and information.
Time (T)	There is usually a time criterion for planning, in terms of a deadline, i.e., a time when the plan must be delivered. In some cases this deadline may be predictable, in other cases not. In the case of simultaneous requests, there may also be limited time available to develop a plan for each request, which again may be a part consequence of limited resources (manpower).
Control (C)	In cases where planning is a routine activity (e.g., ABH), some controls may be possible in the form of checklists. In cases where planning is a non-routine activity, e.g., in case of a disturbance, there are probably no direct controls.

To illustrate how the function identification can take place, consider the 'resources' parameter of 'planning.' This mentions two kinds of resources that easily can be seen as the outcome of another function. One resources is 'manpower,' which presumably is ensured by another organisational function at a higher level (perhaps as close as *R34L*?). A second resource is 'competence', which one can describe as the output of a function called 'training.' Even though there are no specific details about 'training' in the documents describing the organisational change, it is possible to propose the following generic description. (*Kompetensutveckling* is mentioned as a part of *R3D Drift* and *R4D Drift*, but this presumably refers to the competence for the control room operators, rather than for the competence of the people working in *34SP*.)

Table 6: Description of the 'training' function

Function	**Training**
Input (I)	The input can be a request for training or a more regular training schedule.
Output (O)	The output is generically speaking ***competence***, i.e., the ability effectively to do a specific job. The competence may possibly be described in further detail as specific skills or particular knowledge for one or more individuals.
Preconditions (P)	There are no obvious preconditions for training.
Resources (R)	One resource is a training curriculum. Another is, almost paradoxically, that there are competent instructors.
Time (T)	There is usually a limited time set aside for training, e.g., a norm for the training module. This is, however, rarely a problem since training normally is a regular activity rather than one-of-a-kind, hence adapted to the available time.
Control (C)	Training is usually controlled by some kind of test or examination, i.e., a control of the final product. There may also be intermediate controls, if the training is extensive.

6.2.3. FRAM model

The description of system's functions achieved in the previous step constitutes the FRAM model of the system. A FRAM model differs from the classical models, such as fault trees and event trees, by the fact that the model is not the *diagram* or the flowchart, but the *description* of the functions in terms of the six aspects or characteristics. The fact that a FRAM model does not include the actual links

between the elements makes it possible for the analysts to generate a set of instantiations to show the effect that the context (working conditions) can have on the system's performance. Classical models like fault trees and event trees show a single representation of the system, which depicts one set of possible cause-effect relations. In such analyses, the propagation of an event is therefore constrained by the links in the diagram. In FRAM, no such constraints exist.
The description of the six aspects or parameters is generally straightforward but can, in the spirit of the method, always be refined at a later stage of the analysis. When completed, the tabular description defines a set of potential couplings among functions.

6.2.4. FRAM instantiation

When all the functions have been described, the next step is to identify the couplings between the functions. This is achieved by linking together the functions according to the description provided by the tables. The result constitutes a FRAM instantiation of the system, and is often shown graphically. The instantiation of the table-based description shows the normally functioning system. This instantiation can be used as the basis for taking into consideration the effect of the variability of functions and how this may create outcomes that propagate through the system. The variability of functions may also lead to unexpected couplings arising, as well as to expected couplings becoming dysfunctional.

In the FRAM instantiation, the links represent the dependencies among the functions as defined by the six characteristics rather than cause-effect relations or causal flows. Neither does the relative position of the functions in the graphical representation represent a temporal sequence or ordering, nor suggest cause-effect relations. For the purpose of illustration only, the representation of the two functions described above is shown in Figure 10.

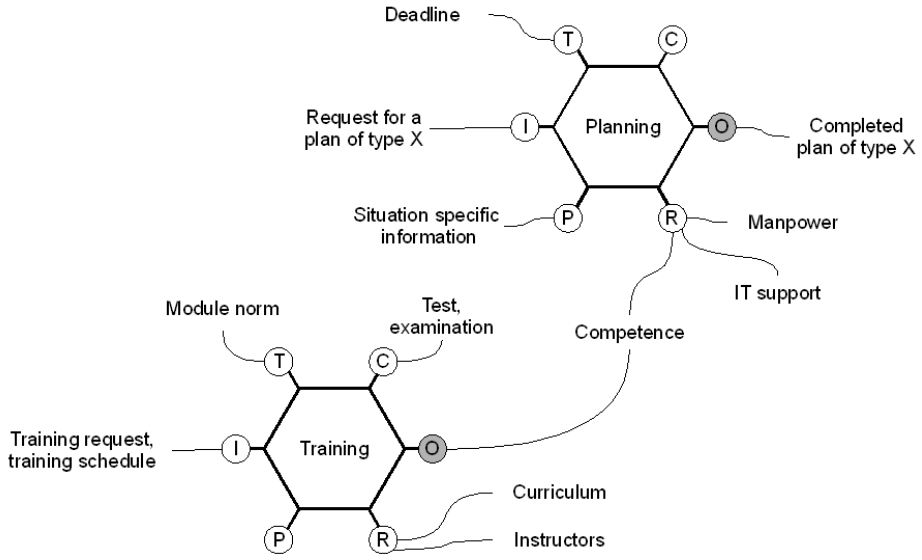

Figure 10: Example of FRAM instantiation

6.3. Step 3: Assessment of Potential Performance Variability

The change from first to second generation HRA methods emphasised that the context was by far the most important factor in shaping performance and creating risks, and that the consequences of this dominated any human error probability, whether hypothetical or real. In FRAM, the performance conditions affect the variability of the functions, in the sense that detrimental performance conditions will increase performance variability while advantageous performance conditions on the whole will reduce it.[6] In order for this change in perspective to be practically useful, it is necessary to understand the origin and nature of performance variability.

As already mentioned, performance variability, in the form of habitual and/or intentional adjustments of performance, is necessary because performance conditions as a rule are underspecified. Performance variability is, however, on the whole a strength rather than a liability and is the primary reason why socio-technical systems work as well as they do – or work at all. The human ability to find effective ways of overcoming problems at work is therefore crucial for safety.

6 Advantageous and detrimental are here used to refer to the performance variability, not the outcome of the activity.

Assessment methods must be able to address both how this can succeed and how it can fail.

In addition to the variability coming from intentional or habitual performance adjustments, performance variability is also the result of a number of internal and external factors. The six main sources of human and organisational performance variability are:

1. Fundamental human physiological and/or psychological characteristics. Examples are fatigue, circadian rhythm, vigilance and attention, refractory periods, forgetting, associations, etc.
2. Pervasive higher level psychological phenomena such as ingenuity, creativity, and adaptability, for instance in overcoming temporal constraints and underspecification.
3. Organisational conditions and requirements, as the need to meet external demands (quality, quantity), stretching resources, substituting goals, etc.
4. Social or team psychological factors, such as meeting expectations of oneself or of colleagues, complying with group working standards, etc.
5. Context variability (ambient working conditions), for instance if the working conditions are too hot, too noisy, too humid, etc.
6. Work environment variability induced by the unpredictability of the domain, e.g., weather conditions, number of flights, pilot variability, technical problems, etc.

6.3.1. Common Conditions

As described by the second FRAM principle, people must adjust their activity to the working conditions or context in order to accomplish their tasks. This adjustment results in a variability of the way in which each function is performed. In order to evaluate the overall human performance variability it is necessary first to consider each function in order to understand how likely it is to vary, and then to consider the interdependence of the functions.[7] The variability may, for instance, lead to a function being carried out even if the pre-conditions are not fulfilled, which in turn may affect other functions. It may also lead to an output failure mode, as described below. The methodology that has been chosen to represent the effect of the context on performance makes use of the Common Conditions. The set of proposed CCs is presented and discussed here below.

[7] In the present case this is partially a moot question, since only two functions have been described.

- **Availability of resources.** Adequate resources are necessary for stable performance, and a lack of resources increases variability. The resources primarily comprise *personnel*, *equipment*, and *material*. Time is in principle also a resource, but since it has a very special nature, it is treated separately.
- **Training and experience (competence).** The *level* and *quality of training* together with the *operational experience*, determines how well prepared people are for various situations, hence how variable their performance will be. According to Mintzberg (1982) training is the learning process that allows humans to gather the knowledge to perform a specified activity. The purpose of training is to adjust and modify operators' behaviour in order to increase their performance and therefore correctly execute their tasks. Training is particularly relevant in case of the introduction of a new task or of a new tool and in case of a change in the working system. Along with training, the working experience that operators have is crucial to achieve a high performance (McGregor, 1969).
- **Quality of communication**, both in terms of *timeliness* and *accuracy*. This refers both to the *technological aspects* (equipment, bandwidth) and the *human or social aspects*. Communication issues are crucial for the pursuit of high-quality performance through the interaction of humans and technology. Communication is defined as the collective interactive process of generating and interpreting messages (Stohl, 1995). The greater the level of system autonomy, complexity and number of components, the greater will be the need for communication and coordination among users and between users and systems to foster observability and awareness of the socio-technical systems and tasks (Woods et al., 1997).
- **HMI and operational support**. This refers to the human/machine interaction in general, including *interface design* and *various forms of operational support*. The HMI is known to have a significant influence on performance variability. A number of factors related to the HMI are known for how they can affect performance, such as feedback quality and feedback control loop, information display, decision making support, etc. (Bastien et al., 1993).
- **Availability of procedures and plans**. The *availability of procedures and plans* (operating and emergency procedures), and *routine patterns of response* affect the variability of performance. Operators use procedures and plans as the reference point for their routine activity. In case of an emergency, procedures are needed to support the response behaviour to degraded situations. In both cases the availability, quality and precision of procedures result in a different level of expected performance by operators.
- **Conditions of work**. The features of the working environment have an influence on the performance. An appropriate working environment may positively impact performance; on the other hand, inadequate working

conditions may create constraints for work that result in a decrease of performance. In the human factors literature a number of factors have been described as influencing human performance, such as ambient lighting (Boyce, 2006), noise (Casali, 2006), temperature (Parsons, 2005), workplace design (Marmaras & Nathanael, 2006), etc.

- **Number of goals and conflict resolution**. The *number of tasks* a person must normally attend to and the rules or principles (criteria) for conflict resolution.

  The Human Factors literature concerning the relation between workload and performance shows that in case of excessive mental workload, defined as the need to manage a large number of goals or to work at several different tasks at the same time, will result in a degradation of performance. This effect is understandable taking into consideration that human mental – and psycho-motor – capacity is limited and that therefore they only can deal with a small number of tasks and objectives at the same time. Conversely, it is also generally assumed that performance can degrade in situations where mental workload is very low, although this assumption may not be fully warranted (Dekker & Hollnagel, 2004).
- **Available time and time pressure**. The *time available to carry out a task* may depend on the synchronisation between task execution and process dynamics. Lack of time, even if subjective, is likely to decrease performance standard. The lack of time is one of the main sources for psychological stress for humans and may lead to a reduction of the quality of performance (Cox & Griffiths, 2005).
- **Circadian rhythm and stress**, i.e., whether or not a *person is adjusted to the current time*. Lack of sleep or asynchronism can seriously disrupt performance. The biological rhythm of human beings follows a cycle organised on the base of 24 hours. This cycle is maintained autonomously by the human nervous system but can be affected by external factors such as the environment or socio-professional factors (Sherrer et al., 1992)
- **Team collaboration quality**. The *quality of the collaboration* among team members, including the overlap between the official and unofficial structure, *level of trust* and *general social climate*. This comprises a set of interrelated knowledge skills/behaviours and attitudes that, taken together, form the competences necessary for effective team performance (Salas et al., 1992) knowledge includes: knowledge of team objectives, cue/strategy associations and team-mate familiarity skills include: assertiveness, shared situational awareness and conflict resolution attitudes include: mutual trust, team cohesion and collective orientation these sets of competences, together with team leadership, mutual performance monitoring, back-up behaviour, and adaptability/flexibility, form the core foundation for teamwork (Salas et al., 2000).

- **Quality and support of the organisation**. This comprises the quality of the *roles and responsibilities of team members, safety culture, safety management systems, instructions,* of *guidelines for externally oriented activities*, and the *role of external agencies*. The adequacy of the organisation refers to the matching of the actual requirements of work ('what needs to be done') to the formal structure of work ('how work is organized'). The correspondence between those two elements is a measure of adequacy. Audits are defined as 'a systematic and independent examination to determine whether the company's activities comply with planned arrangements and whether these arrangements are implemented effectively and are suitable to achieve the objectives' (Kuusisto, 2000). As such, audits can be seen as measuring tools of the adequacy of the organisation, and various types of audits have been developed.

  Kuusisto lists six types of audits: (1) on specific topics; (2) plant technical; (3) site technical; (4) compliance; (5) validation; and (6) management safety. Safety indicators may also be used to measure the adequacy of the organisation. Poor levels of performance, such as high number of accidents or failure to obtain/renew certifications, are good indicators of inadequacy. Hopkins (2009) classifies indicators along two dimensions: time (leading and lagging) and hazards (personal and process). In recent times, researchers have pursued the development of 'organisational culture' and 'safety culture' assessment tools (Reiman, 2007). Such tools, often taking the format of quantitative and qualitative surveys, also provide information about the adequacy of the organisation.

6.3.2. Performance Variability as a Function of Performance Conditions

Table 7 provides information that can be used to determine whether a function is likely to vary given specific working conditions. For a given scenario and a given set of assumptions, each CC is first rated as either 'adequate,' 'inadequate,' or 'unpredictable.' This rating is then used to determine the likely performance variability of a function.

Table 7: Likely performance variability as a function of Common Conditions

	Adequate	Inadequate	Unpredictable
Availability of resources (personnel, materials, equipment)	Small	Noticeable	High
Training and experience (competence)	Small	High	High

Quality of communication (team, organisation)	Small	Noticeable	High
Adequacy of HMI and operational support	Small	Noticeable	High
Availability of procedures and methods	Small	Noticeable	High
Conditions of work	Small	Noticeable	High
Number of goals and conflict resolution	Small	High	High
Available time, time pressure	Small	High	Very high
Circadian rhythm, stress	Small	Noticeable	High
Team collaboration quality	Small	Noticeable	High
Quality and support of the organisation	Small	Noticeable	High

(For example, if 'conditions of work' are adequate, performance variability is assumed to be small. If 'conditions of work' are inadequate, performance variability is assumed to be noticeable. And if finally 'conditions of work' are unpredictable, performance variability is assumed to be high.)
In the case of the organisational change considered here, it is clearly reasonable to expect that Common Conditions shortly after the change has been made will be different from the Common Conditions after a longer period when the situation is more stabilised.[8] For a risk assessment it may nevertheless be more interesting to consider the conditions shortly after the change, since it is likely that the risks will be greater then.
In the case of the change at RAB, the performance conditions can be estimated from the descriptions given by the document *1976916*. On this basis, the following assignment can be proposed. (The assignment is, of course, open to discussion, and should in this report mainly be seen as an illustration of how the method works.)

Table 8: Likely performance conditions shortly after the organisational change

	Rating	Justification (see Table 4)
Availability of resources (personnel, materials, equipment)	Inadequate	Risk number 11, 21
Training and experience (competence)	Inadequate	Risk number 19
Quality of communication (team, organisation)	Inadequate	Risk number 8, 20
Adequacy of HMI and operational support	Adequate	
Availability of procedures and methods	Adequate	

8 It may, of course, happen that organisational changes occur so frequently that work never reaches a stable condition.

Conditions of work	Adequate	
Number of goals and conflict resolution	Adequate	
Available time, time pressure	Inadequate	Risk number 13
Circadian rhythm, stress	Adequate	
Team collaboration quality	Adequate	
Quality and support of the organisation	Adequate	

6.3.3. Performance variability of specific functions

Since functions can be very heterogeneous, it stands to reason that they are not all affected by the CCs in the same way. The determination of whether a function is likely to vary given specific working conditions must therefore take place in two steps. The first step is to characterise the susceptibility of a function to a given CC. In order to make things simple, it is reasonable to begin by applying the three categories of human (M), Technology (T), and organisation (O).

- Functions that depend mainly on the people carrying them out, and which therefore are affected mostly by the variability of people (as individuals), should be classified as M (for 'huMan') functions. Functions such as 'planning' clearly belong to this category.
- Functions that depend mainly on the technology by which they are implemented, and which therefore are affected mostly by the variability of technologies, should be classified as T (for 'technology') functions. An example would be an automated warning system.
- Functions that depend mainly on the organisation, directly or indirectly, and which therefore are affected mostly by the variability of the organisation, should be classified as O (for 'organisation') functions. The function 'training' belongs to this category.

The assignment of a function to one of the MTO categories should be done by the analysis team involved, and should be as completely and as conscientiously as possible. In the current case, *planning* is clearly an M-function.
This step of the method is completed by marking how functions belonging to each of the MTO categories are affected by the CCs, i.e., to determine the relevant CCs for each function. This can be done by using the mapping shown in Table 9.

Table 9: Match between MTO categories and Common Performance Conditions

	Functions affected		
	M	T	O
Availability of resources	X	X	
Training and experience (competence)	X		
Quality of communication	X		X
HMI and operational support	X		
Access to procedures and plans	X		
Conditions of work	X	X	
Number of goals and conflict resolution	X		X
Available time and time pressure	X		X
Circadian rhythm and stress	X		
Team collaboration quality	X		
Quality and support of the organisation			X

Since the function in question is an M-function, Table 9 indicates that it is affected by all CCs except 'quality and support of the organisation.' According to Table 8, four of these CCs are evaluated as being inadequate.

The next step is for each function to determine the effect of the relevant CCs. Since the purpose is to find out whether a given function is likely to vary under given conditions, it is sufficient to use a disjunctive criterion. As a starting point, the following rules can be applied:

Rule #1 If, for a given function, any of the relevant CCs are rated as 'inadequate,' then the variability of that function shall be assumed to be 'noticeable' or 'high,' depending on the rating of the CC in Table 8.

Rule #2 If, for a given function, any of the relevant CCs are rated as 'unpredictable,' then the variability of that function shall be assumed to be 'high,' 'very high,' depending on the rating of the CC in Table 8.

This assignment should be made for the initial conditions when the analysis begins, i.e., the normal functioning. Since, however, the value of the CCs may change as

the scenario develops, it is necessary to update the assignment as the propagation of variability is pursued for an instantiation of the model. This should be done in accordance with the principles outlined above, although the practical details will have to be tested and refined through an actual application of the method.

In the current case, four of the CCs for 'planning' were rated as 'inadequate.' These were 'availability of resources,' 'training and experience,' 'quality of communication,' and 'available time, time pressure.' For two of these, 'training and experience' and 'available time, time pressure,' the likely performance variability was rated as 'high.' In accordance with Rule #1, it is therefore possible that the performance variability of the planning function will be high. This may by itself constitute a risk.

6.4. Step 4: Identification of Functional Resonance

In FRAM, the variability of a function can have consequences in two different ways. One is through the quality of the output from a function. This is analogous to the various possible failure modes (or manifestations) of the output, i.e., the various ways in which the output can differ from what was intended and expected. The failure modes can be characterised as shown in Table 9. The characterisation of outputs in terms of failure modes supports the evaluation of the downstream influence of the variability of a function. As an example, if the output of a function comes *too late*, it will result in a reduction of the time that is available for the other functions to produce their output.
The other way that the variability of a function can have consequences is that performance variability may lead to a change in one or more CCs. Increased variability may, for instance, lead to an increased use of resources, to an increase in the number of goals, or to less time being available. This can establish a second-order feedback, as described by Maryuama (1963). Taken together, this makes it possible to account for both the direct coupling among functions and the influence on common performance conditions. In practice, this will be too complex to be done manually, and determining the propagation of variability should therefore be supported by some kind of software tool.

Table 9: Dimension of failure modes

Timing	Too early / Too late / Omission
Duration	Too long / Too short
Sequence	Reversal / Repetition / Commission / Intrusion
Object	Wrong action / Wrong object
Force	Too much / Too little
Direction	Wrong direction
Speed	Too fast / Too slow
Distance	Too far / Too short

In the case of the planning function, possible failure modes are timing and object. This means that a plan can either be delivered too late or not at all, and that a plan may be incorrect (wrong object). Either of these failure modes may clearly have consequences for the downstream functions that use them as either input or control. In the first case it may be impossible to begin an activity in time because the plan is delayed; a plan may be either an input or a precondition for another functions. At a place of work as complex as a nuclear power plant, this may obviously lead to other consequences. In the second case a function or an activity may be carried out incorrectly if the plan is wrong (incomplete or incorrect); here the plan serves as the control of another function. This may clearly also lead to potentially serious consequences.
The more precise consequences of increased variability of planning cannot be determined before the other functions have been identified and described. Although this is not possible in the present case, the example may nevertheless give an idea about how this can be done.

6.5. Step 5: Identification of Effective Countermeasures

When the possible range of performance variability has been assessed and the potential risks identified, the next and final step is obviously to determine how such risks best can be either eliminated or mitigated. In the case where a risk can be eliminated, e.g., by changing something, this should clearly be done, since elimination or prevention is by far the most effective solution. But in cases where this is not possible, other solutions should be considered.
In the traditional safety thinking, where risks are associated with failures or malfunctions, the general solution is to establish one or more barriers. Such barriers can be either material, functional, symbolic or incorporeal (Hollnagel, 2004). From

a functional perspective one should also consider solutions that more directly address the dynamics of the system, i.e., the way in which the functions are carried out. If the problem is associated with increased performance variability, either of a single function or through the coupling among several functions, then the 'logical' solution is to dampen that variability. Dampening can be achieved in various ways, selected so as to address the most likely source of the variability.[9] Since increased performance variability of a function can lead to unwanted consequences both via the potential couplings between that function and other functions, and via the changes to the common performance conditions, countermeasures must clearly consider both alternatives. Countermeasures must furthermore be able to work in the actual situation, hence require a way to gauge actual performance. This leads into a discussion of performance indicators, which is beyond the scope of this report. Current developments in resilience engineering can provide some guidance for how this can be done in practice, e.g., Hollnagel (2009) and Lay & Wreathall (2008).

9 Notice that this is different from elimination, prevention, and protection because the variability is maintained, only under more controlled conditions.

7. Comparing the Two Approaches

The two risk analyses described in this report represent two different approaches or even two different safety philosophies, cf., Figure 11. In the traditional approach, characteristic of established safety management practices, negative outcomes, and therefore also risks, are seen as caused by failures and malfunctions. Safety is typically defined in terms of a reduced number of adverse events (accidents, incidents, etc.). The emphasis is therefore on how to identify the risks and on how to eliminate or reduce risks and / or their causes as far as possible.

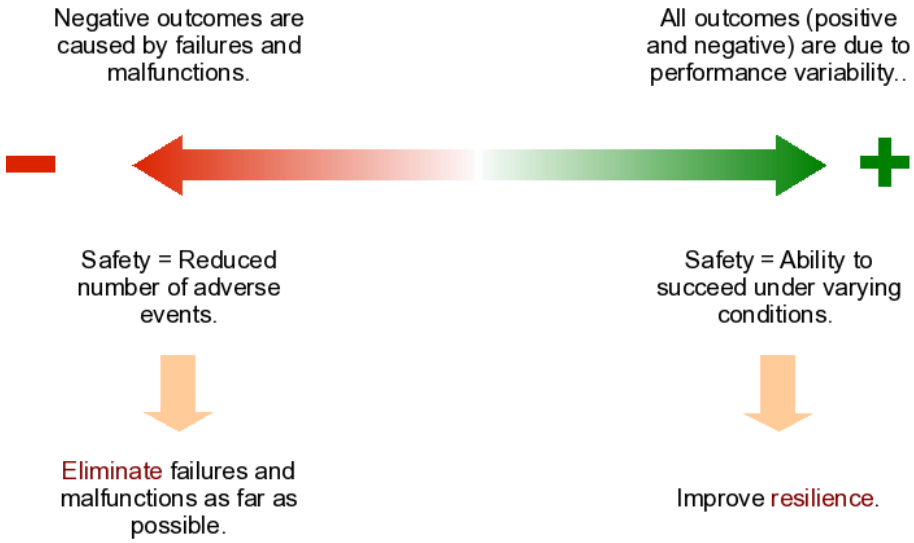

Figure 11: Two approaches to risk assessment: Safety management and resilience engineering.

The resilience engineering approach proposes that all outcomes – whether negative or positive – are due to the variability of normal performance, whether individual or collective. Performance variability is necessary to adjust to underspecified working conditions, and is therefore the norm rather than the exception. Performance variability is furthermore the reason why things usually go right, as well as the reason why things sometimes go wrong. The emphasis of this approach is on describing the system in terms of how it functions, on understanding the way in which functions can vary, on identifying couplings or dependencies among the functions, and finally on finding ways to control the variability – specifically to dampen it if it looks as if it is getting out of hand.

In both philosophies, risk assessment is performed by a series of steps. The steps look deceptively alike, but are nevertheless radically different in terms of what they

entail. The two approaches are shown side-by-side in Figure 12. (Both approaches are shown as having five steps; this is however a more or less arbitrary number that depends on how detailed the description is.)

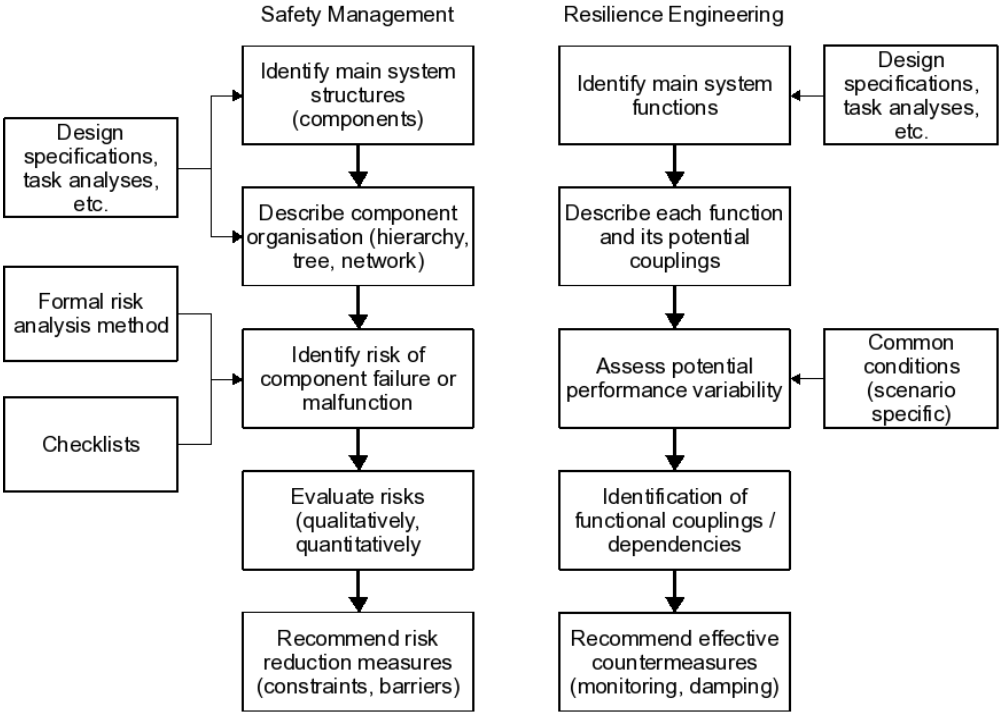

Figure 12: Step-by-step risk assessment in the two approaches.

In the safety management approach shown on the left-hand side of Figure 12, the objective is to identify the risks associated with identifiable system components. (Note that this is a generic description, which includes but is not specific to the assessment of the organisational change at RAB.) The components normally refer to the physical structure of the system, but in the case of organisational changes the reference is rather to 'components' or 'factors' such as competence, resources, instructions, workload, etc. In the concrete case, the RAB risk assessment was based on a checklist of risks. Based on these guidelines, 23 specific risks were identified. The possible risks are loosely described in terms of 'component failure modes,' e.g., 'loss of competence' or 'excessive workload.' Each risk is either considered by itself or in simple combinations with other risks, and the analysis

tries to ascertain the size of the risks. Finally, various risk reduction measures are proposed, often involving different types of barrier systems or performance constraints.

In the resilience engineering approach shown on the right-hand side of Figure 12, the objective is to describe the variability of system functions. This is achieved by first describing the main system functions and then characterise each function using a standardized set of categories. This is followed by assessing the potential performance variability and how couplings among functions may arise by which performance variability can propagate in an upstream-downstream direction. These couplings cannot be described *a priori*, and the outcomes may be non-linear. Finally, various countermeasures are proposed, such as ways of monitoring the system's functions, ways of damping variability, etc.

In order to compare the two approaches in a more practical manner, it is necessary to find a set of relevant criteria. In the previously mentioned report, Hollnagel & Speziali (2008), a summary of different ways of characterising accident investigation method was presented. This described several sets of dimensions or criteria that had been proposed to highlight important aspects of various methods and that therefore also could be used to compare two or more methods. Although the focus in that report was accident investigation rather than risk assessment, it is possible to revise the recommended list to address the issue at hand, i.e., risk assessment of organisational changes. The revised list is shown in Table 10.

Table 10: List of comparison criteria

Predictive capability	The capability of each approach to predict the probable risks in specific situations. If possible, predictions should also include the likely magnitude or risks.
Technical basis	The extent to which the method is grounded in a clearly identifiable model of individual and collective action (performance).
Relation to existing taxonomies	The relation to and/or dependence on existing classification schemes (taxonomies) for organisational risks.
Practicality	The ease with which each approach can be turned into a practical method or made operational.
Cost-effectiveness	The relative costs and benefits that are associated with each approach. The costs include the time and effort (person hours) required to use a method, but not the time required to train people before a first time use.

If the list in Table 10 is used to characterise the two approaches, the outcome will be as shown Table 11. Both approaches require a sizeable investment in time and effort, and it is not possible at present to tell where there will be any significant difference on this dimension. The other dimensions all yield different characterisations, which point to possible differences. The choice of which approach to use must, of course, reflect the priorities and concerns of the organisation. It is therefore not possible to make any absolute statements about which approach is better. Relatively speaking, the safety management approach is well suited to cases where there is a considerable experience with the organisation but less effective for organisations that are new, or where the changes takes the organisation into new territory. The use of a checklist of risks requires a stable organisation in a stable environment, where new risks are unlikely to appear. If that is the case, a checklist can be a very efficient means; if not, the checklist may limit the scope of the analysis and thereby become a risk in itself. Conversely, the resilience engineering approach can be used not just to check against known risks, but also to look for potentially new or unknown risks. It will be easier to integrate with other types of analysis because it is based on an articulated theoretical framework (model). It may also be more suitable than the safety management approach to look at long-term outcome risks, i.e., beyond planning and implementing the change.

The most important difference between the two approaches is perhaps that a safety management approach requires that the organisation or system is tractable whereas a resilience engineering approach does not. This means that the latter in general may be better suited to systems and organisations that are subject to frequent changes due to either internal or external conditions, or where detailed specific descriptions are not available.

Table 11: Comparison of the two approaches

	Approach	
	Vattenfall / RAB (safety management)	FRAM (resilience engineering)
Predictive capability	The approach does not try to predict risks, but instead uses a pre-existing checklists of risks as a basis for assessing the organisational change. Risks are rated qualitatively	The approach aims at identifying possible unintended couplings of functions and the risks that may emerge from performance variability.
Technical basis	The approach does not refer to an articulated model of human or collective	The approach is based on the principles of

	action.	resilience engineering.
Relation to existing taxonomies	The approach uses an experience-based, hence domain specific, list of organisational risks.	The approach focuses on performance variability rather than failures and malfunctions. It refers to a description of the system's functions rather than to risks.
Practicality	The RAB safety analyses (primary, secondary) are specified as flow charts.	FRAM is a well-defined generic method.
Cost-effectiveness	The approach requires a sizeable investment in time and effort.	The approach requires a sizeable investment in time and effort.

8. Conclusions

While it is clear that the two approaches are different, the choice of which to use in a given case cannot simply be made from the comparison presented here. Such a choice must take into account the larger working environment, organisational culture, established *modi operandi*, economic factors, regulatory requirements, etc. The comparison described above may at best be useful by providing additional details that can be taken into account in making such a decision or choice.

Acknowledgement

The kind assistance and support of Mr. Klas Pihlqusit, Vattenfall AB, is gratefully acknowledged.

9. References

Atomic Energy Commission (1975). Reactor safety study: An assessment of accident risks in U.S. Commercial power plants (WASH-1400). Washington, D.C.

Bastien, J. M. C. & Scapin, D. (1993). Ergonomic Criteria for the Evaluation of Human-Computer interfaces. Institut National de recherche en informatique et en automatique, France.

Benner, L. (1975). Accident investigations: Multilinear events sequencing methods. Journal of Safety Research, 7(2), 67-73.

Boyce, P. R. (2006). Illumination. In: Salvendy, G. (Ed.). Handbook of human factors and ergonomics. 3rd ed.Hoboken, NJ: John Wiley & Sons (pp. 643 - 669).

Casali, J. G. (2006). Sound and noise. In: Salvendy, G. (Ed.). Handbook of human factors and ergonomics. 3rd ed. Hoboken, NJ: John Wiley & Sons (pp. 612 - 642).

Cox, T. & Griffiths, A. (2005). The nature and measurement of work-related stress: theory and practice. In:Wilson, J. R. & Corlett, N. (eds.) Evaluation of human work. 3rd ed. Boca Raton, FL: Taylor & Francis. pp. 553 - 571.

Davoudian, K.; Wu, J.-S. & Apostolakis, G. (1994). Incorporating organizational factors into risk assessment through the analysis of work processes. Reliability Engineering & Systems Safety, 45(1-2), 85-105.

Dekker, S. W. A. & Hollnagel, E. (2004). Human factors and folk models. Cognition, Technology & Work, 6, 79–86.

Dougherty, E. M. Jr. (1990). Human reliability analysis - Where shouldst thou turn?. Reliability Engineering and System Safety, 29(3), 283-299.

Hale, A. R. (1978). The role of HM Inspectors of Factories with particular reference to their training. PhD thesis, University of Aston in Birmingham.

Hale, A. & Hovden, J. (1998). Management and culture: The third age of safety. A review of approaches to organizational aspects of safety, health and environment. In A. M. feyer & A. Williamson (Eds.), Occupational Injury: Risk, Prevention, and Intervention. CRC Press.

Heinrich (1931). Industrial accident prevention. McGraw-Hill.

Hollnagel, E. (1998). Cognitive reliability and error analysis method (CREAM). Oxford: Elsevier Science Ltd.

Hollnagel, E. (2004). Barriers and accident prevention. Aldershot: Ashgate Publishing Limited.

Hollnagel, E. (2009). The four cornerstones of resilience engineering. In: C. P. Nemeth, E. Hollnagel & S. Dekker (2009). Resilience Engineering Perspectives, Vol. 2: Preparation and restoration. Aldershot, UK: Ashgate.

Hollnagel, E. & Nygren, M. (2006). Framtagning av bedömningsfaktorer/modell för utvärdering av driftklarhetsverifiering (DKV) inför uppstart efter revisionsavställning. (SKI 2006:03). Stockholm, Sweden: Swedish Nuclear Inspectorate.

Hollnagel, E. & Speziali, J. (2008). Study on developments in accident investigation methods: A survey of the "state-of-the-art" (SKI 2008:50). Stockholm, Sweden: Swedish Nuclear Inspectorate.

Hollnagel, E., Woods D. D. & Leveson, N. (2006). Resilience engineering: Concepts and precepts. Aldershot, UK: Ashgate Publishing.

Hopkins, A. (2009). Thinking about process safety indicators. Safety Science, 47(4), 460–465.

Kirwan, B. (1994). A guide to practical human reliability assessment. London: Taylor & Francis.

Kuusito, A. (2000). Safety management systems - audit tools and reliability of auditing. PhD thesis from Technical Research Centre of Finland, Espoo, Finland.

Lay, E. & Wreathall, J. (2008). Improving resilience by "pinging" to determine risk profile changes during maintenance work. In E. Hollnagel, F. Pieri & E. Rigaud (Eds.), Proceedings of the third Resilience Engineering Symposium. October 28-30, Antibes – Juan-les-Pins, France. (p. 169-176.)

Marmaras, N. & Nathanael, D. (2006). Workplace design. In: Salvendy, G. (Ed.). Handbook of human factors and ergonomics. 3rd ed. Hoboken, NJ: John Wiley & Sons (pp. 575 - 589).

Maruyama, M. (1963): The Second Cybernetics: Deviation-Amplifying Mutual Causal Processes. American Scientist, 5(2), 164—179.

Mc Gregor, D. (1969). La dimension humaine dans l'entreprise, Gauthier-Villars.

Mintzberg, H. (1982). Structure et dynamique des organisations. Paris: Les Editions d'Organisation.

Nouvel, D., Travadel, S. & Hollnagel, E. (2007). Introduction of the concept of functional resonance in the analysis of a near-accident in aviation. 33rd ESReDA Seminar: Future challenges of accident investigation, November 13-14, Ispra, Italy.

Parsons, K. (2005). Ergonomics assessment of thermal environments. In: Wilson, J. R. & Corlett, N.(eds.) Evaluation of human work. 3rd ed. Boca Raton, FL: Taylor & Francis (pp. 643 - 661).

Perrow, C. (1984). Normal accidents: Living with high risk technologies. New York: Basic Books, Inc.

Pidgeon, N. (1997). The Limits to Safety? Culture, Politics, Learning and Man–Made Disasters. Journal of Contingencies and Crisis Management, 5(1), 1-14.

Poucet, A. (1989). Human Factors Reliability Benchmark Exercise - Synthesis Report (EUR 12222 EN). Ispra (VA), Italy: CEC Joint Research Centre.

Reason, J. T. (1997). Managing the risks of organizational accidents. Aldershot: Ashgate Publishing Limited.

Reiman, T. (2007) Assessing Organizational Culture in Complex Socio-technical Systems. Espo, Finland: Technical Research Centre of Finland. (Ph.D. thesis)

Roberts, K. H. (1990). Some Characteristics of One Type of High Reliability Organization. Organization Science, 1(2). 160-176.

Salas, E. Dickinson, T. L., Converse, S. A. & Tannenbaum, S. I. (1992). Toward an understanding of team performance and training. In R. W. Swezey & E. Salas (Eds.), Teams: Their training and performance (pp. 3-29). Norwood, NJ: Ablex.

Salas, E., Burke, C. S. & Cannon-Bowers, J. A. (2000). Teamwork: emerging principles. International Journal of Management Reviews, 2, 339–356.

Sawaragi, T., Horiguchi, Y. & Hina, A. (2006). Safety analysis of systemic accidents triggered by performance deviation. SICE-ICASE International Joint Conference 2006, October 18-21, Bexco, Busan, South Korea

Scherrer J. et coll. (1992). Précis de physiologie du travail. Notions d'ergonomie. 2e édition. Paris: Masson.

Stohl, C. (1995). Organisational communication: Connectedness in action. Sage Newbury Park, CA.

Travers, J. & Milgram, S. (1969). An experimental study of the small world problem. Sociometry, 32(4), 425-443.

Van Schaardenburgh-Verhoeve, K. N. R., Corver, S. & Groeneweg, J. (2007). Ongevalonderzoek buiten de grenzen van de organisatie (Accident investigation beyond the boundaries of organizational control). NVVK Jubileumscongres, 25-26 April 2007, Sessie C, p. 1-11.

Woltjer, R. & Hollnagel, E. (2007). The Alaska Airlines Flight 261 accident: A systemic analysis of functional resonance. Proceedings of the 2007 (14th) International Symposium on Aviation Psychology (ISAP), 763-768, Dayton, OH.

Woods, D. Sarter, N. & Billings, C. (1997). Automation surprises. In G. Salvendy (Ed.), Handbook of Human factors and Ergonomics (2nd ed.). New York: Wiley. (pp. 1926-1943.)

1976916/2.0. (19/02/08). Riskbedömning av omorganisation och sammanslagning av Ringhals 3 och Ringhals 4

1734863/7.0. (25/06/07). Rutin för organisations- och verksamhetsförändringar

1971991 /2.0. (30/12/99). Uppdrag organisationsjustering Ringhals 3 och 4

1972964/2.0. (30/12/99). Ringhals 3 och 4. Planering och genomförande av organisationsförändring

1973584/2.0. (30/12/99). R34 organisationsöversyn - Kontroll av organisationsalternativ

1975451 /2.0. (30/12/99). MTO 01/08 Förebyggande MTO-utredning med anledning av R34 organisationsöversyn.

1977629/3.0. (30/12/99). PSG av Planering och genomförande av omorganisation och sammanslagning av Ringhals 3 och Ringhals 4

1977926 13.0. (30/12/99). R3 R4 Fristående säkerhetsgranskning av gemensam organisation för Ringhals 3 och 4

1978311. (30/12/99). Anmälan - Organisatorisk förändring Ringhals i enlighet med SKIFS 2004: 1 kap 4 5§

990702051 /7.0. (30/12/99). Ringhals fristående säkerhetsgranskning

990706003 I 5.0. (30/12/99). Ringhals primär säkerhetsgranskning

2013:09

The Swedish Radiation Safety Authority has a comprehensive responsibility to ensure that society is safe from the effects of radiation. The Authority works to achieve radiation safety in a number of areas: nuclear power, medical care as well as commercial products and services. The Authority also works to achieve protection from natural radiation and to increase the level of radiation safety internationally.

The Swedish Radiation Safety Authority works proactively and preventively to protect people and the environment from the harmful effects of radiation, now and in the future. The Authority issues regulations and supervises compliance, while also supporting research, providing training and information, and issuing advice. Often, activities involving radiation require licences issued by the Authority. The Swedish Radiation Safety Authority maintains emergency preparedness around the clock with the aim of limiting the aftermath of radiation accidents and the unintentional spreading of radioactive substances. The Authority participates in international co-operation in order to promote radiation safety and finances projects aiming to raise the level of radiation safety in certain Eastern European countries.

The Authority reports to the Ministry of the Environment and has around 270 employees with competencies in the fields of engineering, natural and behavioural sciences, law, economics and communications. We have received quality, environmental and working environment certification.

Strålsäkerhetsmyndigheten
Swedish Radiation Safety Authority

SE-171 16 Stockholm
Solna strandväg 96

Tel: +46 8 799 40 00
Fax: +46 8 799 40 10

E-mail: registrator@ssm.se
Web: stralsakerhetsmyndigheten.se