SKI Report 2008:50

Research

Study on Developments in Accident Investigation Methods: A Survey of the "State-of-the-Art"

Erik Hollnagel
Josephine Speziali

January 2008

ISSN 1104-1374
ISRN SKI-R-08/50-SE

SKI perspective

Background

For incident investigation the Swedish nuclear industry has been using the same method since the 90-ties, the MTO (Man Technology Organisation) method. The basis for the method is that human, organisational, and technical factors should be focused equally in an accident investigation. The method is based on HPES (Human Performance Enhancement System). In order to get a better understanding of how well the MTO method, compared to other methods, can find the root causes and prevent reoccurrences of events there was a need for an overview and evaluation within the field of incident investigation methods.

Purpose

The objective of this project was to survey the main accident investigation methods that have been developed since the early or mid-1990s and to develop well grounded principals or criteria that could be used to characterise the chosen methods.

Result

The different methods were catagorised due to the dimensions of coupling, going from loose to tight, and interactions (tractability*)*. This led to four groups where the nuclear industry fit into the group that are tightly coupled and intractable and therefore need to use methods that are suitable for those. Examples of such methods are FRAM (Functional Resonance Accident Model) and STAMP (Systems-Theoretic Accident Modeling and Process).

The majority of incidents that happens and are investigated by the nuclear industry can however be characterised to the group that is less tightly coupled and more tractable. Methods that suites that group are for example CREAM (Cognitive Reliability and Error Analysis) and the MTO method. There are also many incidents/low level events that can be investigated with even less powerful methods.

To get some guidance in choosing the right method a number of questions can be asked, for example:

1. Was the accident similar to something that has happened before, or was it new and unknown? (The reference should be the history of the installation, as well as industry wide.).
2. Was the organisation ready to respond to the accident, in the sense that there were established procedures or guidelines available?
3. Was the situation quickly brought under control or was the development lengthy?
4. Was the accident and the material consequences confined to a clearly delimited subsystem (technological or organisational) or did it involve multiple subsystems, or the whole installation?
5. Were the consequences on the whole expected / familiar or were they novel / unusual?

6. Were the consequences in proportion to the initiating event, or were they unexpectedly large (or small)?

While it may be convenient, or even necessary, for an organisation to adopt a specific method as its standard, this should always be done knowingly and with a willingness to reconsider the choice when the conditions so demand it.

Through the study the SKI has increased its knowledge of different methods and their range of use. The MTO method is suitable for incidents that are somewhat complex but for simpler incidents/low level events it might be too powerful and time-consuming. The important thing is that one is aware of ones choices and how they affect the result and that the method chosen is appropriate for the situation so that the root causes can be identified. No incidents is however prevented just by investigating them but there is also a need for an organisation that deals with the results and makes sure that the right countermeasures are taken

Further research

There are today no further projects planned by the SKI within this field. We are however following the research in the field that is done by others.

Project information

SKI project coordinator: Pia Jacobsson.

SKI referens: SKI 2007/1819, SSM2008/177

Project number: 200703011

SKI Report 2008:50

Research

Study on Developments in Accident Investigation Methods: A Survey of the "State-of-the-Art"

Erik Hollnagel
Josephine Speziali

Ecole des Mines de Paris
rue Claude Daunesse
F-06904 Sophia Antipolis Cedex
France

January 2008

This report concerns a study which has been conducted for the Swedish Nuclear Power Inspectorate (SKI). The conclusions and viewpoints presented in the report are those of the author/authors and do not necessarily coincide with those of the SKI.

Summary

The objective of this project was to survey the main accident investigation methods that have been developed since the early or mid-1990s. The motivation was the increasing frequency of accidents that defy explanations in simple terms, for instance cause-effect chains or "human error". Whereas the complexity of socio-technical systems is steadily growing across all industrial domains, including nuclear power production, accident investigation methods are only updated when their inability to account for novel types of accidents and incidents becomes inescapable. Accident investigation methods therefore typically lag behind the socio-technological developments by 20 years or more.

The project first compiled a set of methods from the recognised scientific literature and in major major research & development programs, excluding methods limited to risk assessment, technological malfunctions, human reliability, and safety management methods. An initial set of 21 methods was further reduced to seven by retaining only *prima facie* accident investigation methods and avoiding overlapping or highly similar methods.

The second step was to develop a set of criteria used to characterise the methods. The starting point was Perrow's (1984) description of *normal accidents* in socio-technical systems, which used the dimensions of *coupling*, going from loose to tight, and *interactions*, going from linear to complex. For practical reasons, the second dimension was changed to that of *tractability* or how easy it is to describe the system, where the sub-criteria are the level of detail, the availability of an articulated model, and the system dynamics. On this basis the seven selected methods were characterised in terms of the systems – or conditions – they could account for, leading to the following four groups: methods suitable for systems that are loosely coupled and tractable, methods suitable for systems that are tightly coupled and tractable, methods suitable for systems that are loosely coupled and intractable, and methods suitable for systems that are tightly coupled and intractable. The number of methods in each group were four, three, zero, and two, respectively.

Faced with the need to investigate an accident it is essential that the chosen method is appropriate for the system and the situation. Nuclear power plants considered as systems are tightly coupled and more or less intractable and therefore require accident models and accident investigation methods that are capable of accounting for these features. If an accident concerns the NPP operation as a whole, the methods must be suitable for systems that are tightly coupled and intractable. If an accident only concerns the operation of a subsystem or a component, the methods must be suitable for systems that are tightly coupled and tractable, or possible loosely coupled and tractable. The report provides a proposal for how these characteristics can be determined.

The conclusion is that no specific method is the overall best in the sense that it can be used for all conditions. While it may be convenient, or even necessary, for an organisation to adopt a specific method as its standard, this should always be done knowingly and with a willingness to reconsider the choice when the conditions so demand it. In five or ten years we must expect that the methods developed today will have been partly obsolete, not because the methods change but because the nature of socio-technical systems, and therefore the nature of accidents, do.

Table of contents

1 Objective

The complexity of socio-technical systems has for many decades been steadily growing across all industrial domains, including nuclear power production. One tangible consequence is that many of the incidents and accidents that occur today defy simple explanations, for instance in terms of cause-effect chains. To explain what happens requires more elaborate approaches – which means more sophisticated models and more powerful methods. Accident models provide the principles that can be used to explain how accidents happen. They are a convenient way of referring to the set of axioms, assumptions, beliefs, and facts about accidents that form the basis for understanding and explaining specific events. The methods describe – or even prescribe – how an investigation should be performed in order to produce an explanation of the accident, typically in a step-by-step fashion. The purpose of the methods is to ensure that the model concepts are applied consistently and uniformly, thereby limiting the opportunities for subjective interpretations and variations. An accident investigation should clearly not depend on personal insights and skills, but should rely on generalised public knowledge and institutionalised common sense.

The development of new methods and approaches has often been driven by the inability of established methods to account for novel types of accidents and incidents. Another motivation has been a lack of efficiency, in the sense that recommendations and precautions based on the usual explanations have not lead to the desired effects and improvements. A third motivation has been new theoretical insights, although this rarely has happened independently of the former.

The objective of this project was to make a survey of the main accident investigation methods that have been developed in the last decade or so, i.e., since the early or mid-1990s. The work consisted of two equally important parts. One was to compile a list of methods corresponding to the overall selection criteria, and from that to select a subset for more detailed consideration. The other was to develop an argued set of principles or criteria that could be used to characterise the methods. The aim of this survey has not been to recommend any specific method as the overall ‘best’, but rather to provide an analysis and synthesis that can serve as the basis for a choice in concrete cases.

1.1 Accident Investigation and Accident Analysis

While the project was focused on accident investigation methods, it soon became clear that most of the methods – established as well as newcomers – addresses issues of accident analysis rather than accident investigation. The difference between the two is one of scope. An accident investigation logically covers everything from the initial planning of how to investigate an accident, allocation and scheduling of resources, collection of data and information, analysis of the same, recommendations following the analysis, implementation of the recommendations, and finally an evaluation of the effects of the recommendations. An accident analysis focuses on how to understand what happened based on the available data and information. It is thus properly speaking a subset or part of the investigation. The analysis will indirectly determine the data collection, particularly if it is being used regularly in an organisation, and also to some extent constrain the recommendations (Hollnagel, 2008). Although the use of a specific accident analysis method will therefore have consequences for other parts of the investigation, this is normally not addressed by the accident analysis method. Since understanding why an accident happened for obvious reasons is the primary concern, most methods emphasise that and pay little or no attention to the other parts of the investigation.

2 Background

A previous SKI study (Harms-Ringdahl, 1996) surveyed fifteen methods for risk assessment from an industrial perspective. Of these, the following four were characterised as directly applicable to accident investigation:

- Deviation analysis (avvikelseanalys),
- Human Error Analytical Taxonomy (HEAT),
- Management Oversight and Risk Tree (MORT), and
- Safety Management and Organization Review Technique (SMORT),

  while two were considered potentially applicable:
- CRisis Intervention in Offshore Production (CRIOP), and
- International Safety Rating System (ISRS).

2.1 Changing notions of risk and safety

Most of the methods for risk assessment and accident investigation that are used today in nuclear power production, as well as in many other industries, have their origin in the 1960s. This is the period where the technical or engineering analysis methods were developed, in response to the growing complexity of technological systems. Examples are Fault Trees, which were developed in 1961 to evaluate the launch control system for the Minuteman ICBM (cf. Leveson, 1995), Hazard and Operability Analysis (HAZOP) which was developed by Imperial Chemical Industries in England in the early 1960s (CISHC, 1977), and Failure Mode and Effects Analysis (FMEA) which was originally developed by the US military in 1949 but later superceded by the Failure Mode, Effects and Criticality Analysis (FMECA) (MIL-STD-1629A, 1980). Another period of rapid growth occurred in the beginning of the 1980s, mainly in response to the TMI accident in 1979. This led to the recognition that human factors and human errors played a significant role in system safety, hence that it was necessary for risk assessment and accident investigation methods to go beyond the technological system. The concern for the human factor was later extended to cover organisations and organisational factors as well, with the prominence of 'safety culture' as a good example. The direct motivation was also in this case a serious adverse event, namely the Chernobyl accident in 1986. Since the mid-1990s there has been an additional growth, although more often incremental than innovative. This growth has taken place to answer the perceived need among theorists and practitioners of a re-orientation in thinking about safety, in order to develop methods and approaches that are both more efficient in use and better grounded in their concepts and constructs.

Some of the major changes and developments since the mid-1990s have been:

- An increasing emphasis of the organisational factor, spurred by Jim Reason's book on organisational accidents (1997),
- the increasing importance of software (e.g., the concept of Safeware; Leveson, 1995),

- the emphasis on high reliability organisations, (e.g., Weick et al., 1999),
- the changing perspective on causality, moving from sequential models to systemic models (Hollnagel, 2004),
- the associated change in view on "human error", from the "old" look to the "new" look (Dekker, 2006),
- the change from training in specific skills to training in general communication and collaboration (Helmreich et al., 1999),
- the change from reactive to proactive safety, as marked by resilience engineering, (Hollnagel, Woods & Leveson, 2006).

In the same period, i.e., since the mid-1990s, the growing complexity of socio-technical systems has also necessitated the development of more powerful accident investigation methods and analytical principles. This complexity, which was aptly diagnosed by Perrow (1984), has unfortunately often been marked by serious accidents, and shows no sign of abating. Some of the better known examples are the JCO accident at Tokai-Mura, Japan (1999), the space shuttle Columbia disaster (2003), and the Überlingen mid-air collision (2002) – plus literally thousands of small and large accidents in practically every industrial domain. This development is not isolated to a specific industrial domain, such as NPP, but has happened in many different industries and service functions.

One consequence of this has been the realisation that accident investigation and risk assessment are two sides of the same coin, in the sense that they consider the same events or phenomena either after they have happened (retrospectively) or before they happen (prospectively). In the prospective case there is, of course, the possibility that an event may never occur; indeed, the main rationale for risk assessment is to ensure that this is the case. The dependency between accident investigation and risk assessment has been emphasised both by the so-called second generation HRA methods (in particular ATHEANA, Cooper et al., 1996; CREAM, Hollnagel 1998; and MERMOS, Le Bot at al., 1999), and is also a central premise for Resilience Engineering (Hollnagel, Woods, & Leveson, 2006).

3 The Need and Purpose of Accident Investigations

In order to ensure an acceptable level of safety in nuclear power operations, as well as in any other complex industrial process, it is necessary to be able to learn from experience. Knowledge of what has happened previously in an industrial installation such as a NPP, and in particular knowledge of why something went wrong, is essential in order to be able to draw the right conclusions from past events. Such knowledge can serve either to prevent a recurrence or repetition of the same event, to prevent the occurrence of similar events, or to protect against specific types of adverse outcomes.

In the investigation and analysis of past events it is common to distinguish among outcomes of different severity, where typical categories are accidents, incidents, and near-misses (Renborg et al., 2007). The tradition of distinguishing among different types of outcomes was established by Heinrich (1929), who emphasised the difference between the *accident* and the *injury* (or *outcome*). Heinrich argued that it was misleading to consider only accidents which led to major injuries since, according to his own investigations, the ratio of minor injuries to major injuries was 29 to 1. He introduced the category of near-accidents, meaning those events that produced no injury whatsoever although they had the potential power to do so (Ibid, p. 4). From the 1980s and onwards it became common to refer to near misses, defined as situations “where an accident could have happened had there been no timely and effective recovery” (van der Schaaf & Kanse, 2004), and to incidents as something in between. (Depending on the domain, the definitions often refer to the seriousness of the outcome, for instance whether human life was lost.) This project has looked only at accidents, and has not considered incidents or near misses. It is possible, and even likely, that the same approach can be used to characterise how other outcome types are investigated, but to argue this issue has been beyond the scope of the work reported here.

The purpose of an accident investigation is, of course, to understand why the accident happened. This is often expressed as a question of finding the possible cause or causes, and since the late 1970s or early 1980s it has been common both to look for clearly recognisable causes (corresponding to Aristotle’s notion of effective cause[1]) and to point to the “human error” as a main cause of accidents (e.g., Hollnagel, 1998). As far as the latter tendency is concerned, it is important to keep in mind that finding the causes is a psychological rather than a logical process. In particular,

> “... ‘human error’ is not a well defined category of human performance. Attributing error to the actions of some person, team, or organisation is fundamentally a social and psychological process and not an objective, technical one.”
> (Woods et al., 1994, p. xvii)

While there are few who will dispute the need to learn from experience, such learning can come about in many different ways and may range from being thorough to being quite superficial. To learn from experience requires more than collecting data from accidents, incidents, and near-misses or building a company-wide database. Some organisations nevertheless seem to believe that this is sufficient, probably because they confuse data with experience. But 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. Accident investigation is an important part of learning from experience. Some of the fundamental issues that an investigation method must address are: what is reported – and when? how events are analysed? how the results are used and communicated? and what the effects are on safety and daily practice?

An accident investigation always follows a method or a procedure. There are many different methods available, both between and within domains, that may differ with respect to how well formulated and how well founded they are. The importance of having a good method cannot be overstated. The method will direct the investigation to look at certain things and not at others. A root cause analysis, for instance, will tend to look for definitive causes while a ‘Swiss cheese’ or epidemiological analysis will tend to look for latent conditions. It is simply not possible to begin an investigation with a completely open mind, just as it is not possible passively to ‘see’ what is there. Accident

[1] Aristotle proposed a distinction between four types of causes: (1) the material cause is that from which something comes into existence, i.e., the parts of a system; (2) the formal cause tells us what something is, the fundamental principles or general laws; (3) the efficient cause is that from which the change or the ending of the change first starts, corresponding to the present day concept of a cause-effect relation; and (4) the final cause, or the purpose, is that for the sake of which something exists or is done, including both purposeful and instrumental actions and activities.

investigations, as well as searches in general, seem, to conform to the What-You-Look-For-Is-What-You-Find (WYLFIWYF) principle (Hollnagel, 2008). Since an investigation method always will bias the investigation, it is important that investigators not only known the methods they use, in the sense that they are proficient users, but also that they acknowledge the explicit and implicit assumptions that every method makes.

(In terms of the terminology, it is common to find the terms analysis and investigation used as if they were synonyms. This is, of course, not the case, since an accident investigation always is more comprehensive than an accident analysis. In addition to making the analysis, an investigation requires planning, data collection, registration, recommendations, implementation, and evaluation. The objective of this project has been to look at accident investigation methods, but to do so it has been necessary also to consider some accident analysis methods.)

4 The growing complexity of socio-technical systems

The main motivation for developing a new accident investigation method is usually the occurrence of a major accident that defies existing methods, as described above. The reason why this happens is simply that socio-technological systems develop continuously and rapidly, driven by a combination of technological innovation, commercial considerations, and user demands. In contrast to that, risk assessment and safety management methods develop at a far more moderate pace – if at all – which means that they rarely are able to represent or address the actual complexity of industrial systems. To the extent that methods develop, it is usually as a delayed reflection of “new” types of accidents. The outcome can be that methods focus on a specific, salient factor of an event (e.g., violations after Chernobyl), or that they become more comprehensive by trying to draw together the collective experience and changes in view (e.g., second generation HRA).

Existing accident prevention, risk reduction, and safety measures must obviously refer to the established understanding or the commonly accepted state-of-the-art. If anything happens despite these precautions it is therefore something that could not have been addressed by the methods and models that were used, i.e., something that went beyond the established understanding. Such events therefore challenge the methods, and it will be impossible to produce an adequate explanation.

One important characterisation – if not quite an explanation – of this development was given by the American sociologist Charles Perrow in a book called Normal Accidents (Perrow, 1984). The fundamental thesis of the book was that the (Western) society that existed then, and in particular the technological environments that provided the foundation for that society, 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. Since Perrow published his analyses neither the socio-technical systems, nor the problems that follow, have become any simpler.

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 later, such as Challenger, Chernobyl, and Zebrügge.

Perrow proposed two descriptive 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 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.

Perrow used these two dimensions of interactions and coupling to illustrate differences among various types of systems, cf. Figure 1.

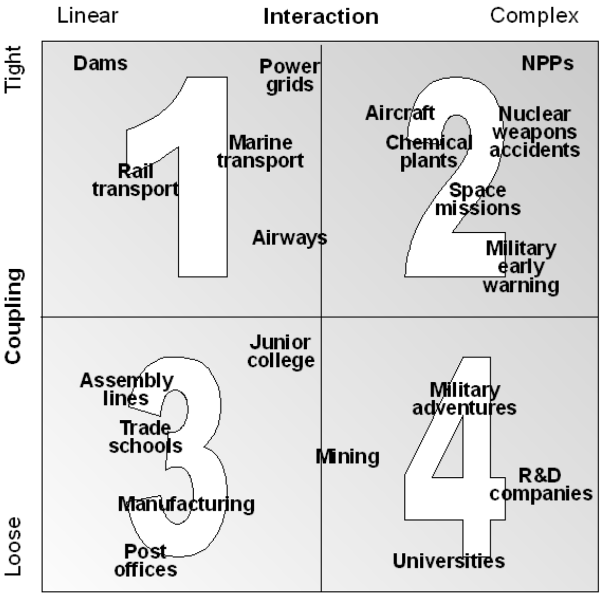


Figure 1: The coupling-interaction diagram (Perrow, 1984)

The worst possible combination with regard to the accident potential is, 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 belong to the same category were, e.g., aircraft and chemical plants. It is characteristic, and probably not a coincidence, that all the systems Perrow describes in the book were tightly coupled and only differed with respect to their complexity, i.e., they were mostly in the second quadrant.

Perrow’s thesis, as expressed by Figure 1, is relevant for accident investigation methods, since the explanation of an accident must be able to account for the nature of interactions and the degree of coupling in the system. If we, for the sake of argument, refer to the four quadrants of Figure 1, then it is clear that systems in quadrant 3 differ in important respects from systems in quadrant 2. A method that may be adequate to explain an accident in a quadrant 3 system, such as a person that is injured while working at an assembly line, is unlikely to be sufficient to explain an accident in a quadrant 2 system, such as an INES event at a nuclear power plant. (Even though the converse is not necessarily true, it may be inefficient to use the more complex and powerful methods to investigate accidents in simple systems.) The diagram therefore provides an external frame of reference for accident investigations methods in addition to the more traditional requirements such as consistency, reliability, usability, etc.

5 Initial Set of Methods

Although genuinely new methods are quite rare, there is nevertheless a steady flow of methods to the “market”. Most of these, however, are variations of the basic approaches, either to address the needs of a specific domain or application, or as a result of studies, research projects, etc.

It is practically impossible to list all the methods that have been proposed during the last 10-15 years. Instead, a set was compiled of methods that have been recognised in the general scientific literature and in the programs of major research & development organisations. The compilation has made use of a number of reports and surveys such as

CCPS (1992), DOE (1999) and Sklet (2002). The methods already described by Harms-Ringdahl (1996) – Deviation Analysis, HEAT, MORT, and SMORT – have not been included in the set. Neither have methods that properly speaking were aimed at risk assessment (e.g., Bayesian Belief Networks combined with Fault Trees), technological malfunctions (e.g., Sneak Path Analysis), human reliability (e.g., ATHEANA), or safety management methods (e.g., TRIPOD).

The first survey of the literature, applying the selection criteria described above, produce a list of 21 accident investigation or accident analysis methods. The methods are briefly identified and described in Table 1 below.

Table 1: Initial set of accident investigation methods.

Acronym	Method name	Short description	Source and Year
AEB	Accident Evolution and Barrier Analysis	The Accident Evolution and Barrier Function (AEB) model provides a method for analysis of incidents and accidents that models the evolution towards an incident/accident as a series of interactions between human and technical systems.	Svensson (2001)
BA	Barrier Analysis	Barrier analysis is used to identify hazards associated with an accident and the barriers that should have been in place to prevent it. A barrier is any means used to control, prevent, or impede the hazard from reaching the target.	Dianous & Fiévez (2006)
CA	Change Analysis	This technique is used to examine an accident by analysing the difference between what has occurred before or was expected and the actual sequence of events. The investigator performing the change analysis identifies specific differences between the accident–free situation and the accident scenario. These differences are evaluated to determine whether the differences caused or contributed to the accident.	DOE (1999)
CREAM	Cognitive Reliability and Error Analysis Method	CREAM can be used both predictively and retrospectively. The retrospective use (accident analysis) is based on a clear distinction between that which can be observed (called phenotypes) and that which must be inferred (called genotypes). The genotypes used in CREAM are divided into three categories: individual, technological and organisational.	Hollnagel (1998)
ECFC	Events and causal factors charting	Events and causal factors charting is a graphical display of the accident's chronology and is used primarily for compiling and organising evidence to portray the sequence of the accident's events.	DOE (1999)

Acronym	Method name	Short description	Source and Year
ECFCA	Events and Causal Factors Charting and Analysis	The events and causal factors chart may be used to determine the causal factors of an accident. This process is an important first step in later determining the root causes of an accident. Events and causal factors analysis requires deductive reasoning to determine which events and/or conditions that contributed to the accident.	DOE (1999)
FRAM	Functional Resonance Accident Model	A method for accident investigation as well as risk assessment based on a description of system functions. Non-linear propagation of events are described by means of functional resonance.	Hollnagel (2004)
HERA	HERA	HERA is a method to identify and quantify the impact of the human factor in incident/accident investigation, safety management and prediction of potential new forms of errors arising from new technology. Human error is seen as a potential weak link in the ATM system and, therefore, measures must be taken to prevent errors and their impact, and to maximise other human qualities such as error detection and recovery. HERA is predicated on the notion that human error is the primary contributor to accidents and incidents.	Isaac et al. (2002)
HFACS	Human Factors Analysis and Classification System	HFACS identifies the human causes of an accident and provides a tool to not only assist in the investigation process, but to target training and prevention efforts. HFACS looks at four levels of human failure, referring to the "Swiss cheese" model. These levels include unsafe acts (operator error), preconditions for unsafe acts (such as fatigue and inadequate communication), unsafe supervision (such as pairing inexperienced aviators for a difficult mission), and organizational influences (such as lack of flight time because of budget constraints).	FAA/NTIS (2000)
HFIT	Human factors investigation tool	HFIT was developed on a theoretical basis with reference to existing tools and models. It collects four types of human factors information including (a) the action errors occurring immediately prior to the incident, (b) error recovery mechanisms, in the case of near misses, (c) the thought processes which lead to the action error and (d) the underlying causes.	Gordon, Flin & Mearns (2005)

Acronym	Method name	Short description	Source and Year
HINT – J-HPES	HINT – J-HPES	HINT is a recent development of J-HPES, the Japanese version of INPO's Human Performance Evaluation System, cf. below. The overall principle is to use a root cause analysis of small events to identify trends, and to as a basis for proactive prevention of accidents. The method comprises a number of steps (similar to SAFER, cf. below). These are: Step 1: Understand the event. Step 2: Collect and classify causal factor data. Step 3: Causal analysis, using root cause analysis. And Step 4: Proposal of countermeasures.	Takano et al. (1994)
HPES	Human Performance Enhancement System	A method sponsored by INPO that utilizes a family of techniques to investigate events, with particular emphasis on determining human performance aspects. The HPES methodology incorporates many tools such as task analysis, change analysis, barrier analysis, cause and effect analysis, and event and causal factor charting. Additionally, many similar methodologies have been developed from HPES and adapted where necessary to suit the specific requirements of individual organizations.	INPO (1989)
MTO	Människa-Teknologi-Organisation	The basis for the MTO-analysis is that human, organisational, and technical factors should be focused equally in an accident investigation. The method is based on HPES (Human Performance Enhancement System)	Rollenhagen (1995); Bento (1992)
PEAT	Procedural Event Analysis Tool	The objective of PEAT is to help airlines develop effective remedial measures to prevent the occurrence of future similar errors. The PEAT process relies on a non-punitive approach to identify key contributing factors to crew decisions. Using this process, the airline safety officer would be able to provide recommendations aimed at controlling the effect of contributing factors. PEAT includes database storage, analysis, and reporting capabilities.	Moodi & Kimball (2004).
RCA	Root cause analysis	Root cause analysis identifies underlying deficiencies in a safety management system that, if corrected, would prevent the same and similar accidents from occurring. Root cause analysis is a systematic process that uses the facts and results from the core analytic techniques to determine the most important reasons for the accident.	E.g., IAEA (1999)

Acronym	Method name	Short description	Source and Year
SAFER	SAFER 2007	SAFER is a generic method for accident investigation developed by TEPCO (J). Step 1 Understand HF Engineering. Step 2 Make an event flow chart: Arrange information to understand the detail of the event and to have a basis for communication and sharing of information. Step 3 Pick up Problematic Points. Step 4 Produce a Background Factors Causality Diagram, that represents causality among the factors. Step 5 Think out measures to cut off the causality from background factors (according to the diagram or event flow chart). Step 6 Prioritize the Measures. Step 7 Implement the Measures. Step 8 Evaluate the Effects	Yoshizawa (1999)
SCAT	Systematic Cause Analysis Technique	The International Loss Control Institute (ILCI) developed SCAT for the support of occupational incident investigation. The ILCI Loss Causation Model is the framework for the SCAT system. The result of an accident is loss, e.g. harm to people, properties, products or the environment. The incident (the contact between the source of energy and the "victim") is the event that precedes the loss. The immediate causes of an accident are the circumstances that immediately precede the contact. They usually can be seen or sensed. Frequently they are called unsafe acts or unsafe conditions, but in the ILCI-model the terms substandard acts (or practices) and substandard conditions are used.	Bird & Germain (1985)
STAMP	STAMP	The hypothesis underlying STAMP is that system theory is a useful way to analyze accidents, particularly system accidents. Accidents occur when external disturbances, component failures, or dysfunctional interactions among system components are not adequately handled by the control system. Safety is viewed as a control problem, and is managed via constraints by a control structure embedded in an adaptive socio-technical system. Understanding why an accident occurred requires determining why the control structure was ineffective. Preventing future accidents requires designing a control structure that will enforce the necessary constraints. Systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control.	Leveson (2004)

Acronym	Method name	Short description	Source and Year
STEP	Sequentially Timed Events Plotting	They propose a systematic process for accident investigation based on multi-linear events sequences and a process view of the accident phenomena. With the process concept, a specific accident begins with the action that started the transformation from the described process to an accident process, and ends with the last connected harmful event of that accident process.	Hendrick and Benner (1987).
Swiss cheese	Reason's Swiss Cheese model	The Swiss Cheese model of accident causation is a model used in the risk analysis and risk management of human systems. It likens human systems to multiple slices of Swiss cheese, stacked together, side by side. It was originally propounded by British psychologist James T. Reason in 1990, and has since gained widespread acceptance and use in healthcare, in the aviation safety industry, and in emergency service organizations. It is sometimes called the cumulative act effect.	Reason (1990, 1997)
TRACEr	Technique for Retrospective Analysis of Cognitive Errors	TRACEr provides a human error identification technique specifically for use in the air traffic control domain. It builds on error models in other fields and integrates Wickens' (1992) model of information processing in ATC. TRACEr is represented in a series of decision flow diagrams. The method marks a shift away from knowledge based errors in other error analysis tools to better reflect the visual and auditory nature of ATM. It has proved successful in analysing errors in AIRPROX reports to derive measures for reducing errors and their adverse effects.	Shorrock and Kirwan (1999; 2002)

It is clear, even from the brief descriptions of the above list, that many methods are related, in the sense that they refer to the same basic principles. Examples are the various methods that look at barriers or the methods that look at root causes. It is therefore necessary to make a selection of a smaller set of methods that deserve a closer look. In order to do so it is necessary first to consider the criteria on which such a selection can be made.

6 Criteria for comparison of accident investigation methods

It is quite common in method surveys to propose some criteria for selection, according to which the “best” method – or methods – can be found. This happens for accident investigation methods, as well as for methods of other kinds, e.g., Swain (1989) or Kirwan (1994). In this project the objective was not to find a “best” method, but provide a basis for selecting methods that are appropriate for a given purpose, i.e., a kind of off-line decision support.

In a study commissioned by the Occupational Safety and Health Administration (OSHA) in the US, Benner (1985) rated 14 different accident models and 17 different accident investigations methods used by various US agencies. He began by a set of evaluation criteria and a rating scheme developed from user data, statutes, applications, and work products.

This led to a set of ten criteria that were used to rate the accident models as shown in Table 2. Most of them actually refer to the quality of the outcome of the analysis (realistic, definitive, satisfying, comprehensive, disciplining, consistent, direct, and understandable or visible) rather than the model as such, although that in some sense also reflects model characteristics. Two criteria relate more directly to the nature of the accident model, namely that it should be functional and non-causal.

Table 2: Benner's (1985) criteria for rating accident models.

Model evaluation criteria	**Definition**
Realistic	The investigation should result in a realistic description of the events that have actually occurred.
Definitive	An investigation process should provide criteria to identify and define the data that is needed to describe what happened.
Satisfying	The results should be satisfying for those who initialised the investigation and other individuals that demand results from the investigations.
Comprehensive	An investigation process should be comprehensive so there is no confusion about what happened, no unsuspected gaps or holes in the explanation, and no conflict of understanding among those who read the report.
Disciplining	An investigation process should provide an orderly, systematic framework and set of procedures to discipline the investigators' tasks in order to focus their efforts on important and necessary tasks and avoid duplicative or irrelevant tasks.
Consistent	Model must be theoretically consistent with an agency's safety program concepts.
Direct	The investigation process should provide results that do not require collection of more data before the needed controls can be identified and changes made.
Functional	An investigation process should be functional in order to make the job efficient, e.g. by helping the investigator to determine which events were part of the accident process as well as those events that were unrelated.
Non-causal	An investigation should be conducted in a non-causal framework and result in an objective description of the accident process events. Attribution of cause or fault can only be considered separate from, and after the understanding of the accident process is completed to satisfy this criterion.
Understandable or visible	The output should be readily understandable.

Benner's initial assumption was that all accident investigation programs were driven by accident models, and that the methods could therefore be evaluated against common criteria. But his analyses led him to conclude that this assumption was not valid. Instead, there were three types of relationships between the accident models and investigation methodologies. In the first case, the accident model came before the accident investigation methodology, hence determined that. In the second case the relation was reversed, i.e., that the investigation methodology determined the accident model. Finally, in the third case, a chosen (institutionalised or traditional) analysis method would determine both the accident model and the investigation methodology, without the model or investigation methodology particularly influencing each other. In view of this conclusion Benner developed separate criteria for evaluating the accident investigation methodologies. These criteria are listed in Table 3.

Table 3: Benner's (1985) criteria for rating accident investigation methods.

Method evaluation criteria	Definition
Encouragement	Methodology must encourage harmonious participation
Independence	Methodology must produce blameless outputs
Initiatives	Methodology must support personal initiatives
Discovery	Methodology must support timely discovery process
Competence	Methodology mus increase employee competence
Standards	Methodology must show definite corrections
Enforcement	Methodology must show expectations and behavioural norms
States	Methodology must encourage States to take responsibility
Accuracy	Methodology must help test accuracy of output
Closed Loop	Methodology must be compatible with "pre-investigations" (or safety analyses) of potential accidents:

It is interesting to note also here that the criteria adress aspects of the methods in use, e.g., encouragement or initiatives, rather than aspects of a method qua method, e.g., reliability or independence of user knowledge.

(It may be of interest to note that the top three accident models, according to Benner's criteria, were the Events Process model, the Energy Flow Process model, and the Fault Tree model. Similarly, the top three accident investigation methods were Events Analysis, the MORT system, and Fault Tree Analysis. Benner concluded his survey by recommending both that "significant accident investigation program changes should be considered in agencies and organizations using lower-ranked accident models or investigation methodologies", and that "a compelling need exists for more exhaustive research into accident model and accident investigation methodology selection decisions." Sklet (2002) looked at 15 different methods using the same criteria, but only characterised them in a final table, without indicating any rank order.)

A different approach is found in a survey of accident models and error classifications (Hollnagel, 1998), which proposed the following six criteria (Table 4).

Table 4: Hollnagel's (1998) criteria for classifying accident models and methods.

Criterion	Definition
Analytic capability	Analytic capability, which refers to the ability of each approach to support a retrospective analysis of events involving human erroneous actions. The specific outcome of a retrospective analysis should be a description of the characteristics of human cognition that are included in the set of assumed causes.
Predictive capability	Predictive capability, which refers to the capability of each approach to predict the probable type of erroneous actions (phenotype) in specific situations. If possible, predictions should also be made of the likely magnitude or severity of the erroneous actions. None of the models are actually very good for making predictions, because predictions require both a valid model and a reliable data base. While better models are gradually emerging a reliable data base still awaits a concerted effort.
Technical basis	Technical content, as the extent to which models generated from within each approach are grounded in a clearly identifiable model of human action.
Relation to existing taxonomies	The relation to and/or dependence on existing classification schemes, as the extent to which each of the three approaches is linked to viable systems for classifying the erroneous actions that occur in a real-world processing environment.
Practicality	Practicality of each approach, which refers to the ease with which each approach can be turned into a practical method or made operational.
Cost-effectiveness	Finally, the relative costs and benefits that are associated with each approach.

These criteria aim more directly at the qualities of the method, both with regard to the theoretical basis and with regard to its efficacy. In some sense they consider both the accident model (analytic capability, predictive capability, technical basis, relation to existing taxonomies) and the investigation method (practicality, cost-effectiveness).

In addition to sets of criteria that aim to distinguish among methods, hence to serve as the basis for a choice in a specific situation, there are also more practical criteria that are common to all methods.

- Reliability – whether the method will give the same result if applied again (or to a similar case), and the degree to which the method is independent of the user/analyst and his/her knowledge and experience.
- Audit capabilities – whether it is possible to retrace the analysis and reconstruct the choices, decisions, or categorisations made during the analysis. This corresponds to Benner's criterion of *comprehensiveness*.
- Time to learn – how long time does it take to learn to use the method and to become a proficient user. Although this clearly is a one-time investment, it is sometimes seen as an argument against adopting a new method.
- Resources needed – or how difficult/easy it is to use the method. Among the main resources are people (hours of work), time, information and documentation needs, etc.
- Validity – whether the findings provided by the method are the proper ones. This is a very contentious issue, since there is no easy way of establishing the correctness of the findings. It is very unusual that the same accident is

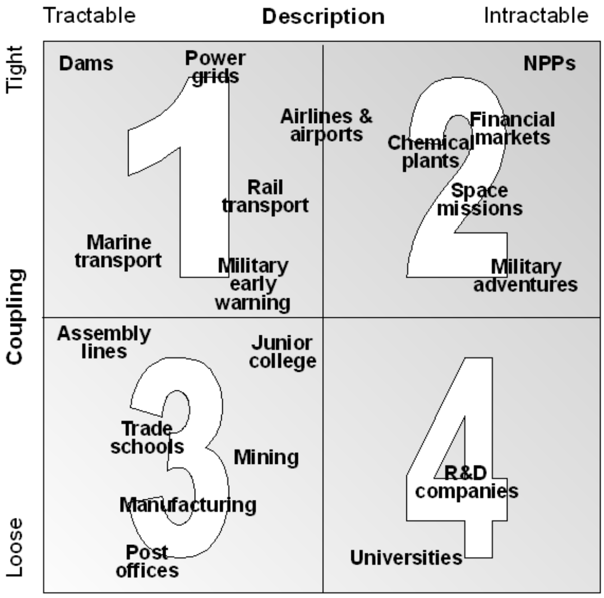
> investigated in more ways than one., and even then there are no obvious independent criteria by which to rate the findings.

The motivation for comparing and rating different methods is to be able to choose the method that is best suited to solve a given problem. Although criteria such as speed, resource demands, and prevalence in an industry are not unimportant, the primary concern must be whether an investigation method can do what it is supposed to do, namely produce an adequate explanation or account of why an adverse event (an accident or an incident) occurred. An investigation method is basically a tool, and it is clearly crucial that the tool is well-suited to the task at hand. Although most tools can be used for different purposes – a wrench can, for instance, be used as hammer – it is obviously better and more efficient if the tool fit the job precisely. This goes for physical tools as well as for methods. It is therefore important to be able to characterise methods with regard to how well they fit the task at hand, which in practice means how well they can represent and account for the complexity of the actual situations.

Few of the criteria referred to above make any reference to this quality, the main exception being Benner's criteria of *functional* and *non-causal*. A good starting point can, however, be found in Perrow's (1984) description of the complexity of socio-technical systems, cf. Figure 1. Perrow proposed the two dimensions of *coupling*, going from loose to tight, and *interactions*, going from linear to complex. While the notion of coupling is relatively straightforward, the notion of complexity must be used with some care, since it can refer either to the ontological or the epistemological complexity[2] (Pringle, 1951). For practical reasons it is preferable to use a different concept, namely how easy it is to describe the system, where the extremes are tractable and intractable systems. A system, or a process, is tractable if the principles of functioning are known, if descriptions are simple and with few details, and most importantly if the system does not change while it is being described. Conversely, a system or a process is intractable if the principles of functioning are only partly known or even unknown, if descriptions are elaborate with many details, and if the system may change before the description is completed. A good example of a tractable system is a post office, or rather the normal functions of a post office, or the operation of a home furnace. Similarly, a good example of an intractable system is the outage at a NPP or the activities in a hospital emergency department. In the latter cases the activities are not standardised and change so rapidly that it is never possible to produce a detailed and complete description.

Using this modification of the terminology, we can propose a new version of Perrow's diagram, as shown in Figure 2. (Note that this also means that some of the examples used by Perrow have to change position; in addition, some examples (e.g., nuclear weapons accidents) have been deleted, while others (financial markets) have been introduced. These changes are, however, illustrative rather than exhaustive.)

[2] Epistemological complexity can be defined as the number of parameters needed to define a system fully in space and time. Ontological complexity has no scientifically discoverable meaning as it is not possible to refer to the complexity of a system independently of how it is viewed or described.



Following this principle, accident investigation methods should be characterised in terms of the systems – or conditions – they can account for. Despite Benner's (1985) concerns, this does depend on the underlying accident model. For instance, a simple linear accident model – such as the domino model (Heinrich, 1931) – can be used to account for certain types of accidents and not for others. The domino model is suitable for systems – hence for accidents – that are loosely coupled and tractable. The reason is simply that most systems were of that type at the time it was developed. Nuclear power plants considered as systems are, however, tightly coupled and more or less intractable. They therefore require accident models and accident investigation methods that are capable of accounting for these features. It is therefore reasonable to characterise investigation methods in terms of which applications they can account for. While this will not by itself determine whether one method is "better" than another, it will make it possible to choose a method that is suitable for a specific purpose and/or system and thereby also to exclude methods that are unable to meet the requirements of an investigation.

7 Selection of accident investigation methods

Following the principles outlined above, it is possible to define four categories of accident investigation methods, corresponding to the four quadrants of Figure 2. The set of 21 methods listed by Table 1 was first reduced to retain only *prima facie* accident investigation methods and to avoid overlapping methods. In consequence of this, the following methods have not been retained: CA (Change Analysis), ECFC (Events and causal factors charting), ECFCA (Events and Causal Factors Charting and Analysis), HFACS (Human Factors Analysis and Classification System), HFIT (Human factors investigation tool), HPES (Human Performance Enhancement System), PEAT (Procedural Event Analysis Tool), SAFER 2007, SCAT (Systematic Cause Analysis

Technique), STEP (Sequentially Timed Events Plotting), and TRACEr (Technique for Retrospective Analysis of Cognitive Errors).

7.1 Methods suitable for systems that are loosely coupled and tractable

In terms of frequency or numbers, most systems are loosely coupled and tractable even today. Although a NPP clearly is not among them, and although few other industries of concern are, many of the commonly used investigation methods nevertheless seem to be best suited for – or even to assume – that the systems they describe are loosely coupled and tractable. In practical terms this implies that it is possible both to have a more or less complete description of the system and to account for events (e.g., failures or malfunctions) one by one or element by element. While these assumptions make for methods that are easier or simpler in terms of use, they also means that such methods are unable to account for complex phenomena, hence to produce practically useful explanations of accidents of that nature.

Each method is described by means of the following characteristics:

- References: The main scientific referens or source of information that describes the method.
- Related methods: Other methods of the same type or that use the same principle.
- Main principle: The main analytical principle on which the method is based.
- Procedure: The main steps in using the method.
- Type of results: The main outcomes that the method produces.
- Operational efficiency and methodological strength: how easy it is to use the method in practice and how much the method depends on the user's knowledge and experience.
- Theoretical grounding, i.e., how well founded the concepts and categories are – in essence which accident model the method implies.
- Practical value, i.e., how well the method support effective recommendations.

There are several sub-categories of methods for loosely coupled and tractable systems. In the following four sub-categories will be described: (1) methods that focus on the identification of failed barriers, (2) methods that focus on human error, (3) methods that focus on root causes in isolation, and (4) methods that focus on root causes in combination.

Example of methods that focus on barriers and/or defences and explain accidents as the result of failed or deficient barriers

Name:	**AEB (Accident Evolution and Barrier Analysis)**
References:	Svensson, O. (2001). Accident and Incident Analysis Based on the Accident Evolution and Barrier Function (AEB) Model. Cognition, Technology & Work, 3(1), 42-52.
Related methods:	Barrier analysis methods in general that focus on the barriers that should, but did not, prevent the occurrence of an adverse event and/or an unwanted outcome. Barrier analysis is used to identify hazards associated with an accident and the barriers that should have been in place to prevent it. A barrier is any means used to control, prevent, or impede the hazard from reaching the target. barrier analysis addresses: barriers that were in place and how they performed, barriers that were in place but not used, barriers that were not in place but were required, barrier(s) that, if present or strengthened, would prevent the same or similar accidents from occurring in the future.
Main principle:	The Accident Evolution and Barrier Function (AEB) model provides a method for analysis of incidents and accidents that models the evolution towards an incident/accident as a series of interactions between human and technical systems. The interaction consists of failures, malfunctions or errors that could lead to or have resulted in an accident. The method forces analysts to integrate human and technical systems simultaneously when performing an accident analysis.
Procedure:	The method starts with the simple flow chart technique of the method. The flow chart initially consists of empty boxes in two parallel columns, one for the human systems and one for the technical systems. During the analysis these error boxes are identified as the failures, malfunctions or errors that constitute the accident evolution. In general, the sequence of error boxes in the diagram follows the time order of events. Between each pair of successive error boxes there is a possibility to arrest the evolution towards an incident/accident. An AEB analysis consists of two main phases. The first phase is to model the accident evolution in a flow diagram. AEB only models errors and is not an event sequence method. The second phase consists of the barrier function analysis. In this phase, the barrier functions are identified (ineffective and/or non existent). The same barrier function can be performed by different barrier function systems. Correspondingly, a barrier function system may perform different barrier functions.
Type of results:	An important purpose of the AEB-analysis is to identify broken barrier functions, the reasons for why there were no barrier functions or why the existing ones failed, and to suggest improvements.
Operational efficiency and methodological strength:	The method is simple to use due to its diagrammatic representation. But since it represents only what went wrong, rather than the whole sequence of events, it is limited in its ability to support recommendations and decisions about precautions and protections. In practice, it can only lead to recommendations about strengthening (failed) barriers.
Theoretical grounding:	The theoretical grounding is linear causality. The method is based on a simple linear accident model, and the graphical representation corresponds to a fault tree without combinations. The method recognises the interplay of human and technical systems.
Practical value:	The method has only had limited practical application.

Examples of methods that focus on human error as the primary contributor to adverse events

Name:	**Human Error in European Air Traffic Management (HERA)**
References:	Isaac, A., Shorrock, S. & Kirwan, B. (2002) Human error in European air traffic management: The HERA project. Reliability Engineering and System Safety, 75(2), 257-272. Additional documentation is available from http://www.eurocontrol.int/humanfactors/public/standard_page/hera.html
Related methods	Technique for Retrospective Analysis of Cognitive Errors (TRACEr)
Main principle:	HERA is a method to identify and quantify the impact of the human factor in incident/accident investigation, safety management and prediction of potential new forms of errors arising from new technology. Human error is seen as a potential weak link in the ATM system and measures must therefore be taken to prevent errors and their impact, and to maximise other human qualities such as error detection and recovery. HERA is predicated on the notion that human error is the primary contributor to accidents and incidents.
Procedure:	1. Defining the error type. 2. Defining the error or rule breaking or violation behaviour through a flowchart. 3. Identifying the Error Detail through a flowchart. 4. Identifying the Error Mechanism and associated Information Processing failures through flowcharts. 5. Identifying the tasks from tables. 6. Identifying the Equipment and Information from tables. 7. Identifying all the Contextual Conditions through a flowchart and tables.
Type of results	Identification of human errors and violations. Quantitative data on the relative frequency of error types and working conditions.
Operational efficiency and methodological strength	HERA is supported by instruction manuals, courses, and some software tools. Given that the premises of the method are accepted (cf., below), it is therefore one of the more mature accident analysis methods. In practice, however, there are often some uncertainty about the precise definition and use of the categories of causes defined by HERA, e.g., violations, mistakes, etc.
Theoretical grounding	The theoretical grounding is linear causality and human error. As the name implies, the method only looks for instances of human errors as causes. The underlying theory is based on various types of human information processing models, as described, e.g., by Reason (1990). The method assumes that the primary cause of adverse events is the human error, and therefore look for this before considering the possible effect of performance shaping conditions.
Practical value	HERA is extensively used by European Air traffic Service organisations, although with varying degrees of success. Eurocontrol has supplemented the development of HERA with related methods, such as HERA-JANUS, HERA-Observe, HERA-PREDICT, and HERA-SMART. The analysis results have been compiled into a database for the purpose of supporting risk assessment of future ATM systems. It is uncertain whether the approach can be transferred to the nuclear domain without a complete revision of the classification system used.

Examples of methods that focus on root causes

Name:	**Root cause analysis (RCA)**
References:	Wilson, P. et. al. (1993). Root cause analysis – A tool for total quality management. Milwaukee, WI: Quality Press. According to Wikipedia, the first use of the term "root cause" can be found in 1905 (an article in *The Lancet*). The term is widely used in the general literature, although there is no specific theory or model of RCA – apart from company brochures, of course. It is a philosophical rather than a scientific concept.
Related methods	TapRooT®
Main principle:	Root cause analysis identifies underlying deficiencies in a safety management system that, if corrected, would prevent the same and similar accidents from occurring. Root cause analysis is a systematic process that uses the facts and results from the core analytic techniques to determine the most important reasons for the accident.
Procedure:	1. Determine sequence of events 2. Define causal factors 3. Analyse each causal factor's root causes 4. Analyse each root cause's generic causes 5. Develop and evaluate corrective actions 6. Report and implement corrective actions
Type of results	Specific (root) causes that can be the object of specific remedial or corrective action.
Operational efficiency and methodological strength	Root cause analysis is used widely and supported by extensive training material and practical guidance (handbooks, triage cars, etc.). It is considered a very efficient method, and since the approach is a simple reverse tracing of causes, it is rather robust. The simplicity of the method, however, also means that the search is severely constrained, hence that the outcomes are limited to the categories defined by the method.
Theoretical grounding	A root cause is defined as "the causal factor(s) that, if corrected, would prevent recurrence of the accident. A root cause analysis is defined as any methodology that identifies the causal factors that, if corrected, would prevent recurrence of the accident. RCA therefore represents the single cause philosophy, I.e., the belief that there is a single cause for any outcome that, if prevented, would prevent the outcome itself. In this context, the root cause is the cause which dominates over all other contributing factors. The type of reasoning relies on the use of counterfactual conditionals. The problem is that one cannot logically conclude that the consequent will be false if the antecedent is false. In other words, one cannot conclude that if the root cause is removed, then the effects will not happen. The reason is simply that there may be several other ways in which the same effects can occur.
Practical value	Root cause analysis is widely used across many industries, including for healthcare and quality management (e.g., the Ishikawa fish-bone diagrams).

Examples of methods that combine multiple factors to explain accidents

Name:	**HINT – J-HPES**
References:	Takano, K., Sawayanagi, K. & Kabetani, T. (1994). System for analysing and evaluating human-related nuclear power plant incidents. Journal of Nuclear Science Technology, 31, 894-913. INPO (1989). Human performance enhancement system: Coordinator manual (INPO 86-016, Rev. 02). Atlanta, GA: Institute of Nuclear Power Operations.
Related methods	The Human Performance Evaluation System (HPES), originally developed by the Institute of Nuclear Power Operations in 1987 (INPO, 1989), uses a family of techniques to investigate events, with particular emphasis on determining human performance aspects. The HPES methodology incorporates many tools such as task analysis, change analysis, barrier analysis, cause and effect analysis, and event and causal factor charting. Additionally, many similar methodologies have been developed from HPES and adapted where necessary to suit the specific requirements of individual organizations.
Main principle:	HINT is a recent development of J-HPES, the Japanese version of the HPES. The overall principle is to use a root cause analysis of small events to identify trends, and to use this as a basis for proactive prevention of accidents. The same principles can be found in SAFER, although the latter method has a wider scope, and therefore may be applicable to accidents in tightly coupled systems as well.
Procedure:	The method comprises the following four steps. Step 1. Understand the event. Step 2: Collect and classify causal factor data. Step 3: Causal analysis, using root cause analysis. Step 4: Proposal of countermeasures.
Type of results	The method focuses on minor human error events. It is intended to provide a trend analysis of these, to enable proactive prevention of serious accidents.
Operational efficiency and methodological strength	The steps of the method are described on a rather high level, and are therefore best applied by people with considerable experience in both the domain and in human factors. The method is aimed at accident investigation rather than accident analysis, but is less direct and explicit in steps 1, 2, and 4 than in step 3.
Theoretical grounding	The method is a variant of root cause analysis enriched by concerns for human and organisational factors (cf., HPES).
Practical value	The method is promoted by the Central Institute for Electric Power Industry (CRIEPI) in Japan. It is presented as an error preventing method for industry and business in general, but the actual level of application is unknown.

7.2 Methods suitable for systems that are tightly coupled and tractable

The increasing frequency of non-trivial accidents during the 1980s and 1990s made it clear that many of these could not be explained as a result of sequences or chains of events, but that it was necessary to account for how combinations of multiple sequences of events, or of events and latent conditions, could arise. This led to the proposal of models that often are classified as epidemiological (Hollnagel, 2004). The prototype is the Swiss cheese model.

Name:	**The Swiss cheese model (SCM)**
References:	Reason, J. T. (1990). Human Error. Cambridge University Press
Related methods:	The TRIPOD concept and set of methods, which in a sense also is the origin of the SCM. The idea behind TRIPOD is that organisational failures are the main factors in accident causation. These factors are more “latent” and, when contributing to an accident, are always followed by a number of technical and human errors. HFACS (Human Factors Analysis and Classification System), used by the Federal Aviation Agency (US).
Main principle:	In the Swiss Cheese model, an organization's defences against failure are modelled as a series of barriers, represented as slices of Swiss cheese. The holes in the cheese slices represent individual weaknesses in individual parts of the system, and are continually varying in size and position in all slices. The system as a whole produces failures when all of the holes in each of the slices momentarily align, permitting "a trajectory of accident opportunity", so that a hazard passes through all of the holes in all of the defenses, leading to a failure.
Procedure:	The basic method for using the SCM is to trace backwards from the accident. The analysis looks for two main phenomena: active failures, which are the unsafe acts committed by people (slips, lapses, fumbles, mistakes, and procedural violations); and latent conditions, which arise from decisions made by designers, builders, procedure writers, and top level management. Latent conditions can translate into error provoking conditions within the local workplace and they can create long-lasting holes or weaknesses in the defences. Unlike active failures, whose specific forms are often hard to foresee, latent conditions can be identified and remedied before an adverse event occurs. Understanding this leads to proactive rather than reactive risk management.
Type of results:	Identification, and classification, of active failures and latent conditions.
Operational efficiency and methodological strength:	The method is initially easy to use, but in its original form lack operational details. This has been remedied in various institutionalised version (e.g., by SHELL), but it still requires an appreciable level of experience to use effectively. The method is supported by a rather extensive set of instructional materials, tutorials, web-based instructions, etc.
Theoretical grounding:	The method represents a complex, linear model. It is quite similar to a fault tree, although the common graphical representation is different – and less detailed. The method focuses on human errors in combination with latent operational conditions, and distinguishes between failures at the sharp and the blunt ends.
Practical value:	The model was originally propounded by James Reason, and has since gained widespread acceptance and use in healthcare, in the aviation safety industry, and in emergency service organizations. It has recently been called into question by several authors.

Name:	**MTO (Människa-Teknologi-Organisation or Man-Technology-Organisation)**
References:	Rollenhagen, C. (1995)*. MTO – En Introduktion: Sambandet Människa, Teknik och Organisation. Lund, Sweden: Studentlitteratur. Bento, J.-P. (1992). Människa, teknik och organisation. Kurs i MTO-analys för Socialstyrelsen. Studsvik, Nyköping: Kärnkraftsäkerhet och Utbildnings AB. Worledge, D. (1992). Role of human performance in emergency systems management. Annual Review of Energy and the Environment, 17, 285-300.
Related methods:	The method is based on INPO's HPES (Human Performance Enhancement System) described above.
Main principle:	The basis for the MTO-analysis is that human, organisational, and technical factors should be focused equally in an accident investigation.
Procedure:	An MTO investigation comprises three methods: 1. Structured analysis by use of an event- and cause-diagram. 2. Change analysis by describing how events have deviated from earlier events or common practice. 3. Barrier analysis by identifying technological and administrative barriers which have failed or are missing. The first step in an MTO-analysis is to develop the event sequence longitudinally and illustrate the event sequence in a block diagram. Then, to identify possible technical and human causes of each event and draw these vertically to the events in the diagram. The next step is to make a change analysis, i.e. to assess how events in the accident progress have deviated from normal situation, or common practice. Further, to analyse which technical, human or organisational barriers have failed or were missing during the accident progress. The basic questions in the analysis are: ● What may have prevented the continuation of the accident sequence? ● What may the organisation have done in the past in order to prevent the accident? The last step in the MTO-analysis is to identify and present recommendations. These should be as realistic and specific as possible, and might be technical, human or organisational.
Type of results:	Details and clarification of factors that either led to or contributed to the accident.
Operational efficiency and methodological strength:	The use of the method is supported by instruction materials and books. It is fairly easy to use, but is not recommended for novices. The identification of specific causes and conditions relies more on experience than on a well-defined set of categories. The method includes several aspects of a full accident investigation, including the recommendations.
Theoretical grounding:	The method refers to a complex, linear accident model. The common representation is, however, more in the nature of a fish bone diagram than a fault tree. The method tends to consider causal factors one by one, rather than in a larger context.
Practical value:	The MTO method has been extensively used by the Swedish NPPs. The principle is also widely used in other domains, such as traffic safety and aviation. The MTO methods has many features common with other methods (Swiss cheese, HPES), but distinguishes itself from the single-factor methods.
	*SKI comment: Rollenhagen has a bool from 2003 on the subject.

Name:	**Cognitive Reliability and Error Assessment Method (CREAM)**
References:	Hollnagel, E. (1998). Cognitive reliability and error analysis method. Oxford, UK: Elsevier Science Ltd.
Related methods:	CREAM is a so-called second generation HRA methods, but differs from other methods of the same type (ATHEANA, MERMOS) by being explicitly developed for both accident investigation and risk assessment.
Main principle:	CREAM was developed to be used both predictively and retrospectively. CREAM uses the Contextual Control Model (COCOM) as a basis for defining four different control modes (strategic, tactical, opportunistic, scrambled). It is assumed that a lower degree of control corresponds to less reliable performance. The level of control is mainly determined by the common performance conditions (CPC). The retrospective use (accident analysis) is based on a clear distinction between that which can be observed (called phenotypes) and that which must be inferred (called genotypes). The genotypes used in CREAM are divided into three categories: individual, technological and organisational, corresponding to the MTO triplet.
Procedure:	The procedure for CREAM comprises the following steps: 1. Produce a description of what actually happened 2. Characterise Common Performance conditions 3. Produce a time-line description of significant events 4. Select all actions of interest 5. For each action, identify failure mode (this is done iteratively) 6. For each failure mode, find relevant antecedent-consequent links (this is done recursively) 7. Provide overall description and draw conclusions.
Type of results:	A graph, or a network, of antecedent actions (functions) and conditions that together constitute an effective explanation of the accident. The graph shows how various actions and conditions affected each other in the given situation.
Operational efficiency and methodological strength:	The CREAM method is clearly described, but not easy to use. This is due to the non-hierarchical nature of the method. The method, however, produces a clear audit trail, which enhances the reliability. The method has recently been supported by a computerised navigation tool, which makes it easier to use, once it has been learned.
Theoretical grounding:	The method does not look for specific causes, but rather for the operational conditions that can lead to a loss of control, hence accidents. It is grounded in cognitive systems engineering. Similar to other second generation methods it rejects consider human error as a meaningful causal category. The basis for the analysis is the event as it happened, rather than preconceived causal factors.
Practical value:	CREAM is a borderline method that in principle can be applied also to accidents in intractable systems. However, the emphasis on tractability of past events, if not of the system itself, means that it should primarily be thought of for use with tractable systems. CREAM has been used extensively in Norway and Sweden as a specific method for traffic accidents under the name of DREAM (D stands for Driver). There has also been a number of uses of the proactive version of CREAM for risk assessment, for instance for NPP emergency procedures and space station operations.

7.3 Methods suitable for systems that are loosely coupled and intractable

There are no investigation methods in this category. The reason for that has to do with the historical development of accident models and investigation methods. At the beginning, effectively in the 1930s, industrial systems were loosely coupled and tractable. As technologies and societies developed, systems became more tightly coupled through vertical and horisontal integration, and at the same time less tractable because new technologies allowed faster operations with more extensive automation. The latter meant in particular that they became more or less self-regulating under normal conditions, which reduced tractability. Since accidents ‘followed’ these developments, methods were developed to be able to adress the new problems. Conversely, few if any accident of note took place in loosely coupled, intractable systems, hence no methods were developed to account for that. The basic reason is that such systems are social rather than technological, e.g., universities, research companies, and the like.

7.4 Methods suitable for systems that are tightly coupled and intractable

The continuously growing complexity of socio-technical systems, and the consequent reduction of tractability, has led to a fundamental change in the approach to risk and safety. The most prominent example of that is the development resilience engineering (Hollnagel, Woods & Leveson, 2006), which changes the focus from failures and actions gone wrong to the usefulness of normal performance variability. With respect to accident investigations this means that the aim is to understand how adverse events can be the result of unexpected combinations of variations in normal performance, thereby avoiding the need to look for a human error or root cause.

This view is often referred to as a systemic view. There are presently two main proposals for a method, STAMP and FRAM.

Name:	**System-theoretic model of accidents (STAMP)**
References:	Leveson, N. G. (2004). A New Accident Model for Engineering Safer Systems. Science, 42(4), 237-270.
Related methods:	Some relation, but not strong, to control theoretic methods such as Acci-map. Also some similarity to the Why-Because Analysis (WBA), cf. http://www.rvs.uni-bielefeld.de/research/WBA/
Main principle:	The hypothesis underlying STAMP is that system theory is a useful way to analyze accidents, particularly system accidents. Accidents occur when external disturbances, component failures, or dysfunctional interactions among system components are not adequately handled by the control system. Safety is viewed as a control problem, and is managed via constraints by a control structure embedded in an adaptive socio-technical system. Understanding why an accident occurred requires determining why the control structure was ineffective. Preventing future accidents requires designing a control structure that will enforce the necessary constraints. Systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. STAMP claims to be general method for explanation of mishaps with teleological systems
Procedure:	Uses a feedback control system as a specific causal model. The analysis proceeds along the following lines: 1. In teleological systems, various subsystems maintain constraints which prevent accidents 2. If an accident has occurred, these constraints have been violated 3. STAMP Investigates the systems involved, especially human-organisational subsystems, to identify missing or inappropriate features (those which fail to maintain the constraints) 4. It proceeds through analysing feedback & control (F&C) operations
Type of results:	The most basic component of STAMP is not an event, but a constraint. Accidents are therefore viewed as resulting from interactions among components that violate the system safety constraints. The control processes that enforce these constraints must limit system behavior to the safe changes and adaptations implied by the constraints. Inadequate control may result from missing safety constraints, inadequately communicated constraints, or from constraints that are not enforced correctly at a lower level.
Operational efficiency and methodological strength:	STAMP can systematically uncover organisational structures and direct the analyst to ask revealing questions. Since STAMP is an analysis method on ly, it depends very much on the quality of the investigation report (data, information). Due to the complexity of the underlying model (cf., below), it requires a considerable effort to use, and is in its present state only fitted for experienced users. A method for a structured presentation of results is not currently available.
Theoretical grounding:	STAMP uses a specific causal model, i.e., a feedback control system. The basic principle is that an accident occurs when operational constraints have been violated. STAMP investigates systems involved, especially human-organisational subsystems, to identify missing or inappropriate features (those which fail to maintain the constraints). It proceeds through analysing feedback & control (F&C) operations, which replaces the traditional chain-of-events model. The model includes software, organizations, management, human decision-making, and migration of systems over time to states of heightened risk.

Practical value:	STAMP has not been widely used and must still be considered under development. The pros and cons of the method have been debated in the RISK forum (http://catless.ncl.ac.uk/risks).

Name:	**Functional Resonance Accident Model (FRAM)**
References:	Hollnagel, E. (2004). Barriers and accident prevention. Ashgate. Nouvel, D.; Travadel, S. & Hollnagel, E. (2007). Introduction of the concept of functional resonance in the analysis of a near-accident in aviation. Ispra, November 2007, 33rd ESReDA Seminar: Future challenges of accident investigation. Sawaragi, T.; Horiguchi, Y. & Hina, A. (2006). Safety analysis of systemic accidents triggered by performance deviation. Bexco, Busan, South Korea, October 18-21. SICE-ICASE International Joint Conference 2006.
Related methods:	There is some relationship to methods such as variation trees or variation diagrams, although these were developed for tractable and loosely coupled systems.
Main principle:	A method for accident investigation as well as risk assessment based on a description of system functions. Non-linear propagation of events are described by means of functional resonance, trigered by normal performance variability.
Procedure:	1. Define the purpose of modelling and describe the situation being analysed. 2. Identify essential system functions; characterise each function by six basic parameters (input, output, time, control, pre-conditions, resources). 3. Characterise the (context dependent) potential variability using a checklist. Consider both normal and worst case variability. 4. Define functional resonance based on possible dependencies (couplings) among functions. 5. Identify barriers for variability (damping factors) and specify required performance monitoring.
Type of results:	The analysis uncovers dependencies among functions or tasks that normally are missed. It also identifies the information needed for the investigation. The concrete result can be a graphical rendering of how the accident developed and/or a detailed written description.
Operational efficiency and methodological strength:	The method is structurally simple and covers several of the accident investigation phases. It, however, requires an initial learning period, due to its different theoretical grounding (cf., below). Since the method does not include a set of causal categories (taxonomy), it is necessary that the user has extensive experience with the domain, as well as with human and organisational factors. FRAM is supported by a software tool (the FRAM visualizer).
Theoretical grounding:	FRAM is based on a specific theory of functional resonance. This enables it to account for non-linear interactions and to dispense with the classical cause-effect relation. The basis, both for analysis and for risk assessment, is a description of system functions (including MTO), rather than system structures or components. It is therefore easily scalable.
Practical value:	FRAM has been used extensively in several different domains (Aviation, Air Traffic Management, Critical Information Infrastructures, Emergency Management, Offshore, Healthcare).

8 Discussion and conclusions

One way of summarising the characterisation of the nine accident investigation methods described in the preceding chapter is to map them onto the modified Perrow diagram of Figure 2. The result is shown in Figure 3. This shows that most methods are applicable to tractable systems, or rather that the assumption is that the systems are tractable. Conversely, one may conclude that these methods should not be used for intractable systems, since they will not be able to produce adequate explanations. Several of the commonly used methods, including root cause analysis, AEB, and HERA, also require that systems only are loosely coupled; in other words, they are unable to account for the consequences of tight couplings, hence adequately to explain accidents in systems of that type.

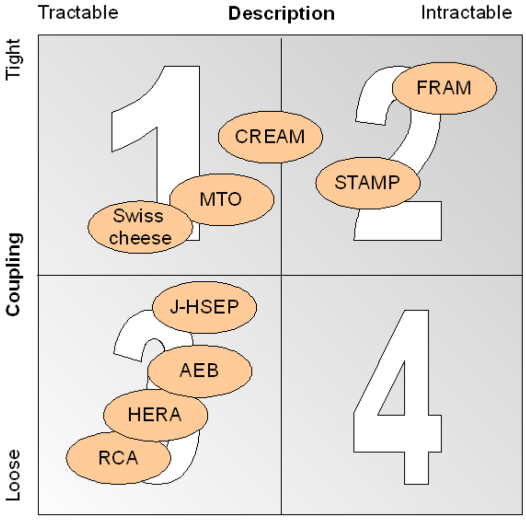


Figure 3: Characterisation of accident investigation methods

It is sensible to assume that any method would be just about adequate for the typical type of problems at the time it was developed. Indeed, there would be little reason to develop a method that was too complex or more powerful than required. As argued in the beginning, new methods are usually developed because the existing methods at some point in time encounter problems for which they are inefficient or inadequate. This, in turn, happens because the socio-technical systems where accidents happen continue to develop and to become more complex and more tightly coupled. The inevitable result is that even new methods after a while become underpowered because the nature of the problems change, although they may have been perfectly adequate for the problems they were developed for in the first place.

The position of the various methods on the diagram in Figure 3 presents a characterisation of the methods using the two dimensions of coupling and tractability, and thereby indirectly represents the developments of socio-technical systems since the 1930s. Without going into the details of this development, the third quadrant can be seen as representing industrial systems before the middle of the 20th Century, i.e., before the large scale application of information technology. The development since then has been one in terms of tighter coupling (moving up into the first quadrant) and a loss of tractability (moving right into the second quadrant). This has in turn required the development of new methods, as shown in the diagram.

The position of a method reflects the assumptions behind the method, specifically what has been called the accident model. The arguments for each method were presented above. To illustrate the significance of the position, consider for instance the two extremes RCA and FRAM.

- Root cause analysis (RCA) assumes that adverse outcomes can be described as the outcome of a sequence (or sequences) of events or a chain (or chains) of causes and effects. The investigation is therefore a backwards tracing from the accident, trying to find the effective cause(s). The method requires that the system is tractable, since it otherwise would be impossible to carry out this backwards tracing. The method also requires that the system is only loosely coupled, since it otherwise would be impossible to feel confident that the correction or elimination of the root cause would prevent a recurrence of the accident.
- The functional resonance accident model (FRAM) assumes that adverse outcomes are the result of unexpected combinations of normal variability of system functions. In other words, it is the tight couplings that lead to adverse outcomes and not sequences of cause(s) and effect(s). Since the investigation furthermore looks for functions rather than structures, it is less problematic if the description is intractable. Indeed, functions may come and go over time whereas system structures must be more permanent. Functions are associated with the social organisation of work and the demands of a specific situation. Structures are associated with the physical system and equipment, which does not change from situation to situation.

This characterisation does not mean that FRAM is a better method than RCA. (A similar argument can be made for any other comparison of two methods.) But it does mean that FRAM is well-suited for some kinds of problems and that RCA is well-suited for others. (It of course also means that there are problems for which either method is ill-suited.).

In order to choose the right method to investigate an accident it is necessary first of all to characterise the accident. This can be achieved by asking a number of questions, for example:

1. Was the accident similar to something that has happened before, or was it new and unknown? (The reference should be the history of the installation, as well as industry wide.).
2. Was the organisation ready to respond to the accident, in the sense that there were established procedures or guidelines available?
3. Was the situation quickly brought under control or was the development lengthy?
4. Was the accident and the material consequences confined to a clearly delimited subsystem (technological or organisational) or did it involve multiple subsystems, or the whole installation?
5. Were the consequences on the whole expected / familiar or were they novel / unusual?

6. Were the consequences in proportion to the initiating event, or were they unexpectedly large (or small)?

(When considering these questions one should bear in mind, of course, that the answers rely on an initial and informal understanding of what may have happened. An experienced accident investigator should be able to do this without being biased by premature assumptions about the nature of the cause.).

The first three questions illustrate issues that relate to the dimension of tractability. If the questions are answered positively, it indicates that the system was tractable, at least to some degree. The opposite is the case if the questions were answered negatively.

Questions 4-6 illustrate issues that relate to the dimension of coupling. If the questions are answered positively, it indicates that the system was of the loosely coupled type. The opposite is the case if the questions were answered negatively.

In conclusion, when faced with the need to investigate an accident it is important that the method chosen is appropriate for the system and the situation, i.e., that it is capable of providing an explanation. If the accident concerns the NPP operation as a whole, the problems correspond to the characteristics of the second quadrant. The investigation method must therefore be able to address systems of that nature. If the accident only concerns the operation of a subsystem or a component, the problems may correspond to the characteristics of the first or even the third quadrant. The investigation method can also therefore be different. The six questions given above suggest how the characteristics of the accident can be determined.

In addition to that other concerns may also play a role, such as resource demands, ease of use, and consistency with other methods within the organisation or industry. While it may be convenient, or even necessary, for an organisation to adopt a specific method as its standard, this should always be done knowingly and with a willingness to reconsider the choice when the conditions so demand it. Socio-technical systems, processes, and organisations continuously change and develop, driven by internal and external forces and demands. The methods that are available to manage those systems and to investigate them when something goes awry, change at a much slower rate. Changes are furthermore usually discrete rather than continuous. The often felt consequence of this is that the available methods lag behind reality, often by as much as a decade or two. The diagram of Figure 3 therefore only represents the situation at the time of writing, i.e., around 2008. In five or ten years we must expect that the methods positioned in quadrant 2 slowly will have been displaced towards quadrant 3, not because the methods have changed but because the systems have. New and more powerful methods will – hopefully – by then have been developed to accommodate this state of affairs.

9 Dictionary

	Engelska	Svenska
ATHEANA	A Technique for Human Event Analysis	En teknik för mänsklig händelseanalys
CICA	Caractéristique Importante de la Conduite Accidentelle	Karakteristika för olycksanalys
CPC	Common Performance Conditions	Kontextuella förutsättningar
CREAM	Cognitive Reliability and Error Analysis Method	Kognitiv pålitlighets- och felanalysmetod
DKV	Operational Readiness Verification (ORV)	Driftklarhetsverifiering
EFC	Error-Forcing Context	Felhandlingsdrivande kontext
ETTO	Efficiency-Thoroughness Trade-Off	Effektivitets- och noggrannhetsavvägning
FRAM	Functional Resonance Accident Model	Resonansolycksmodell
HPES	Human Performance Enhancement System	Mänskligt handlingsförbättrande system
INPO	Institute of Nuclear Power Operation	Institutet för kärnkraftsdrift (USA)
MERMOS	Méthode d'Evaluation des Missions Opérateurs pour la Sécurité	Säkerhetsutvärderingsmetod för operatörer
MTO	Man-Technology-Organisation	Människa – Teknik - Organisation
ORV	Operational Readiness Verification	Driftklarhetsverifiering
WANO	World Association of Nuclear Operators	Världsorganisationen för kärnkraftsdrift

10 References

Benner, L. Jr., (1985). Rating accident models and investigation methodologies. *Journal of Safety Research*, 16, 105-126.

Bento, J.-P. (1992). *Människa, teknik och organisation. Kurs i MTO-analys för Socialstyrelsen*. Studsvik, Nyköping: Kärnkraftsäkerhet och Utbildnings AB.

Bird, F. E. Jr. & Germain, G. L. (1985). *Practical loss control leadership*. Georgia, USA: International Loss Control Institute.

CCPS (1992). *Guidelines for Investigating Chemical Process Incidents*. Center for Chemical Process Safety of the American Institute of Chemical Engineers.

CISHC (Chemical Industry and Safety Council), (1977). *A guide to hazard and operability studies*. London: Chemical Industries Association.

Cooper, S. E., Ramey-Smith, A. M., Wreathall, J., Parry, G. W., Bley, D. C., & Luckas, W. J. (1996). *A Technique for Human Error Analysis (ATHEANA)*. Washington, DC: Nuclear Regulatory Commission.

Dekker, S. (2006). *The field guide to understanding human error*. Aldershot, UK: Ashagte.

Dianous, V. D. & Fiévez, C. (2006). ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance. *Journal of Hazardous Materials, 130*(3), 220-233.

DOE. (1999). *Conducting Accident Investigations: DOE Workbook* (Revision 2, May 1, 1999). Washington, DC: U.S. Department of Energy.

FAA/NTIS (2000). *The Human Factors Analysis and Classification System – HFACS* (DOT/FAA/AM-00/7). Washington, DC: Federal Aviation Administration.

Gordon, R., Flin, R. & Mearns, K. (2005). Designing and evaluating a human factors investigation tool (HFIT) for accident analysis. *Safety Science, 43*, 147–171.

Harms-Ringdahl, L. (1987). *Säkerhetsanalys i skyddsarbetet - En handledning*. Folksam, Stockholm.

Harms-Ringdahl, L. (1993). *Safety analysis - Principles and practice in occupational safety*. Elsevier, London.

Harms-Ringdahl, L. (1996). *Riskanalys i MTO perspektiv: Summering av metoder för industriell tillämpning* (SKI Raport 96:63). Stockholm, Sweden: SKI.

Heinrich, H. W. (1929). The foundation of a major injury. *The Travelers Standard*, 17(1), 1-10.

Heinrich, H. W. (1931). *Industrial accident prevention*: New York: McGraw-Hill.

Helmreich, R. L., Merritt, A. C. & Wilhelm, J. A. (1999). The evolution of Crew Resource Management training in commercial aviation. *International Journal of Aviation Psychology, 9*(1), 19-32.

Hendrick, K. & Benner, L. Jr. (1987). *Investigating accidents with STEP*. Marcel Dekker.

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

Hollnagel, E. (2004). *Barriers and accident prevention*. Aldershot, UK: Ashgate.

Hollnagel, E. (2008). *Investigation as an impediment to learning*. In Hollnagel, E., Nemeth, C. & Dekker, S. (Eds.) *Remaining sensitive to the possibility of failure* (Resilience engineering series). Aldershot, UK: Ashgate.

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

IAEA (1999). *Root cause analysis for fire events at nuclear power plants* (IAEA-TECDOC-1112). Vienna, Austria: IAEA.

INPO (1989). *Human performance enhancement system: Coordinator manual* (INPO 86-016, Rev. 02). Atlanta, GA: Institute of Nuclear Power Operations.

Isaac, A., Shorrock, S. & Kirwan, B. (2002) Human error in European air traffic management: The HERA project. *Reliability Engineering and System Safety*, *75*(2), 257-272.

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

Le Bot, P., Cara, F., & Bieder, C. (1999). *MERMOS, A second generation HRA method*. Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment", Washington, DC.

Leveson, N. G. (1995). *Safeware - system safety and computers*. Reading, MA: Addison-Wesley.

Leveson, N. G. (2004). A New Accident Model for Engineering Safer Systems. *Science*, *42*(4), 237-270.

MIL-STD-1629A (1980). *Procedures for performing a failure mode, effects and criticality analysis*. Washington, DC: Department of Defence.

Moodi, M. & Kimball, S. (2004). *Example application of procedural event analysis tool* (PEAT). Seattle, WA: Boeing Company.

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

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

Pringle, J. W. S. (1951). On the parallel between learning and evolution. *Behaviour, 3*, 175-215.

Reason, J. T. (1990). *Human Error*. Cambridge University Press

Reason, J. T. (1997). *Managing the risk of organisational accidents.* Aldershot, UK: Ashgate.

Renborg, B., Jonsson, K., Broqvist, K. & Keski-Seppälä, S. (2007). *Hantering av händelser, nära misstag* (SKI 2007:16). Stockholm: SKI.

Rollenhagen, C. (1995). *MTO – En Introduktion: Sambandet Människa, Teknik och Organisation*. Lund, Sweden: Studentlitteratur.

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

Shorrock, S. T. & Kirwan, B. (1999). *The development of TRACEr - A technique for the retrospective analysis of cognitive errors in ATM.* Proceedings of the 2nd International Conference, 28-30 Oct. 1998, Oxford, UK. (Vol. 3, pp. 163-171).

Shorrock, S. T. & Kirwan, B. (2002). Development and application of a human error identification tool for air traffic control. *Applied Ergonomics*, *33*, 319–336.

Sklet, S. (2002). *Methods for accident investigation* (ROSS (NTNU) 200208). Trondheim, Norway: NTNU.

Svensson, O. (2001). Accident and Incident Analysis Based on the Accident Evolution and Barrier Function (AEB) Model. *Cognition, Technology & Work*, *3*(1), 42-52.

Swain, A. D. (1989). *Comparative evaluation methods for human reliability analysis*. Köln, Germany: Gessellschaft für Reaktorsicherheit.

Takano, K., Sawayanagi, K. & Kabetani, T. (1994). System for analysing and evaluating human-related nuclear power plant incidents. *Journal of Nuclear Science Technology*, *31*, 894-913.

van der Schaaf, T. & Kanse, L. (2004). Biases in incident reporting databases: an empirical study in the chemical process industry. *Safety Science*, 42, 57-67.

Weick, K. E., Sutcliffe, K. M. & Obstfeld, D. (1999). Organising for high reliability: processes of collective mindfulness. *Research in Organisational Behaviour*, *21*, 81–123.

Wickens, C. D. (1992). *Engineering psychology and human performance*. New York: Harper-Collins.

Wilson, P. et. al., (1993). *Root cause analysis – A tool for total quality management*. Milwaukee, WI: Quality Press.

Woods, D. D., Johannesen, L. J., Cook, R. I. & Sarter, N. B. (1994). *Behind human error: Cognitive systems, computers and hindsight*. Columbus, OH: CSERIAC.

Worledge, D. (1992). Role of human performance in emergency systems management. *Annual Review of Energy and the Environment*, *17*, 285-300.

Yoshizawa,Y. (1999). *Activities for on-site application performed in human factors group*. Proceedings of 3rd International Conference on Human Factors in Nuclear Power Operation (ICNPO-III), Mihama, Japan.

www.ski.se

STATENS KÄRNKRAFTINSPEKTION
Swedish Nuclear Power Inspectorate

POST/POSTAL ADDRESS SE-106 58 Stockholm
BESÖK/OFFICE Klarabergsviadukten 90
TELEFON/TELEPHONE +46 (0)8 698 84 00
TELEFAX +46 (0)8 661 90 86
E-POST/E-MAIL ski@ski.se
WEBBPLATS/WEB SITE www.ski.se