Developing a method to improve safety management systems based on accident investigations : the SAfety FRactal ANalysis

Reference:
Accou Bart, Reniers Genserik.- Developing a method to improve safety management systems based on accident investigations : the SAfety FRactal ANalysis
Safety science - ISSN 0925-7535 - 115(2019), p. 285-293
Full text (Publisher's DOI): https://doi.org/10.1016/J.SSCI.2019.02.016

Developing a method to improve Safety Management Systems based on accident investigations: the SAfety FRactal ANalysis method.

Authors:
Bart Accou, European Union Agency for Railways, France
Genserik Reniers, Safety and Security Science, Delft University of Technology, The Netherlands

Abstract:
The concept of a safety management system (SMS) to control the risks of operational activities has been introduced in high-risk industries already some decades ago. SMS requires accidents/incidents to be reported and analysed and measures to be taken to prevent future events. Additionally, national investigating bodies have been given the role of independently investigating serious events, with the same goal. The current practice in accident and incident investigation however, does not provide a systematic approach to analyse elements of SMS. As a direct consequence, the opportunity to use these investigations for introducing sustainable system changes is often missed.
The paper describes the SAfety FRactal ANalysis (SAFRAN) method that is developed to guide investigators to explore the composing elements of an SMS in a natural and logic way, starting from the findings close to operations that explain the occurrence – being the elements accident investigators are first confronted with. The paper further informs on the application of the SAFRAN method to review a selected set of published railway accident investigations, all reporting on occurrences related to over-speeding, possibly resulting in a (lethal) derailment. The depth and focus of the performed investigations is assessed and compared with a reference mode of expected findings that would result from an analysis that is applying the SAFRAN logic. This demonstrates the need, in order to introduce sustainable changes, to focus accident analysis on an organisation's capability of managing the variability that might put successful process performance at risk.

1. Introduction

The publication of Lord Cullen's (1990) recommendations resulting from the public enquiry he led after the deadly disaster on the oil platform Piper Alpha, first launched the concept of a safety management system (SMS) to continuously improve safety of operations. The concept then quickly found introduction in high-risk industries like transport (aviation, railways …), the production of dangerous goods, occupational health, etc. Furthermore, this transition from an often very prescriptive safety approach towards an approach that is evidence-driven and based on goal-oriented legislation, did not only become normative but even legally mandatory in different industries, with the holding of a SMS to control all risks related to a company's operational activities as the basis for certification and regulation (e.g. Vierendeels et al. 2011; Leveson, 2011a; Grote, 2012; Deharvengt, 2013; Fowler, 2013; Lappalainen, 2017).

Various standards and regulations exist that describe or prescribe the basic SMS components, but they all share the requirement for procedures to ensure that accidents, incidents, near misses and other dangerous occurrences are reported, investigated and analysed. They also have the requirement in common that this analysis should result in necessary measures to prevent similar, future events. Additionally, in some high-risk industries, national investigating bodies have been given the role of independently investigating significant events, with the same aim of preventing future accidents and improving the overall safety of the system. Johnson's review (2004) of the original BFU accident investigation report of the famous Überlingen mid-air collision concludes that the investigation had insufficiently analysed the SMS. He further highlights the importance of looking extensively at organisational factors and their contribution to an accident. This finding is in line with the findings of other

authors (e.g. Antonsen, 2009; Kelly, 2017) that the scope of accident and incident investigations, whether performed internally or externally, is usually limited to investigating the immediate causes and decision making processes related to the accident sequence. Important factors, including management decisions (Dien et al., 2007), contributing to the accident are hereby often overlooked and the weaknesses in the SMS, or its composing elements, are hardly ever analysed. Since the type of data collected during accident investigation and the method used to analyse this data will highly influence and sometimes even constrain the proposed remedial actions (e.g. Hale, 2000; Hollnagel, 2008; Underwood and Waterson, 2013a; Salmon et al., 2016), it should be of no surprise that those investigations don't guide directly towards solutions that can be found within elements of the legally obliged SMS. This, in turn, may result in the perception that the SMS approach does not deliver as much as was hoped for when Cullen published his recommendations.

Different authors assign possible underlying causes that could explain these findings. Where a SMS is based on a holistic approach, with operational, supporting and controlling elements functioning together to improve safety, most accident reporting and investigation methods are not developed in line with a system thinking approach to accident causation (e.g. Reason, 1997; Hollnagel and Speziali, 2008; Lundberg et al., 2009, Dekker, 2011). More fundamentally, as pointed out by Lin (2011) but also by Deharvengt (2013), the top down description of SMS requirements creates problems of understanding how to link the generic management activities, aiming at identifying and controlling risks in a systematic way, with the operational activities of the organisation that create these risks in the first place. This is in line with the observation of Rasmussen (1997) that, by lack of vertical interaction between the different levels of the socio-technical system, there is a problem in incorporating theoretical management models like SMS as a tool for resolving issues related to human performance or technical failure at the operational level. Also, this could at least partly explain the difficulty industry has, to translate accident and incident findings into effective safety initiatives (Salmon et al., 2016).

In order to address these problems, an investigation analysis method, called SAFRAN, is developed and proposed in this paper, that can guide investigators to explore the composing elements of an SMS in a natural and logic way, starting from the findings close to operations that explain the occurrence – being the elements accident investigators are first confronted with. Furthermore, as briefly explained in the following chapter, the method can help to identify those elements of the SMS where interventions might have the greatest impact for improving global system safety.

2. The SAfety FRactal ANalysis (SAFRAN) method

The goal of investigating accidents and incidents is, in the first place, to understand why an adverse event happened, based on the available information. In order to satisfy management's and regulators' need to understand what has gone wrong and how it can be prevented, these investigations mostly focus on finding the cause or causes, attributing error to the actions of a person, team or organisation. This process is described by Woods as "a social and psychological process and not an objective, technical one" (Woods et al., 1994), whereby a pattern of causes and contributory factors is constructed, conforming the What-You-Look-For-Is-What-You-Find (WYLFIWYF) principle (Hollnagel, 2008, Lundberg et al., 2009). In this context, Dekker (2014) suggests that it may be more useful to think in terms of explanations rather than causes, leaving as the primary goal for any investigation method to produce an adequate explanation or account of why an adverse event (an accident or an incident) occurred (Hollnagel and Speziali, 2008).

Furthermore, Hollnagel (1998) states that the development of a system to support the analysis of accidents and events must as a minimum include a method and a classification scheme. The purpose of the method is to provide a step-by-step account of how the analysis shall be performed, in order to ensure a consistent application. The classification scheme is necessary both to define the data that should be collected and to describe the details of an event.

As further detailed below, the SAfety FRactal ANalysis (SAFRAN) method tries to fulfill these requirements by combining three distinct elements. The first element is a generic and dimensionless description of what is required for control of safety related activities (the **Safety Fractal**, see 2.1). It is argued that this Safety Fractal, as a combination of a generic model for process management, inspired on SMS requirements, and a set of sources of performance variability to be managed, will provide the necessary elements for classifying an account of why an adverse event happened. As a second element, an investigation flow that guides investigators where to continue to investigate, using **iterations** (see 2.3) of the same five **basic steps** (see 2.1), provides the required investigation method. Thirdly, in addition, the SAFRAN method provides a way to graphically represent the results of the performed analysis.

2.1. The Safety Fractal

The Safety Fractal builds on the apparent need for similar feedback loops or PDCA cycles at the different hierarchical levels in an organisation (Hardjono and Bakker, 2006; Lin, 2011; Grote 2012). Although proceduralisation of operations at the sharp end can (and most probably should) be very different from proceduralisation of safety management, even within a same organisation (Rosness, 2013), this need for similar feedback loops gives enough foundation to believe that it is possible to identify a generic set of requirements that can assure the design of adequate resources and controls for the proper functioning of processes and safety related activities at all levels in an organisation.

To develop this idea, the basic principles of process capability (ISO, 2004) were compared with the general requirements of safety management systems, as developed by Lin (2011) based on the "Dutch Safety Management Model" that has a pedigree that goes back to the first modelling of SMS at the Delft University of Technology in the early 1990s. This results in the identification of the following steps or attributes forming the basis for performing an activity in a controlled way:

- (1) **Specify**: The scope and desired outcome of an activity is specified, roles and responsibilities identified, disrupting events are anticipated and risk control measures (rules, barriers) are designed (i.e. work as imagined).
- (2) **Implement – train, equip, organise**: All is done to have activities performed by enough competent people, adequate technical resources are put available and maintained, work products and resources to be used are identified and work is planned in detail.
- (3) **Perform**: The activity is executed, responding to real life constraints and disturbances (i.e. work as done).
- (4) **Verify**: The system's performance is monitored, i.e. verifying the match between work as designed and work as actually performed, as well as the elements that could affect this performance in the near term.
- (5) **Adapt**: It is known what has happened and lessons are learned from experience and the adequate changes to control, or implementation elements, are introduced.

Graphically representing an accident and/or the results of an accident analysis has been considered useful by several authors (e.g. Sklet, 2004, Underwood and Waterson, 2013). The below Figure 1 graphically represents the found attributes in the form of a triangle, grouping the composing attributes along the three sides according to the nature of their goal. The left-hand side represents a level of **process performance** that is modelling the direct functioning of the components that interact during process execution ("doing things") and that is also the level where variation against process specifications can be observed. The bottom side groups the elements of **process implementation**, providing the resources and means to ensure the correct functioning ("doing things right") of the process components during process execution. The right-hand side of the triangle stands for a level of **process control**, ensuring the sustainable control of risks related to all activities of the organisation in possibly a changing context ("doing the right things"). The arrows, in turn, indicate the logical order in which these safety management activities normally are performed.

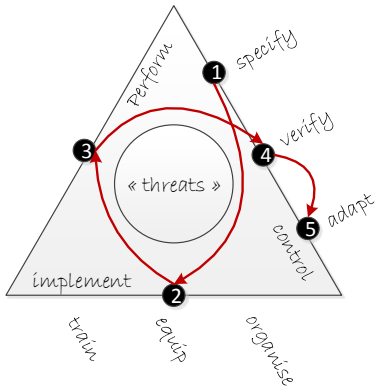

Fig.1: The Safety Fractal

Together, the implementing and the controlling stages define the formal as well as the informal side of safety management and have a direct influence on performance. This representation of the core attributes for safely managing and activity, is in phase with what was proposed by Wahlström and Rollenhagen (2014), in their search for a common approach for modelling systems, subsystems and their interactions; namely to use a control metaphor for the design and assessment of safety management systems (i.e. the control side of the triangle) in combination with the concepts of man, technology, organisational and information systems (MTOI, i.e. the implementation side) to ensure a continued safety of the operated systems (i.e. the perform side of the triangle).

Wahlström and Rollenhagen (2014) further elaborate how this control metaphor, that initially focuses on the safe management of sharp end activities, can also be used for controlling the MTOI-systems as well as different safety management activities, seperately and together; a line of though that can also be found with other authors (e.g. Hollnagel, 1998, van Schaardenburgh-Verhoeve et al., 2007, Lin, 2011 and Leveson, 2011b). We therefore argue that the strength of this simple Safety Fractal model is that it can be applied for all type of activities, including those that form the control and implementing part of it, at every

level of aggregation and at every level within a socio-technical system, which reminds of the characteristics of a fractal[1] – which also explains the name that was given to the model.

Many of the cited authors (e.g. Lin, 2011, Wahlström and Rolenhagen, 2014) still consider the identification and elimination or control of threats that, when initiated by a triggering event will normally come with negative consequences, as the objective of safety management. Hollnagel (2002, 2014), however, argues that there will always be variability in human performance, individually or collectively, and that the best option for managing safety is therefore not to eliminate this performance variability but rather to monitor the system's performance so that potentially uncontrollable variability can be caught early on and dampened by creating those conditions that make work succeed and generate a "resilient performance".
Comparing the Safety Fractal model, that was developed by looking for synergies between the basic principles of process capability and the general requirements of safety management systems, with the four potentials that are proposed by Hollnagel (2009a) as necessary for resilient performance (i.e. the potential 1) to respond, 2) to monitor, 3) to learn and 4) to anticipate), gives a clear indication that the attributes of the Safety Fractal only need to be applied with the right mindset, i.e. making the switch from managing threats to managing performance variability, in order to have the potential to generate resilient performance.

2.2. The investigation logic – basic steps

Over the last two decades, several authors have analysed the evolution in accident investigation methods and have made an attempt to compare them, using different characteristics (e.g. Johnson, 2003, Sklet, 2004, Katsakiori et al., 2009). Some of them did this in an attempt to give guidance to investigators on what method(s) to choose (e.g. Underwood and Waterson, 2013b) or to define what methods are most suited to analyse events in a specific industrial system like nuclear (Hollnagel and Speziali, 2008), railways (Johnson, 2009) or telecommunication (Wienen et al., 2018).

In these reviews, no clear reference was found to methods that explicitly address the analysis of safety managements systems or elements of it. The reason for this may be found in the common accident investigation approach that was distilled by Wienen et al. (2018). When using the categories defined by Hollnagel (2002), based on the underlying accident model the analysis methods use (i.e Sequential, Epidemiological and Systemic), they conclude that essential steps are added as we go from Sequential through Epidemiological to Systemic methods:

1. Find all events that have a causal relationship with the accident
2. Describe the history of the accident by linking these events.
3. Find all conditions that enabled these events, including events that lead to those conditions (only in Epidemiological and Systemic methods).
4. Identify components, feedback mechanisms and control mechanisms that played a role during the development of the accident (only in Systemic methods).
5. Identify at which point the accident could have been prevented and analyse if this can be generalised.
6. Draw conclusions and propose improvement actions.

[1] A fractal is a natural phenomenon or a mathematical set that exhibits a repeating pattern that displays at every scale. It is also known as expanding symmetry or evolving symmetry. If the replication is exactly the same at every scale, it is called a self-similar pattern (Wikipedia; 2018).

Based on this finding, we conclude that only Systemic methods offer and investigator the appropriate toolkit to analyse the feedback and control mechanisms that form the essence of an SMS. So far, the only identified Systemic methods are the Functional Resonance Analysis Method (FRAM - Hollnagel, 2004, 2012) and CAST, the causal analysis method based on the Systems-Theoretic Accident Model and Processes model (STAMP – Leveson, 2011b). However, these systemic analysis methods are not being used within industry (Underwood and Waterson, 2012), mainly because they are perceived as too time consuming and therefore too expensive (e.g. Wienen et al., 2018). In an attempt to address this, an investigation logic was developed, using the elements of the Safety Fractal that can help investigators explore the composing elements of an SMS, starting from their findings close to operations.

Leveson (2000) argues that reasons for proper functioning are derived "top-down" and that, in contrast, causes of improper function depend upon changes in the physical world (i.e. the implementation) and, thus, they are explained "bottom up". Translated to the logic of the Safety Fractal, this means that, where the management of processes starts with the specify element at the level of process control, the investigation of an adverse event should start at the process performance level, by identifying the critical activity as it was performed. The first step in the SAFRAN method therefore aims at finding the answer to the questions who did what?, when? and how? But also finding the answer to what was the intention or expectation of a certain behaviour, the 'local rationality' behind the performance, and what trade-offs people made when trying to balance efficiency and thoroughness in light of system conditions (Hollnagel, 2009b).

In order to be capable of performing and producing in an organised and safe way, any organisation has to define a preferred way of working (e.g. Hale and Borys, 2013; ICSI, 2017). And although these working rules don't need to be explicit for an organisation to perform (Argyris and Schön, 1996) and, according to Leveson (2000), being provided with an incomplete problem representation (specification) can actually lead to worse performance than having no representation at all, a description of work as it is assumed to be -as it is imagined- is considered to be a necessary reference for planning, managing and analysing performance in a sustainable way (Hollnagel, 2018). Therefore, the second step of the SAFRAN method aims at identifying the expected performance and how this was specified in order to be able to control it.

The following and third step in the SAFRAN method is key for guiding investigators where to conduct their further analysis. In essence, this step requires an investigator to look for the reasons why it made sense for those involved in a critical performance to deviate from the specified process in terms of the context of the event, or why the process specification was inappropriate. Both controlled and uncontrolled changes in demands and conditions will require a system to make continually adjustments to its performance, in order to achieve the objectives that are set. Performance of tasks and activities will therefore show variability that can be wanted or unwanted in light of the system's need. Only identifying and changing the contextual factors that led to this variability will allow to make sustainable changes to the system (e.g. Antonsen, 2009; Hollnagel, 2014; Leveson, 2016). In consequence, this third step in the SAFRAN method aims at finding the sources of performance variability (e.g. Kyriakidis et al, 2018) that influenced a critical performance. According to Antonsen (2009), finding the answer to this question requires to take the actors' point of view and aiming at understanding how actors construct their strategies for action - why they do the things they do, in the way they do them.

The fourth step, in turn, looks at finding an answer to the question whether the responsible organisation has identified and is continuously verifying the variability in performance that was initiating the first step of the SAFRAN analysis. Finally, only when there is clear indication that the variability that is under investigation is identified and reported within the organisation, it is required to find an answer to the

question whether the organisation was capable of learning from the detected variability and managed to adapt the system, as a fifth step in the SAFRAN method.

In essence, these consecutive steps in the analysis process can be summarised as follows, with Figure 2 roughly representing the chronology for one iteration of the SAFRAN method:

- STEP 1 – critical performance: starting close to the event sequence, identify the function or activity that showed critical variability in its performance
- STEP 2 – expected performance: for the selected function, identify the expected performance as prescribed and/or specified
- STEP 3 – source(s) of performance variability: identify the factor(s) that can explain the critical variability in performance
- STEP 4 – monitoring of variability : identify whether the responsible organisation is identifying, monitoring and reporting the critical variability
- STEP 5 – learning capability (optional): if reported, identify whether the organisation is learning from the reported (critical) variability

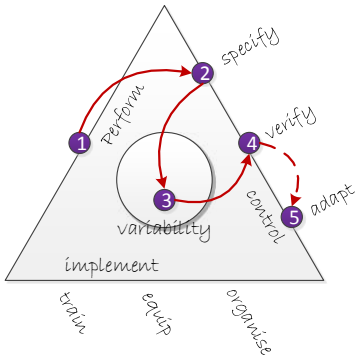

Fig.2: One complete iteration of analysing the Safety Fractal

2.3. The investigation logic – iterate to learn?

Only investigating adverse events will not improve safety performance: lessons need to be learned and the right counter measures need to be taken, by changing an organisation's performance in an intended direction. In that context, several authors (e.g. Dien et al., 2004, Lindberg et al., 2010, Wahlström and Rollenhagen, 2014) highlight that organisations could have been aware of the deficiencies that in the analysis of major accidents are identified as root causes and therefore, in some way or another, suggest the analysis of the controls involved in the feedback of operational experience to be integrated in accident analysis. Del Frate et al. (2011), furthermore, argue that a detailed investigation that backtracks all the events, circumstances and individuals that had some influence on a failure is not worth the effort, because anticipating – or controlling – the future with such detail is simply not feasible and Reason (2008) states that the 'truth', when investigating events, is unknowable, takes many forms and is in any case less important than the practical utility of an analysis method to assist in sense-making and to lead to more effective measures and improved resilience.

Rather than finding elements to constrain performance through a more rigidly definition of activities, in order to control the threats, the effort that is put in accident analysis could therefore better be used to learn an organisation to be resilient in order to compensate for structural shortcomings (van Schaardenburgh-Verhoeve et al., 2007) and to address the weaknesses in the operating feedback systems that hamper a good understanding of vulnerabilities coming from daily, routine functioning (Dien et al., 2007). Investigating an adverse event should then not necessarily give a snapshot of how a system or an organisation has failed, i.e. the classic result of an accident investigation according to Hollnagel (2018), but should focus on collecting information on how well an organisation is capable of ensuring that the internal processes are working properly by monitoring and managing their possible sources of performance variability.

In order to integrate this thinking the logical next steps in the SAFRAN method consist of a new iteration (i.e. a repetition of steps 1 to 5) with functions that either manage the identified source(s) of performance variability or deliver monitoring and/or learning capability. To steer investigators to systematically analyse also these elements of safety management, this "next" iteration is integrated in the proposed method. This results in the following figure, giving an overview of the five identified steps that together form one iteration, as well as the logic to be used for identifying further iterations, here represented as a flow.

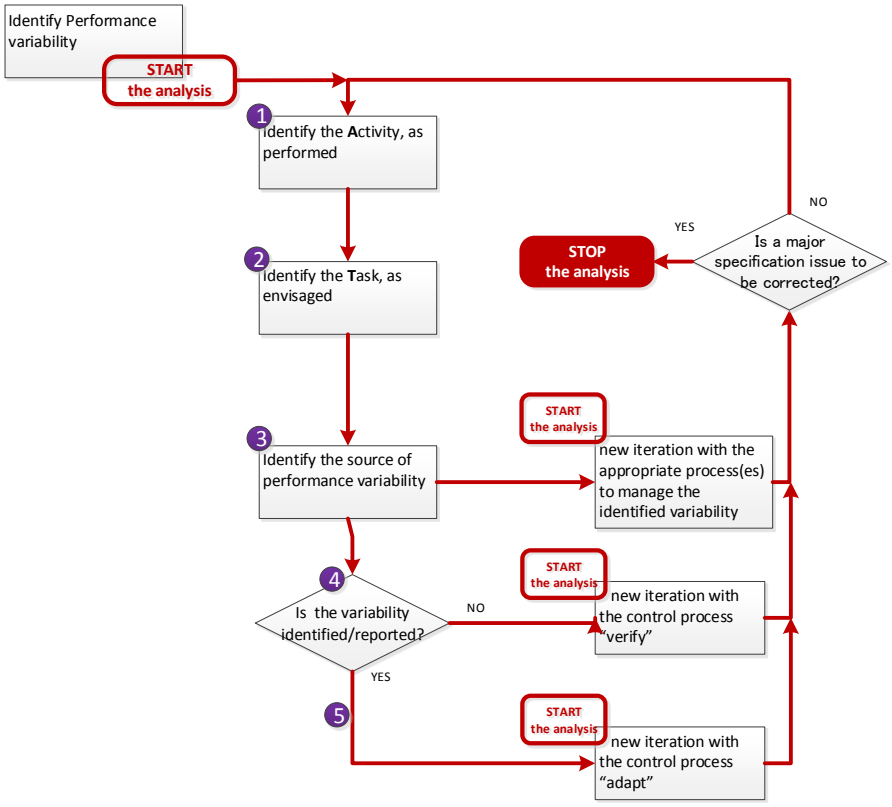

Fig.3: The flow of investigating events with the SAFRAN method

The next section will illustrate a practical application of this SAFRAN method in a railway context, by analysing the depth and focus of published accident investigation reports of, in origin, similar over-

speeding events, where the control of risks is still heavily relying on the variability in the performance of the driver.

3. Case study

As has been demonstrated by several of the most lethal railway accidents over the last decades (e.g. ARAIC, 2007; RAIC, 2014), derailments because of over-speeding form a major risk of the railway system. This will remain at least as long as not all infrastructure and rolling stock is equipped with an automatic train protection system that continuously controls speed requirements. As input for a case study, applying the SAFRAN method in order to evaluate their depth and focus, the authors of this paper have selected a set of six published investigation reports, from 6 different countries and 3 different continents, which analysed the critical variability in maintaining the appropriate speed of a passenger train (see also Accou and Reniers, 2018).

These investigation reports have been analysed, using the logic of the SAFRAN method to set the reference of what to expect of a proper analysis of an over-speeding incident. When applying the SAFRAN method on the specific case of over-speeding incidents, the first step is the identification of the critical variability in the driver's performance of maintaining the appropriate speed. The next step, is to identify the expected performance as prescribed and/or specified. Speed requirements within the railway system, and in particular speed restrictions, are imposed by the assets that are used, in particular through the characteristics of used rolling stock and infrastructure (through design or its actual state). Without an automatic train protection system in use, these constraints are traditionally communicated to the train driver via the lineside signalling equipment. In addition, the trained driver is required to have acquired the necessary route knowledge so that he knows what signalling aspects to expect and where on the line. The third step in the SAFRAN logic then consists of identifying those sources of performance variability (formal and informal) that contributed in shaping the train driver not respecting the applicable speed restriction (e.g. Kyriakidis et al, 2018). The fourth step in the SAFRAN method requires to identify the possibility to identify, analyse and report the critical variability of the specific process that is analysed (i.e. continuously monitoring the match between work as designed and work as actually performed). In this specific case study, this would mean that the investigation has analysed how the concerned organisations are monitoring the actual train speed and its criticality when compared to the allowed speed. With the existing state of technology, train speed is a parameter that is continuously recorded via on board data recorders and could form a basis for managing driver performance (e.g. Balfe and Geoghegan, 2017; EL Rashidy et al., 2017). Monitoring the match between work as designed and work as actually performed, in this context of managing the risk of over-speeding in a sustainable way, would therefore require a railway company to continuously monitor the speed of its trains. Not in order to check driver-compliance, as is traditionally done, but to understand work place reality. Information on these four steps, that together form a first iteration of the SAFRAN method, applied on the driver's activity to "maintain appropriate speed", are expected to be found in the investigation reports.

But, as discussed previously, more is needed if we want to introduce sustainable change. We would also expect to find elements that give indication that the process to "monitor over-speeding" has been analysed in a structured way, in order to assess an organisation's capability to identify critical speed-variability. This represents a second iteration in the SAFRAN method, for which we at least would like to understand the actual and specified performance, as well as eventual factors that can explain the deviation. Finally, we need to understand an organisation's capability to manage those conditions that influenced the driver's performance (i.e. the previously identified sources of performance variability) to better support sustainable and safe performance, which is a next iteration of the SAFRAN method for each identified factor. Here also, we look for actual and specified performance and eventual sources of

performance variability. In summary, the reference model that we look for in the selected investigation reports, can be graphically represented as follows.

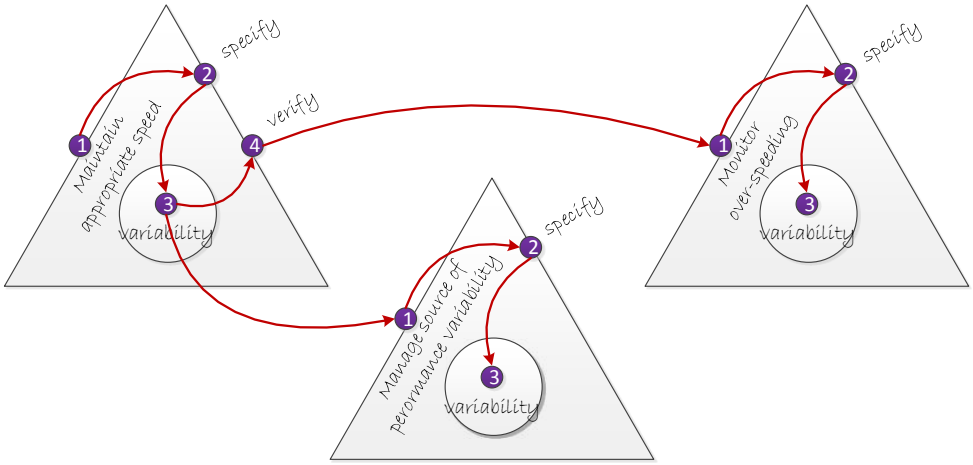

Fig.4: Reference model for investigating over-speeding incidents, based on the SAFRAN logic

When comparing the reviewed investigation reports with the reference model, as illustrated in Figure 4, we found that for the activity of "maintaining an appropriate train speed" they all report on the allowed an actual train speed, the expected performance and the way this is formalised, as well as on the identified factor(s) that can explain the critical variability in the driver's performance when maintaining the appropriate speed (i.e. the first three steps of the SAFRAN method). Moving to step 4 of the SAFRAN method, we found that except for the investigation of the derailment in Philadelphia in 2015 (NTSB, 2016), all other investigation reports mention (potential) elements of over-speed monitoring. But only the investigation reports on the derailment on the Fukuchiyama line (ARAIC, 2007) and the over-speeding incident (RAIB, 2016) at Fletton Junction provide a structured analysis (at least identifying the first three steps of a next SAFRAN iteration) on why the (non-) reporting of previous over-speeding incidents did not adequately address the risks related to speed variability on critical parts of the infrastructure. The former report goes even further and actively reflects on the possibility to monitor speed at critical curves, resulting in a recommendation to monitor speed variability by using already existing technology. For the iteration related to the identified sources of performance variability, we found a very mixed picture, with only the investigation report of the over-speeding incident at Fletton Junction (RAIB, 2016) providing a detailed and structured analysis for the processes related to the management of driver fitness and the equipment of lineside signs and the Philadelphia (NTSB, 2016) investigation report for the process of managing train driver competence. The following Table 1 provides a summary of the elements from the reference model that are addressed in the analysed accident investigation reports.

Process	Event	Fukuchiyama line (JAP) April 25, 2005 (ARAIC, 2007)	Aldershot, Ontario (CAN) February 26, 2012 (TSBC, 2012)	Santiago de Compostela (ESP) July 24, 2013 (RAIC, 2014)	Philadelphia (USA) May 12, 2015 (NTSB, 2016)	Buizingen (BEL) September 10, 2015 (IBRAI, 2017)	Fletton Junction (GBR) September 11, 2015 (RAIB, 2016)
Maintain appropriate speed	step 1	identified	identified	identified	identified	identified	identified
	step 2	identified	identified	identified	identified	identified	identified
	step 3	identified	identified	identified	identified	identified	identified
Monitor over-speeding	step 1	identified	no further structured analysis	identified	no further structured analysis	identified	partly identified
	step 2	identified		identified		identified	partly identified
	step 3	identified		no mention		no mention	partly identified
Manage variability	step 1	no further structured analysis	no further structured analysis	identified	identified	identified	identified
	step 2			identified	identified	identified	identified
	step 3			no mention	partly identified	no mention	partly identified

Table 1. Overview of analysed investigation reports (see also Accou and Reniers (2018) for more detailed findings)

These results show a wide variety in depth and focus of investigation when compared with the areas of investigation that logically would result from an analysis that is applying the SAFRAN method (i.e. the reference model in Figure 4). This leads us to conclude that most of the reviewed reports just partly or not address an organisation's capability of managing the variability that might put successful process performance at risk and therefore miss the opportunity to issue recommendations that could really introduce sustainable change.

The choice to stop this reference model (Figure 4) with only two levels of iteration is a pure efficiency-thoroughness-trade-off (Hollnagel, 2009b). When analysing an incident, iterations of the SAFRAN method can (and probably should, if we want to introduce sustainable change) continue, as long as information is available and activities are more or less specified. This is nicely illustrated in one element of the investigation report on Fletton Junction over-speeding incident (RAIB, 2016). In this report we can read that the Virgin Trains East Coast passenger train service from Newcastle to London King's Cross passed through Fletton Junction, near Peterborough at 51 mph (82 km/h) around twice the permitted speed of 25 mph (40 km/h). The investigation identified that the sign on the up slow line approaching Fletton Junction was 450 mm in diameter, while speed signs are normally 900 mm in diameter and that it is possible that the timing of any response of the driver to correct the train speed would have been affected by the small size of this sign. Although the report gives no indication of why exactly the concerned location was equipped with a small sign (i.e. identified as a critical performance variability), the investigation went

further by analysing why the procedures of Network Rail, the British railway infrastructure manager, did not identify that the speed restriction sign at Fletton Junction was smaller than required by its standards. It is found that work instructions for 'Lineside signs maintenance and renewal' exist, but mainly focus on the visibility of signs, and reporting signs that need maintenance attention or are missing. These instructions however, did not require the workers to know what type of sign should be provided at a particular location. The report therefore concludes in a recommendation that Network Rail should develop and then implement a process to check whether operational signs (e.g. signs associated with speed restrictions) are provided in accordance with relevant documentation (e.g. signalling plans). Applying the SAFRAN logic to graphically represent this part of the investigation report (Figure 5), one can immediately identify a depth of three consecutive iterations.

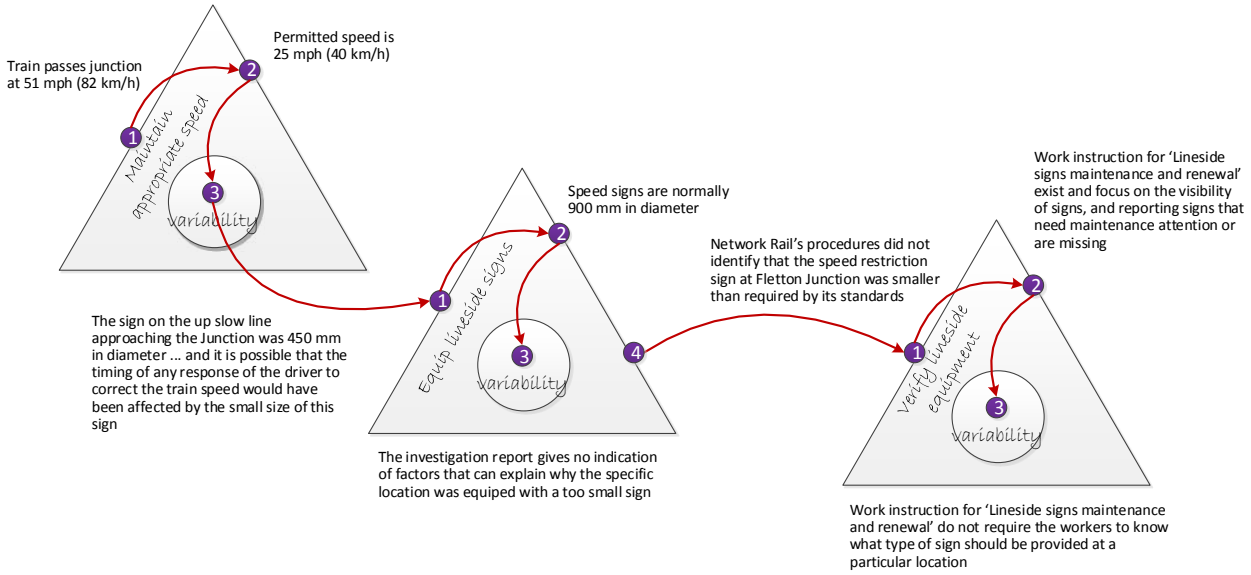

Fig.5: Example of 3 consecutive iterations, as found in the investigation report on the Fletton junction over-speeding incident

Also two of the other reviewed investigation reports, namely on the events in Belgium and Spain, show a similar depth of three consecutive iterations. Both these reports do this however by only comparing the actual performance with the expected and specified performance in the second and third iteration, without creating any understanding on the deviation (i.e. identifying the respective sources of performance variability), and therefore turning the investigation into a pure (non-) compliance exercise. Based on the findings that driver expectations and experience may have influenced the driver not respecting the speed restrictions when approaching a switch, the Buizingen investigation report (IBRAI, 2017) identifies the actual and expected performance for managing and verifying driver competence, concluding that for the specific driver, the training was performed as specified, but without reflecting on why the detected variability was not properly managed. The investigation on Santiago de Compostela, on the other hand, has analysed the decisions on how to equip the line with engineering controls; identifying on the one hand that the Santiago station was not equipped with ERTMS and, on the other hand, that in the performed risk analysis, the risk to maintain the appropriate speed in the curve was consciously exported to the driver. The report further mentions that an authorisation for opening the concerned line was granted by the National Directorate-General of Railways (DGF), according to what is specified by the

concerned Spanish legislation. At no point, the report reflects on whether the specified performance was actually followed and if so, why the related risk was not discovered. In final, this results in the impossibility to improve the related processes.

4. Discussion

In railways, like in other high-risk industries, a lot of energy and resources are put into the investigation and analysis of adverse events, in order to identify elements of improvement and to change the (safety) performance of the respective socio-technical systems in a sustainable way. The scope of these investigations is often limited to the immediate causes and decision making close to the adverse event, insufficiently addressing essential elements of safety management. Consequently, these investigations make it hard to change the railway system in a sustainable way, which should be done by the treatment of wider system failures, identified through system based analysis, rather than the treatment of local factors at the sharp end of system operation (e.g. Rasmussen and Svedung, 2000; Reason and Hobbs, 2003; Dekker, 2011).

Using Hale's statement that when investigating, one is inclined to see the factors we have categories for, prompting those investigating to ask particular questions (Hale, 2000), it is argued that the introduction of the SAfety FRactal ANalysis (SAFRAN) method in this paper, will provide investigators with a practical framework that enables them to ask questions that help to gain deeper understanding of organisational factors. By focusing the investigation on the capability of an organisation to monitor and manage safety critical variability (i.e. enhancing resilience performance) there is no more need to look for human error or root causes. This is a capacity that is also attributed to the FRAM method (Woltjer, 2008, Herrera and Woltjer, 2009), but it is our belief that SAFRAN offers the possibility to do this in a more direct way, hereby tackling the arguments that it is inefficient to use systematic methods to analyse accidents in simple systems (e.g. Underwood and Waterson, 2013, Wienen et al., 2018) and at least to partly break down the multi-faceted barrier that prevents practitioners from adopting a systemic approach (Underwood and Waterson, 2012).

Herrera and Woltjer (2009) explain how FRAM's recursive way of functional modelling is suitable for modelling functions at operational, tactical as well as strategical (i.e. control & command) levels. Building on the generic elements that compose a SMS, SAFRAN offers a similar possibility, by iterating the same simple five steps to evaluate the performance of the different processes, regardless of the hierarchical level they are situated at. Furthermore, using the idea of nested control loops at operational, organisational, regulatory and even political level, that together form a socio-technical system (e.g. Rasmussen and Svedung, 2000; Leveson, 2016), a similar investigation logic could easily be extended beyond an organisation's SMS. This addresses the findings of several authors in the past (e.g. Sklet, 2004, van Schaardenburgh-Verhoeve et al., 2007, Groeneweg, et al., 2010) that investigations going outside the borders of an organisation and focussing on government and regulators lack appropriate analysis methods. Taking into account the substantial role humans play at all levels in the systems, such a method would require the possibility to analyse how actions and decisions taken by individuals or teams at all these levels are affected by their local goals, resource constraints and external influences (Underwood and Waterson, 2013). As it does for functions at the sharp end, applying SAFRAN to assess performance variability at these higher levels in the socio-technical system, can guide investigators to ask the appropriate questions to discover also the "local rationality" of decision and policy makers. Addressing these levels in an accident investigation is in particular important, since the introduction of SMS can be seen as part of a regulatory strategy to place the responsibility for managing safety at the level of the organisation best able to do so (Deharvengt, 2013; Kringen, 2013), challenging them to identify in a structured way what activities are critical for safety and what kind of safety management best fits their particular situation in order to achieve acceptable levels of safety performance, rather than blindly

complying with prescriptive rules and regulations (Daniellou et al., 2010; Fowler, 2013; Grote and Weichbrodt, 2013; Kelly 2017).

The application of the SAFRAN method was demonstrated in this study, by reviewing a selected set of published railway accident investigation reports, all reporting on an occurrence related to over-speeding. A logical focus for the analysis of such an adverse event would be to check a duty-holder's capacity to monitor the speed of its trains, to analyse it and to learn from experience. When issues discovered, it should be obvious that the issued recommendations will no longer be on the driver not respecting a speed limit and the individual corrective actions that need to be taken, but on the objectives of the monitoring process and the related management responsibilities. The identified countermeasures can then address both single-loop (i.e. correcting errors within the range set by organisational norms for performance) and double-loop (i.e. when correcting errors requires to change the organisational norms for performance) learning (Argyris and Schön, 1996), herewith offering a solution for the criticism of Wienen et al. (2018) that applying systemic methods make it harder to formulate corrective measures that can be implemented by management, since safety is considered an emergent property and therefore there is no more causal link to protect with a barrier.

Although the first finding of users are very promising, the authors recognise that the SAFRAN method does not offer the possibility to cover all steps of the common accident investigation approach of Wienen et al. (2018). In particular the first two steps; being 1) finding the events that have a causal relationship with the accident and 2) describing the history of the accident by linking these events, are not supported by the proposed method. This should not be a problem, since it was found (e.g. Underwood and Waterson, 2013) that no single technique can cover the complexity of a system and that it may be better to use more than one method so that the strengths of one technique can compensate for the weaknesses of another. This is in line with Farooqi's recommendation (2015) to use different methods alongside each other in an investigator toolkit. Furthermore, a limitation of the performed review is that all findings are solely based on the elements that are available in the published reports and could not take into account analysed elements that are not reported upon. The authors have no information on the methods that were used to perform the accident investigation that resulted in the reviewed reports. It is also acknowledged that the organisational, political and societal context in which the investigations have been performed can highly influence their scope and focus (e.g. Dien et al., 2007, Hutchings, 2017). Further testing of the SAFRAN method during the investigation or re-investigation (e.g. Groeneweg, et al., 2010) of events by accident investigation practitioners could give a better indication of the type of additional factors that can be found compared with a more traditional accident investigation. In addition, future research will have to provide more evidence for the claim that SAFRAN does not suffer from the same ailments as the other systemic methods that make them inefficient to be used by industry.

5. Conclusions

Despite the introduction of the concept of SMS in high risk industries for several years, if not decades, accident investigation practice is still poor in analysing the basic elements that compose an SMS. In this paper, the SAfety FRactal ANalysis method is introduced as a combination of a generic model of process management, an investigation flow and a graphical representation. The, for investigators, most appealing element of the method lies in the identification of five recognisable investigation steps that, when iterated, provide a structured way to guide them to evaluate all processes throughout a socio-technical system in a similar way. Based on the performed analysis, the authors belief that, when it comes to investigating and analysing elements of SMS in a structured way in order to create a sustainable change in safety performance, the current investigation practice could gain from applying the SAFRAN method.

References

Accou, B., Reniers, G., 2018. Analysing the depth of railway accident investigation reports on over-speeding incidents, using an innovative method called “SAFRAN”. 55th European Safety, Reliability & Data Association (ESReDA) seminar, Book of Proceedings, to be publsihed.

ARAIC, 2007. Train Derailment Accident between Tsukaguchi and Amagasaki Stations of the Fukuchiyama Line of the West Japan Railway Company, April 25, 2005. Aircraft and Railway Accidents Investigation Commission (ARAIC), Report RA2007-3-1.

Antonsen, S., 2009. Safety culture: theory, method and improvement. Ashgate Publishing Limited.

Argyrys C. and Schön D.A., 1996. Organizational Learning II - Theory, Method, and Practice. Addison-Wesley Publishing Company.

Balfe, N., Geoghegan, S., 2017. Human factors applications of On-Train-Data-Recorders. Sixth International Human Factors Rail Conference, Book of Proceedings, 152-161.

Cullen, The Hon. Lord, 1990. The public inquiry into the Piper Alpha disaster. The Department of Energy. Vol 1-2.

Czech, B.A., Groff, L., Straunch, B., 2014. Safety cultures and accidents investigation: Lessons learned from a National Transportation Safety Board Forum, Adelaide Australia.

Daniellou, F., Simard, M., Boissières, I., 2010. Facteurs Humains et Organisationnels de la Sécurité Industrielle: Un état de l'art. Les Cahiers de la Sécurité Industrielle. Institut pour une Culture de Sécurité Industrielle (ICSI).

Deharvengt, S., 2013. Regulating Airlines' Safety Management System: When Proceduralization of Risks Meets Risk Owners. In C. Bieder, M. Bourrier (Eds.), Trapping safety into rules: how desirable or avoidable is proceduralization? Ashgate Publishing Limited (157-171).

Dekker, S., 2014. The psychology of accident investigation: epistemological, preventive, moral and existential meaning making. Theoretical issues in Ergonomics Science.

Dekker, S., 2011. Drift into failure: from hunting broken components to understanding complex systems. Ashgate Publishing.

Del Frate, L., Zwart, S.D., Kroes, P.A., 2011. Root cause as a U-turn. Engineering Failure Analysis 18 (2011), 747-758.

Dien, Y., Llory, M., Montmayeul, R., 2004. Organisational accident investigation methodology and lessons learned. Journal of Hazardous Materials, 111 (2004), 147-153.

Dien, Y., Dechy, N., Guillaume, E., 2007. Accident investigation: from searching direct causes to finding in-depth causes. Problem of analysis or/and of analyst?. Dechy, N.; Cojazzi, G.G.M. 33. ESReDA seminar, Nov 2007, Ispra, Italy, European communities. Luxembourg, pp.16, 2007.

EL Rashidy, R., Hughes, P., Figueres-Esteban, M., Van Gulijk, C., 2017. Operational Safety Indicators Using Real Train Driving Data. Sixth International Human Factors Rail Conference, Book of Proceedings, 162-169.

Farooqi, A.T., 2015. Methods for the Investigation of Work and Human Errors in Rail Engineering Contexts. PhD Thesis, University of Nottingham.

Fowler, D., 2013. Proceduralization of safety Assessment: A Barrier to Rational Thinking. In C. Bieder, M. Bourrier (Eds.), Trapping safety into rules: how desirable or avoidable is proceduralization? Ashgate Publishing Limited (87-106).

Groeneweg, J., Van Shaardenburgh-Verhoeve, K.N.R., Corver, S.C., Lancioni, G.E., 2010. Widening the Scope of Accident Investigations. SPE International Conference on Health, Safety and Environment in Oil and Gas Exploration and Production, 12-14 April, Rio de Janeiro, Brazil.

Grote, G., 2012. Safety management in different high-risk domains - All the same? Safety Science 50 (2012) 1983-1992.

Grote, G., Weichbrodt, J., 2013. Why Regulators Should Stay Away From Safety Culture and Stick to Rules Instead. In C. Bieder, M. Bourrier (Eds.), Trapping safety into rules: how desirable or avoidable is proceduralization? Ashgate Publishing Limited (225-240).

Hale, A., Borys, D., 2013. Working to Rule, or Working Safely. In C. Bieder, M. Bourrier (Eds.), Trapping safety into rules: how desirable or avoidable is proceduralization? Ashgate Publishing Limited (43-68).

Hale, A.R., 2000. Culture's confusions. Safety Science 34 (2000), 1-14.

Hardjono, T.W., Bakker, R.J.M., 2006. Management van processen: Identificeren, besturen, beheersen en vernieuwen (Derde, geheel herziene druk). Kluwer.

Herrera, I.A., Woltjer, R., 2009. Comparing a multi-linear (STEP) and systemic (FRAM) method for accident analysis. Safety, Reliability and Risk Analysis: Theory, Methods and Applications - Martorell et al. (eds.). Taylor & Francis Group, London.

Hollnagel, E., 1998. Cognitive Reliability and Error Analysis Method (CREAM). Elsevier Science Ltd.

Hollnagel, E., 2002. Understanding Accidents - From Root Causes to Performance Variability. Proceedings of the 2002 IEEE 7th Conference on Human Factors and Power Plants.

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 (259-268).

Hollnagel, E., 2009a. The four cornerstones of resilience engineering. In C.P.Nemeth, E. Hollnagel and S. Dekker (Eds.), Preparation and Restoration (pp.117-134). Aldershot, UK, Ashgate.

Hollnagel, E., 2009b. The ETTO Principle: Efficiency-Thoroughness Trade-Off - Why Things That Go Right Sometimes Go Wrong. Ashgate Publishing.

Holnagel, E., 2012. FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems. Aldershot, UK, Ashgate.

Hollnagel, E., 2014. Safety-I and Safety-II: The past and future of safety management. Ashgate Publishing.

Hollnagel, E., 2018. Safety-II in practice: Developing the resilience potentials. Routledge.

Hollnagel, E., Speziali, J., 2008. Study on Developments in Accident Investigation Methods: A Survey of the "State-of-the-Art". SKI Report 2008:50.

Hutchings, J., 2017. Systemic factors in the investigation of South African railway occurrences. PhD thesis, University of the Witwatersrand, Johannesburg.

IBRAI, 2017. Derailment of a SNCB/NMBS passenger train, Buizingen – 10 September 2015. Investigation Body for Railway Accidents and Incidents (IBRAI).

ICSI, 2017. La culture de sécurité; Comprendre pour agir - n° 2017-01 de la collection Les Cahiers de la sécurité industrielle. Institut pour une culture de sécurité industrielle (ICSI).

ISO, 2004. ISO/IEC 15504-2:2003, Information technology -- Process assessment -- Part 2: Performing an assessment. International Organization for Standardization (ISO).

Johnson., C.W., 2003. Failure in Safety-Critical Systems: A handbook of incident and accident reporting. Glasgow University Press.

Johnson, C., 2004. Review of the BFU Überlingen Accident Report - Final report. Eurocontrol Contract C/1.369/HQ/SS/04.

Johnson., C.W., 2009. Review of accident investigation methodologies - Final report. European Railway Agency contract ERA/2009/SAF/NP/02

Katsakiori, P., Sakellarropoulos, G., Manatakis, E., 2009. Towards an evaluation of accident investigation methods in terms of their alignment with accident causation models. Safety Science 47 (2009), 1007-1015.

Kelly, T., 2017. The Role of the Regulator in SMS. ITF Discussion Paper 2017-17. OECD/ITF 2017.

Kringen, J., 2013. Proceduralization and Regulation of Culture: Experiments on the Fontiers of Risk Regulation. In C. Bieder, M. Bourrier (Eds.), Trapping safety into rules: how desirable or avoidable is proceduralization? Ashgate Publishing Limited (205-224)

Kyriakidis, M., Kant, V., Amir, S. Dang, V.N., 2018. Understanding human performance in sociotechnical systems – Steps towards a generic framework. Safety Science 108, 202-215.

Lappalainen, J., 2017. Overcoming Obstacles to implmenting SMS. ITF Discussion Paper 2017-20. OECD/ITF 2017.

Leveson, N.G., 2000. Intent Specifications: An Approach to Building Human-Centered Specifications. IEEE Transactions on software engineering, VOL.26, NO.1, 15-35.

Leveson, N., 2011a. The use of safety cases in certification and regulation. Journal of System Safety.

Leveson, N.G., 2011b. Engineering a safer world. MIT press.

Leveson, N.G., 2016. Rasmussen's legacy: A paradigm change in engineering for safety. Applied Ergonomics 59, 581-591.

Lin, P-H., 2011. Safety management and risk modelling in aviation: The challenge of quantifying management influences. PhD thesis - Next Generation Infrastructures Foundation. uuid:3b293559-81ed-4450-aa78-005bbd9054f1

Lindberg, A.-K., Hansson, S.O., Rollenhagen, C., 2010. Learning from accidents - What more do we need to know?. Safety Science 48 (2010), 714-721.

Lundberg, J., Rollenhagen, C., Hollnagel, E., 2009. What-You-Look-For-Is-What-You-Find - The consequences of underlying accident models in eight accident investigation manuals. Safety Science 47 (2009), 1297-1311.

NTSB, 2016. Derailment of Amtrak Passenger Train 188, Philadelphia, Pennsylvania, May 12, 2015. National Transportation Safety Board (NTSB), Railroad Accident Report NTSB/RAR-16/02 PB2016-103218.

RAIB, 2016. Overspeed at Fletton Junction, Peterborough, 11 September 2015 - Report 14/2016. Rail Accident investigation Branch (RAIB), Department for Transport.

RAIC, 2014. Final report on serious railway accident NO 0054/2013 of 24.07.2013 near Santiago de Compostela station (a Coruña). Railway Accidents Investigation Commission (RAIC), Investigation report ERA-2014-0070-00-00-ESEN.

Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Safety Sience, Vol. 27 (182-213).

Rasmussen, J., Svedung, I., 2000. Proactive risk management in a dynamic society. Swedish Rescue Services Agency, Karlstad, Sweden.

Reason, J., 1997. Managing the risk of organisational accidents. Ashgate Publishing.

Reason, J., Hobbs, A., 2003. Managing Maintenance Error: A practical guide. Ashgate Publishing.

Reason, J. 2008. The human contribution: Unsafe acts, accidents and heroic recoveries.Farnham: Ashgate.

Rosness, R. 2013.The Proceduralization of Traffic safety and Safety Management in the Norwegian Rail Administration: A Comparative Case Study. In C. Bieder, M. Bourrier (Eds.), Trapping safety into rules: how desirable or avoidable is proceduralization? Ashgate Publishing Limited (173-189).

Salmon, P.M., Goode, N., Taylor, N., Lenne, M.G., Dallat, C.E, Finch, C.F., 2016. Rasmussen's legacy in the great outdoors: A new incident reporting and learning system for led outdoor activities. Applied Ergonomics 59, 637-648.

Sklet, S., 2004. Comparison of some selected methods for accident investigation. Journal of Hazardous Materials 111 (2004), 29-37.

TSBC, 2012. Main-track Derailment VIA Rail Canada Inc. Passenger Train No.92 Aldershot, Ontario, 26 February 2012. Transportation Safety Board of Canada (TSBC), Railway Investigation Report R12T0038.

Underwood, P., Waterson, P., 2013a. Systemic accident analysis: examining the gap between research and practice. Accident Analysis Prevention 55, 154-164.

Underwood, P.J., Waterson, P.E., 2013b. Accident analysis models and methods: guidance for safety professionals. Loughborough: Loughborough University, 28 pp.

van Schaardenburgh-Verhoeve, K.N.R., Corver, S., Groenweg, J., 2007. Ongevalsonderzoek buiten de grenzen van de organisatie. Nederlandse Vereniging Voor Veiligheidskunde (NVVK) Jubileumcongres 25-26 april 2007.

Vierendeels, G., Reniers, G.L.L., Ale, B.J.M., 2011. Modelling the major accident prevention legislation change process within Europe. Safety Sience 49 (3), 513-521.

Wahlström, B., Rollenhagen, C., 2014. Safety management - A multi-level control problem. Safety Science 69 (2014), 3-17

Wienen, H.C.A., Bukhsh, F.A., Vriezekolk, E., Wieringa, R.J., 2017. Accident Analysis Methods and Models - A Systematic Literature Review. Centre for Telematics and Information Technology (CTIT), Technical Report No.TR-CTIT-17-04

Wikipedia, 2018. https://en.wikipedia.org/wiki/Fractal (accessed on 05/01/2018)

Woltjer. R., 2008. Resilience assessment based on models of functional resonance. Proceedings of the 3rdResilience Engineering Symposium, October 28-30, 2008, Antibes - Juan-les-Pins. Publisher: École des mines de Paris. Editors: Hollnagel, E., Pieri, E., Rigaud, E.

Woods, D.D., Johannsen, L.J., Sarter, N.B., 1994. Behind human error: cognitive systems, computers and hindsight, SOAR report 94-01, Wright-Patterson Air Force Base.