Exploring the potential of Safety Management Systems to support New Approaches based on Safety Fractals

Accou, B.O.R.

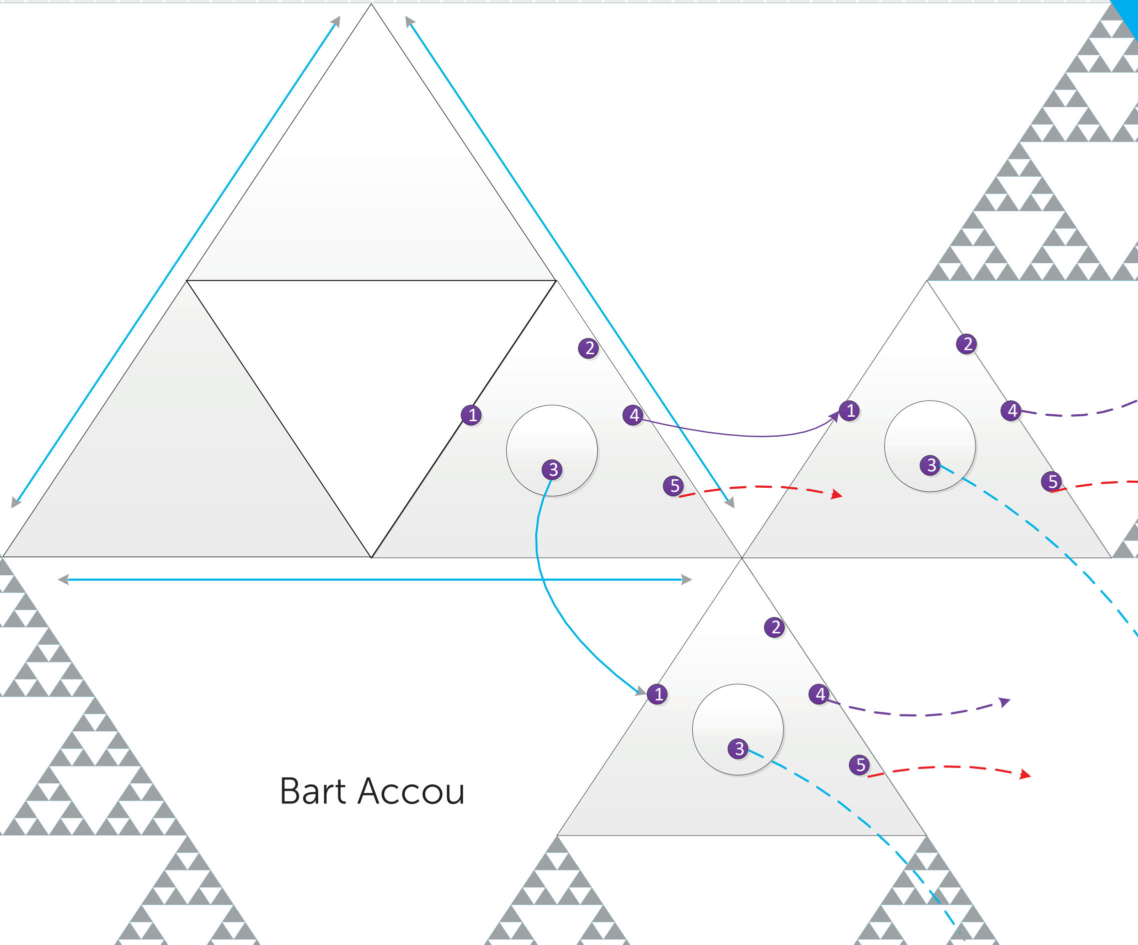
DOI
10.4233/uuid:e6f2307f-0b46-402a-92d3-aa98a63754f6

Publication date
2023

Document Version
Final published version

Citation (APA)
Accou, B. O. R. (2023). *Exploring the potential of Safety Management Systems to support New Approaches based on Safety Fractals*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:e6f2307f-0b46-402a-92d3-aa98a63754f6

Exploring the potential of Safety Management Systems to support New Approaches based on Safety Fractals



Bart Accou

Exploring the potential of Safety Management Systems to support New Approaches based on Safety Fractals

BART ACCOU

ISBN:
Cover design: Wendy Bour-van Telgen
Lay-out: Wendy Bour-van Telgen
Printing: GildePrint

Exploring the potential of Safety Management Systems to support New Approaches based on Safety Fractals

Dissertation
for the purpose of obtaining the degree of doctor
at Delft University of Technology
by the authority the Rector Magnificus Prof. dr. ir. T.H.J.J. van der Hagen
Chair of the Board of Doctorates
To be defended publicly on Thursday 6 July at 15:00 o'clock

by

Bart Oscar Rik ACCOU
Master of Science in Civil Engineering, Vrije Universiteit Brussel, Belgium
born in Nieuwpoort, Belgium

This dissertation has been approved by the promotors.

Composition of the doctoral committee:

Rector Magnificus	Chairperson
Prof. dr. ir. G.L.L.M.E. Reniers	Delft University of Technology, promotor
Prof. dr. J. Groeneweg	Delft University of Technology, copromotor

Independent members:

Prof. dr. ir. C.W. Johnson	Queen’s University, Belfast, UK
Prof. dr. G.R. Braithwaite	Cranfield University, UK
Prof. dr. M. Young	University of Southampton, UK
Prof. dr. ir. J.A.A.M. Stoop	Delft University of Technology
Dr. ir. J. van den Top	Inspectie Leefomgeving en Transport, NL
Prof. dr. ir. P.H.A.J.M. van Gelder	Delft University of Technology, reserve member

TABLE OF CONTENTS

PREFACE AND ACKNOWLEDGEMENT

I can proudly state that this thesis and the articles that are part of it were mainly written during my free time. My PhD research thus became a hobby that has taken up many weekends and vacation days during all these years. For me, this effort has never felt like a sacrifice, but I can only be grateful to An for giving me the necessary space. Rens, Maan and Neel were already at an age where they could only appreciate the extra freedom - at least that's what I hope.

The choice to complete this project outside working hours has undeniably had an impact on its duration. Between the first contact with TU Delft and the presentation of the end result, almost 10 years will have finally passed. This has the great advantage that the ideas have matured and that the proposed approach could be sufficiently tested in different settings and could be maximally adjusted to meet the needs of real accident investigation practice. This, in turn, would not have been possible without the help and cooperation (consciously and sometimes unconsciously) of many colleagues. It's impossible to list them all, but some have to be: George and Daphné were the very first guinea pigs to apply the ideas for event analysis into a real incident; Philippe (SUST), Dominique and John (RAIB) freed up valuable time to apply a first version of the analysis method to some of their ongoing investigations and have provided valuable feedback for further development. An important test for the practical applicability but also a rich source of inspiration came from explaining the analysis method and the underlying ideas to students and/or investigation practitioners. This would not have been possible without the active support of "early believers" like Genserik (also my valued interlocutor as promoter), Mircea and Sever (AGIFER), Ryan (NTSB) and especially Yani (Cranfield). In particular, she ensured that the method was also actively tested as part of Cranfield's Master's degree programme, with the work of Michelle and Gunar providing a valuable resource for the final validation of the method. I would also like to thank Fabrice especially. He recognised the great potential of the Safety Fractal from the first explanation, has been an important touchstone ever since, and still actively contributes to the further development and promotion of the method.

Finally, I also like to remind the late Dr. Jane Rajan. With her characteristic enthusiasm, she was the one who, as my supervisor at the time, first lit the fire to start this PhD research.

SUMMARY

The concept of a safety management system (SMS) to control the risks of operational activities has already been introduced in high-risk industries some decades ago. Nevertheless, such an SMS is often criticized as burdensome and complex. Through its requirement to formalise all main activities, the SMS is perceived as bureaucratic and as a vehicle for pure compliance, exemplary for the old view on safety management. Furthermore, the SMS is often perceived as detached from an organisation's core and operational activities, and as incompatible with local practice. It is questioned whether it can deliver the expected safe performance.

By comparing the models behind SMS with specific requirements for process capability, this research has identified a Safety Fractal that reflects the basic requirements that are needed to control safety related activities at all levels within an organisation. This Safety Fractal forms a unique unit of analysis, with three distinct levels to observe the functioning of a process: A first level of process performance that represents the direct functioning of the components that interact during process execution. This is also the level where variation with respect to process specifications and/or expectations can be observed. A second level of process implementation provides the resources and means to ensure the correct functioning of the process components during process execution. And finally, a third level of process control ensures the sustainable control of risks related to all activities of the organisation.

Furthermore, part of the conducted research has given clear indication that the constituent elements of this Safety Fractal, and herewith the concept of SMS, appear to be particularly suitable for organising resilient performance, provided that a strategy that embraces adaptive cultures and performance variability is explicitly identified as the safety strategy to follow. Positioning this approach alongside common safety management concepts as management system maturity, leadership, and safety culture, led to the development of an Extended Safety Fractal, hereby creating the potential for a systematic and a more comprehensive view on how to approach and measure safety performance and the basic elements of resilience.

Even though the concept of SMS has already been mandatory in most high-risk industries for several years and the systems approach to accident analysis has been the dominant research paradigm, research shows that accident investigation practice still underperforms in analysing the basic elements that compose an SMS and in embracing system theory. The scope of accident and incident investigations usually stays limited to investigating the immediate causes and decision-making processes related to the accident sequence. Important factors, including design and planning decisions, that contribute to accidents are hereby often overlooked and the weaknesses in the SMS are hardly ever analysed. As a direct consequence, the opportunity to use these investigations for introducing sustainable system changes is often missed.

In an effort to remedy these issues, the SAfety FRactal ANalysis (SAFRAN) method is introduced as a combination of an investigation flow and a graphical representation that complements the Safety Fractal. The method, which ultimately forms the central subject of this research, offers a structured way to systematically identify human and organisational factors throughout a socio-technical system, more closely aligned to the logic of accident investigation practice than other systemic methods. Starting from the critical variability close to an accident, the application of the method guides investigators in analysing the state of the entire system in its capability to monitor and control this variability. It provides them a structured and iterative way to move from analysing a single event into analysing the wider socio-technical system around it. The essence of using the SAFRAN method for evaluating the performance of the different processes in a socio-technical system, is to approach them in a similar way, building on the generic elements that compose a SMS and systematically looking at the Human and Organisational Factors (HOF) that influenced actions and decision making, regardless of the hierarchical level at which they are situated. For investigators, the 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 towards evaluating all processes throughout a socio-technical system in a similar way. In doing so, the SAFRAN method is designed not only to allow combining human analysis with a systems-oriented analysis but, in addition, to generate the necessary analytical trail to better communicate the results of such an analysis and to bring forward more demonstrable elements that might convince decision makers to adapt the system.

Throughout this project, the chosen design research approach offered the possibility to iterate the consecutive steps of: (1) targeted review of state-of-the-art literature, (2) (improved) design of the models and (3) validation through practical application and comparison with actual safety management and accident investigation practices. This allowed the identification of user needs together with testing of the usability of the concepts. To validate the method, finally, a series of practical tests, often involving active accident investigators, made it possible to examine the SAFRAN method against a set of carefully selected and recognised criteria for evaluating systemic accident analysis models and methods. Although the method needs an established sequence of events as a starting point, the performed evaluation gives clear indication that SAFRAN offers a valuable addition to an investigator’s toolkit and that the developed models have the potential to (re)vitalize the concept of SMS and to make the most of its full power in support of established as well as new approaches in safety management.

SAMENVATTING

Het concept van een veiligheidsbeheersysteem (VBS) om de risico's van operationele activiteiten te beheersen, is al enkele decennia geleden geïntroduceerd in risicovolle industrieën. Toch wordt dit VBS vaak bekritiseerd als belastend en complex. Door de eis om alle hoofdactiviteiten te formaliseren, wordt het VBS gezien als bureaucratisch en als een middel dat enkel de naleving van regels nastreeft; exemplarisch voor de oude visie op veiligheidsbeheer. Bovendien wordt het VBS vaak gezien als losstaand van de kern- en operationele activiteiten van een organisatie en indruisend tegen lokale werkwijzen. De vraag wordt dan ook gesteld of het de veilige prestatie kan leveren waarop initieel werd gehoopt.

Door de modellen achter een VBS te vergelijken met specifieke vereisten voor procescapaciteit, heeft dit onderzoek een Safety Fractal geïdentificeerd die de basisvereisten weerspiegelt die nodig zijn om veiligheidsgerelateerde activiteiten op alle niveaus binnen een organisatie te beheersen. Deze Safety Fractal vormt een unieke eenheid voor analyse, met drie verschillende niveaus om het functioneren van een proces te observeren: Een eerste niveau van procesprestaties vertegenwoordigt de directe werking van de componenten die op elkaar inwerken tijdens de procesuitvoering. Dit is ook het niveau waarop variatie ten opzichte van processpecificaties en/of verwachtingen kan worden waargenomen. Een tweede niveau van procesimplementatie, verschaft de mensen en middelen om de correcte werking van de procescomponenten tijdens de procesuitvoering te verzekeren. En tot slot zorgt een derde niveau van procesbeheersing voor een duurzame beheersing van risico's die verband houden met alle activiteiten van de organisatie.

Verder heeft een deel van het uitgevoerde onderzoek duidelijke aanwijzingen opgeleverd dat de samenstellende elementen van deze Safety Fractal, en daarmee het concept van VBS, bijzonder geschikt lijken om veerkrachtige prestaties te organiseren, op voorwaarde dat een strategie die adaptieve culturen en prestatievariabiliteit omarmt expliciet wordt geïdentificeerd als de te volgen veiligheidsstrategie. Door deze benadering te positioneren ten opzichte van gekende concepten voor veiligheidsbeheer als maturiteit van managementsystemen, leiderschap en veiligheidscultuur, is de ontwikkeling van een Extended Safety Fractal tot stand gebracht, waarmee het potentieel wordt gecreëerd voor een systematische en meer omvattende visie op het benaderen en meten van veiligheidsprestaties en de basiselementen van veerkracht.

Ondanks dat het concept van VBS al enkele jaren verplicht is in de meeste sectoren met een hoog risico en de systeembenadering van ongevallenanalyse het dominante onderzoeksparadigma is, toont onderzoek aan dat de praktijk van ongevallenonderzoek

nog steeds slecht is in het analyseren van de basiselementen waaruit een VBS bestaat en in het omarmen van systeemtheorie. De reikwijdte van onderzoek naar ongevallen en incidenten blijft meestal beperkt tot het onderzoeken van de directe oorzaken en besluitvormingsprocessen met betrekking tot de voortgang van een ongeval. Belangrijke factoren, waaronder ontwerp- en planningsbeslissingen, die bijdragen aan ongevallen, worden hierbij vaak over het hoofd gezien en de zwakke punten in het VBS worden nauwelijks geanalyseerd. Als een direct gevolg wordt hierdoor vaak de kans gemist om deze onderzoeken te gebruiken voor het doorvoeren van duurzame systeemveranderingen.

In een poging om deze problemen op te lossen, wordt de SAfety FRactal ANalysis (SAFRAN)-methode geïntroduceerd als een combinatie van een onderzoeksstroom en een grafische weergave die de Safety Fractal aanvult. De methode, die uiteindelijk het centrale onderwerp vormt van dit onderzoek, biedt een gestructureerde aanpak om systematisch menselijke en organisatorische factoren te identificeren in een socio-technisch systeem die beter is afgestemd op de dagelijkse praktijk van ongevallenonderzoek dan andere systemische methoden. Uitgaande van de kritische variabiliteit in de buurt van een ongeval, begeleidt de toepassing van de methode onderzoekers bij het analyseren van de toestand van het gehele systeem in zijn vermogen om deze variabiliteit te bewaken en te beheersen. Het toont hen een gestructureerde en iteratieve manier om van het analyseren van een enkele gebeurtenis over te gaan naar het analyseren van het bredere socio-technische systeem eromheen. De essentie van het gebruik van de SAFRAN-methode voor het evalueren van de prestaties van de verschillende processen in een socio-technisch systeem is om ze op een vergelijkbare manier te benaderen. Daarbij wordt voortgebouwd op de generieke elementen die een VBS vormen en wordt systematisch gekeken naar de menselijke en organisatorische factoren die acties en besluitvorming beïnvloeden, ongeacht het hiërarchische niveau waarop ze zich bevinden. Het voor onderzoekers meest aantrekkelijke element van de methode ligt in de identificatie van vijf herkenbare onderzoeksstappen die, wanneer herhaald, een gestructureerde manier bieden om hen te begeleiden om alle processen in een socio-technisch systeem op een vergelijkbare manier te evalueren. Door dit te doen, is de SAFRAN-methode niet alleen ontworpen om menselijke analyse te combineren met een systeemgerichte analyse, maar bovendien om het nodige analytische spoor te genereren om de resultaten van een dergelijke analyse beter te communiceren en meer aantoonbare elementen naar voren te brengen die besluitvormers kunnen overtuigen om het systeem aan te passen.

Doorheen dit project bood de gekozen ontwerponderzoeksaanpak de mogelijkheid om de opeenvolgende stappen te herhalen van: (1) gericht nazicht van state-of-the-art literatuur, (2) (verbeterd) ontwerp van de modellen en (3) validatie door middel van praktische toepassing en vergelijking met daadwerkelijke werkwijzen op het gebied van veiligheidsbeheer en ongevallenonderzoek. Hierdoor konden de gebruikersbehoeften worden geïdentificeerd en de bruikbaarheid van de concepten worden getest. Om de methode te valideren, tenslotte, maakte een reeks praktische tests, waarbij vaak actieve ongevalsonderzoekers betrokken waren, het mogelijk om de SAFRAN-methode te toetsen aan een reeks zorgvuldig geselecteerde en erkende criteria voor het evalueren van systemische modellen en methoden voor ongevalanalyse. Hoewel de methode een vastgestelde reeks gebeurtenissen als uitgangspunt nodig heeft, geeft de uitgevoerde evaluatie een duidelijke indicatie dat SAFRAN een waardevolle aanvulling is op de toolkit van een onderzoeker en dat de ontwikkelde modellen het potentieel hebben om het concept van VBS te (re)vitaliseren en zijn volledige kracht optimaal te benutten ter ondersteuning van ook nieuwe benaderingen in veiligheidsbeheer.

RESEARCH OBJECTIVE AND APPROACH

For several decades now, safety management systems (SMS) have been promoted as the way to proactively deal with hazards and risks. Hale et al. (1997) see the origin of SMS as the result of regulatory interest in many European countries in the 1980's to move away from detailed regulation to framework legislation, shifting the focus from detailed technical safety concerns towards issues of decision making and safety management. This move was strengthened by a series of official reports following major disasters (e.g. Zeebrugge, 1987; Piper Alpha, 1988) that highlighted the failings of management to organise their operational activities with sufficient safety and was quickly picked up by high-risk industries, most of the time becoming a legal requirement.

This change in focus for safety management is part of an evolution that follows the complexity of (socio-technical) systems to be managed (Waterson et al., 2015) and that, depending on the point of view, is considered a third age or a second wave in this evolution. Hale and Hovden (cited in Borys et al., 2009) considered the introduction of SMS as a third "age of safety", following a first, technical age and a second, human factors age. Hudson (cited in Borys et al., 2009), on the other hand, suggests that safety management has developed through "waves" that consecutively focussed on technical, systems and culture related aspects. A fourth age of "integration" was introduced by Glendon et al. (cited in Borys et al., 2009), stressing the need not to lose the previous ways of thinking but rather to build upon them. Borys et al. (2009), in turn, complement this with a fifth age of safety: an "adaptive age" that transcends all other ages without discounting them and that introduces the concept of "adaptation" in order to sustain required operations under both expected and unexpected conditions.

However, having worked on the regulatory as well as the operational side of SMS development and implementation in the European railway system, I can confirm the finding of several authors that the concept of SMS is often poorly understood, and the maturity of implementation is in general very low, bureaucratic and compliance based (e.g. Beausang, 2019). Based on these observations, I can only conclude that practice often does not yet follow theory and that the operational reality is caught somewhere between the different theoretical waves of the safety evolution. As pointed out by Lin (2011) but also by Deharvengt (2013), the top-down description of SMS requirements creates problems in understanding how to link the generic management activities, aimed at identifying and controlling risks in a systematic way, with the operational activities of the organisation that create these risks in the first place. Rasmussen (1997), on the other hand, observed that the different hierarchical levels that he used to describe the complexity of a socio-technical system in control of safety (i.e. work, staff, management, company, regulators and government) have traditionally been studied and modelled by different research disciplines, without much interaction. This might partly explain why there is still 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.

This finding has led to the formulation of the following, initial research question for this project:

- Q1 – *How can generic SMS requirements be better integrated to improve (the management of) operational performance?*

Surprisingly, the relevance of SMS as a viable concept within the "fifth age" of safety management only arose at a later stage of the project, while working on the above research question. The complexity of the socio-technical system in most of the high-risk industries has increased significantly in recent decades and continues to do so, making it less transparent for the human operator and the overall performance of the system less predictable. In addition, the current moment of history, where surprises of different kinds have become part of our expectations, requires from safety-critical systems that they be able to adapt to uncertain and potentially fast changing environments (Le Coze, 2019). This has led to questioning of the traditional way of managing safety (e.g. Hollnagel 2014, Leveson, 2020) and to alternatives being sought. In the multitude of often conflicting opinions and models, the idea that the performance of a (socio-technical) system should be approached in its entirety, seems to be endorsed by a large part of the safety management community. This requires acknowledging (human) variability as well as taking into account the complex and emergent phenomena that result from system interactions, to complement more traditional safety approaches (Reiman and Viitanen, 2019). Highly critical of what he calls the "New-view" approaches, Cooper (2022) raises the question whether more traditional (i.e. Safety I) and newer approaches can ever be reconciled or coexist in harmony. Referring to Gelfland's work (2019) on cultural tightness-looseness, Cooper sees potential in the identification of areas where a tight approach is required as opposed to areas, in a same facility, where culture looseness may be appropriate. In the same line of thought, Denyer (2017) introduces the concept of 'paradoxical thinking', where leaders need to balance the different approaches on safety management, in order to find the right fit for their organisation. In a more dynamic approach, fully in line with the fifth age of safety mentioned above. Grote (2019) identifies the need for leaders to develop the capability to perceive, understand, and proactively manage the tensions between (changing) demands for stability and flexibility within their organisations.

Against this background of very distinct and possibly contradicting approaches that have dominated the discussions on safety management over the last decades, and with SMS as a clear artifact of a more traditional approach, this led to the following, and for this research almost existential, second research question:

- Q2 – *Can the concept of SMS contribute to the new perspective(s) on safety management?*

To answer to the above research questions, relevant models for both SMS and process capability were compared. This resulted in a set of generic and scale invariant requirements for good safety management, that was coined the Safety Fractal. Although the initial tests with this Safety Fractal were more oriented towards SMS implementation and SMS assessment, a combination of coincidence and practical restrictions guided the research described here towards the interesting field of accident investigation and analysis. As a direct consequence, the core subject of this research is aiming at improving safety management (systems) through accident analysis.

Being a clear requirement for any SMS, the investigation practice I came across in the railway sector, whether performed internally or externally, was usually limited to investigating the immediate causes and decision-making processes related to the sequence of events. Potential weaknesses in the SMS were hardly ever analysed. This finding, which was unfortunately largely confirmed during further research steps, is in line with previous findings by authors like Antonsen (2009), Kelly (2017) or Johnson (2004), the latter being made when reviewing the original accident investigation report of the famous Überlingen mid-air collision. Different authors assign possible underlying causes that could explain these findings (e.g. Reason, 1997; Hollnagel and Speziali, 2008; Lundberg et al., 2009; Dekker, 2011) with the underlying accident model that is used to guide the investigation methods as a main cause. Since most accident reporting and investigation methods are not developed in line with a system thinking approach to accident causation, they hardly cover elements of the SMS, which is based on operational, supporting and controlling processes functioning together to improve safety. Knowing that 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 is a logical consequence that investigations using those traditional methods don't directly guide towards solutions that can be found within elements of the SMS.

Furthermore, applying the existing systemic accident investigation methods also appears to be problematic. Wienen et al. (2018) find them inefficient to analyse accidents in simple systems and, as identified by Underwood and Waterson (2013), their perceived complexity and high demand for resources partly explain the multi-faceted barrier that prevents practitioners from adopting a systemic approach. This resulted in the following main research question to be put forward:

- *Q3 - What accident and incident analysis method can guide investigators to identify those elements of the SMS where interventions might have the greatest impact for improving system safety?*

In order to achieve this objective, a "design through research" approach (Faste and Faste, 2012) was chosen. In summary, the research has iterated the following consecutive steps:

1. targeted review of state-of-the-art literature,
2. (improved) design of the proposed accident analysis methodology
3. testing through practical application and comparison with current occurrence investigating practices

This iterative approach has proven to be very effective, allowing for both the identification of user needs as well as the testing of the usability of the developed concepts. Almost inevitably, this also led to consecutive, underlying research questions that had to be answered.

Dekker (2006) claims that the aim of investigating human performance is to find out how peoples' assessments and actions made sense at the time, given the circumstances that surrounded them. The data that needs to be gathered therefore should cover all possible features of the system and situation that surrounded people at the time and with which they interacted (ICSI, 2013). The factual information that is collected about an accident must form the basis for and drive the analysis process in all investigations (AIBN, 2015). Getting the data, however, is only one side of an investigator's task. The remaining task is then to make sense of these data and to reconstruct how people contributed to an unfolding sequence of events, leaving some kind of analytical trace from the collected data to the human and organisational factor(s) that help to explain their actions and decisions (Dekker, 2006). Unfortunately, after having read and analysed more than 100 publicly available investigation reports during the course of this study, we can only conclude that in general the actual practice of railway accident investigation lacks proper human and organisational factors (HOF) knowledge to achieve this objective. This seems to confirm the findings of Dul et al. (2012) that, despite decades of history, knowledge on HOF has not yet found wide-spread recognition nor implementation and the potential of HOF remains under-exploited. To achieve this, the collection and analysis of data on HOF should be just as methodical and complete as for technical systems and the use of a proper tool or method can help to ensure the effectiveness and thoroughness of the investigations (Reinach and Viale, 2006). This leads to the following sub-question:

- Q3.1 – *How can non-HOF experts be guided to identify HOF elements during accident investigations?*

Furthermore, following the International Society of Air Safety Investigators (ISASI), the aforementioned need to understand local rationality in the context of accident investigation is not only valid for decisions and actions of operational personnel. The analysis should encompass all the people concerned with the occurrence and/or performance under investigation, which could easily lead to activities and decisions away from the occurrence in space and time. This should not even be limited to the SMS of an organisation and also actions and decisions of regulators and governmental policy makers should be included. In the past, several authors (e.g. Sklet, 2004, van Schaardenburgh-Verhoeve et al., 2007, Groeneweg, et al., 2010) have however found that investigations going outside the boundaries of an organisation and focussing on government and regulators lack appropriate analysis methods, which leads to the following sub-question:

- Q3.2 – *How can an investigator be guided to analyse the SMS and wider system functions in a structured way?*

This thesis brings together a collection of complementing papers that (except for chapter 4) were published and that answer the above research questions, as illustrated in the following figure.

Chapter Question	1	2	3	4	5
Q1	▨				▨
Q2	▨				▨
Q3		▨	▨	▨	▨
Q3.1			▨	▨	▨
Q3.2		▨			▨

In chapter 1, the need to make a sustainable safety strategy explicit and to implement it throughout formal as well as informal safety management practices is addressed, providing an answer to research question Q2, related to the validity of the concept of SMS to support the recent developments in safety management thinking. This builds on earlier research outputs that provided and answer to research question Q1, aiming at bridging the gap between the theoretical management models and the management of operational processes, and that are also presented in this chapter.

Chapter 2 provides an answer to research question Q3, with a particular focus on answering research question Q3.2 to better guide investigators to analyse SMS components and the wider socio-technical system and proposes a structured investigation flow as well as a graphical representation of the proposed accident analysis method.

Chapters 3 and 4 focus on the integration of human and organisational factors in the proposed approach, providing an answer to research question Q3.1.

Underwood (2013) mentions a lack of (empirical) validation as the most likely aspect related to the development of an accident model or investigation method that would affect its selection and use by practitioners. Several studies also mention validity and reliability of an accident analysis method as a prime evaluation criterion (e.g. Katsakiori et al., 2009; Waterson et al., 2015 or Hollnagel, cited in Speziali and Hollnagel, 2008). Yet, for most of the existing systemic accident analysis methods, a proper validation appears to be missing (Underwood, 2013). Although the previous chapters already provide some partial input for the final validation of the models and investigation method that were designed during this research, the formal validation against a recognised and tested evaluation framework for systemic accident analysis methods is presented in chapter 5.

Each of these chapters is also preceded by a brief and more personal introduction, which places the chapter within the evolution of the project and reflects on how the related experience and interactions influenced the further research. To improve the readability of the manuscript as a whole, and to avoid too many repetitions of the same basic concepts that support the proposed methodology, those recurring parts that figure in the original papers on which the different chapters are based, have been removed and, if not clear from the context, replaced by a reference to the chapter where the concepts are introduced. Finally, an epilogue at the end of this thesis summarises and critically reviews the answers that are provided in the different chapters for each of the above research questions. Possibilities for further research are also highlighted in this last chapter.

1

Introducing the Extended Safety Fractal: Reusing the concept of Safety Management Systems to organise resilient organisations

This chapter is based on the article with the same title, published in the *International Journal of Environmental Research and Public Health*, 2020, 17, 5478 by Bart Accou *(role: concept, methodology, analysis and writing)* and Genserik Reniers *(role: review and supervision)*.

INTRODUCTION TO CHAPTER 1

Although the paper that served as basis for this chapter is not the first publication on SAFRAN, it makes sense to present these ideas first. In this chapter, the basic elements that were used for the developed accident analysis approach are the most theoretically substantiated. The development of the Extended Safety Fractal was triggered by the recurring demand from both colleagues and stakeholders to explain the (remaining) role and relevance of a SMS at a time when I was professionally developing and promoting material around safety culture and safety leadership -both concepts that were newly introduced in European railway legislation. In addition to extensively reviewing the literature on safety culture and leadership, it led me to return to the literature on SMS and SMS as a tool to measure the safety state of an organisation, which characterised the beginning of my research. This also offered the opportunity to explain how the Safety Fractal was built, which was not yet covered in one of the other papers that focus more on accident analysis.

ABSTRACT

Although mandatory in most high-risk industries, the safety management system (SMS) is often criticized as burdensome and complex. Through its requirement to formalize all main activities, the SMS is perceived as bureaucratic and a vehicle for pure compliance and Safety I (one). Furthermore, the SMS is often detached from an organisation's core activities, goes against local practice and does not deliver the safe performance that was hoped for. By comparing the model behind SMS with specific requirements for process capability, this chapter identifies a safety fractal that reflects the basic requirements that are needed to control safety related activities at all levels within an organisation. It is further argued that the constituent elements of this safety fractal are particularly suitable to organise resilient performance, provided that resilience is explicitly identified as the safety strategy to follow and, as such, consequently implemented. This approach is then positioned alongside common safety management concepts as management system maturity, leadership and safety culture, leading to a systematic and a more comprehensive view on how to measure safety performance and resilience.

1.1. INTRODUCTION

The concept of a safety management system (SMS), to continuously improve safety of operations, was introduced already some decades ago. Historically, the introduction of SMS can be situated in the context of a changing interest of regulators in the 1970s and 1980s from detailed technical concerns to issues of decision-making. A series of investigation reports following serious accidents (e.g., Herald of Free Enterprise and Clapham Junction) acted as a catalyst, indicating failings of management as a contributing factor (Hale et al., 1997). In particular, the Cullen report on the Piper Alpha disaster (Cullen, 1990) required, as one of 106 detailed recommendations, to have a safety case accepted by the UK safety authorities for anyone operating an offshore installation. This launched the idea of an auditable SMS that quickly found an audience in high-risk industries like transport (aviation, railways, etc.), the production of dangerous goods, occupational health, etc. 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 these industries. Consequently, the establishment and maintenance of an SMS to control all risks related to a company's operational activities became the basis for certification and regulation (Vierendeels and Reniers, 2011; Leveson, 2011; Grote, 2012; Deharvengt, 2013; Fowler, 2013; Lappalainen, 2017).

Maurino (2017) describes the introduction of SMS as the logical and coordinated integration of three different tracks that has guided safety and organisational thinking since the 1950s. The first track is system safety engineering which aimed to design for minimum risk (Hollnagel, 2018). Human factors, the second track, proposed a multi-disciplinary approach to optimise the relationship between people and their operational environment. Business management, finally, introduced the concept of quality management systems and a striving for continuous improvement. In a wider context, when discussing SMS as the formal aspect of the organisational focus surrounding safety, several authors (Antonsen, 2009; Guldenmund, 2015; ICSI, 2017) refer to it as the third age of safety science. This third age not only follows, but also integrates the elements of the first age, focusing on technology, and of the second age, focusing on human behaviour and competence.

The introduction of SMS can also 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). Rather than blindly complying with prescriptive rules and regulations, they are challenged 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, (Fowler, 2013; Daniellou et al., 2010; Grote and Weichbrodt, 2013; Kelly, 2017). In addition, the organisational changes and the rational thinking about safety required for the successful implementation of an SMS are believed to have a positive impact on safety culture (Cambon, 2007; Schröder-Hinrichs et al., 2015), as well as on an organisation's financial, economic and competitive performance (Maurino, 2017; Bottani et al., 2009; RSSB, 2020; Mohammadfam et al. 2017).

On the other hand, as reported upon by several authors, success is not guaranteed when implementing an SMS and there are multiple difficulties to overcome. The SMS can be made too burdensome and complex, resulting in processes that are incompatible with an organisation's core activities (Maurino, 2017) and going against the common sense found in local practice (Lappalainen, 2017; Cambon, 2007). In addition, Lin (2011) reports on a practical gap she identified in companies that tried to incorporate theoretical management models as a tool for resolving issues related to human performance or technical failure. Furthermore, through its requirement to establish procedures and documentation for all main activities, the SMS is often perceived as too normative and bureaucratic (Lappalainen, 2017; Cambon, 2007; Zwetsloot, 2000; Pariès et al. 2019), pushing companies directly to a "work as imagined" and compliance-focused perspective (Schröder-Hinrichs et al. 2015; Hollnagel, 2014). A similar struggle to shift from an enforcement-based or "control and command" relationship towards a partnership aimed at achieving an agreed safety performance is identified at the level of regulatory bodies (Maurino, 2017; Zwetsloot, 2000). This has even led Kelly (2017) to conclude that "most regulatory bodies are unable to assess the effectiveness of a company's SMS", a bold statement that probably finds its origin in the joint finding of various authors that many existing (SMS audit) tools are not linked to defined and established underlying SMS models (Peltonen, 2013) and do not enable the consistent measurement of the process' effectiveness to deliver safe performance (Cambon, 2007; Groeneweg, 1992; Kuusisto, 2000).

Despite the often well-founded criticism they formulate about its implementation and current use, most of the above-mentioned authors do not argue in favor of abandoning the concept of SMS. On the contrary, they believe that SMS has the potential to better integrate proactive safety management (Kelly, 2017) and to make them more resilient by shifting the focus towards more interactive methods to predict and detect undesired outcomes (Lofquist, 2017). In that context, also measuring the effectiveness of an SMS or its processes is seen as a way to better capture the true safety state of an evolving organisation (Hale et al. 1997; Cambon, 2007; Groeneweg, 1992).

Sharing this belief, this research is aiming to revitalise the concept of SMS to deal with the recent paradigm shift in safety management. Hereby, a specific focus is put on linking the generic management activities, aiming to identify and control risks in a systematic way, with the operational activities of the organisation that create these risks in the first place. Building on the apparent need for similar feedback loops or plan-do-check-act (PDCA) cycles at the different hierarchical levels in an organisation (Grote, 2012; Lin, 2011; Hardjano and Bakker, 2006), the second section of this chapter explains how the safety fractal is developed. This safety fractal is representing 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 and wider socio-technical system. This is done by comparing the basic principles of process capability (ISO, 2004) with the general requirements of SMS, using 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 (Lin, 2011). The third section of this chapter further reflects on how this safety fractal can be used to introduce the management of performance variability into SMS and how the basic processes of an SMS can also foster resilience engineering. This is then positioned alongside common safety management concepts, such as management system maturity, leadership and safety culture, in order to propose improved ways for measuring SMS performance, to organize resilience as well as for in-depth analysis of accidents and incidents, by using the (extended) safety fractal. The use of these models, to address the above-mentioned weaknesses of SMS, finally, is discussed in section four.

1.2. BUILDING THE SAFETY FRACTAL

Despite (or maybe because of) the industry-wide introduction of SMS as the cornerstone for safety management in high-risk industries, there is little consensus about what an SMS is and how it should be managed (Grote, 2012; Lappalainen, 2017; Pariès et al., 2019; Lofquist, 2017). As a first example, the International Civil Aviation Organisation (ICAO) (2013), in its Annex 19, defines SMS as "a systematic approach to managing safety, including the necessary organisational structures, accountabilities, policies and procedures". The same Annex 19 (ICAO, 2013) further identifies "safety policies and objectives", "safety risk management", "safety assurance" and "safety promotion" as the basic building blocks of an SMS. In a top-down manner, this develops the general safety policy into a number of generic management activities (Lin, 2011). Similar lists of building blocks or basic elements for an SMS exist across the different literatures and industries. Grote (2012) summarised these elements into the following set, representing a common denominator: (1) safety policy; (2) safety resources and responsibilities; (3) risk identification and mitigation; (4) human factor-based system design; (5) safety training; (6) safety performance monitoring; (7) incident reporting and investigation; (8) auditing; (9) continuous improvement; (10) management of change.

The European Railway Safety Directive (EU, 2016, EU, 2004), on the other hand, defines SMS as “the organisation, arrangements and procedures established by an infrastructure manager or a railway undertaking to ensure the safe management of its operations”, highlighting herewith the need to integrate safety in the daily operations of an organisation in a formalised way. Unfortunately, this emphasis is not further developed into the published list of ”basic elements” for an SMS that shows remarkable similarities with the top-down list of Grote (2012).

The quest to make the ideas behind the SMS requirements operational is partly what has been driving this research. On the one the hand, organisations invest in the standardisation of management activities, as promoted by SMS principles. On the other hand, it is common practice to elaborate safety rules or procedures at operator level, in order to prescribe how to carry out safety critical tasks or activities. Both are part of a broad historical evolution of safety (Rosness, 2013; Le Coze and Wiig, 2013) that was denominated “Safety Proceduralisation” by Bourier and Bieder (Bourrier and Bieder, 2013). In addition, most SMS standards or models identify the management of procedures as one of the principal elements, requiring written documentation (Hale and Borys, 2013). Veweire (2014) goes even further, by identifying a clear process orientation and a thorough understanding of the company’s operational processes as key differentiating characteristics that set operationally excellent firms apart from other companies.

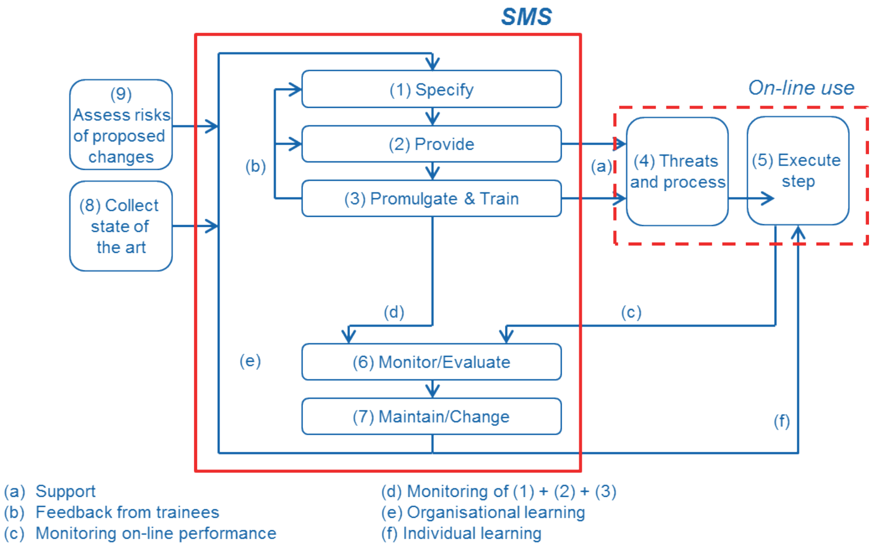
Proceduralisation of operations at the sharp end can (and most probably should) be very different from proceduralisation of safety management, even within a same organisation (Rosness, 2013). Nevertheless, the apparent need for similar feedback loops or cycles at the different hierarchical levels in an organisation (Grote, 2012; Lin, 2011; Hardjono and Bakker, 2013) 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 these levels. This idea of scale invariance, which also features, for instance, the functional resonance analysis method (FRAM) (Hollnagel, 2012) and that is reminiscent of the characteristics of a fractal, explains the name that was given to the model. 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 (wikipdia, 2018). The following sections will elaborate the consecutive steps that were followed to build this “Safety Fractal”.

1.2.1. Modelling safety management processes

To be able to comply more effectively with the legal requirements for having an SMS, several industries have attempted an explicit modelling of not only the operational risk-scenarios, but also the safety management processes driving them (Lin, 2011). With the goal to identify self-similar attributes for safety management, as discussed above, several of these models and standards have been reviewed, mainly relying on the work of Peltonen (2013).

From all reviewed models, the Dutch Safety Management Model showed the highest potential to be used as a starting point for detailed comparison with requirements for process management as described in standards on process capability (e.g. ISO/IEC 15504). Since the early 1990s the Delft University of Technology started modelling SMS, and the resulting model has a long development history through several consecutive projects. It has been tested and peer reviewed a number of times and has finally been validated through comparison with aviation models (e.g., accident models, technical models, and safety audit programs) and international standards (Lin, 2011). Furthermore, the model combines management control and monitoring loops, as defined in top-down SMS descriptions, with the systematic logic to represent entities and their activities imposed by the use of SADT (structured analysis and design technique) (Hale et al. 1997). This creates a natural bridge to process management, and as a consequence of this approach, the developed generic model already tries to link the traditional SMS elements with the direct aspects of the execution of an action.

The "Dutch" model, which will be used for further reflection and development, contains a nine-step generic management process that is applicable to all delivery systems, managing human and technical performance. In this model, depicted in Figure 1.1, a closed loop learning system is formed, making a clear distinction between the internal processes of the management level (i.e., all steps except (4) and (5)) and the output of each delivery at the operational level (i.e., steps (4) and (5)).



.

Figure 1.1. General structure of the delivery systems in an SMS (Lin, 2011).

The seven steps at the management level define the elements any delivery system should contain to ensure proper safety management:

(1) Specify: defining the processes, identifying risks and control measures, based on task analysis of human and technological performance as risk control measure.

(2) Provide: ensuring that the measure is designed, built, procured, installed and adjusted to its operating circumstances.

(3) Promulgate and train: informing and training workforce to perform the designated actions.

(6) Monitor/evaluation: detecting (potential) deviations from the specified functioning of risk control measures and evaluating performance at both the operational and management level.

(7) Maintain/change: restoring or improving the functioning of risk control measures, including organisational learning.

(8) Collect state of the art: learning from internal and/or external sources to improve operational and managerial performance.

(9) Assess risks of proposed changes: identifying the potential impact when deciding to change risk control measures or delivery systems.

Safety management is herewith identified as ″the process to provide the resources and controls designed to ensure that the internal processes are working properly, taking into account the threats that interfere with it″. This focus on the management of processes is modelled at the operational level, by identifying the following steps:

(4) Threats and the internal process: the threats that could put in danger the adequate performance of human behaviour, the technical system and/or the interaction between both, and that are to be managed by the steps at the management level of the delivery system.

(5) Actions executed at the sharp end: the direct execution of the primary work process, by humans and technology, to be compared with the expected performance.

In this model, the identified threats or influencing factors for human performance are either internal (physiological and psychological factors which might influence human information processing, e.g., technical and interpersonal skills, physical fitness, psychological fitness and motivation to commit to safety) or external (factors external to the human which might influence the information processing, e.g., clear and relevant guides, technology-man-machine interface, data and information and environment in which the action needs to be performed). For the technical performance, errors in the design and manufacturing process and in the maintenance and inspection program are identified as main threats. In addition, the possibility of iterating the human threats deeper into another level of human error and organisation, to be able to model design and/or maintenance error, is identified. This goes along with the aim of the analysis in this chapter to identify a generic set of self-similar requirements for safety management, applicable at all levels in an organisation or wider socio-technical system.

1.2.2. Taking into account process capability

As a next step in the research, this "Dutch" model for SMS was compared with the ISO/IEC 15504 standards on process capability, in order to define a set of requirements that are equally valid at process as well as system level. ISO/IEC 15504 (ISO, 2004) is in fact a set of standards, originally focusing on software development processes and derived from the process lifecycle standard ISO/IEC 12207. The standards contain a reference model defining a process dimension and a capability dimension and therewith provide a structured approach for the assessment of processes.

The standard identifies two principal contexts for the use of process assessment (ISO, 2004). Firstly, within a process improvement context, process assessment provides the means of characterising the current practice within an organisational unit in terms of the capability of the selected processes. Analysis of the results identifies strengths, weaknesses and risks inherent in the processes. These provide the drivers for prioritising improvements to processes. Process capability determination, on the other hand, is concerned with analysing of the proposed capability of selected processes against a target process capability profile in order to identify some of the risks involved in undertaking a project using the selected processes. For the purpose of building a set of generic requirements that is equally valid at process as well as at system level, primarily the capability dimension of this standard is of use. This capability dimension, as summarised in Table 1.1, provides a scale of six levels using the following nine process attributes (PA) to measure the capability of processes.

Table 1.1 ISO 15504 capability levels and attributes (ISO, 2004).

Level 0: Incomplete process The process is not implemented, or fails to achieve its process purpose.	
Level 1: Performed process The implemented process achieves its process purpose.	PA 1.1 Process performance attribute
Level 2: Managed process The previously described Performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.	PA 2.1 Performance management attribute PA 2.2 Work product management attribute
Level 3: Established process The previously described Managed process is now implemented using a defined process that is capable of achieving its process outcomes.	PA 3.1 Process definition attribute PA 3.2 Process deployment attribute
Level 4: Predictable process The previously described Established process now operates within defined limits to achieve its process outcomes.	PA 4.1 Process measurement attribute PA 4.2 Process control attribute
Level 5: Optimizing process The previously described Predictable process is continuously improved to meet relevant current and projected business goals	PA 5.1 Process innovation attribute PA 5.2 Process optimization attribute

Each of these attributes is further detailed with a set of specific requirements. When ordering these detailed requirements of the attributes at process level, according to the steps of the "Dutch" generic safety management process, three (instead of the initial two) levels or types of safety-related activities become apparent:

- A level of process performance that is modelling the direct functioning of the components that interact during process execution ("doing things"). This is also the level where variation against process specifications can be observed. The direct execution, as well as the sustainable performance, of a process results from the adequateness and capability of the delivery system that is composed of the following levels of process implementation and process control. This is in line with the definition of safety management, introduced by Lin (Lin, 2011), as "the process to provide the resources and controls designed to ensure that the internal processes are working properly to analyse and deal with the threats that interfere with it, so that they are managed to an acceptable level".
- A level of process implementation, providing the resources and means to ensure the correct functioning ("doing things right" according to Zwetsloot, (2000)) of the process

components during process execution. Where the "Dutch" model identifies a behavioural and a technological component as relevant to be managed for control over process execution, the performed analysis identifies the additional need to also manage an organisational component of process design and deployment. This finding emphasizes what already in 1965 was stated by Leavitt, in his diamond: that the performance of people and technology are affected by an organisation's structure and the processes or tasks to be performed (in Deschoolmeester and Braet, (2004)). Managing process performance will therefore require not only managing the separate components (an organisation's structure, the tasks or processes to be performed, the people and its technology) but also the possible interactions between them.

- A level of process control, ensuring the sustainable control of risks related to all activities of the organisation in a possibly changing context ("doing the right things" according to Zwetsloot, (2000)). The PDCA-cycle that is characteristic for the management system standards and that is also part of the "Dutch" safety management model finds its roots in system thinking and cybernetics (Hardjono and Bakker, 2006). Within a specified system, a process is executed to achieve a defined purpose, according to a specified pattern of progress. Because of external, environmental factors, progress can show some variation that is monitored at regular or irregular intervals to identify the gap between the desired and the actual state of the system. When a gap is identified, the system state is adapted. The identification of variables that allow the measurement of process performance is therefore an essential prerequisite. A similar logic is clearly present in the process attributes of the ISO 15504 capability model (ISO, 2004), resulting in the specification of three elements that together need to ensure the continuous and sustainable control of risks within a changing context: specify, verify and adapt.

In conclusion, comparing relevant models for both SMS and process capability shows a high degree of similarity, enabling the set of generic and scale invariant requirements for good safety management at all levels in an organisation we were looking for to be built. The detailed requirements for each identified level that result from this comparison can be found in the following Table 1.2.

Table 1.2. Detailed requirements at process implementation and control level

Implement	Train (3)		personnel performing the defined process are competent on the basis of appropriate education, training, and experience
	Equip (2)		resources (energy, matter, …)
			infrastructure (equipment, hardware, software, …)
			work environment
	Organise		process purpose / output (i.e., production of an artefact, a significant change of state, meeting of specified constraints, e.g., requirements, goals, etc.)
			process performance objectives
			process performance planning
			work products
			work product requirements
			a standard process (i.e., the fundamental elements to be incorporated into a defined process)
			clear and appropriate tailoring guidelines
Control	Specify (1)	process scope	process performance conditions and objectives
			process interfaces / (internal/external) partnerships
			the sequence and interaction of the standard process with other processes / (internal/external partnerships)
			process information needs in support of relevant defined business goals
			quantitative objectives for process performance in support of relevant business goals
		responsibilities	responsibilities for performing the process
			authorities for performing the process
			accountability for process performance

risks	risks to the achievement of the process objectives, to the achievement of the business objectives or related to regulatory obligations
	control activities that contribute to the mitigation of risks to the achievement of process/business objectives or regulatory obligations
	control limits of variation for normal process performance
	process improvement objectives that support the relevant business goals
change (9)	
Verify (6)	effectiveness (i.e., delivered process output vs expected output)
	compliance (i.e., process execution vs planning)
	quality control (i.e., supplied quality of work products vs expected or required quality level of work products)
	process efficiency (i.e., optimal resource consumption in relation to obtained results)
	efficiency of risk control measures (i.e., variation in performance of RCM)
	quality perception (i.e., outcome vs business goals/strategy)
	benchmark (i.e., performance compared to competitors or internal/external 3rd parties)
Adapt (7)	to adjust process performance to meet plans
	to adjust work products as necessary to meet requirements
	to improve the suitability and effectiveness of the process
	to address special causes of variation
	to re-establish control limits (as necessary) following corrective action
	to address opportunities for best practice and innovation
	to integrate new technologies and process concepts

Note: the figures between brackets "(x)" refer to the corresponding steps in the "Dutch" model.

1.2.3. The resulting Safety Fractal

Compared to the 'Dutch" generic SMS model, three distinct process-related type of activities are defined (process performance, process implementation and process control) and an additional organisational component is added to cover the impact that task design and organisational structure could have on process performance. This results in the representation of a safety fractal that is describing, in a self-similar way, a five-step safety management delivery system with the following logic:

(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.

The Figure 1.2 below graphically represents the found attributes of the safety fractal 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 the level of process performance ("doing things"). 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, finally, stands for the level of process control, ensuring the sustainable control of risks related to all activities of the organisation in a potentially changing context ("doing the right things"). The arrows, in turn, indicate the logical order in which these safety management activities are normally performed.

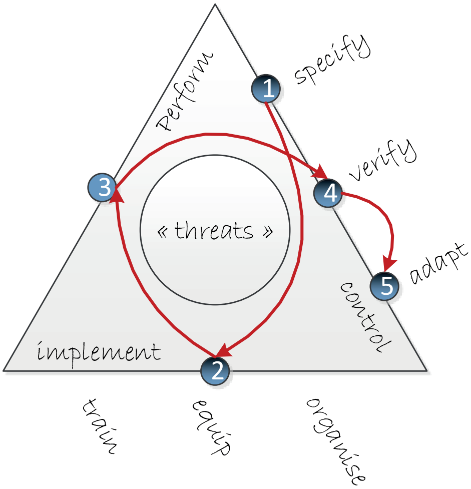


Figure 1.2. The Safety Fractal.

Together, the implementing and 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 an activity is aligned with the common approach for modelling systems, subsystems and their interactions, as proposed by Wahlström and Rollenhagen (2014). They propose using a control metaphor for the design and assessment of SMS in combination with the concepts of man, technology and organisational and information systems (MTOI) to ensure the continued safety of the operated systems. 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, separately and together. A similar line of thought can also be found with other authors (Lin, 2011; Hollnagel, 1998; van Schaardenburgh-Verhoeve et al., 2007). This strengthens our belief that this simple safety fractal model can be applied for all types 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.

Concretely, this would mean that the same Safety Fractal logic could be used to design and/or to evaluate the planning of as well as performing the maintenance of the chassis plate of a locomotive. But also a sub-task of the latter, like repairing eventual cracks in this chassis plate by welding, could be assessed by using the Safety Fractal. In addition, the same logic would be applicable for managing the competence of welders, as well as for the wider competence management and for specifying the maintenance manual. But also looking at SMS supervision by a national safety authority or specific sub-elements regarding the supervision of maintenance, operational monitoring processes or competence management could follow a same logic, as well as the eventual auditing of this safety authority, whether done internally of by an external partner. This line of thought and how best to exploit it will be further developed and explored in the following sections and chapters.

1.3. ORGANISING RESILIENCE THROUGH THE SAFETY FRACTAL

Mainly for historical reasons, SMS is considered by some authors (Herrera et al., 2010) as a vehicle for reactive safety management. The idea that the concept can also be used to introduce resilience into an organisation is, however, gaining ground (Schröder-Hinrichs et al., 2015; Lofquist, 2017). This view is confirmed by Pariès et al. (2019), who state that several safety strategies can fit within an SMS framework, describing the SMS as defining the "piping" of the system, generating safety. This pipework is presented in contrast to the safety strategy, i.e., the models or theories that can help us make sense of the diversity that can be observed in the real world, as the substance that "should flow through the pipes". Like other authors before us (Pariès, 2019; Lofquist, 2017; Johnsen, 2010), we propose resilience as the strategy to be used to improve safety in complex systems. In the following sections, the fitness of the Safety Fractal to host the constituent elements for achieving resilience is first tested. Next, these findings are positioned alongside common safety management concepts, such as management system maturity, leadership and safety culture, leading to an extended Safety Fractal that summarises, in a structured and coherent way, all elements that are required for organising sustainable and safe performance.

1.3.1. From managing threats to managing performance variability

Many of the cited authors (e.g. Lin, 2011; Deschoolmeester and Braet, 2004) still consider the identification and elimination or control of threats and the possible negative consequences that come with it as the objective of safety management. Hollnagel (2002, 2008, 2009), however, argues that there will always be variability in human performance, individually or collectively. 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. In addition, creating those conditions that make work succeed should then dampen the critical variability and generate "resilient performance".

Resilience is defined as the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions (Hollnagel et al. 2006). For this research, the Safety Fractal model, that was developed by looking for synergies between the basic principles of process capability and the general requirements of SMS, was compared with the four potentials that are proposed by Hollnagel (2008, 2009) as necessary for resilient performance (i.e., the potential (1) to respond, (2) to monitor, (3) to learn and (4) to anticipate). This already 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.

Denyer (2017) translates this into four core processes: (1) insight (i.e., interpret and respond to your present conditions), (2) oversight (i.e., monitor and review what has happened and assess changes), (3) hindsight (i.e., learn the right lessons from your experience) and (4) foresight (i.e., anticipate, predict and prepare for the future). He presents these processes as complementary and to be combined with the classical PDCA cycle to offer a structured framework towards continual improvement and innovation in ways that add real value to stakeholders and mitigate the impact of disruptions. He also introduces the concept of "paradoxical thinking" as a solution to manage the inherent tensions between the distinct perceptions that have dominated the discussions on safety management over the past decades. On the one hand, there is the tension between behaviours that are defensive (i.e., stopping bad things happen) and those that are progressive (making good things happen). On the other hand, there is also the tension between behaviours that are consistent and those that are flexible. Leaders then need to demonstrate paradoxical thinking to balance these different approaches and perceptions, in order to find the right fit for their organisation. This is building on the reflections of authors like Hollnagel (2008), who emphasize the need to complement safety by design (analytical safety) with safety by management (operational safety). Or, even earlier, Wildavsky (1988, ref. in (Pariès et al., 2019)), who described anticipation (predict and prevent danger before damage is done) and resilience (cope with and learn from unanticipated hazards after they have become manifest) as complementary and necessary safety strategies. All these elements mainly point towards the "control" level in the Safety Fractal (i.e., specify, verify and adapt), confirming the view that safety management is, in essence, controlling the organisational functions and practices that together produce safe performance (van Schaardenburgh-Verhoeve, 2007; Hollnagel, 2008).

Logically, the "specify" element of the Safety Fractal will cover the ability to anticipate and prepare for normal operations and foreseeable hazards. However, several authors (e.g., Le Coze, 2020) also argue that part of the response to sudden disruptions should be included in the design of the system. Positioning the seven resilience principles identified by Johnsen (2010) in the Safety Fractal, confirms this view. He argues for graceful and controlled degradation (1), redundancy (2), in having alternate ways to perform a function, flexibility (3) and the reduction of both complexity (4) and coupling (5), all to be integrated during the specification phase of the system based on common mental models (6).

Johnsen (2010) further identifies the management of margins (7) as a key aspect of resilience. This is to ensure that performance boundaries are not crossed through the monitoring of both the slow erosion of the system (Lofquits, 2017; Dekker, 2011), as well as the more dynamic decisions that balance productivity versus safety (Hollnagel, 2009). This will require continuous monitoring of the system that fits well within the "verify" element of the Safety Fractal. It is an already long accepted fact that the traditional metrics for measuring safety, which are primarily based on negative outcomes, cannot capture the true safety state of an evolving system (Groeneweg, 1992; Herrera et al., 2010; Amalberti, 2001, 2013). The search for adequate proactive or leading indicators remains, however, a challenge. One of the reasons for this might be that in complex systems, with non-linear interactions, it becomes more difficult to understand the "mechanisms" that lead to risks (Hollnagel, 2008). Herrera et al. (2010) suggest a solution that combines more traditional lagging indicators with indicators reflecting risk influencing factors found through the analysis of incidents and indicators relevant for (variability in) normal operations. In addition, Lofquist (2017, 2010) points to the interactive phase of his integrated safety management model as the most critical phase where discrepancies and undesired outcomes must be dealt with. To be able to notice and act upon safety- and performance-related issues, it should be clear that this will require a transfer of system control from the past towards the present of the process. A move that Pariès et al. (2019) also link with a transfer of control from the top towards the bottom of the organisation, which will require proper education, training, understanding and experience of the people taking real-time decisions (Lofquist, 2010). In addition, Johnsen (2010) highlights the need to integrate resilience in the implementation phase of systems, namely through technical solutions, organisational routines and the knowledge and ability of the users of the system, herewith only confirming the logic of the Safety Fractal. The overview above shows that resilience, as a safety strategy, can be fully embedded by the elements of the Safety Fractal. On the other hand, it also indicates which elements must be specifically developed and how, in order to create the processes that can optimally support resilient performance.

1.3.2. The informal aspect of managing safety

Resilience relies heavily on the ability of people, be it at the sharp end or at the blunt end, to adapt what they do in order to ensure that the system continues to function and achieve the set objectives under changing condition (Pariès et al., 2019; Hollnagel et al., 2006; Lofquist, 2010). Denyer (2017) for instance, when describing preventive control, mindful action, performance optimization and adaptive innovation as the four perspectives of organisational resilience, relies heavily on an informal and behavioural component. It seems therefore only logical that the contribution of safety culture to the achievement of sustainable and safe performance is also considered.

Unlike the SMS, that is providing the formal foundation for safety management by defining and prescribing what is required through control and implementation processes and arrangements, safety culture is not something that can be agreed between management and workers or between a safety authority and a regulated company based on a norm or standard. Culture should rather be seen as "emerging where people interact and have to accomplish something together" (Antonsen, 2009, Guldenmund, 2015). To understand if and how (safety) culture can contribute to improve sustainable safety performance, at least a basic understanding of the complex social processes that create culture within an organisation is needed. This will also help to identify the type of internal and/or external interventions by which safety culture might be influenced.

In particular the model developed by Guldenmund (2015) on how culture develops within an organisation is helpful in the context of this analysis. Guldenmund explains that a member of management or staff in an organisation, when experiencing a specific situation, develops his or her own perceptions and tries to "make sense". This becomes his or her individual understanding of reality, influenced in the first place by his or her own individual context (knowledge, individual attitudes, skills and ability, personal characteristics, emotions, state of mind, history, etc.) on which he or she decides or acts. Through an "interaction" phase, members of the group then exchange meanings, giving rise to mutual adjustments, agreements and expectations with regard to each other's behaviours, eventually resulting in partly shared understandings. Next, the organisation starts officialising a specific set of shared representations and actions, mainly through the "formalisation" of structure. This mainly happens through the distribution of tasks, roles and responsibilities and the description of procedures and rules, as well as through more physical structures like technology. These organisational structures, rules and procedures are then instructed and "disseminated" in various forms of communication and education. Through the following step of 're-enforcement', using various organisational processes and with an important role played by leaders, meanings, standards and expectations are finally accepted as the "way to do things". Members of the group will now share a comparable understanding of reality and structures, which will be the reference for individuals within this group to understand and cope with reality and which will influence the way they make sense of and act on the new situations they experience. These shared patterns of thinking and acting are then what embodies culture.

Through this cycle of (1) sense-making, (2) interacting; (3) formalising, (4) disseminating, (5) re-enforcing, it becomes obvious that the SMS, which is the instrument par excellence for formalising safety management, is an important enabler for the development of organisational culture. This leads to the possibility of deploying the SMS as an instrument to exert a positive influence on an organisation's safety culture. To achieve this, the SMS should be built consciously to impact the physical environment, as well as the behaviour of employees in a manner that promotes and facilitates sustainable and safe performance. Another aspect that is highlighted by the above cultural development model is that culture, as common patterns of behaviour and thinking, is constructed through the interactions between actors. This explains the high importance that is given in most safety culture norms and models to traits like transparency, trust and leadership. The signs given by management through organisational decisions and managerial behaviour (listening attitude, recognition, sanctioning, etc.) not only impact the behaviour of sharp end operators through positive and negative reinforcement (Agnew and Daniels, 2010), but also impact an organisation's capacity to learn (Argyris and Schön, 1996). What is important however, is to understand that this process of cultural development will take place in all situations where a group of people is trying to achieve a common goal. This means that, as earlier identified for the SMS, only a consistent translation and implementation of a consciously chosen and fitting safety strategy into the complete cycle of "cultural enablers" will lead towards an organisational context in which, in due course, a culture can develop that will support sustainable and safe performance.

1.3.3. Developing the Extended Safety Fractal

Based on the above reflections, organising for resilient, sustainable and safe performance requires a conscious decision for resilience as a safety strategy, with clear choices that provide guidance and direction. In order to have this implemented and "lived" by the whole organisation, this strategy then needs to be consistently integrated throughout the organisation in all interacting, disseminating and re-enforcing actions, as well as in the more formal SMS. However, strategy implementation is difficult, because it forces people to change their behaviour and it requires strong leadership capabilities (Verweire, 2014). Safety leadership can thus be understood as the ability of a manager or staff member to influence behaviour so that it becomes safer (ICSI, 2018). The "Leadership in Safety Working Group" (ICSI, 2018) identified the following seven general leadership principles that summarise good practice and action principles aimed at safety leaders at all levels in high-risk organisations:

(1) create a safety vision that is coherent with the values and principles of management;

(2) give safety its rightful place in the organisation and management and oversee it on a daily basis;

(3) share the safety vision: influence, persuade and promote the flow of information through the hierarchy;

(4) be credible: provide a coherent example;

(5) promote team spirit and horizontal cooperation;

(6) be available on-site to observe, listen and communicate effectively;

(7) acknowledge good practice and apply fair sanctions.

When we interpret these general leadership principles within the context developed earlier in this paper, we can only conclude that safety leadership is the combination of having (developed) a safety vision and consequently implementing it through the more informal cultural enablers (i.e., interacting, dissemination and re-enforcing) within an organisation or wider socio-technical system.

Management system maturity models, on the other hand, appear to measure the level of implementation of a pro-active safety strategy into the SMS. Maturity models, also including the ISO 15504 model (ISO, 2004) presented above, find their origin in the total quality management movement from the late 1970s. They build on the idea that small, evolutionary steps, rather than revolutionary ones, are the basis for continuous improvement (De Cnudde et al., 2004). These quality maturity models mainly provide guidance on how to improve people's competence, processes and technology (i.e., the formal side of safety management) within an organisation in order to move towards sustainable performance. The different stages of maturity should then guide an organisation to move from ad hoc, reactive and often chaotic management towards well-established and predictable processes, with continuous improvement as a major objective. These ideas were then picked up to describe maturity levels also for safety management and safety management systems, with, for instance, Zwetsloot (2000) describing an occupational, health and safety management system that distinguishes four stages of maturity: (1) ad hoc, (2) systematisation, (3) systems approach and (4) proactive and integrative.

To summarise, these elements of SMS and SMS maturity, safety vision, safety culture and safety leadership, that all have been identified as essential to organise resilient and sustainable performance, can be graphically represented in an "Extended Safety Fractal", as depicted in Figure 1.3.

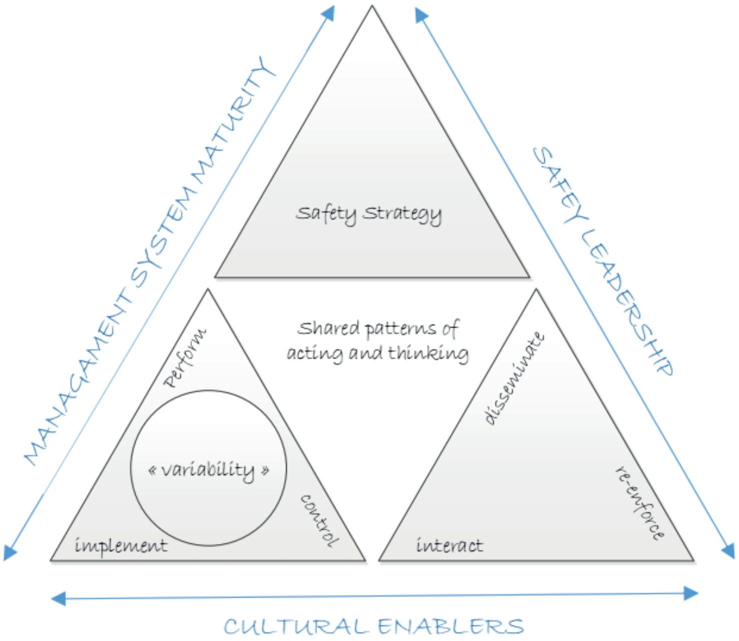


Figure 1.3. The Extended Safety Fractal.

The left side of this figure shows at the bottom the original Safety Fractal, developed in Section 1.2 of this chapter, which represents the effort required for formal and organised safety management. As explained in Section 1.3.1, sustainable safety management requires the systematic implementation of a safety strategy that is the top of this Extended Safety Fractal. Management system maturity then measures the extent to which the safety strategy is also effectively embedded in the SMS or the underlying processes. The right side of the figure represents the extent to which leaders across the organisation promote and support that same agreed safety strategy in their daily activities to achieve sustainable safety management. The bottom side, finally, collects the elements identified in Section 1.3.2 as the enablers for the development of an organisational culture. The "shared patterns of acting and thinking", in the middle of the figure, is then the (safety) culture that emerges as a result of the interaction between the surrounding elements.

1.4. DISCUSSION

The way in which the Safety Fractal and its extended version are constructed creates the expectation that they will be applicable at different levels within an organisation and even a broader socio-technical system. The possibility of repetition and the self-similarity of the models allows us to intuitively bring the logic of generic SMS processes closer to the operational activities of an organisation and to integrate them in a natural way. As argued, the importance of a clear safety strategy for this cannot be underestimated. Resilience as safety strategy, and a focus on managing performance variability rather than eliminating threats, can easily be integrated in the developed models. As a result, both models lend themselves perfectly as a vehicle for the recent paradigm shift in safety management, making optimal use of the experience gained with SMS over the past decades.

Discussing the resilience of an organisation is, however, only of academic value if it is not possible to assess, in advance of accidents and disasters, whether an organisation has the required qualities (Hale et al., 2006). Measuring the effectiveness of an organisation's processes is seen as a better way to capture the true state of evolving organisation and the formal part of safety management, the SMS, looks like the most appropriate starting point. Several authors (e.g. Kelly, 2017; Kuusisto, 2000; Costella, 2009) have reviewed existing methods and proposed alternative categories for classifying SMS audit and evaluation techniques, with Peltonen (2013) even providing an overview of more than 50 existing techniques.

The most straightforward classification is, however, provided by Cambon (2007), who identifies three traditional ways of measuring SMS performance: (1) the analysis of achieved result, (2) the analysis of the approach that is used for setting up the SMS and (3) the comparison of an SMS with an existing reference. The same author also identifies three fundamental attributes of an SMS that need to be captured in order to be able to build a picture of SMS performance: (1) the degree of SMS formalisation, which is similar to attributes of the earlier discussed process capability methods, (2) the quality of the implementation, by assessing whether the SMS effectively manages to prevent accidents from happening and (3) the level of ownership of the SMS by members of the staff in the organisation, looking at the more informal aspect. The proposed approach then combines a questionnaire, based on the TRIPOD methodology (Groeneweg, 1992), to capture SMS ownership with more traditional audit techniques, like document review, interviews and observations, to result in an integrated picture of SMS performance.

Lofquist (2017), on the other hand, when making a case for building resilience into SMS, proposes two areas that can improve the measurement of effectiveness in SMS in order to capture the signals of drift (Dekker, 2011) towards and beyond the system's safe boundaries: (1) the functioning of reporting systems and (2) (improved) safety climate surveys, an idea that also Johnsen (2010) promotes. A similar conclusion is made by Hale et al. (Hale et al., 2006), who state that SMS audit tools can provide the hooks to assess resilience, provided that a closer coupling can be made between the traditional SMS structure and safety culture. This is in line with the description of Hollnagel (2018) of resilience as an expression of how people, alone or together, cope with everyday situations by adjusting their performance to the actual operating conditions. With the resilience assessment grid (RAG), he suggests measuring resilience through the proxy of the four resilience potentials (i.e., the potential to respond, to monitor, to learn and to anticipate).

The Extended Safety Fractal (Figure 1.3) summarises a set of essential elements needed for an organisation to come to a sustainable, safe and resilient performance and which is believed to be the necessary scope for measuring the effectiveness of the safety management of a complex system. This will require a combination of different techniques with clear and explicit focus on an organisation's safety strategy. Furthermore, measuring the effectiveness of safety management will require to assess how the different elements of the Extended Safety Fractal are aligned to implement that strategy, in order to fit the specific mission and sector (Denyer, 2017). A similar focus on the need for strategic alignment can be found in the integrated performance management framework (Verweire, 2014) presented by Verweire as a prerequisite for excellent performance. Depending on the situation and the scope and context of the assessment, the focus may move from the whole system towards more detailed implementation and control processes of the previously identified (Extended) Safety Fractal, and vice versa, making optimal use of the self-similar attributes of the proposed models.

With SMS still the cornerstone of regulatory safety management obligations in several high-risk industries, assessments using the developed models can help to move from pure compliance to a more integrated approach based on dialogue. As mentioned earlier, there is no point in regulating the informal aspects of safety management. However, the Extended Safety Fractal, in particular, offers the opportunity for safety authorities to develop a more holistic approach. An initial experience to develop adapted supervision strategies using the Extended Safety Fractal, together with some national safety authorities within the European railway sector, promises positive results in that regard (Haug and Accou, 2021).

In high-risk industries, a lot of time and effort also goes into incident investigation to collect very little useful information vis-à-vis explicit safety-risk management (Kelly, 2017). The main reason for this is that 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. Further chapters in this thesis will explain how the concept of the Safety Fractal is used to develop an innovative accident and incident analysis method that guides investigators to explore the composite 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 same simple five steps, inspired from the Safety Fractal, are iterated to evaluate the performance of relevant SMS processes. The idea of nested control loops (e.g., Rasmussen and Svedung, 2000; Leveson, 2016) is then used to identify the relevant set of control and implementation processes that influenced the chain of events. This leads investigators through the different operational, tactical and strategical levels that together form a socio-technical system in a more intuitive way. Moreover, this allows the analysis of 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) and to discover the "local rationality" of decision and policy makers. Haavik et al. (2019) describes this as the need to combine in-depth studies of work with an understanding of the organisational settings in which this work takes place. This is expected to result in recommendations that address the capability of responsible organisations to manage safety critical variability, leading them towards more resilient performance.

1.5. CONCLUSIONS

Resilient performance cannot be managed or controlled directly but can be managed indirectly through the known characteristics that lead to it. By comparing the model behind SMS with specific requirements for process capability, this chapter identifies a Safety Fractal that can help to understand how to build resilience into the SMS at all levels of a socio-technical system. This requires that resilience is explicitly identified as the safety strategy to follow, which should then be consequently implemented through both formal and informal cultural enablers. This mechanism, as modelled through the extended Safety Fractal, offers a systematic and more comprehensive framework to understand, organise and assess safety and resilience performance management. Further research should identify how this could best be realised in a practical and cost-effective way.

The first, practical examples presented above, already demonstrate the potential of the developed models to (re)vitalise the concept of SMS and to make the most of its full power. Further chapters will describe the validation of these models in an operational context, mainly by applying the Safety Fractal through the SAFRAN accident analysis method. The (Extended) Safety Fractal offers the possibility to also assess an organisation's capability for resilience in earlier stages, e.g., by using scenario-based assessments. The main argument for this is the fractal nature of the innovative approach that allows the same basic components to be used for both system wide and more detailed analysis. Future research could lead to identifying the most effective way of doing this.

2

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

This chapter is based on the article with the same title, published in *Safety Science* 115, 285-293 by Bart Accou *(role: concept, methodology, analysis and writing)* and Genserik Reniers *(role: review and supervision)* and complemented with element from the conference paper presented at the 55th European Safety, Reliability & Data Association (ESReDA) seminar, hosted by the Romanian Railway Investigation Agency AGIFER, 9-10 October, 2018, Bucharest, Romania.

The conference paper was published as: "Accou, B. Reniers, G. 2019. Developing a method to improve safety management systems based on accident investigations: The SAfety FRactal ANalysis. In *Accident Investigation and Learning to Improve Safety Management in Complex System: Remaining Challenges - Proceedings of the 55th ESReDA Seminar, 2019*, edited by Paul, S., Marsden, E., Verschueren, F., Tulonen, T., Ferjencik, M., Dien, Y., Simola, K., Kopustinskas, V., p 210-220."

INTRODUCTION TO CHAPTER 2

Soon after developing the component parts of the Safety Fractal (without already calling it like that), it became clear that a graphical representation would help explaining the ideas behind it. Due to the generic and apparent scale-invariant nature of the developed concept (i.e. same properties at process level as at system level) I quickly arrived at the idea of a fractal. The basic constraint I considered was to be able to represent the three very distinct levels to assess and understand the functioning of a process or activity: process performance, process implementation and process control. In addition to some very complex and especially colourful images of fractals, a google search also yielded an image of Sierpinski's triangle (e.g. Fractalen: definitie, theorie en voorbeelden | Wetenschap: Wiskunde (infonu.nl)), which eventually inspired me to use a triangle as the graphical representation of the Safety Fractal.

For accident analysis, the Safety Fractal was first used in a case study, to guide the investigation of a switch-maintenance-incident. I still see myself drawing pictures of triangles on the whiteboard in the office in the station of Namur, to explain what I was expecting. The enthusiastic investigation team was composed of a senior accident investigator with long operational experience and a junior accident investigator, with extensive audit experience as well as being a trained human factors specialist. Compared to the kind of accident investigations that were usually carried out, the result was remarkable. For all critical variabilities that were detected, both on the side of the track maintenance team as for the signaller involved, the investigation resulted in a completion of all elements of a Safety Fractal. But although I (thought I) had explained this as a main objective, there was no analysis of the company's SMS. The investigators' feedback after trying the Safety Fractal approach in this first case study reflected mainly the need for guidance to select the "next process" to investigate. This resulted in the development of the investigation flow and, with the whole research orienting more and more towards the development of an accident analysis method, into the introduction of a new name: the SAfety FRactal ANalysis (SAFRAN) method.

The ESReDA paper that is integrated in this chapter also marks the first presentation of the SAFRAN method for a public audience.

ABSTRACT

With the publication of the public enquiry on the Piper Alpha disaster (1990), the concept of a safety management system (SMS) has found its introduction in high-risk industries. This concept went further than being "good practice" and became legally mandatory in some industries, where holding a certificate/licence, issued on the basis of a SMS, is necessary to operate. SMS requires continuous improvement, based on a combination of "knowing the unknown" (risk assessment) and "learning on experience" (occurrence analysis). To do so, accidents/incidents need to be reported and analysed and measures need 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. Where a SMS is based on a holistic approach, with operational, supporting and controlling elements functioning together to improve safety, most reporting/investigation methods are not developed in line with a system thinking approach to accident causation. Also, how to link the top-down description of SMS requirements with the operational activities of the organisation that create these risks in the first place, is poorly understood. In result, the current practice in accident and incident investigation 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.

Building on the Safety Fractal that is elaborated in the previous chapter, this chapter 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 chapter 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 model 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. In addition, the proposed methodology provides an innovative visual representation of the investigation process.

2.1. INTRODUCTION

In the evening of November 1, 1918, a Brighton Beach Train of the Brooklyn Rapid Transit Company, packed with a rush hour crowd, derailed on a sharp curve approaching the tunnel at Malbone Street, in Brooklyn, and plunged into a concrete partition between the north and south bound tracks. When entering the reverse curve, which had a speed limit of 10 km/h, the train was operating at a speed of 48 km/h or more. At least 93 people died, making it one of the deadliest train crashes in the history of the United States. (NY Times, 1918; Wikipedia, 2018).

Now, 100 years later, the management of safety risks in railways, as in many other high-risk industries, is mainly relying on the holding of a safety management system (SMS). This organisational concept to continuously improve safety of operations, was launched with the recommendations resulting from the public enquiry after the deadly disaster on the oil platform Piper Alpha (Cullen's, 1990) and introduced the transition from an often very prescriptive safety approach towards an approach that is evidence-driven and based on goal-oriented legislation. In different industries, the holding of a SMS to control all risks related to a company's operational activities not only became normative but even legally mandatory, forming the basis for certification and regulation (e.g. Vierendeels et al. 2011; Leveson, 2011; 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 chapter, 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 section, the method can help to identify those elements of the SMS where interventions might have the greatest impact for improving global system safety.

2.2. 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 section 1.2). 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** of the same five **basic steps**, provides the required investigation method. Thirdly, in addition, the SAFRAN method provides a way to graphically represent the results of the performed analysis.

2.2.1. 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.

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, according to Speziali and Hollnagel (2008), the only identified Systemic methods, suitable to analyse systems that are tightly coupled and intractable, 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 widely used within large parts of high-risk industries (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

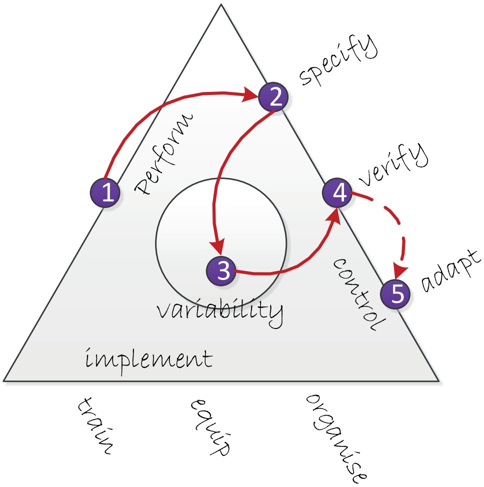


Fig.2.1: One complete iteration of analysing the Safety Fractal

The attentive reader will have noticed that although the basic triangle is the same, the numbering and consequently the order of the arrows is different from that presented in Figure 1.2. While Figure 1.2 depicts the logic followed when seeking control over an activity, as in an SMS, Figure 2.1 depicts (with reference to the essential steps of an investigation as proposed by Wienen et al. (2018)) the logical sequence for an investigator to understand and analyse an event.

2.2.2. 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. This should ensure that not only the performance part of a process or function is investigated but also the implementation and control dimension of that function. To steer investigators to analyse these elements of safety management systematically, this "next" iteration is integrated in the proposed method. In addition, it is suggested to stop the iterations in a particular branch of the analysis only when there is a major specification issue to be corrected in a control process.

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.

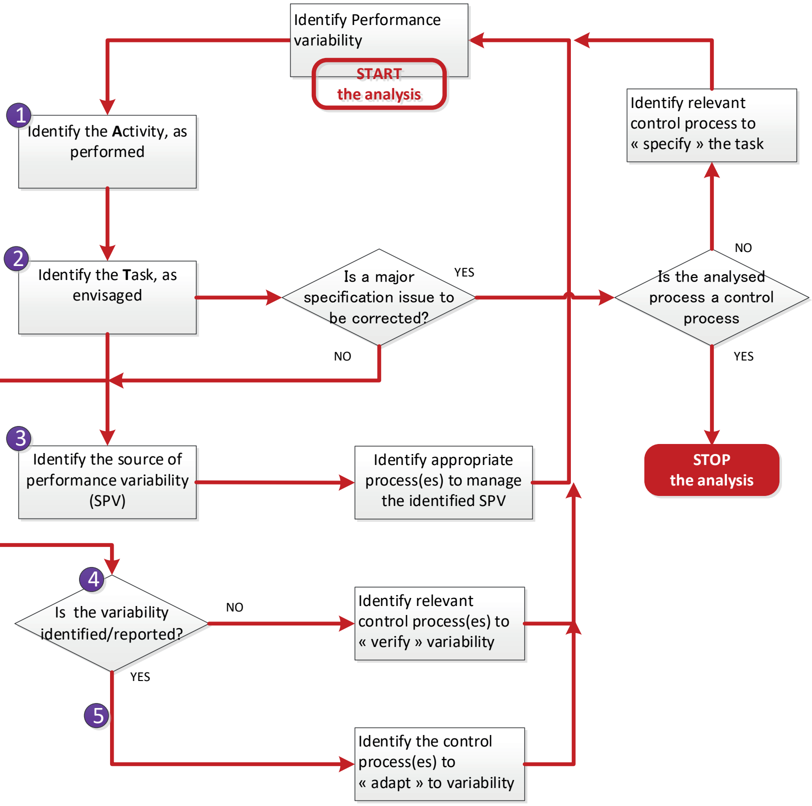

Identify Performance variability
START the analysis
1
Identify the Activity, as performed
2
Identify the Task, as envisaged
Is a major specification issue to be corrected?
YES
NO
Is the analysed process a control process
NO
YES
Identify relevant control process to « specify » the task
STOP the analysis
3
Identify the source of performance variability (SPV)
Identify appropriate process(es) to manage the identified SPV
4
Is the variability identified/reported?
NO
YES
5
Identify relevant control process(es) to « verify » variability
Identify the control process(es) to « adapt » to variability

Fig.2.2: 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.

2.3. CASE STUDY

As long as not all infrastructure and rolling stock is equipped with an automatic train protection system that continuously controls speed requirements, derailments because of over-speeding will remain a major risk of the railway system, as has been demonstrated by several of the most lethal railway accidents over the last decades. As input for this case study, a set of six published investigation reports has been selected to check their depth and focus when investigating accidents or incidents caused by over-speeding. This selection has been made taking into account a geographical spread, the similarity of the accident (i.e. a critical variability in maintaining the appropriate speed of a passenger train), the author of the report in all cases being a national and independent investigating body and the availability of the report in a language that can be read by the author of this paper (that is English, Dutch, French or German). The following Table 1 provides an overview of the selected investigation reports, the allowed and actual train speed and the consequences of the adverse event.

event	critical performance	consequences
Train derailment accident between Tsukaguchi and Amagasaki stations of the Fukuchiyama line of the West Japan Railway Company, April 25, 2005	allowed train speed: 70 km/h actual train speed: 116 km/h	107 people killed 562 people injured
Main-track derailment of a Via Rail Canada passenger train in Aldershot, Ontario, February 26, 2012	allowed train speed: 15 mph (24 km/h) actual train speed: 67 mph (108 km/h)	3 people killed 45 people injured
Derailment of a passenger train near Santiago de Compostela station (ESP), July 24, 2013	allowed train speed: 80 km/h actual train speed: 179 km/h	80 people killed 73 people seriously injured
Derailment of Amtrak passenger train 188 in Philadelphia, Pennsylvania (USA), May 12, 2015	allowed train speed: 50 mph (80 km/h) actual train speed: 106 mph (171 km/h)	8 people killed 185 people injured
Derailment of a SNCB/NMBS passenger train in Buizingen (BEL), September 10, 2015	allowed train speed: 50 km/h actual train speed: 120 km/h	39 people injured
Overspeed at Fletton Junction, Peterborough (GBR), September 11, 2015	allowed train speed: 25 mph (40 km/h) actual train speed: 51 mph (82 km/h)	4 people minor injured

Table 2.1. Overview of analysed investigation reports and the identified critical performance

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 workplace 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.

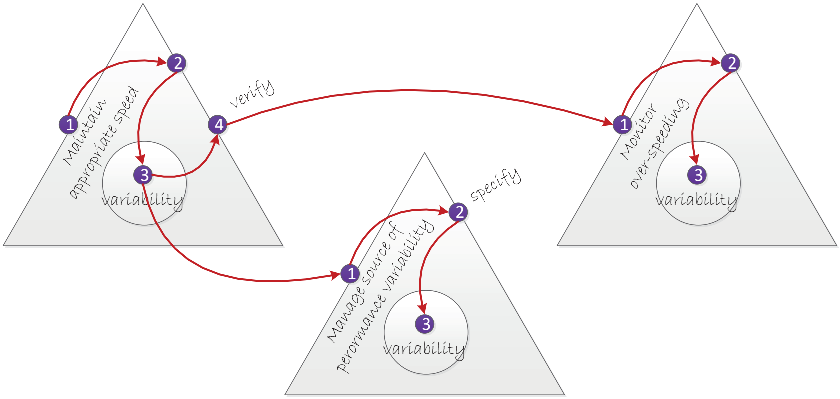


Fig.2.3: Reference model for investigating over-speeding incidents, based on the SAFRAN logic

When comparing the reviewed investigation reports with the reference model, as illustrated in Figure 2.3, we found that they all report on the permitted as well as the actual train speed. Furthermore, all reviewed investigation reports mention the expected performance and the way this is formalised (i.e. the second step in a SAFRAN iteration) in a detailed way. Also, all reports identify the factor(s) that can explain the critical variability in the driver's performance when maintaining the appropriate speed (i.e. step 3 in the first iteration of the SAFRAN method). Table 2 (see annex to this paper) provides an overview of all these sources of variability that were identified. 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. The reports on the derailments in Buizingen (IBRAI, 2017) and Santiago de Compostela (RAIC, 2014) both witness on the identification of monitoring activities that took place to detect over-speeding incidents and conclude on the inadequateness of these activities. All this, however, without analysing possible factors that influenced this poor monitoring and with the Buizingen-report surprisingly stating "the difficult detection of this type of events" as an explaining argument. The investigation reports on the derailments in Philadelphia (NTSB, 2016) and Aldershot (TSBC, 2012), in turn, do not mention any reflection on the railway companies' activities to detect over-speeding. In particular for the latter report this is curious, since the implementation and maintenance of an SMS, including monitoring and evaluation processes for all aspects of operations, is explicitly mentioned as a legal obligation, in order to integrate safety into day-to-day operations (TSBC, 2012). For the iteration related to the identified sources of performance variability, we found that two of the reviewed investigation reports (i.e. Fukuchiyama line and Aldershot) do not further analyse the capability to manage these. The investigation on Santiago de Compostela identifies a lot of relevant management processes, but systematically only compares the actual performance with the expected and specified performance, turning the investigation into a pure (non-) compliance exercise. A similar remark can be made for most of the processes that are identified to manage sources of performance variability in the Buizingen and Philadelphia investigation reports, with the exception of the analysis of the respective processes that manage train driver competence. The investigation report of the over-speeding incident at Fletton Junction, finally, gives a mixed image. On the one hand there is only mention of the specifications for the processes related to equipping engineering controls and, on the other hand, a detailed and structured analysis is providing for the processes related to the management of driver fitness and the equipment of lineside signs. A complete overview of these findings is provided in Table 2, as an annex to this paper. It has to be noted that all these findings are solely based on the elements that are available in the published reports and cannot take into account analysed elements that are not reported upon.

The following Table 2.2 provides a summary of the elements from the reference model that are addressed in the analysed accident investigation reports, where the three mentioned processes in the most left column of the table (i.e. “maintain appropriate speed”, “monitor over-speeding” and “manage source of variability”) each correspond with a triangle and the related steps (1, 2, 3) as depicted in Figure 2.3.

Event Process		**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
step 4 **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 source of 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 2.2. Overview of analysed investigation reports (see also Table 2.3 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 2.3). 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. An overview of the more detailed findings of this analysis is provided in the Table 2.3, at the end of this chapter.

The choice to stop this reference model 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 2.4), one can immediately identify a depth of three consecutive iterations.

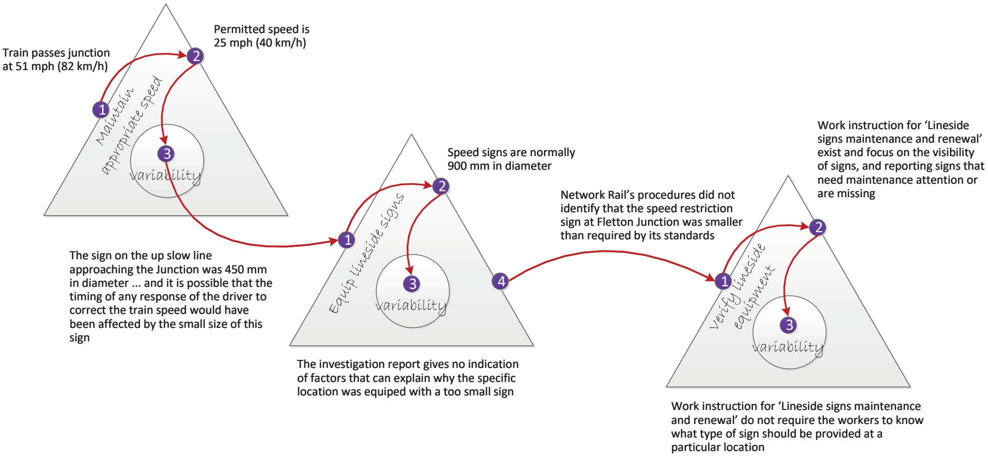

Train passes junction
at 51 mph (82 km/h)
Permitted speed is
25 mph (40 km/h)
1
2
3
Maintain appropriate speed
variability
The sign on the up slow line approaching the Junction was 450 mm in diameter ... and it is possible that the timing of any response of the driver to correct the train speed would have been affected by the small size of this sign
Speed signs are normally 900 mm in diameter
1
2
3
4
Equip lineside signs
variability
The investigation report gives no indication of factors that can explain why the specific location was equiped with a too small sign
Network Rail's procedures did not identify that the speed restriction sign at Fletton Junction was smaller than required by its standards
Work instruction for 'Lineside signs maintenance and renewal' exist and focus on the visibility of signs, and reporting signs that need maintenance attention or are missing
1
2
3
Verify lineside equipment
variability
Work instruction for 'Lineside signs maintenance and renewal' do not require the workers to know what type of sign should be provided at a particular location

Fig.2.4: 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.

2.4. 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 weaknesses in these areas are 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, it should be recognised 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. No information is available 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.

2.5. 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 chapter, the SAfety FRactal ANalysis method was 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. 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.

event	sources of performance variability	iteration of the process to "manage source of variability"	elements of monitoring (over-)speed	iteration of the process to "monitor over-speeding"
Fukuchiyama line (JAP) April 25, 2005	driver attention, impacted by: -> stress, due to earlier station overrun -> pressure to contact train conductor -> driver taking notes -> negative reinforcement regime missing engineering control system	no further structured analysis	non-reporting of prior occurrences, although required	non-reporting of prior occurrences, due to: -> negative reinforcement regime active reflection on possibility to monitor speed at critical curves, resulting in a recommendation to monitor speed using already existing technology
Aldershot, Ontario (CAN) February 26, 2012	driver memory driver expectations driver experience quality of rules visibility crew interaction missing engineering control system	no further structured analysis	prior similar occurrences listed	not mentioned in the report curiously enough, the regulatory requirement to implement and maintain an SMS is mentioned, including the obligation to have "monitoring and evaluation processes for all aspects of operations."

event	sources of performance variability	iteration of the process to "manage source of variability"	elements of monitoring (over-)speed	iteration of the process to "monitor over-speeding"
Santiago de Compostela (ESP) July 24, 2013	driver attention, impacted by: -> answering an internal telephone call lineside signs system design missing engineering control system task complexity task monotony	for processes to "manage driver competence" and "equip lineside signs" only specifications have been identified - limiting the investigation to a pure compliance check for processes to "equip engineering controls" also the "verification process" has been analysed, but for all only specifications have been identified	performed by railway undertaking: - accompany of train - review of safety recorder content performed by infrastructure manager: - inspection of speed recorders	internal regulations and number of performed monitoring activities are listed no reflection on why these monitoring activities did not enable to identify the critical variability
Philadelphia (USA) May 12, 2015	driver attention, impacted by: -> emergency situation with other train missing engineering control system driver competence driver fatigue driver fitness to work driver vigilance task complexity	process to "train crewmembers" has been further analysed (steps 1, 2 and 3) for process to "equip engineering controls" only specifications have been identified	not mentioned in the report	not mentioned in the report

event	sources of performance variability	iteration of the process to "manage source of variability"	elements of monitoring (over-)speed	iteration of the process to "monitor over-speeding"
Buizingen (BEL) September 10, 2015	driver expectations driver experience decision making skills, impacted by: -> recent leave lineside signs	process to "manage driver competence" has been further analysed (steps 1, 2 and 4), without however identifying what could be the critical variability	sample based analysis of speed recorder data	identification of poor monitoring capability no further structured analysis is elaborated, with the report surprisingly stating "the difficult detection of this type of events" as an argument to explain poor monitoring
Fletton Junction (GBR) September 11, 2015	driver fatigue engineering control system lineside signs driver experience driver expectations time pressure	processes to "manage driver fitness" and "equip lineside signs" have been further analysed for process to "equip engineering controls" only specifications have been identified	(non-)reporting of over-speeding incidents OTDR downloads to monitor compliance with speed restrictions	only the monitoring (and learning) capability based on reported incidents has been further analysed, identifying (monitoring) task instructions and supervisor training as possible sources of performance variability for the process of "monitoring over-speeding".

Table 2.3 Overview of analysis findings

3

Systematically investigating human and organisational factors in complex socio-technical systems by using the “SAfety FRactal ANalysis” method

This chapter is based on the article with the same title, published in *Applied Ergonomics* 100 (2022) 103662 by Bart Accou and Fabrice Carpinelli (*role for both authors: concept, methodology, analysis, writing and review*).

INTRODUCTION TO CHAPTER 3

In applying the SAFRAN analysis method, several investigation practitioners have encountered practical difficulties in answering its essential third step, which aims at understanding the 'local rationality' of actions and decisions. Without wanting to create the illusion that the method allows for an in-depth analysis of human and organisational factors (HOF), which will always require deep-rooted expertise, we wanted to provide investigation practitioners a guideline to at least identify the relevant HOF elements. The approach for this is described in this chapter.

An earlier version of the published paper on which this chapter is based, was presented at the 7th International Human Factors Rail Conference, which was hosted online from June 23 to 25, 2021. The conference triggered the publication of a special issue of the journal Applied Ergonomics.

ABSTRACT

In order to manage the performance of socio-technical systems in a safe and sustainable way, the importance of looking at human and organisational factors (HOF) and their contribution to adverse events is widely recognised. In reality, however, the scope of accident and incident investigations stays usually limited to investigating the immediate causes and decision-making processes related to the accident sequence (e.g. Antonsen, 2009). Important factors, including design and planning decisions, contributing to accidents are hereby often overlooked and the weaknesses in the Safety Management System are hardly ever analysed.

The SAFRAN method can guide investigators in an intuitive and logic way, to ask questions that help to gain deeper understanding of the capability of organisations to monitor and manage safety critical variability. The essence of using the SAFRAN method for evaluating the performance of the different processes in a socio-technical system, is to approach them in a similar way, building on the generic elements that compose a SMS and systematically looking at the HOF that influenced actions and decision making, regardless of the hierarchical level they are situated at. This chapter presents the SAFRAN method, specifying a dedicated HOF taxonomy and sharing examples of supporting HOF questions. The approach enables non-experts in HOF to systematically identify the different elements that introduce critical variability in performance and to recognise what additional expertise can be called upon when needed.

3.1. INTRODUCTION

Commissioned by the International Ergonomics Association (IEA), Dul et al. (2012) have published a position paper for the human factors/ergonomics (HFE) community in 2012, in which they provide an up-to-date picture of where HFE stands as a professional discipline and which strategies should be used to strengthen this position for the future. They conclude that, despite more than 50 years of history, HFE knowledge has not yet found wide-spread recognition nor implementation and the potential of HFE remains under-exploited. The main reasons for this, still according to Dul et al. (2012), can be found in: (1) no strong stakeholder demand by lack of awareness, (2) no readily available HFE knowledge in design projects, resulting in sub-optimal solutions, (3) no explicit reference to HFE as a discipline, when incorporated in wider design projects and (4) confusion and ambiguity on what HFE is, due to its multi-disciplinary base.

The main strategy direction Dul et al. (2012) propose towards the world-wide application of HFE excellence is to strengthen the demand and application of high-quality HFE through improved communication, the building of partnership with all identified stakeholders (i.e. system actors, system experts, system decision makers and system influencers) and the promotion of high-quality standards for HFE knowledge.

While fully supporting the starting point that HFE has great potential to optimise human performance and well-being, based on their own professional experience with implementing safety management in the railway system in Europe, based on own experience, we can only confirm that almost a decade after the publication of this position paper, the need for a better integration and application of HFE knowledge is not only still very recognisable but also urgent. To achieve this, more than better marketing for HFE by the HFE community will be required. HFE should be accepted as an essential prerequisite for safe and sustainable performance and not as an expendable add-on, as it is still too often perceived (Hollnagel, 2014). In that context, Dul and Neumann (2009) argue that HFE can add value to a company's business strategy to create organisational effectiveness. Grote (2014) elaborates on this idea and suggest to embed system design in the management of uncertainty (and the management of risk more general) that should be part of the overall objectives in individual and organisational decision-making in order to gain and maintain control of activities to achieve desired goals. Within the European railway legislative framework (European Commission, 2018, 2020), a first step in this direction has been taken by introducing explicit requirements to take a systematic approach to supporting human performance and managing human and organisational factors within the safety management system (SMS).

In line with what Dul and Neumann (2009) suggest, we can agree that every opportunity to link variability in safety (and wider business) performance with (lack of proper implementation of) HFE should be exploited in order to convince stakeholders, and in particular decision-makers, of the importance of taking HFE into account as a strategic element in controlling activities. An important success factor here is that not only HFE experts are able to do this, but everyone who is involved in the analysis of an operational context, such as auditors and accident investigators. Furthermore, it is important to recognise that the nature of work in the railway sector and therefore also the work environment has changed dramatically over the last decades, with the centralisation of traffic control centers and the still increasing automation of train control and traffic management as only a few examples. As argued by Hollnagel (2014), for HFE to be able to anticipate and properly support these new types of work, the scope of possible interventions should aim beyond the pure design of artefacts and focus on the broad organisation of activities. This also requires the capability to deal with the organisational dimension of socio-technical systems. To put a focus on this need to envisage a broader scope for HFE activities, it is preferred to refer to "human and organisational factors" and to use the acronym "HOF" (rather than HFE) in the remaining part of this chapter.

With the above in the background, this chapter describes how the SAfety FRactal ANalysis (SAFRAN) method can be used by non-HOF-experts to identify the different HOF elements that introduce (critical, either positive or negative) variability in all relevant processes and to recognise what additional HOF expertise can be called upon when needed.

3.2. USING THE SAFRAN LOGIC TO SYSTEMATICALLY IDENTIFY HOF

As specified in previous chapters, the SAFRAN method was developed to guide accident investigators in exploring the composing elements of an SMS in a natural and logic way, starting from the findings close to operations that explain the occurrence. Initially, it was introduced as a combination of a generic model of process management, an investigation flow, and a matching graphical representation. The most appealing element of the method lies in the identification of five recognisable investigation steps that, when iterated, provide a structured way to guide investigators to evaluate any relevant process of the socio-technical system. The logic of this repetition provides an ideal pattern to examine the concerned HOF in a systematic way throughout the socio-technical system.

3.2.1. The Safety Fractal as an instrument to manage sustainable performance

The Safety Fractal forms the basis of the SAFRAN method. It describes, in a generic and self-similar way, a five-step safety management delivery system 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.

This Safety Fractal represents a repeatable unit of analysis in which HOF elements can be identified as those factors that could create critical variability in the human or wider system performance. These sources of performance variability (SPV) are always part of a process, function or activity. The main idea behind the proposed approach is that performance variability and the SPV that influence it (i.e. step 3 in the Safety Fractal), once identified in a concrete situation, can be linked to respectively the control and implementing processes, to form the basis for managing safe and sustainable performance.

The "specify" element (1) of the Safety Fractal will cover the ability to anticipate and prepare for normal operations and foreseeable hazards. Several authors (e.g. Le Coze, 2020) also argue that part of the response to sudden disruptions should be included at this stage, in the design of the system, which will require a reflection on possible SPV. This is in line with the view of pioneers such as Chapanis (in Fitts, 1951) or Norman (2002), who indicated the importance of considering the users of each part of the system in their interactions with it, right from the design stages. The origin of performance variability and the potential room for improvement should therefore not only be sought in the process that failed (or in which operational users err), but also in the whole system. Furthermore, in line with Norman (1983) who pointed that "people will make errors, so make the system insensitive to them", questioning HOF influences should go beyond the process taken at the start of the analysis and cover most of the possible interactions within the socio-technical system.

Continuous monitoring of the system to ensure that performance boundaries are not crossed is represented by the "verify" element (4) of the Safety Fractal. To cope with the fact that in complex system, with non-linear interactions, it is more difficult to understand the "latent condition pathways" (Reason, 1997) or the "mechanisms" that lead to risks (Hollnagel, 2008), this monitoring will have to shift from looking at past performance (i.e. the more traditional lagging indicators) towards looking at actual performance and resources (i.e. the leading indicators). Knowing what to measure then requires an understanding of the (effect of) SPV (on performance), which in turn requires regular input from the people taking real-time decisions.

Finally, dampening the critical variability, i.e. the solution to create "resilient performance" according to Hollnagel (2008), could be achieved by the implementing processes, in step (2) of the Safety Fractal, that impact the SPV and that should create those HOF-conditions that make work succeed. By choosing resilience, and more specifically managing critical variability in performance, as the main goal for each Safety Fractal, the need to integrate HOF in SMS is explicitly recognised.

Repeating this logic for all relevant processes in the different hierarchical levels of the socio-technical system will help investigators to overcome the downfall that, according to Salmon et al. (2013), characterises the already existing systems-oriented analysis methods, namely losing the fine-grained analysis provided by methods that focus more on the individual behaviour. They suggest using both system and individual oriented approaches in a complimentary manner as the solution, and further claim that a better understanding of the complexities of human behaviour and the impact of the system on behaviour will support the development of more exhaustive countermeasures.

The proposed SAFRAN method nurtures and structures the repetition of a set of basic questions, guiding investigators both through the socio-technical system processes and through the potential influences of/on HOF. In other words, it offers the combination of both human (i.e. the identification of SPV) and system analysis (i.e. iteration logic) approaches together. By doing so, the method also offers the potential to find the right balance between looking for latent conditions and accounting for the active errors Young et al. (2004) are looking for.

3.2.2. Illustration of the SAFRAN analysis

Analysing the performance of processes through the identification of HOF elements (i.e. SPV) and repeating this logic for the processes that should manage the related performance variability, was first tested in the context of accident and incident investigations. To develop this illustration, the information contained in the RAIB report (2017) on the overturning of a tram at Sandilands junction, at Croydon on 9 November 2016, has been identified and restructured.

In the early morning of that day, a tram did not slow down to the required 20 km/h (as trams normally do) and was still travelling at 78 km/h when approaching a sharp curve in the tracks. The driver applied the brakes, but the tram was still travelling at 73 km/h when it entered the sharp curve and began to turn over onto its right-hand side. The accident resulted in seven fatalities, nineteen people seriously injured, and 43 passengers with minor physical injuries (including the tram driver). This accident was chosen because of the comprehensiveness of the final investigation report (RAIB, 2017), identifying HOF throughout a complex socio-technical system. It has also to be noted that elements not related to the over-speeding (e.g. evacuation of passengers) were not included in the SAFRAN analysis.

Starting close to the sequence of events, the first function that is reported showing critical variability, is to maintain appropriate speed. For this function, the RAIB report lists the following SPV: situational awareness, fatigue, low workload and the infrastructure design element related the tight left hand curve and the elements approaching the curve (i.e. three closely spaced tunnels and the visibility of lineside signs). In application of the SAFRAN analysis logic, the next functions to be analysed would then either represent the management of these identified sources of performance variability or the delivery of monitoring and/or learning capability related to over-speeding. For each of these functions, the same logic (i.e. identifying critical variability, SPV and the next functions to analyse) can then be repeated, resulting in yet further iterations. The result of the full analysis can be seen in the following Table 1. The notion "NFI" indicates that "no further information" on the item was available in the investigation report.

From this analysis, we can conclude that the report contains information on relevant HOF (i.e. the SPV) for all identified functions throughout the investigated socio-technical system. Except for one SPV identified in the first iteration (i.e. low workload), for all the other SPV that influenced the over-speeding the investigations has looked at the functions that are expected to manage them.

However, we can also conclude that this approach is no longer followed for further iterations. The lack of adequate guidance on fatigue management for drivers, for example, is noted, but the function to develop and manage this guidance appears not to be analysed. On the side of monitoring critical variability, all elements that could have influenced the potential of the concerned organisation to be aware of drivers not respecting speed limits are not analysed. The role of the regulator to provide oversight on the SMS and thus most of the control and implementation processes is not further analysed.

What is considered by the investigation report as ending points, strong enough to recommend mitigations, can also serve as new starting points for further iterating the logic of the analysis through the relevant SPV and (control) processes. These further iterations (corresponding to the NFI in Table 3.1.), when further explored during an investigation analysis, may lead to more sustainable mitigations and contribute to consider more latent failures within the socio-technical system.

Function *and identified critical variability*	*Identified source(s) of performance variability*	*Next function: Manage SPV*	*Next function: monitoring critical variability*
Maintain appropriate speed: curve with allowed train speed of 20 km/h entered with 73 km/h	Situational awareness	**Verify driver's situational awareness**	**Monitor over-speeding** (at critical points)
	Fatigue	**Manage driver fatigue**	
	Low workload	NFI	
	Infrastructure design issues	**Design – identify risks**	
Monitor over-speeding: – Reluctance of drivers to report own mistakes – Potential learning from customer complaints not fully exploited – Tram speed checks did not identify drivers travelling above permitted speed	Drivers believing that reporting would result in unnecessary action and/or disciplinary action	**Measure perception/culture**	**Oversight of tramway system**
	Driver's lack of trust with line controllers and senior management		
	On track data recorders overwrite older data	NFI	
Verify driver's situational awareness: driver's situational awareness not controlled	No device capable of detecting driver's loss of awareness	NFI	NFI
Manage driver fatigue: – Fostering a culture that encourages to report fatigue – Poor review process for checking time sheets for excess hours	No adequate guidance for drivers	NFI	**Measure perception/culture**
	Rostering and the monitoring of rest day working	NFI	
	Published industry practice not followed	NFI	

Function *and identified critical variability*	*Identified source(s) of performance variability*	*Next function: Manage SPV*	*Next function: monitoring critical variability*
Design – identify risks: – Actual level of risk associated with over-speeding on a curve not recognised – Little evidence of use of common risk assessment techniques – Formal recording of route hazard assessment	Rely on driver to mitigate risks of over-speeding	NFI	**Oversight of tramway system**
	Risk not fully understood	NFI	
	Evidence from other transport systems not fully taken into account	NFI	
	Limited bus and coach experience of consultant facilitating risk assessment workshops	NFI	
	Desire among designers, residents and others for the amount of land of acquisition to be minimised	NFI	
Measure perception/culture: – Biennial staff surveys – Regulator’s audit of safety culture and SMS	Actual response to address identified issues was considered sufficient	NFI	NFI
Oversight of tramway system: Regulatory strategy provided a lower level of intervention for tramway than for other sectors	Availability of resources	NFI	NFI

Table 3.1: Available information on the Sandiland junction derailment structured according to the SAFRAN logic

3.2.3. Identifying sources of performance variability

When investigating incidents or accidents, the aim (and the challenge) of investigating human performance is to find out how peoples' assessments and actions made sense at the time, given the circumstances that surrounded them. When testing the SAFRAN method for use in the aviation sector, Flovenz (2020) highlighted the possibility to have taxonomies to support the analysis as possible area for improvement, in order to guide the investigators "to ask the appropriate question to determine whether such (i.e. human and organisational) factors need to be included or excluded.". Based on similar needs expressed by other investigators that were informally testing the method, it was decided to develop a set of reference SPV that match the SAFRAN investigation logic. This taxonomy could then help investigators to formulate hypothesis on HOF elements that may have influenced a certain decision or action and that can be checked.

Numerous studies have tried to understand human performance, in order to improve safety and accident prevention. This has led to the general acceptance that human actions can only be described meaningfully in relation to the detailed context and conditions that accompanied and produced them. These conditions have generally been referred to as "performance shaping factors" (PSFs) and although there is a basic agreement on a core set of these factors, competing lists of various lengths exist (Hollnagel, 1998). A suitable taxonomy may, however, possitively affect the efficiency and effectiveness of an accident analysis method (Underwood, 2013). Also several other authors consider the availability of a taxonomy, that allows for classifying the factors that contribute to an event, as a critical element when evaluating accident analysis methods (e.g. Speziali and Hollnagel, 2008; Salmon et al., 2013; Waterson et al., 2015).

As explained before, the essence of using the SAFRAN method for evaluating the performance of the different processes in a socio-technical system, is to approach them in a similar way. The strength of the method is that its logic can be applied regardless of the hierarchical level at which these processes are situated. Therefore, the main characteristic of a taxonomy, to be useful in the SAFRAN method, is that it must be generic and can be used for all functions and all layers of a socio-technical system. This requirement appeared to be problematic for most of the taxonomies that were reviewed. The majority of existing taxonomies is domain specific and strongly referring to situational, organisational or environmental elements that characterise the purpose or field they were developed for. This problem was recognised by Kyriakidis et al. (2018), who consequently proposed a basic unit that needs to be considered when peforming an event analyis and that emphasises that human knowing and acting are intertwined and constrain each other. Therefore, the individual and the technical environment cannot be investigated seperately – a position that is also taken by resilience engineering (Hollnagel, 2018). The systems approach also argues that, in order to understand performance, it is the interaction between components that is of interest rather than the components themselves.

But also the taxonomy used to support this basic unit of analysis of the human in a socio-technical context (Kyriakidis et al., 2018) appeared problematic. For application with the SAFRAN method, having "SMS" (an element that figures in the existing taxonomy of Kyriakidis et al., 2018) as a source of performance variability is much too related to a fixed dimension or scale of analysis, therefore preventing it to be used at higher levels of iteration. Furthermore, a SMS is a combination of mutually dependent processes and arrangements for which the composing elements should be covered in much more detail when analysing implementing and control processes of a certain function and eventual further iterations. In the same line of thought, Hollnagel (2018) refers to safety culture (another element from the existing taxonomy of Kyriakidis et al., 2018) as a "monolithic explanation", often used in an attempt to provide a single and simple solution to a (complex) problem. Rather than being the end point of an investigation, the finding that a pattern of (unsafe) acting or thinking is shared by a group of people should be an anchor point in the investigation to try to identify how this behaviour developed and became part of the organisational culture. A structured way to approach this as part of a SAFRAN analysis is explained in a following chapter.

To solve these problems with existing lists, it was decided to develop a separate taxonomy. Inspired by the work of Kyriakidis et al. (2018), a dynamic- versus static-logic was chosen for both features of the individuals (and teams) and of the situation that can specify an event. A fifth category was added to enable a focus also on socio-psychological interactions, resulting in the following five groups: dynamic staff, dynamic situational, static staff, static situational and socio-interactional (see Figure 3.1). This choice was mainly driven by the aim of providing non-HOF experts with a quick but well-defined and solid overview of the most critical HOF, forging a "HOF mindset" and allowing a more systemic approach when questioning and documenting variability in system performance. The staff-situational duality refers to the classical distinction in existing taxonomies between internal and external factors, with the latter describing situational characteristics, job and task characteristics or environmental circumstances, whereas the internal factors refer to individual characteristics (Kumamoto and Henley, 1965 – cited in Kyriakidis et al., 2018). The dynamic versus static duality, on the other hand, refers to whether or not the factors are strongly related to the precise moment of performance or the exact moment that the occurrence took place (Kyriakidis et al. 2015, 2018). The socio-interactional category, finally, covers the interactions between people while in a situation and certainly in reference to an organised context, with individuals and teams working and communicating towards the achievement of a common goal.

This new grouping was used as a reference structure to build a more pragmatic taxonomy of which each factor will be presented in detail further on. The taxonomy was first stabilised with the help of several series of works that describe the organisational and human factors as critical in socio-technical systems have been taken into account: e.g. the AcciMap introduced by Rasmussen (1980, 1997) and the HFACS introduced by Shappell & Wiegmann (2000). In a next step, the resulting list was cross checked with another recent but already well-established incident factors classification system for railways (Gibson et al. 2017). Furthermore, the list was verified against the work of Teperi et al. (2017). Based on an extensive review of existing human factor research, they developed an HF tool for the nuclear industry, based on their initial work for air traffic management. In relation to systemic analysis methods, the groups of possible causes for potential variability organised around technology-, human and organisation-based functions for FRAM (Hollnagel, 2012) and both the individual and organisational error taxonomies, proposed by Stringfellow (2010) to be used with STAMP, were taken into account. This system-oriented analysis was completed with a review of the archetypes of human and organisational processes in accidents that Kontogiannis (2012) developed, using systems dynamics. Finally, when developing the approach to use the SAFRAN method for safety culture (see also chapter 4), relevant elements were checked (e.g. Cooper 2000, 2016). This resulted in the identification of two not yet listed factors that could influence behaviour, namely "emotions" (Young et al., 2004) and "power issues" (Antonsen, 2009b).

An initial list of categories and factors was then available and within each of the five categories, with the input of non-HOF experts, the resulting list has been simplified and for each of the five categories of SPV, five factors have been chosen, resulting in a "5x5" structure easy to memorise and remind by investigation practitioners. All this finally results in the grouping of possible SPV to be used with the SAFRAN method as represented in the following Figure 3.1.

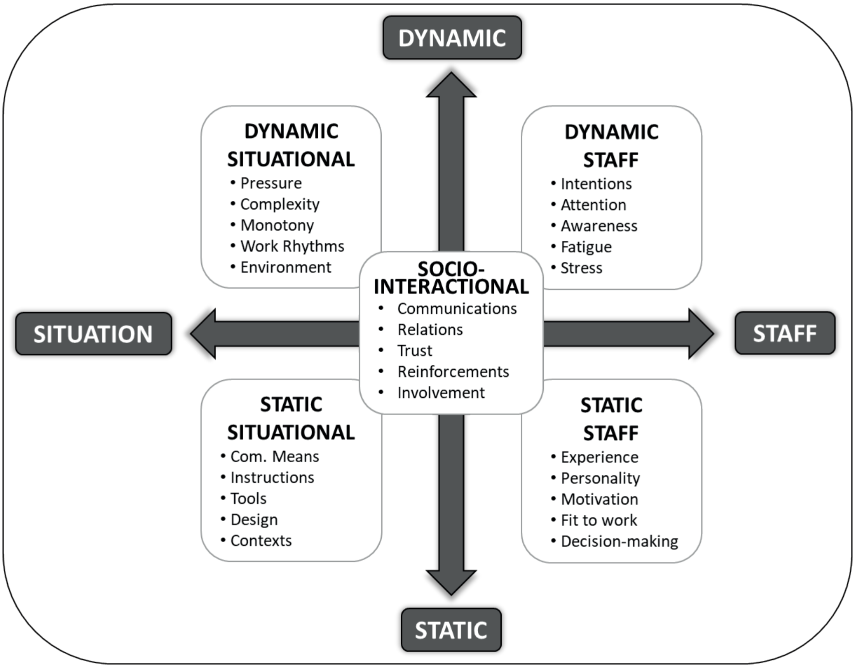


Figure 3.1: A pragmatic 5x5 taxonomy to support a HOF mindset

Although we refer to this set of factors as a taxonomy, its main objective is not to traditionally classify the causes of an event, but rather to help non-HOF experts seeing human performance as shaped by the constraints of the environment and to provide them with a structured overview of the HOF universe that needs to be explored when trying to understand the system performance. Furthermore, when using this universe of factors, possible interdependencies between factors cannot be excluded (Kyriakidis et al. 2018). Such interdependencies, which are at the heart of classical HOF definitions, are in fact handled by the iterative application of SAFRAN. As a consequence, the order of exploring the different factors is not important as such. However, according to our first audience, the investigators, it seemed more practical and logical to start with the dynamic factors, since they may require a more immediate attention, earlier in the investigation process, in order to stabilise the evidence. The following sections will describe the different identified factors in more detail.

3.2.3.1. Dynamic Staff Factors

With this first set of factors, that covers intentions, attention, awareness, fatigue and stress, we propose to explore whether there are any temporary characteristics of the individuals and teams who have influenced (or could influence – if the questioning is used in a proactive approach) the course of a situation.

It is crucial to understand the persons' **Intentions**, which in the situation (hic and nunc) motivated them to decide and act as they did, as well as the type of the produced variation. Questioning this factor should refer to three aspects: intention during the actions (e.g. what we wanted to do, to achieve, for what purpose, by avoiding what); reasoning in a situation (e.g. in function of what the person(s) had imagined the situation); and, the correct understanding of the type of variability (e.g. (in-) voluntary, type of error, type of violation).

Equally important is to identify all the external and/or personal elements that may have disturbed the **Attention** or concentration of the people concerned. This refers to at least two aspects. One is external and concerns the different concurrent tasks forcing the attentional capacity to be divided or switching, and therefore reduced. The other is internal and refers to the more personal aspects of concentration that can influence the choice of what to focus on at any given time.

Situational **Awareness** (SA) refers to three aspects that enable both the individual workers and teams to represent the situation and thus to base their decisions on. Self-awareness of previous decisions and actions and of the consequences already experienced. Awareness of the situation, of the related risks and how to understand them. Finally, a representation of the real situation based on the information perceived and captured. This factor should indicate what the concerned people have been able to pick up from the available information (1), their understanding of this information and how to process it (2), in order to achieve the desired outcome at the precise moment they had to (3).

The factor **Fatigue**, refers to sleep-related fatigue (in quality/quantity), which is a temporary condition that can lead to variability, for example due to missed information, inadequate analysis or failed action. This factor refers to the search for indicators of fatigue at the time of variability, during the performance itself, as well as in the days preceding it.

Stress, finally, is to be explored in a broad sense. It includes specific emotions as well as other psychosocial or situational factors. Nowadays, a very common reference situation for stress is when people (individuals, groups) feel there is an imbalance between what they are asked to do professionally and the resources they have to do it (time, instructions, competences, tools,...).

3.2.3.2. Dynamic Situational Factors

A second set of factors, covering pressure, complexity, monotony, work rhythms and environment, aims at exploring if there are any temporary or even fugacious characteristics of the situation that have influenced (or could influence – if the questioning is used in a proactive approach) the individuals and the teams.

The factor **Pressure** explores two aspects: the pressure generated by uncertainties, changes and the results to be achieved and the pressure linked to the time available to analyse, anticipate, coordinate, decide, act or react, check.

Complexity explores two aspects. On the one hand complexity, with the ambiguity of information, its timing, its interacting activities and actors, and their dynamic evolution. On the other hand, autonomy in making decisions, carrying out actions, recovering them, and the delays before their consequences.

Also the factor **Monotony** mainly relates to two aspects. There is the boredom of repetition of a situation (routine) and also the habit of acting or thinking in a particular way (more mechanical, more automatic). The challenge for people is to get out of the largely dominant normal work logic at the right time and to act differently then, in a way that is no longer necessarily well controlled. This may require taking into account elements that are necessarily rarer or even surprising, temporarily undetected.

The **Work-Rhythms** factor covers the hours or periods of time actually worked. This takes into account the distribution of physical and mental loads during these periods of work (quality of the work repartition within the time of work) as well as the sequence of the actual work periods, with beginning and end, the effective breaks, timing and quality of the work shifts, etc.

The factor **Environment**, finally, explores the variable characteristics of the workplace that can have an influence on the physical, mental and emotional state of the worker including cognitive and social activities in general. This factor relates to e.g. visibility, noise, vibrations, accessibility, working positions, static and dynamic loads, distances to be covered and weather conditions.

3.2.3.3. Static Staff Factors

With this third set of factors, that contain experience, personality, motivation fit-to-work and decision-making, we propose to explore if there are lasting characteristics, repetitive elements in the concerned individuals and teams that have influenced (or could influence – if the questioning is used in a proactive approach) the situation or other concerned people.

The factor **Experience** refers firstly the level of familiarity with the activities and secondly the individual experience and career path related to the activities and working circumstances (incl. the problematic situation encountered).

The factor **Personality** refers to the individual moral and psychological characteristics of the people concerned. These are fundamental attitudes that influence behaviour at work like self-confidence, confidence in others, openness to experience, conscientiousness, extraversion, agreeableness, emotional stability, etc.

The factor **Motivation** refers to the commitment and adherence of the people concerned to the company's objectives, its values and priorities, but also its organisation, its main rules, and the way it manages risks and major changes.

The factor **Fit-to-work** refers to a good match (sufficient is not always enough) between the people concerned and the requirements of the roles, activities and responsibilities. This includes all the competencies: knowledge, hard skills, soft skills (or non-technical skills, NTS), well-being at work, and health (incl. physical and moral states) as well as their level (which can vary in time), including the necessary periodic checks and monitoring of all these elements.

Decision-making, finally, refers to the capability to make decisions based on available information, their interpretation, the context, and who the decision-maker is in particular (e.g. creativity, ingenuity, ability to interpret situations, quality of memory processes, tendency to follow more or less the procedures, tendency to be of service for others, etc.).

3.2.3.4. Static Situational Factors

With this fourth set of factors, we propose to explore whether there are more lasting or repetitive characteristics of a situation that have influenced (or will influence - if the questioning is used in a proactive approach) the individuals or teams at work, or the context in which the activities take place. These static situational factors cover: communication-means, instructions, design, tools and context.

The factor **Communication-means** refers both to the communication standards and protocols as well as to the technical means and tools, and their influences on the individuals and teams concerned.

The factor **Instructions**, then explores the directives, regulations, rules, procedures, and instructions produced for the standardised performance of tasks. This includes not only their existence (or not) but also their quality (design, maintenance) to enable the work to be carried out properly while controlling the related risks.

The factor **Design** refers to the end-user based approach when defining the tasks (e.g. allocation, workload, autonomy and significance/meaning), the procedures and instructions, the levels of automation and all the human-machine interfaces and their cooperation from the simplest to the most complex.

With the factor **Tools**, we examine the planning, the availability, the good working order and maintenance, the suitability of the tools to be used for the planned tasks and actual activities in situ. This also includes the checking of the equipment and devices made available to the people concerned before and after the work is carried out.

The factor related to **Context**, finally takes into account the influences that the societal and institutional context may have on the people concerned and their work situations. This could be the influences of the regulation of the sector (national, EU), the economy, politics, the media, and societal events (sabotage, terrorism, social climate, security climate, health crisis...).

3.2.3.5. Socio-interactional Factors

With this fifth and final set of factors, that contains communications, relationships, trust, reinforcement and involvement, we propose to explore if the relationships between the people concerned and around them have influenced (or could influence – if the questioning is used in a proactive approach) the work situation or the people themselves in their reactions, attitudes, perceptions.

A first factor **Communications** examines the message and content of the communication, the way in which the interlocutors understand each other and coordinate (between workers within a team, between teams, with the line manager, between organisations, etc.).

The **Relationships** factor concerns the management of the plots of power inherent in any social relationship between people organised in small or larger groups, in particular with issues such as sharing resources, achieving objectives, the context of promotion or career management, the relationship to one's own leaders as well as with collaborators (if any), etc.

The factor **Trust** examines the level of (reciprocal) confidence with which the people concerned (individuals or groups) can rely on information, management, colleagues, technical means... to carry out their tasks and assume their responsibilities.

The factor **Reinforcement** refers to anything that stimulates (positively or negatively) professional practices, in particular concerning safety (directly or indirectly), whether with an individual or group effect.

The factor **Involvement**, finally, examines the consultation, participation and empowerment of individuals or groups through different kind of organisational opportunities for actions and decisions.

3.2.4. Applying SAFRAN on 55 railway derailments

To validate the above set of identified SPV, a selection of published accident investigation reports has been reviewed in a similar way as was presented for the Sandilands junction derailment above. In application of the Railway Safety Directive (2004), all European member states have established an independent accident investigating body (NIB) that analyses railway accidents and events with the sole objective of improving the European railway system. The final reports that result from these investigations were published in ERAIL, a database that was hosted by the European Union Agency for Railways (ERA). In this database, the highest number of investigated events represent derailments. At the moment of analysis, the most recent years with a high percentage of finalised reports were 2017 and 2018. From the 151 available final investigation reports for derailments that occurred in 2017 or 2018, 49 have been randomly selected for review. The review consisted in classifying the HOF elements that were identified in the report according to the above set of SPV. These classifications were in turn validated by two experts separately and any deviating result was discussed in order to come to an agreed classification. Furthermore, and to ensure that at least one report was taken into account from each NIB that investigated a derailment in the defined period, 6 additional investigation reports were analysed. As a result of this analysis, the following conclusions can be drawn.

18 of the overall 55 analysed reports identified variability in human performance close to the sequence of events as a direct cause (e.g. turning a switch under a train or over-speeding) or contributing factor (e.g. braking patterns, loading) to the derailment under investigation. Almost half of these investigation reports only provide a description

of the activities without any reflection that could explain why a certain activity or decision made sense for the involved operators. Often, these reports also state non-compliance with existing rules as the "main cause" for the accident. Only two of remaining reports show an in-depth analysis of the HOF factors and as a result identify both dynamic and static SPV that can explain the identified variability in human performance. The other investigation reports in this sub-group of 18 provide only a limited investigation of human performance, almost always resulting in findings on static SPV, related to poor quality of work instructions, operator (in-) experience or bad weather conditions influencing performance. The remaining 37 derailments were caused by technical failures on the side of the infrastructure, the involved rolling stock or a combination of these. In all cases these technical failures were linked with activities of human performance that involve the control of the status of these technical sub-systems, like pre-departure checks and maintenance activities. With few exceptions, the investigation of the human performance for these activities is limited to findings, without in-depth analysis, and resulting in the identification of no or only static SPV, like again the quality of work instructions, the identification of roles and responsibilities and the availability of adequate resources. Finally, in none of the analysed reports an organisational analysis could be found that goes beyond what would represent a first or second iteration when applying the SAFRAN method. Table 3.2 provides an overview of these findings.

151 derailments for 2017-2018 in ERAIL	55 analysed (covering all EU member states)	18 Human performance	2 systemic analysis of HOF factors (dynamic + static)	
			8 limited investigation of HOF (mainly static: work-instructions + operator experience)	
			8 « non-compliance »	
		37 Technical failure	37 Human performance (maintenance + pre-departure checks)	37 no systemic analysis of context or organisation, no or only static factors identified

Table 3.2 overview of HOF in derailment investigation reports

Based on the above findings, we can only conclude that in general the actual practice of railway accident investigation lacks proper HOF knowledge, which confirms the findings of Dul et al. (2012) that, despite decades of history, HOF knowledge has not yet found wide-spread recognition nor implementation and the potential of HOF remains under-exploited. The few exceptions that do attest to a thorough analysis of HOF elements show however the potential of a more structured approach. Although through the above and a similar number of less structured tests, we were capable of classifying all identified

HOF elements with the proposed taxonomy, this review clearly makes a case to invest in further support for accident investigators, helping them to identify HOF elements at both the operational as well as the wider organisational levels.

3.2.5. Further steps

In general, when it comes to understanding a work situation, i.e. identifying the SPV, two distinct approaches are recognised. The "thick descriptions" approach (Geertz, 1973; Dechy et al., 2012; EUROCONTROL, 2014) integrates the organisational circumstances in which decisions and actions were taken by the individuals and teams involved. These decisions and actions are seen as behaviours that, in order to be made intelligible, require an understanding of the organisational and cultural context. To reach this, it is necessary to collect not only the facts and evidence but also the comments and interpretations of the individuals and teams concerned. Next to that, ergonomic or psychological analysis of work situations recommends a systemic and multi-stage approach, effectively taking into account workers' perceptions; in particular, through observation, questioning, substitution, etc. and focusing on the study of the real activities (Leplat, 1997; Singleton, 1978; Faverge et al., 1958). This reflects the foundations of Ergonomics that are end-user-centred. One of its recent developments can be shown in the "You are not the user": a mission statement of user experience for designers (Daumal, 2018).

In the context of an accident investigation, next to analysing the recordings of performance parameters, Dekker (2006) recommends the debriefing of participants as a good source to gather HOF data of an event under investigation. This should help to reconstruct the situation that surrounded people at the time and to get their point of view on the situation. To guide investigators to structure such debriefings or interviews, a set of supporting questions has been developed for each of the twenty-five factors in the proposed taxonomy, that can help to identify whether they have (the potential to) generate(d) some variability in a specific function under analysis. An example of this questioning, for the SPV "Pressure", is proposed in the Table 3.3, but it goes without saying that these standard questions need to be adapted by the interviewer case by case. As an additional support of the SAFRAN logic, and for each of the 5x5 SPV factors, the best-known processes (to explore in a further iteration) that could manage the SPV, can be identified. This should contribute to better mitigating the critical variability of the function and achieving sustainable management of the overall system performance.

SPV factor	Exploring question	Process to explore further[1]
Pressure	● At the moment you decided to act as you did, what were your uncertainties, your doubts? It could be about the information you received, the procedure to apply, some resources unavailable, the priorities, the risks involved or some recent changes? ● In your opinion, were there any conflicting, opposing objectives? How would you describe them? How did you know what to favour? Were these priorities clear to you? And did you agree with these priorities? Did you see clearly how to achieve them? Did you see any obstacles or difficulties in getting there? Could you talk about them and did you want to? ● Was there any pressure on the results to be achieved? (If yes) How would you describe this pressure? Would you say that you were under time pressure to decide, to act; and more generally to analyse, anticipate, coordinate, or react? How did this pressure manifest itself (via other agents or managers, service requests, site requirements, equipment constraints, management of certain risks, a question of punctuality or other)? ● What effect(s) do you think this pressure may have had on you at that time, when you think back now? Would you have found it useful to be able to "stop", or to ask another colleague or manager? Do you think it is it possible in your work environment?	Implement > Train > personnel performing the defined process are competent on the basis of appropriate education, training, and experience > Equip > resources > Organise > process purpose / output > process performance objectives > process performance planning Specify > responsibilities / authorities > for performing the process

Table 3.3: An example of the SPV questions to nurture the processes analysis

Even though a structured set of questions can support investigators in the debriefing of participants in an accident or occurrence, it is obvious that other skills are further needed to professionalise the interview (e.g. practicing rewording, silences and non-critical behaviour, dealing with the retrospective bias risks), and to build the necessary trust and respect with the interviewee(s). Such methods of questioning HOF factors already exist and can be learned during appropriate training courses (e.g. RSSB, 2019; Carpinelli et al, 2021).

Furthermore, the debriefing of participants should always be done with caution as it would be an illusion to think that an exact and reliable reconstruction of a past event is possible based on the memory of persons involved in the event – if even possible at all. As explained by Shaw (2016), our memory of an event is built on how we perceive the world with all our senses as well as on past experience in a similar situation. Since all our senses have limitations and no two situations can ever be exactly the same, our memory will be flawed already from the start. Furthermore, our memory in not stable when time passes. Every time someone tries to remember an event from his or her memory, this memory will be vulnerable for transformation or loss. Possible sources of contamination that will have to be taken into account when debriefing participants is the use of guiding questions or pictures, the sharing of information with others and the phenomenon of "verbal overshadowing" where the verbalising of previously seen visual stimuli may impair subsequent recognition. Namely for some of the more dynamic SPV, where the memory of participants may be the sole source for collecting relevant HOF-data, this could be an indication that a debriefing should be organised as soon as possible after the event. Unfortunately, a similar approach is not possible for many of the often not-explicitly documented decisions that are taken within an organisation and that, with hindsight, may appear to have contributed in creating the context that lead to an event. But even here, interviewing the concerned actors can still lead to the identification of relevant HOF elements.

The proposed, structured approach of combining both individual (i.e. the SPV) and system analysis can be used also in other settings than accident investigation as a practical instrument to enable non-HOF-experts to recognise the different HOF elements that introduce (critical) variability in operational performance and decision-taking. In this context, the initial feedback on using the structured questioning from two operational services within a European infrastructure manager, in charge of coordinating field activities with safety as a top priority, is promising: the list of questions was well received, understood, and perceived usable for exploring the interactions between HOF and other parts of the railway system. Furthermore, more recently, pilot sessions of a training module that is developed to introduce the proposed approach, indicate that the 5x5 logic of structuring the HOF elements, with the dynamic-versus-static and the staff-versus-situation dualities, is easily captured and remembered.

Testing the identification of HOF elements on pictures and in a railway incident case before and after the introduction of the taxonomy, during the same training sessions, further indicates that the scope of identified HOF elements that might require further investigation increased significantly. Once these sources of variability have been identified, it becomes more logic for participants to ask how the SMS manages or is expected to manage them. This is where the SAFRAN logic, when strictly followed in its SMS-oriented questioning, demonstrates its value: participants say they feel better guided in the systemic and systematic questioning of the HOF elements that can explain the decisions and actions of the safety management functions involved, even if sometimes quite distant from the sequence of events. As the case study has shown, this is a depth of analysis that is most often lacking in the current railway accident investigation practice. Further efforts to train and disseminate this approach, with the aim of testing and improving it where necessary, will be continued. In addition, the taxonomy is proposed to be integrated in European legislation on occurrence reporting in the railway sector.

3.3. CONCLUSIONS

As pointed out by Dekker et al. (2011), the very act of separating important or contributing events and decision from unimportant ones is an act of construction, strongly influenced by the analyst's background, preferences, experiences, biases, beliefs and purposes. Rather than following a chain of causal reasoning or trying to reconstruct conditions that may no longer exist, the effort put in the organisational accident investigation should therefore focus on assessing the capability of organisations to manage (critical) variability and thus the actual daily functioning of the socio-technical system.

The SAFRAN method is developed with exactly this objective in mind: starting from findings close to the event, and in particular the related HOF-elements, an investigator will be guided in identifying the relevant implementing and control processes; an investigation logic that can then be repeated for all relevant processes throughout the entire socio-technical system.

This chapter has presented the SAFRAN method with its related HOF taxonomy and supporting questions as a vehicle to enable non-experts in human and organisational factors to identify the different elements that introduce variability in all relevant processes. It has been shown that the SAFRAN method nurtures and structures the repetition of classical "why's" questions, guiding investigators both through the socio-technical system processes and through the potential influences of/on HOF. In other words, it offers the combination of both human and system analysis.

Performing this type of analysis, that covers several dimensions of an entire system, requires however knowledge from different disciplines to interpret data at several strata of complex socio-technical systems (Le Coze, 2013). Like Le Coze, we believe that this requirement is more likely to be met when several specialist or experts interact on the same accident analysis (if needed including HOF experts).

By explicitly and repetitively linking performance variability of one process with the analyses of underlying management processes, the SAFRAN method creates an analytical trace, offering the same advantages that are characteristic for ATSB's link-to-link approach (ATSB, 2008): 1) more safety issues being identified and communicated, particularly those more remote from the occurrence, 2) a richer description of the factors involved in the development of an occurrence and thus better learning opportunities, 3) less potential for determining blame or liability and thus less potential for the existence of barriers to learning. A similar, structured use of the proposed approach is possible in the context of audits or other techniques for organisational diagnosis and could help to overcome the obstacle that possible signals of danger are only visible to an analyst with hindsight, after an event. As argued by Dechy et al. (2012), the generic issues of organising work and managing safety are similar, whether analysed before or after an event, and these similarities are the key points that could guide data collection, analysis and interpretation with adequate HOF skills.

This proposed approach is fully in line with the main strategy direction Dul et al. (2012) have put forward towards the world-wide application of HOF excellence, namely, to strengthen the demand and application of high-quality HOF by building partnerships with main stakeholders. Within this context, the SAFRAN method is a practical tool that can be used in different settings, for better integrating HOF knowledge in railways and other high-risk domains. With the aim of not only optimising human performance and well-being but optimising performance of the socio-technical system overall.

4

Using the SAfety FRactal ANalysis method to investigate human and organisational factor beyond the sharp end. A critical socio-technical analysis of the Santiago de Compostela train crash investigation

INTRODUCTION TO CHAPTER 4

When applying the iterative characteristic that is inherent to the SAFRAN method, this approach should in principle be applicable at all levels of a socio-technical system. How this corresponds with the results of an actual accident investigation was tested for this chapter on the most high-profile railway accident of the last decades in Europe. The result of this analysis and the analysis on a larger set of derailments, presented in the previous chapters, showed me for the first time in a concrete and structured way that the analysis of HOF in general weakens (or is simply more difficult?) the more distance there is from the direct operational actions and decisions. In building the appropriate HOF taxonomy, we also stumbled upon pre-existing lists that mention safety culture as a cause of accidents. Because stopping an investigation with such a finding can impossibility lead to concrete improvement actions, this chapter is also used to propose an alternative way of integrating safety culture in accident investigations.

ABSTRACT

Starting from the findings close to operations that explain the occurrence – the elements accident investigators are first confronted with – the SAfety FRactal ANalysis (SAFRAN) method can guide investigators in an intuitive and logical way, to ask questions that help to gain a deeper understanding of the capability of organisations to monitor and manage safety critical variability. The essence of using the SAFRAN method for evaluating the performance of the different processes in a socio-technical system, is to approach them in a similar way. This is done by building on the generic elements that compose a SMS and systematically looking at the human and organisational factors that influenced actions and decision making, regardless of the hierarchical level at which they are situated. This chapter details how this innovative accident analysis method can be employed to find the right balance for investigating human and organisational factors, while systematically creating the necessary analytical trace. Ultimately, this will help to identify possible areas for improvement and safety learning from the sharp end to the Board room, and beyond. Against this theoretical framework, the official accident investigation report on the 2013 catastrophic train derailment in Santiago de Compostela (RAIC, 2014) is critically analysed.

4.1. INTRODUCTION

The initial idea behind the development of the SAFRAN method was to provide accident investigators with a more straightforward tool to investigate SMS and wider organisational factors. Young et al. (2004) warn however that a balance must be struck between investigating the organisational contribution to accidents and accounting for the role of active errors. The aim (and the challenge) of investigating human performance, is to find out how peoples' assessments and actions made sense at the time, given the circumstances that surrounded them (Dekker, 2006). The data that needs to be gathered therefore should cover all possible features of the system and situation that surrounded people at the time and with which they interacted (ICSI, 2013). Moreover, following the International Society of Air Safety Investigators (ISASI), this is not only valid for decisions and actions of operational personnel. The analysis should encompass all of the people concerned with the occurrence and/or performance under investigation, which in a SAFRAN analysis could easily lead to activities and decisions away from the occurrence in space and time within a few iterations.

Considering the substantial role humans play at all levels in the systems, this 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). Through this analysis, accident investigations may also provide an opportunity to discover shared and systematic patterns underlying decisions and/or behaviours in organisations (Nævestad et al., 2019) or wider industries. However, this must be done with caution: the behaviour of a single person does not necessarily indicate a cultural trait. Moreover, in the context of accident or incident investigation, the concept of safety culture is often used as an underlying cause to explain a range of individual or organisational, and sometimes political conditions that created the accident. This risks to reduce all aspects of safety management to matters of culture, thereby distracting attention from manifest organisational and management problems (Grote, 2012). The finding that a pattern of (unsafe) acting or thinking is shared by a group of people however, should not be the end point of an investigation.

4.2. INVESTIGATING SAFETY CULTURE

An alternative approach starts from the idea that "cultures emerge where people interact and have to accomplish something together" (Antonsen, 2009a; Guldenmund, 2015). Safety culture here refers to that part of an organisation's culture (i.e. a combined way of acting and thinking that is largely in common to a group of actors in the organisation), which can impact the management of major risks related to its activities. It has been progressively constructed through interactions and communication between the concerned actors and continues to evolve, encouraged or discouraged by people or systems over time. Linking an observation (e.g. an operator ignoring a rule) with possible attributes of safety culture must not be considered as an end but as a starting point for further questioning (Bernard, 2014). In that context, Strauch (2015) argues in favour of examining company actions and decisions related to an accident, in order to provide insights, albeit indirectly, into a company's safety culture, rather than attempting to assess safety culture directly. The investigation should go further, in capturing those elements that influence(d) safety-related actions and decisions and look for the organisational factors that are identifiable and assessable as indications of what are otherwise subjective issues (Grote, 2012). Similarly, Czech et al. (2014) argue for a thorough examination of an organisation's performance on measurable safety management functions, in order to avoiding the difficulties of defining or measuring safety culture. The same difficulties surrounding defining and measuring safety culture bring French and Steel (2017, 2018) to conclude that a good starting place for investigating the safety culture of an organisation is to examine and explore in depth any organisational factors relating to the accident.

A possible solution to approach this in a structured way, is offered through the 'growing conditions' of culture (Antonsen, 2009a). Guldenmund (2015) identified these conditions as the different stages in a model of development of culture that help an individual, as part of a group, to make sense of a situation and to understand and cope with reality. In chapter 1, this basic understanding of safety culture was used this to develop the Extended Safety Fractal (Figure 1.3), that provides a framework for explaining the interactions between elements like SMS and SMS maturity, safety vision/strategy, safety culture and safety leadership, which all have been identified in literature as essential to organise sustainable and safe performance.

When applying this model, a practical first step for introducing safety culture in the context of an accident investigation would then be to identify whether a specific, critical behaviour that is identified during the investigation of an event, is part of a wider shared way of acting and thinking. This could become apparent when identifying the underlying factors during the investigation, as we will see in the following case study. In other events, like e.g. the investigations into the derailment of a passenger train on Fukuchiyama Line (JAP) in 2005 (ARAIC, 2007) and the overturning of a tram at Sandilands Junction (UK) in 2016 (RAIB, 2017), a questionnaire has been used to gather information on normal and shared behaviour of operators. In a second step, the investigation will have to understand the safety strategy that is used by the organisation(s) under analysis and define whether this could lead to sustainable and safe performance. Several authors (e.g. Denyer, 2017; Pariès et al. 2019) have highlighted the importance of a clear safety strategy. Also Grant et al. (2018) have identified an interesting set of essential characteristics related to system performance, which may provide a suitable approach for predicting system states and can help in assessing safety strategies. As a third step, if a clear strategy appears to be available, the investigation can analyse whether this strategy is systematically implemented and supported in both formal and informal elements of safety management (i.e. the cultural enablers). This investigation logic is based on the Extended Safety Fractal that was developed in chapter 1.

The next sections, by analysing the published investigation report on the catastrophic derailment of a passenger train in Spain in July 2013 (RAIC, 2014), will illustrate with a practical application how the SAFRAN method can help investigators in identifying the HOF elements, and eventually the underlying safety culture, that influenced decision taking at different hierarchical and organisational levels.

4.3. CASE STUDY

In the evening of July 24, 2013, a long-distance train 150/151 from Renfe Operadore, derailed in a sharp bend, approaching the station of Santiago de Compostela. The train crashed against a concrete wall. When entering the curve, allowing for a maximum speed of 80 km/h, the train was driving at a speed of 179 km/h. At least 80 passengers were killed and 73 are seriously injured. The official investigation report into this accident (RAIC, 2014) identified excessive speed of the train due to a breach of the speed requirements by the driver as the direct cause of the accident. Reduced attention of the driver when answering a service telephone call is mentioned as a contributory cause.

The Railway Accidents Investigation Commission (RAIC) has been established in Spain as the official National Investigating Body, herewith being the sole authority under the Railway Safety Directive (EU, 2004) to independently investigate serious railway accidents. Its role is to investigate with the objective to improve, where possible, railway safety and the prevention of accidents, without apportioning blame or liability. As such, RAIC investigation reports form the official basis for learning from accidents in the Spanish and wider European railway sector. The investigation of this accident, with critical variability in human performance when maintaining the appropriate speed of a passenger train, was used as input to test the potential of the SAFRAN method.

4.3.1. Timeline of events

In order to understand this accident, which was one of the deadliest train crashes in the history of European railways, and the context in which it occurred, the following description of events is adapted from the RAIC investigation report (RAIC, 2014).

Long-distance passenger train 150/151, run by the incumbent Spanish railway undertaking Renfe Operadora, consisted of 13 vehicles. It was coming from Madrid-Chamartín and bound for Ferrol (A Coruña). After making a scheduled stop at Ourense station with changeover of driver, it continued on its route via the Ourense – Santiago line. It departed from Ourense with a four-minute delay.

The train covered the first 78 km of the line at an approximate speed of 200 km/h, with all signals on its path indicating 'track clear'. About 6 km before the start of the curve leading to the A Grandeira branch, that brings lines 082 and 822 towards the Santiago station, the driver answered a service call from the train manager (guard) on his corporate mobile telephone.

Knowing that the driver was aware of this information, the train manager called the driver to ask whether the train would fit on track 2 at the Puentedeume station, close towards the end of the service. An initiative the train manager had taken to facilitate the alighting of a family getting off at Puentedeume, in order to improve the service and convenience for the passengers. He always made calls of this type in similar situations. Having received the information, the train manager, would call the traffic management centre to ask them to switch to one track or another.

During the call, the train continued along track 1 of line 082, where a long straight line of 4.377 m suddenly changes into a sharp curve with a radius of 402 m and a total length of 666 m, also called the Angrois bend. Access to the A Grandeira branch in the direction from Ourense to Santiago is protected by entry signal E7 which, in turn, is announced by caution signal E´7. E7 is a tall signal with three lights (green, yellow and red), positioned at the exit from the 641 meter long Santiago tunnel. E´7 is also a tall signal with three lights (of which only two are operative: green and yellow) and is located some 3,5 km before E7 and a little before the entrance to the 1.285 m long Marrozos tunnel. Associated with this signal E´7, three proximity boards have been set up nearby, with an intermediate distance of about 200 meters, to warn for the upcoming signals. The path set for train 150/151 was, at all times, up to signal E8 at the entry to the Santiago station on track 1. Therefore the caution signal and the entry signal (E´7 and E7 respectively) for the A Grandeira branch were showing 'track clear' (green). The next signal E'8, a caution signal for entry to Santiago de Compostela was announcing an upcoming 'stop' (yellow); while entry signal E8 at Santiago was showing 'stop' (red).

43 seconds into the telephone call, the driver passed signal E'7, which is normally his reference point to start braking and reduce the speed from 200 km/h to 80 km/h. In this case he did not start braking in time to adjust to the prescribed speed for the upcoming Angrois bend; according to his statements afterwards because he never saw the proximity

boards (without knowing why) and had therefore missed the location of the caution signal E´7. The last sound of the telephone conversation was recorded very close to signal E7, at the start of the branch. This was 100 seconds after the start of the call, during which 5.540 metres were travelled. Directly afterwards, while travelling through the Santiago tunnel, an acoustic signal is heard in the locomotive, when a balise prior to signal E7 is passed indicating 'track clear.' Seconds later, the driver applies the emergency brake. At that moment, train 150/151 was already very near the start of the curve. It derailed on the curve, 185 metres from the start of it and 7 seconds after applying the emergency brake, still travelling at 179 km/h. The following table summarises the main events in this timeline.

15:00	19:55		20:39:06		20:39:58	20:40:55	20:41:02	20:41:03	20:41:06
train 150/151 departs from station of origin, Madrid-Chamartín	train 150/151 makes scheduled halt at Ourense station, with changeover of driver	train passes first 78 km at app. 200 km/h, with all signals at "track clear"	driver receives call on the corporate mobile telephone, train drives at 199 km/h	train passes the first two proximity signs for caution signal E´7 and maintains speed	train passes caution signal E´7 for A Grandeira branch and maintans speed (199 km/h)	the last sound of the voice of the driver can be heard in the telephone call, 100 seconds after the start of the call, during which 5 540 metres were travelled	train passes the balise at the foot of signal E7, showing *track clear* (with acoustic signal from the system) at 195 km/h	the transition to the Angrois bend begins - this is the start of the 80 km/h speed limit, the train slows to around 191 km/h	the derailment begins, near the end of the initial transition stretch of the Angrois bend

Table 4.1: Summary of the main events in the timeline

The train was equipped with a cab-signalling system that incorporates automatic train protection with continuous speed control (ERTMS/ETCS)., Due to problems of reliability and availability with the ERTMS configuration between the rolling stock and the infrastructure, however, the operator received authorisation from the infrastructure manager to operate on line 082 under protection of a system with only punctual speed control (ASFA Digital), shortly after commencement of commercial operation on the Ourense-Santiago line. With this system, emergency braking occurs when a train passes a signal at danger (i.e. showing a 'stop' aspect) or if a previous balise indicates a stop at the next signal and the speed at which the train is travelling is more than that required to stop the train. While it is possible that the train involved in the accident might have travelled with ERTMS, this system would not have completly limited the speed of entry to the

Angrois bend. The reason for this is that the point of the derailment, at the A Grandeira branch, is already beyond the stretch fitted with ERTMS. It that context, it would still have been up to the driver to reduce speed.

4.3.2. Methodology

To perform this analysis, the information contained in the RAIC report (2014) was analysed in detail to identify the different functions throughout the railway socio-technical system that showed critical variability in relation to the accident as well as the SPV that could explain this. This safety information was then structured according to the SAFRAN logic. Firstly, in section 4.3.3.1, the different functions within the socio-technical system that can be found in the investigation report, whether purely operational or rather safety management oriented, have been identified and ordered. This allows to check whether the information contained in the investigation report covers the entire railway socio-technical system and is therefore a good basis for testing if the SAFRAN method applies system thinking. As a next step, in section 4.3.3.2, the SAFRAN logic has been used to establish a link-to-link relationship between these functions, starting from the critical variability close to the event, which is the driver's performance. Providing this possibility to examine all components of a system (i.e. human and technical), as well as the relationship between them, is considered by Underwood (2013) as an essential characteristic of systemic analysis methods and provides for the analytical trace that fosters the potential for better learning (ATSB, 2008).

This approach to link the different functions, which is an essential element of the SAFRAN method, is graphically depicted in Figures 4.1 and 4.2, where each triangle represents a separate function or process. The sides of a triangle respectively represent the elements of *process performance* (left side), *process implementation* (bottom) and *process control* (right side), as also presented previously in this thesis. The different steps of one SAFRAN iteration are then represented by the numbered buttons that are depicted with each triangle. The arrows, starting from these numbered buttons, on the other hand, represent the links that can be drawn between the different processes. In application of the SAFRAN analysis logic, such a link then either represents the management of the identified source(s) of performance variability or the delivery of monitoring and/or learning capability for the variability in a function analysed in a previous iteration. In the former case, the arrow will start from a button with number "3", in the latter case, the arrow will start from a button with number "4". To help the reader of this paper in easily detecting this difference, the arrows are also colour-coded in the following way: when showing how the identification of an SPV that caused critical variability for one process leads to the investigation of a process that should manage this SPV, the arrow is coloured light blue; when, on the other hand, the next process to be analysed is defined by the wish to investigate the capability of an organisation to monitor the identified critical variability, the arrow is coloured purple. The example for one such iteration is depicted in Figure 4.1.

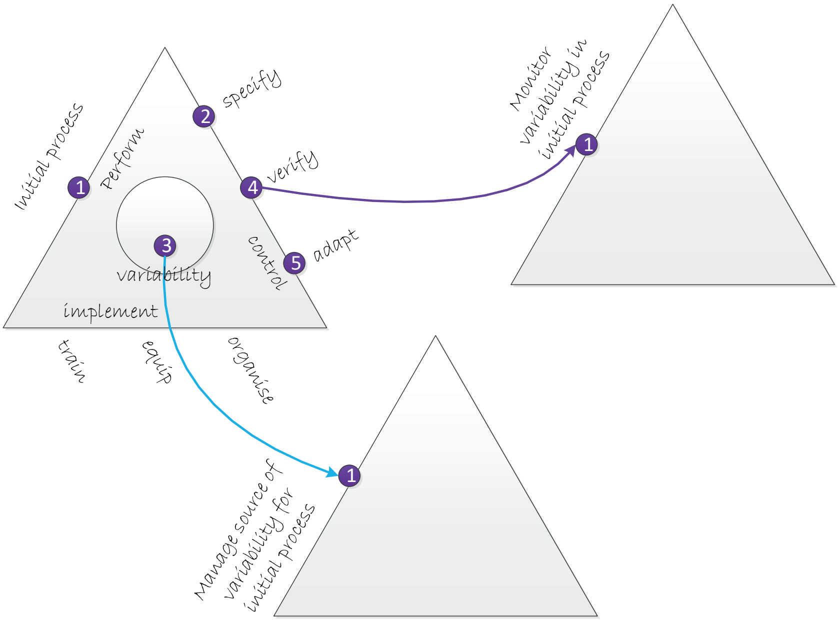


Figure 4.1: Graphic representation of the methodology for structuring the information: the variability in one process leads to the identification further management processes to investigate

For each of the identified management processes, a new SAFRAN iteration can be started by analysing the performance of the newly identified processes, leading to again a next set of processes that can be further analysed. Within few iterations, this will lead to the identification of all processes in the socio-technical system that are relevant for the investigation. This logic is depicted in Figure 4.2, with the dotted arrows characterising the idea that this analysis logic can be continued as long as relevant processes are identified and information on the different dimensions of their functioning is available. The red dotted arrows, finally, represent the possibility to investigate the capability of an organisation to adapt. This should follow whenever the analysis of a monitoring process shows adequate performance that is not followed up with concrete measure to change a situation that could lead to critical variability.

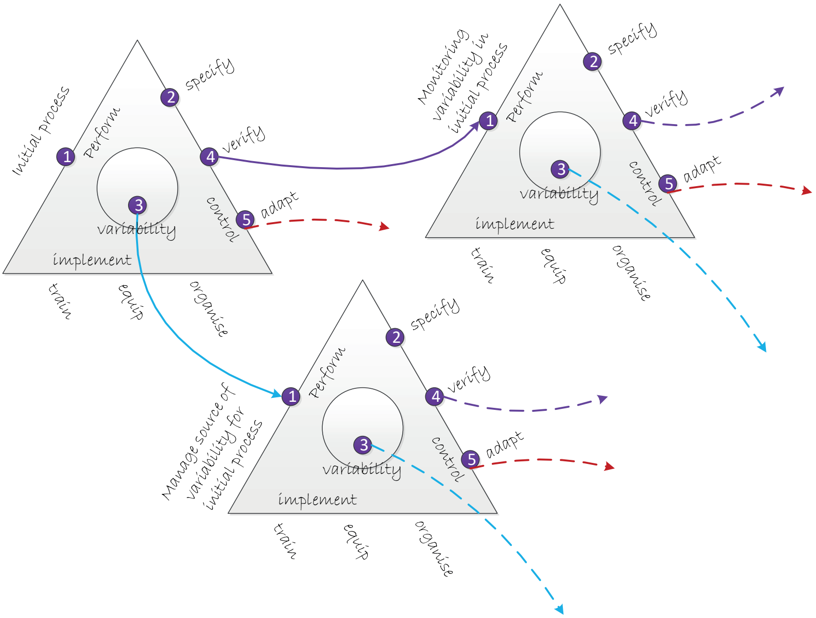


Figure 4.2: Graphic representation of the methodology for structuring the information: with each next process that is analysed, the same logic for identifying next processes can be applied

In order to understand how an action or decision that was (under)taken made sense at the time, at least information to cover the first three steps of the SAFRAN method should be available. In particular the critical variability in performance (step (1)) and its sources, i.e. the human and organisational factors that influenced the behaviour (step (3)), are relevant for this. In section 4.3.3.3, this is used as a reference to evaluate the completeness of available information in the RAIC investigation report to allow the understanding of decision making that was underlying to the accident. In combination with the established link between the different functions, this approach offers the combination of both human and system analysis, herewith overcoming the downfall of losing fine-grained analysis of the human aspect that according to Salmon et al. (2013) characterises the already existing systemic analysis methods. Furthermore, by doing so, the SAFRAN method offers the potential of analysing the co-ordination of decision making at all levels of the system.

In addition, the information in the RAIC report (2014) is evaluated on its potential for further and in-depth analysis of the event (see section 4.3.3.4) that could lead towards sustainable change. In application of the SAFRAN logic, this correspsonds to analysing the potential an organisation (or in a wider context, the entire socio-technical system) has to monitor and control critical variability. This can be done by going through the previously identified and linked functions and checking whether iterations can be identified that build on steps (3), (4) and (5) of a previous iteration, as explained above. Finally, building on the approach that is presented in section 2.3, the potential of this case to further explore the growing conditions for a positive safety culture are discussed in section 4.3.3.5.

4.3.3. Results

The following sections present the results of applying the SAFRAN method on the information available in RAIC's investigation report of the Santiago de Compostela train crash. It not only allows to structure the information but also gives an indication of elements that can provide additional direction for further investigation when applying the SAFRAN method.

4.3.3.1. Coverage of the socio-technical system

From the above timeline of events, it is clear that the RAIC report (2014) focuses mainly on two operational functions: *(a)* the *maintenance of appropriate speed* by the train driver and the telephone conversation to *exchange information between the train manager and the driver (b)*. But also other functions, which describe activities related to safety management, have been reported upon in the investigation report. Both the operator and the infrastructure manager appear to have a function in place to *(c) monitor variability in driver performance* and so also to check the respect of speed limits, either through the analysis of recorded train data or by accompanying operating trains. According to the documentation analysed by RAIC (2014) however, none of these identified any critical variability. The capability to the risk of over-speeding in the Angrois bend was nevertheless identified by a leader driver, and reported internally. This information never reached the infrastructure manager and the operator reacted by intensifying the *training of* its *drivers (d)*, herewith showing only limited capability to *adapt the management of speed (e)* for this critical configuration. Further safety management functions that are reported upon (RAIC, 2014) deal with the *setting up of lineside signs (f)* to inform on abrupt changes of maximum speed, the *equipping of infrastructure with an automatic train protection system (g)* and how this is *authorised (h)* as well as the *equipping of rolling stock with an automatic train protection system (i)* and its *authorisation (j)*. Except for the highest level, which is Government, this list of identified functions covers all hierarchical levels of risk management in a socio-technical system (i.e. Work, Staff, Management, Company and Regulators) as identified by Rasmussen (1997). Therefore, the report is considered to offer a sufficient basis for a thorough analysis of all critical variabilities throughout the socio-technical system that ultimately led to the known fatal outcome.

4.3.3.2. The analytical trace: understanding the link between the reported functions

Establishing a clear link between the occurrence and the proposed changes will help to convince decision makers to take action. The SAFRAN method provides a structure way to identify these links, avoiding the trap of judging causation/contribution based on a relationship to the investigated occurrence, by focusing for each function or process on the capability of an organisation to monitor critical variability and to manage the potential sources of this variability. Addressing this capability of an organisation to manage critical variability is what is needed to establish sustainable and safe performance. When applying this SAFRAN analysis logic, it is possible to establish a logic link-to-link relationship between all identified functions in the investigation report, as drawn in Figure 4.3, below.

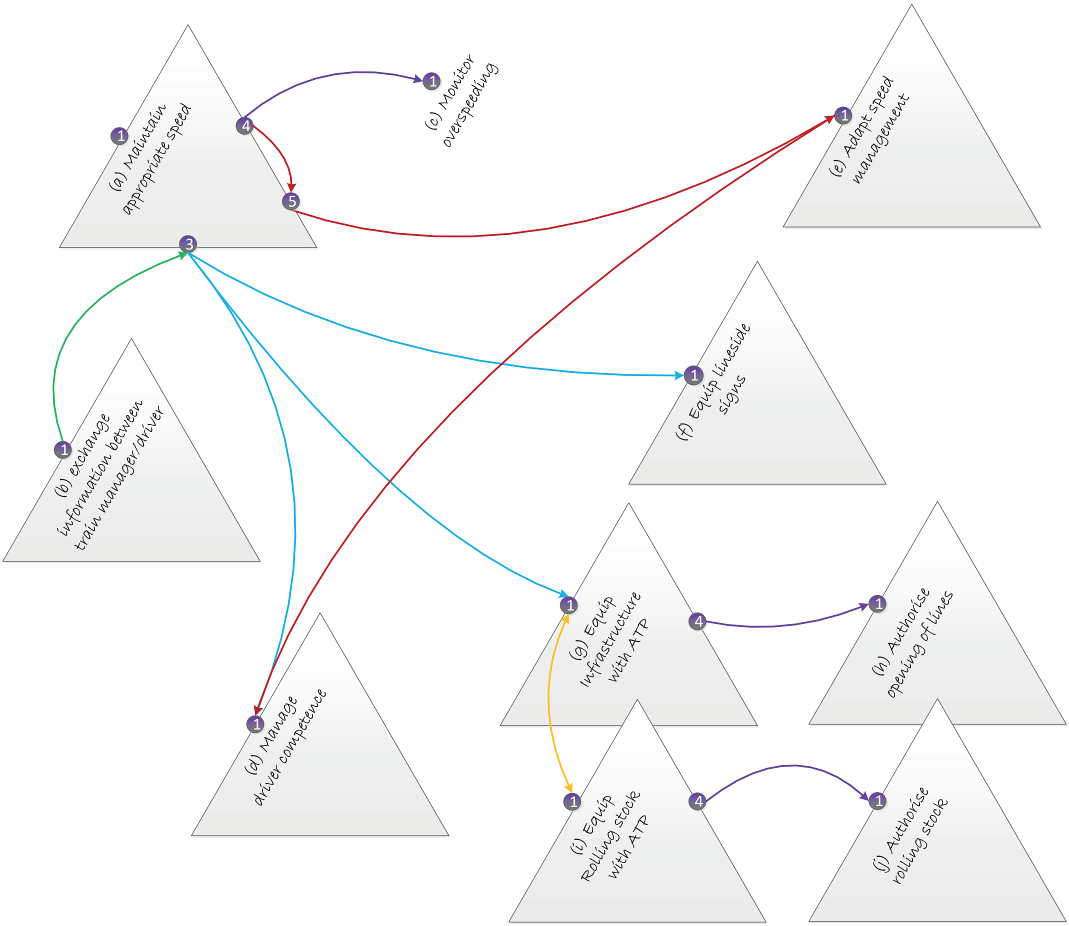

(a) Maintain appropriate speed
1
4
5
3
(c) Monitor overspeeding
1
(e) Adapt speed management
1
(b) exchange information between train manager/driver
1
(f) Equip lineside signs
1
(g) Equip infrastructure with ATP
1
4
(h) Authorise opening of lines
1
(d) Manage driver competence
1
(i) Equip Rolling stock with ATP
1
4
(j) Authorise rolling stock
1

Figure 4.3: Graphic representation of the link between the identified functions

Following the colour-code that was introduced in Figures 4.1 and 4.2, and starting from one of the two operational functions, namely the task for the train driver to maintain appropriate speed, the light blue arrows lead to the processes that should manage the different identified source(s) of performance variability. For none of the other functions, the possibility that is proposed by the SAFRAN method to further investigate from this angle has been exploited in the investigation report. This result in blue arrows only starting from the triangle that is representing the function (a) – Maintain appropriate speed – in Figure 4.3. The purple arrows represent the link between the delivery of monitoring and/or learning capability for a function analysed in a previous iteration. This potential, to deepen the investigation when applying the SAFRAN method, has been used for only three out of the ten identified functions. Therefore, in Figure 4.3, only three triangles have a purple arrow connecting it with a next triangle. The yellow arrows in turn, are used to highlight the required compatibility between on track and on board train protection systems, while the red arrows depict how the operator reacted to the identified risk of over-speeding in the Angrois bend. The details of this will be further explained in the following sections.

4.3.3.3. Understanding the rationale behind actions and decisions

As a next step, the RAIC investigation report (2014) has been further searched to find information that could cover the different elements of a basic Safety Fractal, applied to each of these functions. As argued before, at least information to cover the first three steps of the SAFRAN method should be available to understand the performance variability of a certain function. It can be noted that the RAIC report (2014) identifies for all the above functions the expected performance as prescribed in procedures and or regulation, which corresponds to the second step in the SAFRAN investigation logic. Only for defining what type of fixed signs must be set up to warn for the extreme change of maximum speed (i.e. function (f)) no regulation was found.

The further analysis therefore focuses on elements in the investigation report that could provide an indication on possible SPV that can help to understand how the actions and decisions that are (under)taken, made sense at the time. The result of this analysis for all functions is summarised in Table 4.2 below, with reference in the last column to the classification for SPV established in chapter 3.

Function	(Critical) performance	Source of performance variability (SPV)
a) Maintain appropriate speed	Excessive speed of train, travelling at 179 km/h on a curve with speed limit of 80 km/h	***Dynamic staff factor – attention***: Driver distracted by answering internal telephone call from train manager ***Static task factor – design***: No fixed signage to warn driver ***Static task factor – design***: No ERTMS protection, only ASFA ***Dynamic task factor – complexity***: Train 150/151 runs between Madrid an Ferrol on lines with different technical features ***Dynamic task factor – monotony***: "You eat up the km in no time, at high speed" ***Interactional factor – negative reinforcement***: Penalty when the driver's documentation is not up-to-date
b) Exchange of information between train manager/driver	Train driver in conversation with train manager for 100 seconds	***Static staff factor – experience***: Using the company's telephone is part of the job ***Static staff factor – motivation***: … for the convenience of passengers alighting from the train ***Static task factor – design***: Poor coverage for using mobile phone from Santiago to A Coruña ***Dynamic task factor – pressure***: Other activities to perform by train manager when at Santiago station (control passenger access, boarding/ alighting of passengers, …)
c) Monitor overspeeding	No finding of critical variability in speed Identification of risk in Angrois bend by leader driver	No SPV identified in report

Function	*(Critical) performance*	*Source of performance variability (SPV)*
d) Manage driver competence	No initial performance identified in report	No SPV identified in report
e) Adapt speed management	Decision to intensify the training of all drivers	***Static staff factor – motivation***: The change of speed is in line with the regulation in force
	No record that leader driver's warning was passed to infrastructure manager	No SPV identified in report
f) Equip with lineside signs	No fixed signage to warn driver	***Static task factor – instructions***: No rules exist
g) Equip infrastructure with ATP	Santiago station not equipped with ERTMS – risk of speed control in curve exported to driver	***Static task factor – contexts***: Ensure continuity of traffic (by choosing Iberian track gauge -rather than standard- throughout the line) and time savings (would be eroded when having two gauge changeovers in just 90km)
h) Authorise opening of lines	Authorisation for opening line 082 granted	No SPV identified in report
i) Equip rolling stock with ATP	Rolling stock protected with ASFA (and not ERTMS)	***Static task factor – design***: Incompatibility between ERTMS version on board and on the infrastructure
j) Authorise rolling stock	Initial testing did not discover incompatibility between ERTMS on train and in infrastructure	No SPV identified in report
	Authorisation to run with ASFA (and not ERTMS)	No SPV identified in report

Table 4.2: Critical performance and source(s) of performance variability for the different functions

This analysis shows that for five out of the ten identified functions enough information is available in the RAIC investigation report (2014) to build an understanding of why the actions and decisions, that with hindsight appeared to be critical to the course of the accident, made sense at the time. This is in particular the case for the operational activities close to the event, i.e. the control of the appropriate speed by the train driver (a) and the exchange of information between the train manager and the train driver (b). To a lesser degree, this is also valid for the decisions not to equip the curve with specific, fixed signage to warn the drivers for the drastic change of maximum speed (f) and not to equip the Santiago station with ERTMS protection (g), as well as for the decision only to intensify the training of drivers (e) in order to mitigate the risk of over-speeding in the Angrois bend. The analysis of the other functions just provides a compliance check against existing regulation, without explaining the (variability in) performance. Systematically applying the SAFRAN method would have required to also collect this further information.

4.3.3.4. Depth of the investigation

Another interesting observation lies in the fact that only for the function to maintain appropriate speed (a) the management of related SPV, which is one of the proposed iterations by the SAFRAN method, has been further analysed, and this for three out of six identified SPV. This is represented by the light blue arrows in Figure 4. Together with the finding that ten out of a total of fourteen identified SPV are related to the two operational functions closest to the event (i.e. (a) and (b)), this confirms that SPV close to operations are the ones actively looked for. Finding SPV for functions further away from the operational action, despite the sometimes critical variability of actions and decisions they may show, appears not to be the main focus of the investigation. Remarkably, the function to verify performance variability, which is the other criterion proposed by the SAFRAN method to start a new iteration, is available for more functions. This type of iteration, represented by the purple arrows in Figure 4, is present not only for the function to maintain appropriate speed ((a), verified through (c)) but also for the functions to equip both infrastructure ((g), verified through (h)) and rolling stock with an ATP system ((i), verified through (j)). The most logical explanation for this is that these authorisation functions are regulated in legislation.

In general, these results lead us to conclude that, except maybe for the function of the driver to maintain appropriate speed, the RAIC report (2014) does not contain enough information to complete all steps of the Safety Fractal for the identified functions, thereby leaving the full potential for further and in-depth analysis of the event underexploited. As such, the question if the risk of over-speeding in the Angrois bend for instance, could be discovered by the normal driver monitoring activities of the operator or the infrastructure manager (i.e. critical performance of function (c)) remains unanswered. Similar for the question whether normal testing could discover the incompatibility between track and on board ERTMS (i.e. critical performance of function (j)). Also further iterations of other possible functions, that would logically follow when applying the SAFRAN method, remain untreated. How is, for instance, the monotony and/or complexity related to the driver's task (i.e. SPV for function (a)) managed by the operator? Systematically applying the SAFRAN method would at least have opened these pathways for further in-depth investigations.

4.3.3.5 The potential for investigating Safety Culture

One of the most remarkable finding however, when analysing the elements from the RAIC investigation report (2014), is the fact that all involved parties, throughout the entire socio-technical system under investigation, appear to accept that the risk for controlling the sudden reduction in maximum speed is exported to the driver. This started with the design choice for the infrastructure not to install ERTMS (function (g)) in the area of the Santiago station and the safety case for this. This study clearly identified the risk but exported the control of it to the driver having to comply with the "maximum speed table" and obeying the indications displayed by the trackside signaling. This safety case is then going through the whole approval and authorisation process (function (h)) without further comments. It continues with the operator mitigating the risk, only when identified and reported by the leader driver, by intensifying the training of all drivers, "given that the change of speed was in line with the regulations in force". But also the driver, when answering to the public prosecutor's questions with: "The thing is, it all depends on me having to know that, at that point, I must adjust to this speed. There's nothing else to it.". And even the investigating body itself, when concluding that: "… none of the events investigated … had features similar to the Santiago de Compostela derailment…". The latter, despite having investigated at least six derailments primarily caused by excess speed while passing curves. Their main argument for this conclusion being that all investigated derailments occurred on curves with permanent speed limits, while the Santiago derailment occurred by exceeding the maximum speed prescribed for the route in the "maximum speed table" and therefore was a design choice.

Taking into account the Extended Safety Fractal developed earlier in this thesis (chapter 1), this sector-wide shared pattern of thinking shows us a clear example of how applying the SAFRAN method can help identifying safety culture elements emerging through the investigation of different functions related to an event. A first step further in the investigation, as explained above, could then be to understand the safety strategy that is used by the organisation(s) under analysis and define whether this could lead to sustainable and safe performance: (How) do they focus on major risk when taking safety related decisions? What mechanisms are in place and what expertise is used to understand workplace reality? This analysis, in turn, could then lead towards changes that could address the growing conditions for a positive safety culture at the level of organisations and/or the wider socio-technical system.

4.3.4. Discussion

The application of the SAFRAN method was demonstrated in this study by reviewing the published accident investigation report of one of the most lethal accidents the European railway system has known. The analysed case study only partly confirms the findings of other authors (e.g. Antonsen 2009a) that the scope of accident investigations usually stays limited to investigating the immediate causes and decision-making processes related to the accident sequence. Also here the operational activities closest to the event are the ones for which most SPV are identified, but other relevant functions that could offer the potential for further and more in-depth analysis of other safety management decisions are identified and their (expected) performance is documented.

The factual information that is collected about an accident must form the basis for and drive the analysis process in all investigations (AIBN, 2015). Getting the data, however, is only one side of the problem. The remaining task is then to make sense of these data and to reconstruct how people contributed to an unfolding sequence of events, leaving some kind of analytical trace from the collected data to the human and organisational factor(s) that help to explain their actions and decisions (Dekker, 2006). To achieve this, the collection and analysis of data on human and organisational factors should be just as methodical and complete as for technical systems (ISASI) and the use of a proper tool or method can help to ensure the effectiveness and thoroughness of the investigations (Reinach and Viale, 2006). As demonstrated through the case study, applying the SAFRAN method can offer this investigation rigour. Systematically looking for information to complete SAFRAN's generic steps allows for the identification of the human and organisational factors that influenced actions and decisions – whatever the function under analysis. Further following the SAFRAN investigation logic, will then allow the identification of the next relevant functions in the socio-technical system to analyse.

This will automatically lead to the desired treatment of variability in the wider system. A possible dilemma when establishing the analytical trace between findings and occurrences is that the most effective findings for safety enhancement are often the most difficult to justify (ATSB, 2008). Several authors (e.g. Cook, 2000) even argue that the traditional views of "cause" limit the effectiveness of defences against future events and that the focus should rather be on error-generating mechanisms (Groeneweg, 1992) or the capability of an organisation to monitor and manage safety critical variability. Also here, when following the investigation logic to identify functions for further iterations, the SAFRAN method offers an elegant in-between.

Farooqi (2015) however, clearly identified a number of railway incidents where, although latent and or organisational factors were present, active failures still played a critical role, leading her to conclude, as did Young et al. (2004), that it is important also to consider why active failures occurred and not only to focus on organisational factors. By systematically combining both the *performance* (i.e. individual) and the *implementation/control* (i.e. systemic) level for each iteration under analysis, the SAFRAN method provides the necessary guidance for investigators to find the right balance for investigating human factors, while still following a systemic approach. Furthermore, the method helps in systematically creating the necessary analytical trace, and ultimately to draft recommendations that can improve the railway system in a sustainable way by creating the capability to understand and cope with what will happen through a better understanding of what happened.

A limitation of the performed review is that all findings are solely based on the elements that are available in the published investigation report and could not take into account elements that are not reported upon. But the published report, with the same limitations, forms the basis for learning in the Spanish and wider European railway sector and what is evaluated with the case study is how sound this basis is. Since no information is available on the methods that were used to investigate the Santiago derailment, no conclusions can be made in comparison to other accident analysis methods. Further testing of the SAFRAN method during the (re-) investigation of events by accident investigation practitioners is therefore ongoing, in order to further validate the method and to gain a better indication of the type of additional factors that can be found compared to more traditional accident investigation practices.

4.4. CONCLUSIONS

In this chapter, we presented the SAFRAN method as a structured way to systematically identify human and organisational factors throughout a socio-technical system, more closely aligned to the logic of accident investigation practice than other systemic methods. Starting from the critical variability close to an accident, the application of the method guides investigators in analysing the state of the entire system in its capability to monitor and control this variability. It shows them a structured and iterative way to move from analysing a single event into analysing the wider socio-technical system around it. The SAFRAN method not only allows to combine human analysis with a systems-oriented analysis but, in addition, generates the necessary analytical trail to better communicate the results of such an analysis and to bring forward more demonstrable elements that might convince decision makers to adapt the system.

With the analysis logic that results from the SAFRAN method as a reference, the official accident investigation report that was published on the Compostela train crash is critically analysed. The results of this exercise shows that, while all major levels of the rail system are covered in the report, there is insufficient depth in the analysis to form a clear picture of the rationality of actions and decisions that are further removed from the sequence of events and that ultimately led to the fatal crash. Therefore, when it comes to analysing human and organisational factors in a structured manner that goes beyond understanding just the actions and decisions at the operating level in a socio-technical system, the accident investigation practice could gain from applying the SAFRAN method. Based on the above, it is assumed, that this will lead to recommendations that can change systems in a more sustainable way.

5

Towards a new way of analysing the resilience of socio-technical systems: the SAfety FRactal ANalysis method evaluated

This chapter is based on the article with the same title, published in *Safety*, 2022, 8, by Bart Accou (*role: concept, methodology, analysis and writing*) and Genserik Reniers (*role: review and supervision*).

INTRODUCTION TO CHAPTER 5

Writing the paper for this last chapter has reminded me how many times, during the various stages of the development process, the SAFRAN method has already been tested and tried. However, the effective application of the method in investigation practice has been limited, mainly due to available time and lack of volunteering organisations. This made me realise that effectively convincing accident investigation practitioners and, maybe even more importantly, their managers to apply the SAFRAN method in a systematic way will require more than a well-founded theory. I am therefore already thinking about the next steps that can be taken to achieve this goal. That provides an almost inexhaustible source of energy to continue working on developing and promoting the SAFRAN method.

ABSTRACT

Despite the systems approach to accident analysis being the dominant research paradigm and the concept of SMS being introduced in high-risk industries already for several years, accident investigation practice is still poor in analysing the basic elements that compose a safety management system (SMS) and in embracing system theory. In search for a systemic method for accident analysis that is easily applicable and less resource demanding than the actual methods, the SAfety FRactal ANalysis (SAFRAN) method was developed. The method, which is based on the principles of a SMS with resilience as the explicit safety strategy, aims at finding a good balance between examining the complexity of a socio-technical system and making optimal use of limited resources and people; factors that often restrict the possibility for in-depth analysis of accidents. A series of practical tests, often involving active accident investigators, made it possible to examine and validate the SAFRAN method against the criteria Underwood (2013) developed to evaluate systemic accident analysis methods. Based on the performed evaluation, that includes elements related to the development of the method as well as system approach and usability characteristics, the study concludes that, when it comes to applying a systems approach to accident analysis and with the aim of creating more sustainable and resilient performance, the current investigation practice could gain from having the SAFRAN method as part of the investigation toolkit.

5.1. INTRODUCTION

The complexity of the socio-technical system in most of the high-risk industries has increased significantly in recent decades and continues to increase. This has led to the current way of managing safety being questioned (e.g. Hollnagel 2014, Leveson, 2020) and alternatives being sought. In the multitude of often conflicting opinions, the idea that the performance of a (socio-technical) system should be approached in its entirety seems to be endorsed by everyone as well as the need to strive for resilience, i.e. the ability to perform in a resilient manner. Underwood and Waterson (2013) identified this system thinking approach to understanding socio-technical system accidents as the dominant paradigm in accident analysis research. However, this seems to be in stark contrast to current accident investigation practice. In addition, also the lack of in-depth analysis into (elements of) safety management systems (SMS) can be considered as a problem of current accident investigation practice. This, even though the concept of SMS was introduced and, in most cases, even legally imposed as the appropriate way to organise safety management in most high-risk industries, already for several years if not decades.

To provide a constructive answer to this problem, the SAfety FRactal ANanalysis (SAFRAN) method was developed, with the main aim to guide accident investigators, in an intuitive and logical way, to ask questions that help gain a deeper understanding of the capability of organisations to monitor and manage safety critical variability. The following sections of this chapter aim at validating SAFRAN as a method that allows to analyse the performance of socio-technical systems and that will lead to the identification of countermeasures that introduce a sustainable change towards a more resilient performance. Section 5.2 explains the methodology that was used to achieve this.

5.2. METHODOLOGY

Underwood (2013) mentions a lack of (empirical) validation as the most likely aspect related to the development of an accident model or investigation method that would affect its selection and use by practitioners. Several studies equally mention validity and reliability of an accident analysis method as a prime evaluation criterion (e.g. Katsakiori et al., 2009; Waterson et al., 2015 or Hollnagel, cited in Speziali and Hollnagel, 2008). Yet, for most of the existing systemic accident analysis methods, a proper validation appears to be missing (Underwood, 2013). In that context, practical and resource constraints could be mentioned as a main reason why it is difficult to conduct controlled experiments in this field of research, as well as the often very subjective nature of accident analysis, which results in main findings and recommendations depending highly on the analysist and his or her knowledge and experience. To validate the SAFRAN method, it was therefore opted to check the method and its composing elements against a set of tested criteria, still trying to ensure a high level of practitioner involvement.

5.2.1. Evaluation criteria

With the aim of examining how the theoretical and practical characteristics may hinder their adoption and use by accident investigation practitioners, Underwood (2013) has designed an evaluation framework that allows to assess and compare accident analysis methods. As graphically summarised in Figure 1, below, this evaluation framework is composed of a set of criteria that cover three basic elements: the development process of the analysis method (A), its potential to cover a systems approach (B) and its essential usage characteristics (C).

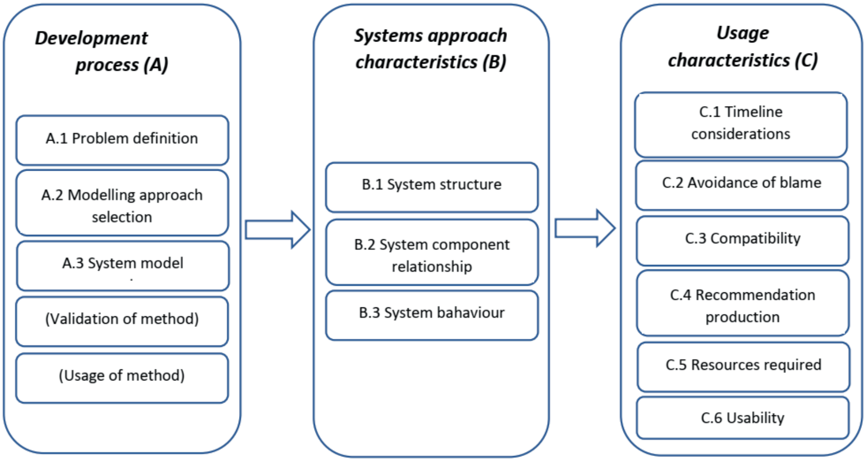


Figure 5.1: The evaluation framework, adapted after Underwood (2013)

To ensure the relevance of this evaluation framework as the reference to evaluate and validate the SAFRAN method, its different components were compared with criteria identified in other research papers that either examined and compared the characteristics of accident analysis methods (Benner (1985) and Hollnagel (1998) in Hollnagel and Speziali, 2008; Sklet, 2004; Katsakiori et al., 2009, Salmon et al., 2012) or provided guidance on the selection of such methods for practitioners (Speziali and Hollnagel, 2008; Underwood and Waterson, 2013a; Wienen et al., 2017). This comparison confirmed Underwood's evaluation framework as a solid reference to evaluate the weaknesses and strengths of accident analysis methods, not only to cover the complexity of socio-technical systems but also to gain acceptance by accident investigation practitioners. Based on this analysis, the only adaptation of this initial evaluation framework that is proposed, is to widen the scope of the timeline component, that is part of the usage characteristics, to a more broader capability to provide a comprehensive and clear picture that paints the narrative of the accident. Further nuances in the description of the different components between the above authors, when relevant for this study, will be treated when describing the evaluation of the SAFRAN method in section three of this paper. A summary of the different elements covered by each of the cited authors is available in Annex 1.

To be able to evaluate the SAFRAN method against this evaluation framework, a series of diverse tests has been conducted.

After a short introduction to the method by the author, two Master students at Cranfield University have each applied the SAFRAN method in order to compare the results with previous in-company investigations that were performed without following a specific investigation or analysis method. In one case study, Flovenz (2020) used the actual incident data from a jet blast incident of a commercial airline company, he previously investigated, to re-analyse the event with the SAFRAN method. Malone (2020) also used the incident data from an event she previously analysed and compared the results from the SAFRAN analysis of a railway construction incident, where a worker entered an unsupported excavation, with similar analyses performed with the STEP and the Barrier analysis methods. The results of both case studies provide valuable input for evaluating the useability of the method and its potential to cover different elements of the respective safety management and wider socio-technical systems, compared to in-company investigations using no specific method, which is still the main accident investigation practice (Underwood, 2013).

In addition, during the different phases of development of the method, the author also has had the chance, at different occasions, to train both students and active investigation practitioners in using the SAFRAN method. Although the received feedback was not consistently gathered in a formal way, this gave a good insight in how easy it is to understand the method and what time and effort is needed to learn to apply the SAFRAN method. In addition, some of these investigators also freely provided useful feedback after first applications of the method. This was especially the case for the Swiss Transportation Safety Investigation Board (STSB) and UK's Rail Accident Investigation Branch (RAIB), with whom a separate feedback session was organised.

Finally, similar to what Underwood and Waterson (2013b) did to compare the ATSB, AcciMap and STAMP models, the SAFRAN method has been used to analyse in detail the 2007 Grayrigg train derailment as described by the UK's Rail Accident Investigation Branch in its independent investigation of this accident (RAIB, 2011). This allows for an additional comparison, this time also using the SAFRAN method. The analysis of the Grayrigg train derailment formed the capstone of a series of close to 100 similar studies, where the information from publicly available accident investigation reports was ordered in a SAFRAN-logic. Although also investigation reports from other types of transport modes (e.g. shipping and aviation) were analysed, most of the studies were related to the railways, and derailment events, in particular.

5.2.2. Applying SAFRAN to the Grayrigg accident

To justify their choice of using the Grayrigg accident for testing whether the widely used Swiss Cheese Model can provide for a systems thinking approach, Underwood and Waterson (2013b) argue that the combination of railways as a complex socio-technical system with many stakeholders and the scope and comprehensiveness of the final investigation report (RAIB, 2011) provide a solid basis and data source for a systemic analysis.

The derailment of an express passenger train at Grayrigg on 23 February 2007, causing the fatality of one passenger, represents one of the highest profile accidents in UK rail history. The investigation concluded that the accident was caused by the unsafe state of a switch, forcing some of the wheelsets from the first vehicle into the reducing gauge between both switch rails. As a result, all the other vehicles of the train derailed and eight of all nine derailed vehicles subsequently fell down an embankment with five turning on their side. Of the total of 4 crew members and at least 105 passengers, one passenger was killed, 28 passengers, the train driver and one other crew member received serious injuries, while 58 passengers got minorly injured. A scheduled inspection in the week before the accident, which should have detected the degradation, was omitted. Also, several shortcomings in inspection and maintenance practices and, more general, the safety management arrangements of the responsible infrastructure manager were identified as underlying factors.

The information available in RAIB's investigation report was analysed in detail to identify the different functions throughout the railway socio-technical system that showed critical variability in relation to the accident as well as the sources of performance variability that could explain this. This safety information was then structured and graphically represented using the SAFRAN investigation logic, linking the functions through either the implementation side or the control side of a triangle. In a next step, in order to facilitate the comparison with the results of Underwood and Waterson (2013b), the different elements that resulted from this work were put next to their analysis and, when relevant, the code or labeling of the information was aligned. Finally, the timeline with the sequence of events, that explains the physical mechanism that led the switch to be in an unsafe state, was added. The result of this analysis is represented below, in Figure 5.2 and the accompanying table.

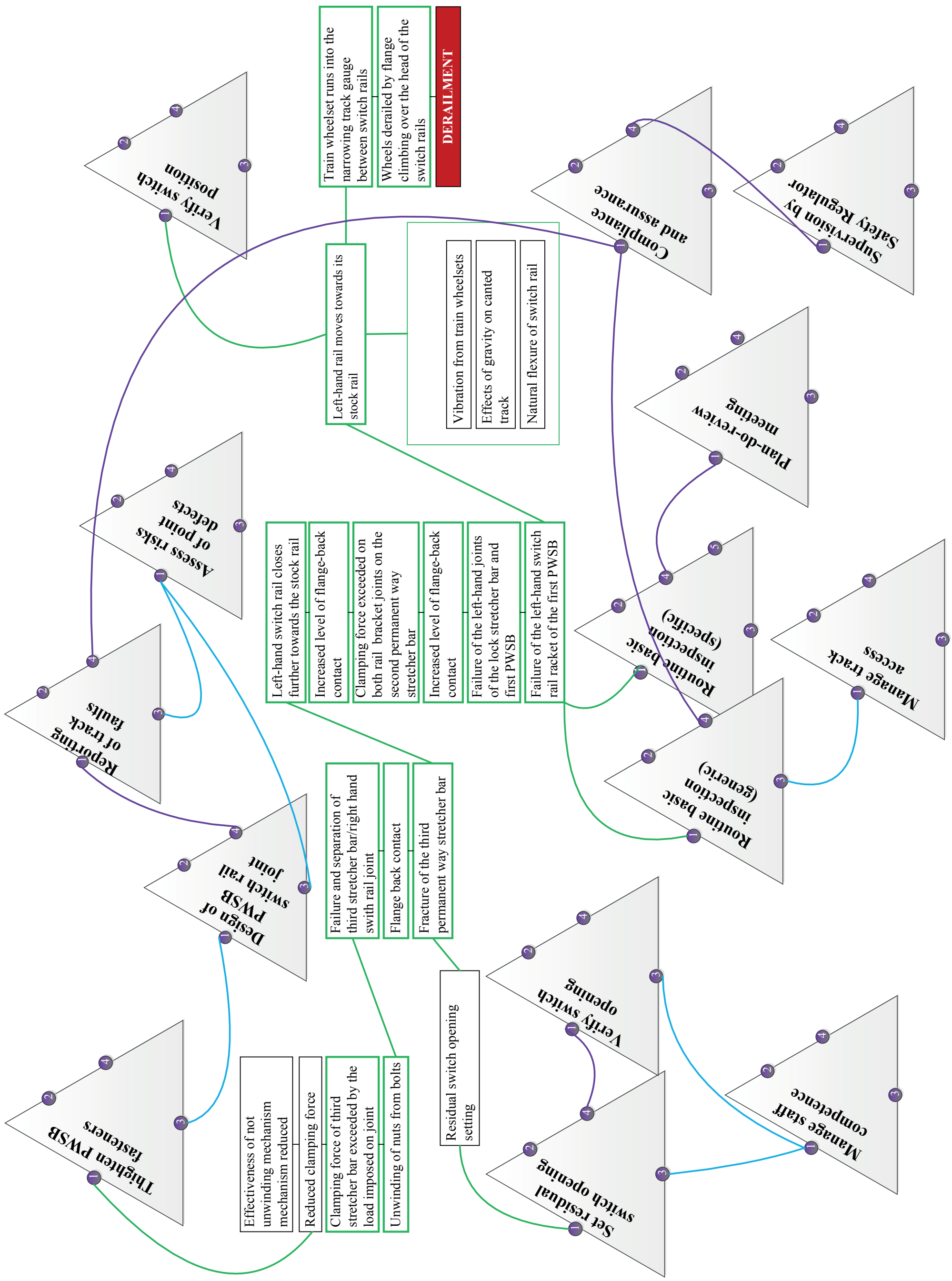

Verify switch position
Train wheelset runs into the narrowing track gauge between switch rails
Wheels derailed by flange climbing over the head of the switch rails
DERAILMENT
Compliance and assurance
Supervision by Safety Regulator
Left-hand rail moves towards its stock rail
Vibration from train wheelsets
Effects of gravity on canted track
Natural flexure of switch rail
Plan-do-review meeting
Assess risks of point defects
Left-hand switch rail closes further towards the stock rail
Increased level of flange-back contact
Clamping force exceeded on both rail bracket joints on the second permanent way stretcher bar
Increased level of flange-back contact
Failure of the left-hand joints of the lock stretcher bar and first PWSB
Failure of the left-hand switch rail racket of the first PWSB
Routine basic inspection (specific)
Manage track access
Reporting of track faults
Routine basic inspection (generic)
Design of PWSB switch rail joint
Failure and separation of third stretcher bar/right hand swith rail joint
Flange back contact
Fracture of the third permanent way stretcher bar
Verify switch opening
Residual switch opening setting
Thighten PWSB fasteners
Effectiveness of not unwinding mechanism mechanism reduced
Reduced clamping force
Clamping force of third stretcher bar exceeded by the load imposed on joint
Unwinding of nuts from bolts
Set residual switch opening
Manage staff competence

Figure 5.2: SAFRAN representation of the Grayrigg acciden

Function	Step	Linked function
Tighten PWSB fasteners	1. Re-use of threaded fasteners by maintenance team	Effectiveness of not unwinding mechanism reduced
	2. -	
	3.1 Understanding of design, inspection and maintenance requirements	Design of PWSB switch rail joint
	3.2 No standards/procedures on re-use of threaded fasteners	
	3.3 NR special instruction notices (do not specify tightening activity)	
	3.4 Limited awareness of fastener pre-load loss	
	4. Loose PSWB nuts not detected	
Design of PWSB switch rail joint	1. Understanding of design, inspection and maintenance requirements	
	2. -	
	3.1 (Non) application of maintenance standards	
	3.2 Incorrect perception of PWSB risk	Assess risk of point defects
	4.1 Lack of asset condition knowledge	
	4.2 Underreporting of faults	Reporting of track faults
	4.3 Lack of asset condition surveys	
Reporting of track faults	1. Underreporting of faults	
	2. -	
	3.1 Management information system not configured for efficient asset fault analysis	
	3.2 Process for performance measurement of S&C not based on understanding of risk and control management	Assess risk of point defects
	3.3. Key performance indicators	
	4.1 No independent inspection of assets	
	4.2 Audits of asset conditions and maintenance activities	Compliance and assurance

Assess risk of point defects	1. Process for performance measurement of S&C not based on understanding of risk and control management	
	2. -	
	3. Use of inappropriate tools for risk assessment	
Verify switch position	1. Left-hand rail moves towards its stock rail	
	2. -	
	3. Switch rail separated from detected rod	
Set residual switch opening		Residual switch opening setting
	2. -	
	3.1 Communication of maintenance responsibilities	
	3.2 Need to check residual switch opening not specified in work instruction (PA11)	
	3.3 Staff competence	Manage staff competence
	4. Switch opening not detected	Verify switch opening
Verify switch opening	1. Switch opening not detected	
	2. Patrol procedures	
	3.1 Communication of maintenance responsibilities	
	3.2 Incorrect perception of PWSB risk	
	3.3 Staff competence	Manage staff competence
Manage staff competence	1. Joint points training did not take place	
	2. -	
	3. RAIB could not establish reason	

Routine basic inspection (specific)	1.1 Points failure not detected	
	1.2 Track section manager forgot to perform agreed inspection of 2B points	
	2. Patrol procedures	
	3.1 Roster sheet not provided	
	3.2 Extended working hours	
	3.3 Increased workload	
	3.4 Unplanned, urgent work	
	3.5 Decision to combine supervisory inspection with basic inspection	
	4.1 Missed inspection not identified	Plan-do-review meeting
	4.2 Track maintenance engineer not informed of missed inspection	
	5. Missed inspection not reinstated	
Plan-do-review meeting	1. Missed inspection not identified	
	2. -	
	3.1 Inaccurate data input	
	3.2 Substituted inspection report procedures	
	4. Audits of asset conditions and maintenance activities	Compliance and assurance

Routine basic inspection (generic)	1.1 Points failure not detected	
	1.2 Loose PSWB nuts not detected	
	2. Patrol procedures	
	3.1 Staffing level demands	
	3.2 Restricted track access	
	3.3 Difficult to visually identify loosening of PWSB nuts	
	3.4 Limited time for inspection	
	3.5 Reduced daylight in winter	
	3.6 Track access policies	Manage track access
	4.1 Supervisor's inspection	
	4.2 Engineer's inspection	
	4.3 Audits of asset conditions and maintenance activities	Compliance and assurance
Manage track access	1. Several attempts to manage situation failed	
	2. -	
Compliance and assurance	1. Audits of asset conditions and maintenance activities	
	2. -	
	3. On track maintenance not in focus of audit protocols	
	4. No specific focus on switches & crossings in delivery plan	Supervision by Safety Regulator
Supervision by Safety Regulator	1. No specific focus on switches & crossings in delivery plan	
	2. Primary purpose of delivery plan is NR's management processes (not the examination of assets)	
	3.1 Previous accidents gave no indication of problems with S&C design or maintenance	
	3.2 Believe that engineering management had improved based on inspection results	

In this graphical representation, the boxes with a green lining represent the physical sequence of events. From this sequence, focusing on variability in performance of the system, the initial SAFRAN analysis only picked up the information on the setting of the residual switch opening and the unsafe state of the switch. The boxes that describe the gradual deterioration of the switches were added. In the accompanying table, lines filled with a similar colour present the same or related information, while the lines with red text represent information that is covered in the SAFRAN figure but is not available in the ATSB or AcciMap as proposed by Underwood and Waterson (2013b).

The triangles represent the system functions that, based on the information provided in the investigation report (RAIB, 2011), showed critical performance variability. For each of these triangles, information on the actual performance (left hand side of the triangle and represented by the numbers 1), the sources of performance variability (bottom of each triangle, and represented by the numbers 3) and the control elements of the function (right hand side of each triangle and representing respectively the "specify" (numbers 2), "verify" (numbers 4) and "adapt" (numbers 5) elements). Five of the fourteen identified functions represent a first iteration, describing either an activity that led to the unsafe state of the switch (i.e. tightening switch bar fasteners and setting the residual switch opening) or an activity to identify the status of the switch in several grades of deterioration (i.e. the routine basic inspections, analysed separately for its generic process characteristics and for the specific case where a planned inspection was missed, and the (non-) verification of the switch position when the switch rail is separated from the detector rod). The verification of the residual switch opening could also be considered as verifying the status of the switch (and thus a first iteration) but is here considered as the capability to verify the initial setting of the switch and thus a second iteration. With the functions that represent the design of the switch rail joint, the assessment of risks of point defects, the management of staff competence and the management of track access, second iterations were initiated to analyse whether the management of identified sources of performance variability is detected. The triangles that represent the reporting of track faults, the plan-do-review meetings, the audits of asset conditions, the compliance and assurance regime and the supervision by the safety regulators show consecutive iterations following the hierarchical control structure both inside and outside the organisation responsible for keeping the switch in a good operational state.

The red coloured numbers on the side of the triangles, finally, represent a logic continuation of the investigation when applying the SAFRAN method, that is not covered in the analysed investigation report. Except for the function to "Manage track access", where no source of performance variability could be identified, all other red numbers represent the possibility to further investigate the capability of the responsible organisation(s) to identify possible variability in the performance of the related functions. This step is comparable to the feedback loop in a STAMP analysis, with as a nuance that SAFRAN urges to focus this analysis on identifying performance variability and does not require to identify the entire control structure, but rather describes it with each new iteration. As will be argued further on in this paper, systematically analysing the capability to identify (and control) variability could however be the most viable source to generate recommendations that may lead to more sustainable change of a specific function, and probably the entire system with it. In addition, also the management of several of the identified sources of performance variability could have offered an opportunity for further investigation.

5.3. FINDINGS

In the following sections, the combined findings of the gathered experience with applying the SAFRAN method will be used to evaluate the method against the different elements of Underwood's evaluation framework (2013).

5.3.1. A. Development process

The first pillar in the evaluation framework represents the cumulative stages that should be followed when developing an analysis tool according to Wahlström (cited in Underwood, 2013). For obvious reasons, the last two stages (i.e. validation and usage of the method) of the proposed scheme will not be covered in this section of the paper. The formal validation of the SAFRAN method forms the subject of the entire paper. And although we could already report on some first usage of the method, the available information is considered insufficient to present a valid picture of how the method is used in practice. The remaining evaluation criteria therefore are: the problem definition (A.1), the selection of the modelling approach (A.2) and the creation of a system model (A.3) when applying the method.

5.3.1.1 - A.1 Problem definition

A first requirement is the problem definition: is the reason for creating the model or method well defined?

Several authors (e.g. Antonsen, 2009; Kelly, 2017) already concluded that the current scope of accident and incident investigations 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 weaknesses in the SMS are hardly ever analysed (Johnson, 2004). It should therefore be of no surprise that those investigations don't guide directly towards solutions that can be found within elements of the legally obliged SMS. While the

SMS, based on a holistic approach with operational, supporting and controlling elements functioning together, is identified as an appropriate vehicle to support the organisation of resilience in an organisation, this means that the actual accident investigation practice misses a giant opportunity to improve the system under investigation in a more sustainable way.

Underlying causes that could explain these findings refer to investigation methods not being developed in line with a system thinking approach to accident causation (e.g. Reason, 1997; Speziali and Hollnagel, 2008; Lundberg et al., 2009, Dekker, 2011) but also a lack of vertical interaction between the different levels of the socio-technical system, resulting in a problem of incorporating theoretical management models like SMS as a tool for resolving issues related to human performance or technical failure at the operational level (Rasmussen, 1997).

To address these problems, SAFRAN was developed as an investigation analysis method, with the aim of guiding investigators to better explore the composing elements of an SMS in a natural and logic way.

5.3.1.2.- A.2 Modelling approach selection

A second criterion, linked with the model development process, is whether there is clarity on the conceptual approach that has been adopted or has influenced the method. Similar requirements were put forward by Sklet (2004) and Katsakiori et al. (2009), who explicitly refer to an underlying accident model. Speziali and Hollnagel (2008), in addition, mention the consistency requirement with an organisation's safety program concepts, put forward by Benner (1985), and the need to have a method grounded in a clear identifiable model of human action, referring to earlier work of Hollnagel (1998).

The SAFRAN method is built around a unique unit of analysis, called the Safety Fractal. This model or unit is reflecting a generic set of basic requirements that are needed to control safety related activities. It was constructed by comparing a theoretical model describing the desired functioning of a SMS with specific requirements for process capability that can represent the management of activities at an operational level. Building on the similarities between both references, a five-step safety management delivery system was identified.

While the SMS may be considered by some authors as a product of reactive safety management (e.g. Hollnagel, 2014), Pariès et al. (2019) argue that several safety strategies can fit within an SMS framework. This logic was followed for the Safety Fractal, by "translating" Hollnagel's four potentials required for a resilient performance (2009) as well as Denyer's ideas on "paradoxical thinking" (2017) into the above steps. As a result, with resilience explicitly identified as the safety strategy to follow, the focus for managing safety with the Safety Fractal shifts from eliminating threats towards controlling the variability in process performance. In this context, all contextual elements that could create variability in the human performance of the process should be considered to understand a work situation. A set of these "sources of performance variability" (SPV) was identified that fit the self-similar concept of the Safety Fractal. Furthermore, when grouping the 5 steps of the Safety Fractal according to the nature of their goal, three distinct levels to observe the functioning of a process can be identified. A level of **process performance** in step (3) that is representing the direct functioning of the components that interact during process execution ("doing things"). This is also the level where variation against process specifications and/or expectations can be observed. A level of **process implementation** through step (2), providing the resources and means to ensure the correct functioning ("doing things right") of the process components during process execution. And finally, a level of **process control**, composed of the steps (1), (4) and (5), ensuring the sustainable control of risks related to all activities of the organisation ("doing the right things"). Together, the implementing and controlling stages define the formal as well as the informal side of safety management and have a direct influence on performance. As such, the Safety Fractal represents a unique unit of analysis that can support the recent paradigm shift in safety management, still making optimal use of the experience gained with SMS over the past decades.

Continuing earlier developments of the Dutch Safety Management Model, Lin (2011) proposed a way to connect the higher system level management controls with human and technical factors at the lower level. Similarly, Wahlström and Rollenhagen (2014) propose using a control metaphor for the design and assessment of SMS in combination with the concepts of man, technology and organisational and information systems (MTOI) to ensure the continued safety of the operated systems. They 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, separately and together. Also Lin (2011) used a general structured safety management model to further specify lower level delivery systems that should ensure the management of individual factors that influence the performance of human and hardware. Following this line of thought, we conclude that the Safety Fractal model can be applied to develop and/or assess all types 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. This idea of a repeating pattern that displays at every scale, characteristic for fractals, also explains the name that was given to the model.

The above Safety Fractal was then compared with the common accident investigation approach that was distilled by Wienen et al. (2018), resulting in the 5-step investigation logic that is characteristic for the SAFRAN method.

5.3.1.3 - A.3 System model creation

With the adequate examination of a system's environmental boundary, hierarchy and component relationships all covered by the second pillar in the evaluation framework, Underwood (2013) limits the criterion of system model creation (i.e. the capability of a method to build a system diagram) to the question whether the system under investigation is graphically represented. Focusing specifically on the graphical output of a method, Underwood and Waterson (2013a) further complement this by questioning whether the produced graphical output helps to facilitate the analysis (e.g. by identifying evidence gaps) and provides a useful means of communicating the findings of an analysis with others. Sklet (2004), on the other hand, also stresses the need for a method to provide a graphical description of the event sequence, which is more related to the timeline consideration in the third pillar of the evaluation framework and will be further discussed in that part. Closer to the concept of system model creation however, he also reflects on whether an accident investigation method is inductive, deductive, morphological, or non-system oriented. In this view, a deductive approach involves reasoning from the general to the specific, an inductive approach means reasoning from individual cases to a general conclusion while the morphological approach would be based on the structure of the system under investigation.

For the graphical representation of a Safety Fractal, a triangle has been chosen, with each of the sides representing one of the three identified levels that can be used to observe the functioning of an activity or process. The left-hand side represents the **process performance** and describes how an activity was executed. The bottom side groups the sources of performance variability, that are believed to explain the variability in the execution of the process. In a further iteration, the reflection on how to manage these sources of performance variability will lead to elements of **process implementation**, providing the resources and means to ensure the correct functioning 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. The related control processes of specifying, verifying, and adapting performance are systematically numbered 2, 4 and 5 respectively. The name of the analysed function is written in the centre of the triangle, while the related findings for each of the levels are placed in a text box on the corresponding side of the triangle. The following figure 3, zooming in on one of the analysed functions from the Grayrigg accident investigation, illustrates the approach.

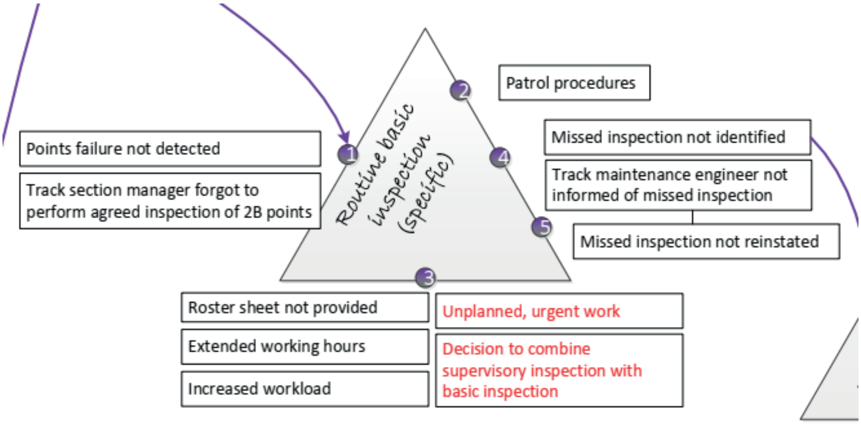

Routine basic inspection (specific)
1
2
3
4
5
Patrol procedures
Points failure not detected
Track section manager forgot to perform agreed inspection of 2B points
Missed inspection not identified
Track maintenance engineer not informed of missed inspection
Missed inspection not reinstated
Roster sheet not provided
Extended working hours
Increased workload
Unplanned, urgent work
Decision to combine supervisory inspection with basic inspection

Figure 5.3: Graphical representation of one analysed function

When starting from the (critical) variability identified close to the sequence of events, the relevant parts of the system are identified, and a graphical model of the system is built. Rather than building a model of the entire system, however, it was chosen to only represent those elements that are identified as showing critical variability in their performance that appeared relevant for the accident under investigation. Applying such a morphological approach, the model is then growing each time the SAFRAN logic is applied for a new iteration. This approach allows to overcome the resource demanding description of the entire system as required by FRAM (Hollnagel, 2012), with its focus on describing in detail how something is done, or STAMP (Leveson, 2012), where step 3 of the method requires to document the entire control structure in place.

As demonstrated with the Grayrigg analysis, as well as with a similar analysis of the 2013 Santiago de Compostela train crash investigation (chapter 4), the graphical representation of a SAFRAN analysis can easily support the investigation as such. To fully understand how the variability of a function is controlled, all elements of a triangle -i.e. a full iteration of the SAFRAN method with one function- should be available. If this is not the case, this may indicate that further evidence needs to be found as well as the type of evidence an investigator needs to look for. Furthermore, for each identified SPV, it can easily be verified whether a link exists with a new function to manage this SPV. If not, this could identify the need for a next step in the investigation, with clear focus on what to investigate. A similar logic is equally valid for the functions to verify performance variability.

5.3.2. B. Systems approach characteristics

The second pillar in the evaluation framework aims at verifying whether a method or model applies system thinking. To be able to perform this evaluation, Underwood (2013) has identified three interrelated themes that broadly reflect the different elements that exist in literature on systems theory: system structure (B.1), system component relationship (B.2) and system behaviour (B.3). This is in line with a later publication of Leveson (2020), that defines a system as "a set of things (referred to as system components) that act together as a whole to achieve some common goal, objective or end.", still emphasizing that the concept of a system is an abstraction, i.e. a model conceived by the viewer.

5.3.2.1 - B.1 System structure

Leveson (2020) identifies having a common goal or objective as the most fundamental part of a system. In a system, this goal is then normally achieved by a hierarchy of subsystems and to understand the overall functioning of the system it is necessary to examine each relevant hierarchical level. Examining lower levels of a system will reveal how a system functions to meet the set objectives, while moving up that hierarchy will provide a deeper understanding of a system's goal (Vincente, cited in Underwood and Waterson, 2013). Being able to represent a system's hierarchy will therefore be an essential part of any systemic analysis method. Similarly, Salmon et al. (2011) require a systemic method to be capable of covering the entire socio-technical system, while Sklet (2004) already referred to the possibility to include the six levels of a socio-technical system as identified by Rasmussen (i.e. work, staff, management, company, regulators and government). Being able to describe a system, also includes a clear view on the system boundaries and the system's environment, i.e. those elements or components that are situated outside the system but whose behaviour can still affect the system state. This requirement to define boundaries between system elements is equally covered by Waterson et al. (2015), who also refer to the capability to address external and environmental aspects of the work domain (e.g. regulatory or economic influences on safety).

By systematically guiding investigators to identify the functions that can either manage the sources of performance variability as well as the capability of the related organisations to verify and control the performance variability, the SAFRAN method actively supports the description of the hierarchy of functions in the system under investigation. As illustrated in Figure 5, below, it took only three or four iterations to reach the regulatory level in the Grayrigg case.

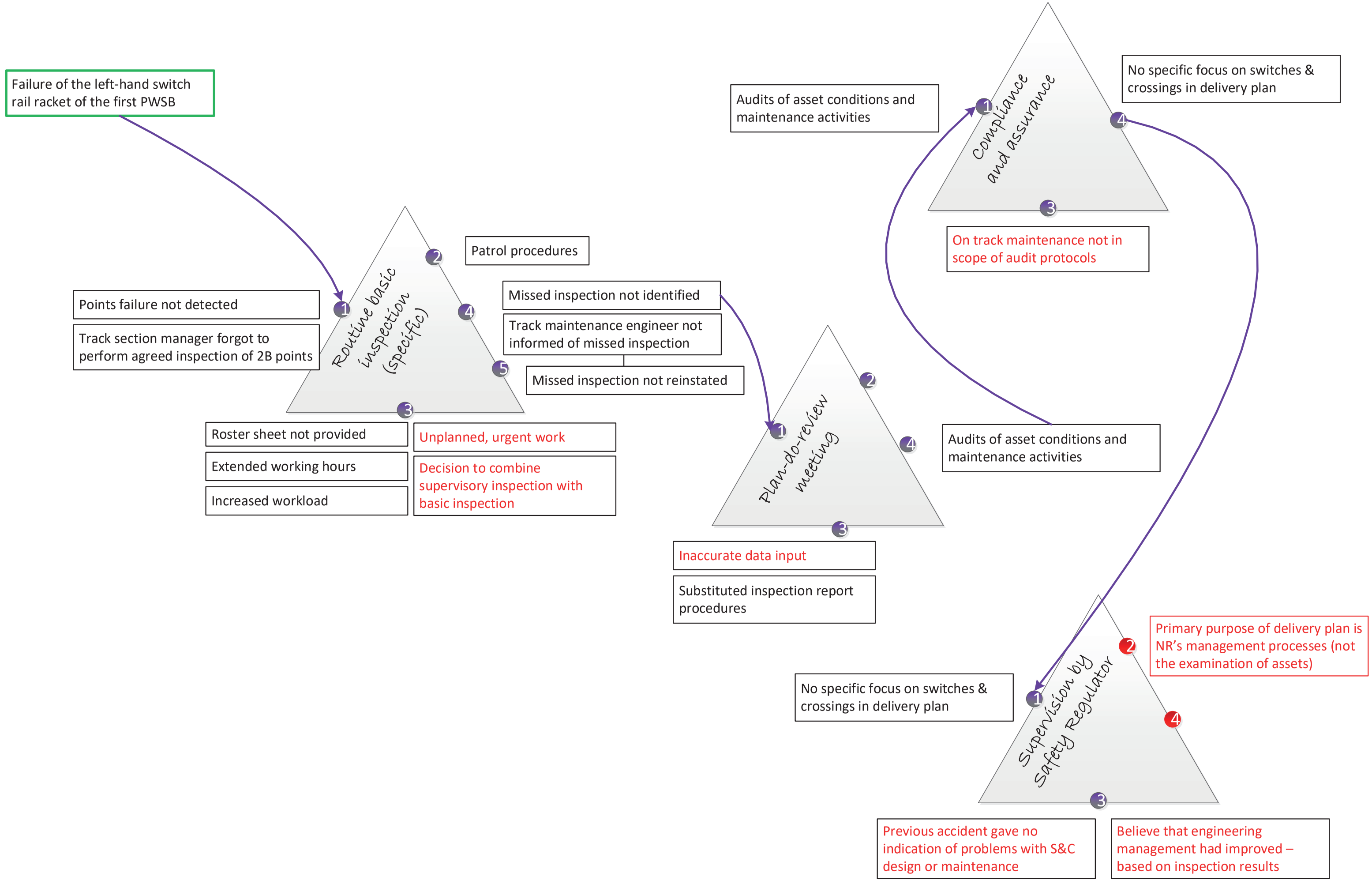

Failure of the left-hand switch rail racket of the first PWSB
Routine basic inspection (specific)
1
2
3
4
5
Points failure not detected
Track section manager forgot to perform agreed inspection of 2B points
Patrol procedures
Missed inspection not identified
Track maintenance engineer not informed of missed inspection
Missed inspection not reinstated
Roster sheet not provided
Extended working hours
Increased workload
Unplanned, urgent work
Decision to combine supervisory inspection with basic inspection
Plan-do-review meeting
1
2
3
4
Inaccurate data input
Substituted inspection report procedures
Audits of asset conditions and maintenance activities
Compliance and assurance
1
3
4
Audits of asset conditions and maintenance activities
No specific focus on switches & crossings in delivery plan
On track maintenance not in scope of audit protocols
Supervision by Safety Regulator
1
2
3
4
No specific focus on switches & crossings in delivery plan
Primary purpose of delivery plan is NR's management processes (not the examination of assets)
Previous accident gave no indication of problems with S&C design or maintenance
Believe that engineering management had improved – based on inspection results

Figure 5.4: Illustration of hierarchical levels of control with SAFRAN for the Grayrigg accident

Furthermore, for each iteration, the SAFRAN method requires not only to describe events actions and conditions that can explain the performance of a function – something that is, according to the study of Underwood and Waterson (2013b) characteristic for the ATSB and AcciMap method. Similar to what is required for a STAMP analysis, the SAFRAN method combines this with the requirement to also document and analyse the functioning of the system control structure, as far as relevant for the performance variability that was identified at lower levels in the system. Analysing the specification of the objectives to be achieved by the consecutive functions with each new iteration as well as the related responsibilities also defines the boundaries of the (parts of the) system under investigation.

5.3.2.2 - B.2 System component relationship

Underwood (2013) requires with this criterion the possibility to study a system in a holistic way, considering all components (i.e. human and technical) as well as the relationships between them. Leveson (2020) refers to this as the 'atomistic' characteristic of systems, meaning that a system can be separated into components with interactive behaviour or relationships between the components. Both precise that in socio-technical systems, however, there will be some "emergent" system properties for which the analysis of individual components cannot be combined to explain the overall system performance.

Similar to what Underwood and Waterson (2013b) found for the ATSB, the AcciMap and the STAMP method, SAFRAN requires the analyst to take a holistic view by examining the interaction between the various elements of the system. Like described above for the system structure criterion, also for the system component relationship the SAFRAN method combines the outputs of the relationships, characteristic for the ATSB and AcciMapp, with a description of these relationship between the various components, as is required for STAMP. The former is done when describing the performance of a single triangle, the latter is achieved by linking the control elements of consecutive iterations with triangles that describe the nested control loops in the system.

5.3.2.3 - B.3 System behaviour

The last criterion that is proposed by Underwood (2013) to verify whether a method applies system thinking, is its capability to address the various factors which may affect safety. This covers a set of elements as broad as: inputs and outputs of an activity and the associated transformation process, control and feedback loops, equifinality (i.e. a goal can be achieved from different starting points) and multifinality (i.e. a same starting point can produce a range of outputs), system adaptation, and the context in which performance takes place. Leveson (2020), from a higher system perspective, refers to the possibility to describe the state of a system as a set of relevant properties describing it at any time.

Hollnagel (cited in Speziali and Hollnagel, 2008), on the other hand, requires an analytical capability to deliver a description of the characteristics of human cognition that are included in the set of assumed causes. Other authors identify similar or related requirements to search for underlying causes (Katsakiori et al., 2009) or the ability to identify contributing factors that can explain complex human decision making and organisational failures (Salmon et al., 2011).

With the SAFRAN method, the output of a function or system component -which is logically the first thing an investigator will be confronted with- is covered in the chart on the left side of each triangle when the actual performance is described. When following the method's investigation logic, in the next steps also the input conditions will be identified (the "specify" element in Step 2) as well as the reasons that explain performance variability, i.e. the associate transformation, through the analysis of SPV (Step 3). The identification of these SPV, for each individual iteration, will also cover the requirement to take into account the context in which actions and decisions are taken, and eventual system adaption. Control and feedback loops are covered by analysing the "specify" and "verify" (and eventually the "adapt") elements on the control side of each triangle. Equi- and multifinality, finally, are implicitly included when recognising resilience, and thus controlling the variability in process performance, as the strategy for managing safety and thus as the goal of each triangle or function that is investigated.

5.3.3. C. Model usage characteristics

The third and last pillar in the evaluation framework, provides a set of criteria that are representative of the easy acceptance and overall usability of an analysis method for practical application.

5.3.3.1 - C.1 Accident description

Underwood (2013) introduces a timeline consideration criterion, by evaluating whether a method or model incorporates the concept of time in the accident development process. Katsakiori et al. (2009), later followed by Wienen et al. (2017), require a method to be able to provide a comprehensive and clear picture that paints the narrative of the accident under investigation. This is in line with Hollnagel's requirement (cited in Speziali and Hollnagel, 2008) for a method to produce an adequate explanation or account of why an adverse event (accident or incident) occurred. Also, Benner (cited in Speziali and Hollnagel, 2008) requires an investigation to result in a realistic description of the events that have occurred. He also requires the result of an investigation to be comprehensive and without confusion about what happened, without unsuspected gaps or holes in the explanation and with no conflict of understanding among those who read the report. Hollnagel, in turn, links this with audit capability, requiring it to be possible to retrace the analysis and reconstruct the choices, decisions, or categorisations made during the analysis.

Focusing on analysing the SMS and wider socio-technical system, the SAFRAN method requires an already established sequence of events to be able to start the analysis. Based on this sequence of events, that should be describing the mechanisms and operational decisions that led to an incident or accident, those events that showed critical variability can be selected and with consecutive iterations the relevant "underlying" elements can be further analysed. For each analysed function, throughout the entire socio-technical system, the SAFRAN method will look to understand the variability in performance (i.e. why actions or decisions were taken). And when strictly applied, the structured and iterative approach that characterizes the method will ensure full traceability of the analysis process.

5.3.3.2 - C.2 Avoidance of blame

Benner (cited in Speziali and Hollnagel, 2008) requires an investigation method to provide a non-causal framework and the resulting analysis to provide an objective description of the accident process. The attribution of cause or fault can then only be considered separate from the analysis and after a full understanding of the accident process is achieved. Underwood (2013) translated this avoidance of blame into the question whether a method directs the analyst towards identifying a root cause. Del Frate et al. (2011), on the other hand, 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. In the same line of thought, 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.

As will be further argued under the section that reflects on the production of recommendations, the aim of accident investigations should be to learn an organisation to be resilient in order to compensate for structural shortcomings (van Schaardenburgh-Verhoeve et al., 2007) as well as 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 an individual or even organisation has failed, but should rather 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. This is exactly the focus that is integrated into and ensured by the investigation logic of the SAFRAN method.

5.3.3.3 - C.3 Model compatibility

A next criterion proposed by Underwood (2013), to validate the usability of an accident investigation or analysis method, is whether it can be used in conjunction with other analysis techniques. As explained earlier, the SAFRAN method focuses on analysing the SMS, starting from an already established sequence of events. It can therefore be classified as a "secondary" method, according to the terminology introduced by Sklet (2004), providing special input as supplement to other methods. In contrary to a primary method, that would be a stand-alone investigation technique.

5.3.3.4 - C.4 Recommendation production

The investigation of adverse events is not an objective as such. The effort should lead to improving safety performance, lessons need to be learned and the right counter measures need to be taken, preferably by changing an organisation's performance in an intended direction. Underwood (2013) therefore suggests questioning whether a method aids the analyst in producing safety recommendations and providing generic insights into accident causation. Also Katsakiori et al. (2009) put forward a consequential requirement, questioning whether a method generates recommendations for improved safety, while similarly, Salmon et al. (2011) require a method to support the development of appropriate countermeasures, as opposed to countermeasure that are focused on individual operators. In the same context, Benner (cited in Speziali and Hollnagel, 2008) requires an investigation method also to be direct and satisfying. Direct, in a sense that the investigation should provide results that do not require the collection of additional data before the needed controls can be identified and implemented. The results should also be satisfying for those who initialised the investigation and other individuals that may demand results from an investigation. This requirement comes close to the criterion proposed by Wiener et al. (2017), namely, to question whether an investigation method can produce recommendations that can persuade management to take action.

With the structured review of a selected set of published railway accident investigation reports, all related to over-speeding accidents, it was already demonstrated in chapter 3 that applying the SAFRAN method will automatically lead to issuing recommendations that can address both single-loop learning (i.e. correcting errors within the range, set by organisational norms, for performance) and double-loop learning (i.e. when correcting errors requires to change the organisational norms for performance). Also the third type of learning that was identified by Argyris and Schön (1996), called organisational deutero-learning and referring to the capability of an organisation to "learn how to learn", is actively supported by the SAFRAN method. This will be the case when recommendations are issued to improve the functioning of the processes that define the control part of each triangle (i.e. specify, verify and adapt). Every iteration of the SAFRAN method that is triggered by the further analysis of an organisation's capability to monitor and control variability will offer this opportunity.

5.3.3.5 - C.5 Resources required

A next criterion, proposed by Underwood (2013) to evaluate the ease of use for an investigation method, is the resources and data an analyst would require when using the method. Here, Hollnagel (cited by Speziali and Hollnagel, 2008) makes a distinction between the effective resources needed, the time to learn and the cost-effectiveness of an investigation method. The main resources that will define how difficult or easy it is to use a specific method are: people (hours of work), time, information and documentation and additional needs like specialist software e.g. Equally important is how easy a method is to understand and the time it takes to learn to use it and to become a proficient user. The cost-effectiveness parameter, in turn, relates to the relative costs and benefits associated with using a specific method. These elements summarise similar practical requirements that are put forward by also other authors (e.g. Katsakiori et al., 2009; Waterson et al., 2015; Wienen et al., 2017).

In general, learning and applying the SAFRAN method is not considered as very time consuming. Flovenz (2020), for instance, states that: "While training and practical application under the supervision of an experienced practitioner appears to be clearly required, the method is relatively simple to use and easy to learn. It is comprehensive, while at the same time not overly time consuming to use". Similarly, RAIB (2019) reports that "using the same approach (i.e. applying the consecutive steps of one SAFRAN iteration) to every factor of the on-going investigation went well" and STSB (2019) states that "the method has the particularity of not being complicated to use". Future tests should somehow allow for a more quantitative measurement to further substantiate these statements.

5.3.3.6 - C.6 Usability

A last criterion, put forward by Underwood (2013) in his evaluation framework, relates to the features that may affect the efficiency and effectiveness of a method. A more concrete interpretation of this criterion can be found with Benner (cited in Speziali and Hollnagel, 2008), who requires an investigation method to be disciplining, functional and definitive. The requirement to be disciplining refers the capability of a method to provide an orderly, systematic framework and a set of procedure to discipline the investigators' task in order to focus their efforts on important and necessary tasks. A similar reasoning can be found with Underwood and Waterson (2013a), who suggest questioning whether a method has a structured application process. Benner's functional requirement aims at helping the investigators to determine which events were part of the accident process as well as those events that were unrelated. Waterson et al. (2015) relate this to the need for a method to support for analysing interactions across system levels. The requirement for a method to be definitive, on the other hand, is explained by the need to provide criteria to identify and define the data that is needed to describe what happened. This could be linked to the requirement to have a taxonomy available that allows for classifying the factors that contribute to an event, as is put forward by several authors (e.g. Hollnagel, cited in Speziali and Hollnagel, 2008; Salmon et al., 2013; Waterson et al., 2015). A last element that relates to the usability of an investigation method, put forward by Salmon et al. (2011), is whether the method is generally applicable and not sector specific.

In its feedback on a first application of the SAFRAN method, RAIB (2019) reports that systematically following the 5 steps for each iteration was useful and introduced rigour into the investigation. Malone (2020) then reports that applying the SAFRAN methods prevents from transforming the investigation into an SMS audit and that "using the 'Function' step in SAFRAN ensured focus remained on the specific SMS section under analysis.". This provides evidence that the SAFRAN method, through its concept, provides guidance on what to look for and in what order for being able to understand each relevant decision and action in the different levels of a socio-technical system, as well as on how to link the different functions across system levels; herewith satisfying both the disciplining and the functional requirement. Finally, the general applicability of the SAFRAN method was explicitly addressed by the study of Flovenz (2020), who validated the method for use in the aviation sector using real safety investigation data and concluding that "the SAFRAN method has shown itself to be well suited for applications to internal aviation safety investigations". Taking into account the similarities in requirements that exist between the different high-risk sectors in which the implementation of a SMS is a legal obligation, it would surprise if this finding is also not valid in other domains where safety risk have to be managed. As for the Resource related criterion, future tests should somehow allow for a more quantitative measurement to further substantiate these statements.

5.3.4. Discussion

The above evaluation against a well-defined set of structured criteria gives clear indication of the potential that the SAFRAN method offers.

The development process of the analysis method (A) started from a precise problem definition (A.1) with the wish to develop an investigation method that can better guide investigators towards a structured analysis of the relevant element of an SMS, and even the wider socio-technical system, as the reason for developing SAFRAN. The modelling approach (A.2) contains different layers. Firstly, the SAFRAN method is built around a unique unit of analysis, called the Safety Fractal, that reflects a generic set of basic requirements that are needed to manage activities at three distinct levels: performance, implementation and control. When applying this unit with resilience performance as the explicit objective underlying these requirements, the focus for managing safety shifts from eliminating threats towards controlling the variability in safety performance. This is also what guides the questioning that forms the investigation logic, with two possible ways of identifying the next process to analyse: firstly, for each of the identified SPV of the previously investigated function, the process that would logically manage this as part of an SMS, and secondly, the process that represents the capability of the system to verify the variability in the performance of the initially investigated function. The possibility to graphically represent the investigation results (A.3) is created through linking triangles, where each side represents one of the three identified levels that can be used to observe an activity. Each triangle, in turn, represents a unique process or activity.

The structured approach that is characteristic of the method allows not only to link the operational findings of an accident in a logical way to the management processes of an SMS but also to the wider regulatory framework. This analysis of a system structure, the relationships of its components and its behaviour, is indicative for a system's approach (Underwood, 2013). Furthermore, by systematically repeating the same questioning at all levels under investigation, SAFRAN guides investigators to understand the context or 'local rationality' of decisions at not only the operational but also the tactical, strategical and policy levels of a socio-technical system. This addresses the need to gain better understanding of management decisions that are contributing to accidents (e.g. Dien et al., 2007) as well as the finding that investigations going outside the border of an organisation and focusing on government and regulators lack appropriate analysis methods (e.g. van Schaardenburgh-Verhoeve et al., 2007). Still, the iterative aspect of the SAFRAN method, when starting from the identified critical variability closest to event sequence, will prevent investigators from overlooking the importance of cognitive issues at the sharp end in favour of those organisational and wider systemic issue; a risk identified by Young et al. (2004) related to the use of Reason's Swiss Cheese Model.

Equally, it was demonstrated that the SAFRAN method also guarantees a systems approach (B), characterised by the capability to cover system structure (B.1), system component relationship (B.2) and system behaviour (B.3). Applying the SAFRAN logic, leads investigators to describe not only the performance of a single function but also a hierarchy of functions, starting from the functions closest to the event under investigation towards functions that can either manage the sources of performance variability or the capability of the related organisations to verify and manage performance variability.

We need to be more critical about the capacity of the used graphical representation to help communicating the findings of an investigation with others. In general, based on feedback when explaining the method to investigators or students with concrete examples, the graphical representation of the findings is perceived as complex. RAIB (2009), when providing feedback on an early application of the method for an on-going investigation, reported that "the investigators are not keen on using the triangle representation that is perceived to be overly complicating the picture". For a large part, this can be related to the trade-off that each time needs to be made between showing an overview on a restricted display and keeping structure in the logic and hierarchy of the findings. This is also reflected in the analysis performed by Flovenz (2020), who reports on a "rapid consumption of space" when using the triangular shapes with related text boxes and a lack of flexibility related to the Microsoft Visio software that is currently used when creating the graphical representations. This is particularly true when more complex incidents or accidents are analysed. Also Malone (2020) reports on similar difficulties to produce graphical illustrations of analysis iterations. The perceived complexity of the current graphical representation led some of the early testers of the method to look for alternative representations (Flovenz, 2020) or to integrate the SAFRAN findings into the graphical representation they are currently using and that is fault-tree inspired (RAIB, 2019). More work is definitely needed to achieve a satisfactory result which provides maximum support for investigators. This experience, in which one has succeeded in integrating the SAFRAN results into existing and already proven techniques, may on the other hand also be an indication for the flexibility of the method.

Also, the evaluation of the usage characteristics (C) of the SAFRAN method reflects on its presumed flexibility and usability. For the accident description (C.1), with the method requiring an already established sequence of events to start the analysis, the initial design of the graphical representation did not take that into account. Flovenz (2020), when evaluating his use of the SAFRAN method, suggests adding a timeline to the graphical representation of the analysis results. He justifies this choice by stating that constructing a timeline enables the investigator to have a point of reference from which to conduct his systemic analysis, even if he or she is not using a sequential method. This idea was picked up for the analysis of the Grayrigg accident, where the physical sequence of events that describes the gradual deterioration of the switches was added (i.e. the boxes with a green lining in Appendix A). Focusing on variability in performance of the system, an initial SAFRAN analysis would only have shown the setting of the residual switch opening and the unsafe state of the switch as starting points for further analysis. In addition, RAIB (2019), when providing feedback on an early application of the SAFRAN method for an on-going investigation, reported that "there were no difficulties transferring the result of the SAFRAN analysis into the RAIB report format".

Again Flovenz (2020) argues that the SAFRAN approach, with its logic of looking at performance variability and its sources "before moving on to work-as-imagined and how the process was conceived" avoids "investigators to assume that the problem originated with the variable human element at the sharp end". This also satisfies the requirement to avoid blame when analysing an event (C.2). With SAFRAN being a "secondary" method, focussing more on the analytical interpretation of an event rather a descriptive reconstruction, compatibility with other methods (C.3) is a prerequisite. This is also reflected in Malone's feedback on applying the SAFRAN method (Malone, 2020): "SAFRAN's focus is SMS investigations, so cannot be compared to other analysis method in terms of how to get to root causes. However, it does complement other analysis methods and should be used as a supplement to them". The SAFRAN method should therefore be used in complement to methods that allow to establish the sequence of events or the physical mechanism that describes an accident. In that context, Malone (2020) notes that "STEP and SAFRAN appear to make good partners to support investigators in understanding causal factors in relation to an effective SMS.". This again is in line with the finding of other authors (Underwood and Waterson, 2013; Farooqi, 2015) that no single technique can cover the complexity of a system and that it is therefore better to use different methods alongside each other in an investigator toolkit.

So far, the way how applying the SAFRAN method could lead to the production of (improved) recommendations (C.4) could not be extensively tested. From a theoretical point of view however, the three degrees of learning "depth", as introduced by Argyris and Schön (1996), correspond nicely with the three sides of the Safety Fractal: improving process performance corresponds with single-loop learning, improving process implementation corresponds to double-loop learning and improving process control corresponds with deutero- or triple-loop learning. This also counters the criticism of Wienen et al. (2017) that applying systemic methods make it harder to formulate corrective measures that can be implemented by management. This idea is supported by Flovenz's finding (2020) that within few iterations with the SAFRAN method he arrived at questions that generated management discomfort, which he considers being a measure of success for systemic methods.

Moreover, applying the SAFRAN method to investigate the different hierarchical layers, will disclose how actions and decisions taken by individuals or teams at all these levels are affected by their local goals, resource constraints and external influences and to discover the "local rationality" of decision and policy makers. This is expected to result in recommendations that address the capability of the entire socio-technical system to manage safety critical variability, leading towards more resilient performance. As such, application of the SAFRAN method promises to create a greater impact on improving global system safety by moving away from the traditionally identified countermeasures that protect a causal link with a barrier, as suggested by Groeneweg (1992), hereby fully embracing the idea that safety is an emergent property. To fully exploit this potential, some additional explanation during the training of users might be required, since Malone (2020) reported she found it "not clear how SMS recommendation are developed, although this could be through verification of SPV's".

The relative easiness of learning and using the SAFRAN method may help to solve the problem of high resource requirements (C.5) that is often assimilated to the existing systemic accident analysis methods (e.g. Wienen et al. 2017). Based on the practice of training investigators in applying the SAFRAN method, different degrees of complexity for understanding how to apply the method for achieving its maximum potential can be recognised. Understanding the basic steps of one iteration is easy and is perceived as being close to the normal accident investigation practice. Making the shift in mindset from failure to performance variability and understanding actions and behaviours in their context, is already a next step in understanding how to adequately apply the method. The last step is then to find "the next function to investigate" and to understand how to apply the investigation logic to move through the different management processes and hierarchical layers of the socio-technical system.

When applied consistently, the SAFRAN method will require various types of data to be collected, first to complete the different steps in one iteration and then similarly from all relevant parts of the socio-technical system. Both Flovenz (2020) and Malone (2020) report that, compared to a less structured investigation, the SAFRAN method quickly brought them to identify the existing framework that is supposed to control and regulate the identified variability. In that context, RAIB (2019) reported that finding the right information to reply to step 2 of a single iteration "is not always as straight forward as one might expect, particularly if there is nothing in place". In their analysis of 55 derailment accident investigation reports, Accou and Carpinelli (2022) also identified that the actual practice of railway accident investigation might lack proper knowledge on human and organisational factors to be able to consistently provide answer to the step 3 of a single SAFRAN iteration. This appears to be even more the case for further iterations. STSB (2019) on the other hand, reports on difficulties in finding relevant information when systematically applying the SAFRAN method for management processes that are more distant from the sequence of events, already from a second iteration onwards. The main cause they see for this is the reluctance of the parties involved to disclose weaknesses in their processes to an (investigation) authority. A similar finding, that interviewees often do not (want to?)

understand the relevance of more in depth SAFRAN guided questions for a specific accident and are therefore reluctant to provide the necessary information, even if available, was informally reported by one investigator after trying to apply the SAFRAN method for an in-company accident investigation. This leads to the conclusion that the usability of a systemic investigation method not only depends on the expertise of the investigators in using the method but also on the understanding of stakeholders for the need to provide the necessary information in order to improve the system.

The structured approach that is characteristic for the SAFRAN method can help to explain the interaction between the different hierarchical layers in the socio-technical system and how they ultimately contribute in controlling critical system variability. But to gain full effect, however, management and other stakeholders would have to be trained in system thinking as well. A last element, related to the use of resources, is the application of a stop rule. Both RAIB (2019) and Flovenz (2020) report that the SAFRAN would benefit from clear criteria or at least guidance on how far to take the analysis. Also Malone (2020) found it difficult to determine when to stop the analysis. The initial investigation logic (chapter 2) proposed to stop the analysis when a major specification issue for a control process was identified that could be corrected, leading the investigation towards the formulation of recommendations that would create sustainable change. As mentioned above, on the other hand, STSB (2019) identified the lack of available information as a natural way of stopping the analysis. Here, also the ability to adapt the method to the scale and scope of the investigation can be considered an asset.

According to Flovenz (2020), "SAFRAN is perhaps the systemic analysis method which best achieves the much-needed compromise between thoroughness and efficiency, which would encourage the more widespread use of systemic analysis methods, especially for internal investigations within organisations.". A warning, however, might be in order here. As argued also above, the SAFRAN method aims at producing recommendations that address the capability of responsible organisations to manage safety critical variability, leading them towards more resilient performance. As such, application of the SAFRAN method promises to create a greater impact on improving global system safety by moving away from the traditionally identified countermeasures that protect a causal link with a barrier (Groeneweg, 1992). Performing this type of analysis, that covers several dimensions of an entire system, requires however knowledge from many different disciplines to interpret data at several strata of complex socio-technical systems (Le Coze, 2013). Following Le Coze's (2013) argumentation, this requirement is more likely to be met when several specialist or experts interact on the same accident analysis. A similar reflection was made in chapter 3, when describing SAFRAN and the related SPV taxonomy as a vehicle to enable non-experts in human and organisational factors to identify the different elements that that introduce variability in (operational) performance and to recognise what additional expertise can be called upon when needed.

Also Flovenz (2022) highlights the possibility to have taxonomies to support the SAFRAN analysis as possible area to increase usability (C.6), in order to guide the investigators "to ask the appropriate question to determine whether such (i.e. human and organisational) factors need to be included or excluded.". Based on similar needs expressed by other investigators that were informally testing the method, it was decided to develop a set of SPV and a related questionnaire (Accou and Carpinelli, 2022) that match the SAFRAN investigation logic. Also Flovenz's (2020) second argument that justifies the development of taxonomies in support of the SAFRAN method, namely to allow classifying the encountered issues for further (statistical) monitoring, has been addressed during the development phase. Rather than just classifying individual factors or combinations of these, the choice was made to try to identify the relevant taxonomies that would allow to classify the entire logic of completed SAFRAN investigations. First reflections show that a combination of the following taxonomies would allow the systematic classification of SAFRAN investigations in the railway domain: a) a list of domain specific events (e.g. collision, derailment, …), b) a list of domain specific operational functions with the potential for performance variability that could lead to an accident (e.g. Ryan et al., 2021), c) a set of elements describing the human and organisational factors that can explain individual actions and decisions that create critical performance variability (e.g. the list of SPV in Accou and Carpinelli, 2022) and d) a list of management functions that could cover the implementation (i.e. train, equip, organise) and control (i.e. specify, verify, adapt) parts of the Safety Fractal. First results of such a classification of investigation result show a high potential for identifying similar patterns in (weaknesses) of safety management and SMS that would not be detected with a more traditional classification of incidents and accident precursors or even contributing factors in databases.

Finally, also training on the methods and corresponding guidance material should help to gain better understanding and increased usability. In particular, the development of concrete examples was an idea that was proposed by several of the participants to already delivered training sessions.

A concluding limitation can be mentioned, more related to the general validation of the method as such: none of the tests performed have yet used the SAFRAN method as a starting point for data collection. This is only partially offset by the testing conducted with on-going accident investigations (RAIB, 2019; STSB, 2019) and specifically also by the work of Flovenz (2020), who, as the original investigator of his case study, was able to provide some answers to additional questions to be posed when applying the SAFRAN method.

As an overall, last comment, it is worth stressing that I do not want give the impression that high-risk industries are in generally unsafe. Consecutive decades of structured risk analysis and safety design have created a solid baseline of safe performance. But (sometimes critical) variability in this performance still exists – and will continue to exist. The remaining challenge is to improve the control of this variability.

5.4. CONCLUSION

Despite the systems approach to accident analysis being the dominant research paradigm and the concept of SMS being introduced in high-risk industries already for several years, accident investigation practice is still poor in analysing the basic elements that compose an SMS and in embracing system theory. In this paper, the different elements that compose the SAfety FRactal ANalysis method are critically evaluated against a set of tested criteria, hereby trying to ensure a high level of practitioner involvement. The element of the method that offers the highest potential to be easily adopted by accident investigation practitioners 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. The structured but also guided approach provides the necessary rigour that will allow to keep a good balance between examining the complexity of a socio-technical system and the restricted availability of resources and people that often limit the possibility for in-depth analysis of accidents. Based on the performed evaluation, I believe that, when it comes to applying a systems approach to accident analysis, with the aim of creating more sustainable and resilient performance, the current investigation practice could gain from applying the SAFRAN method.

Annex 5.1 – Comparing Underwood's evaluation framework with other authors

Underwood (2013) - evaluation framework	**A - Model development process**			**B - Systems approach characteristics**		
	A.1 -Problem definition - Is the reason for creating the model well defined?	**A.2 - Modelling approach selection - What conceptual approach has been adopted?**	**A.3 - System model creation - How is the system graphically represented by the model?**	**B.1 - System structure - How does the model represent a system's hierarchy and component differentiation?**	**B.2 - System component relationships - How are the interactions between system components analysed?**	**B.3 - System behaviour - How does the model address the various factors which affect safety, e.g. controlling the transformation of system inputs?**
Wienen et al. (2017)	-	-	-	-	Does the method takes into account the socio-technical context?	Does the method allows to describe control-feedback loops at different hierarchical levels?

Underwood (2013) - evaluation framework	A - Model development process			B - Systems approach characteristics		
Waterson et al. (2015)	-	-	-	Defining what is meant by a STS approach to safety: identifying the core constructs and elements of STS	The coverage of STS and its application to safety: address external and environmental aspects of the work domain (e.g. regulatory, economic influences on safety) + define boundaries between system elements	-
Underwood and Waterson (2013)	-	-	Does the graphical output of the method help facilitate the analysis (e.g. identify evidence gaps)? Does the method provide a useful means of communicating the findings of an analysis with others?	How complex is the system to be analysed? How much of the system will be analysed?	-	-

Underwood (2013) - evaluation framework	A - Model development process			B - Systems approach characteristics		
Salmon et al. (2011)	-	-	-	Coverage of the overall socio-technical system	Linkage of failures within an between levels	Ability to identify (all of the) contributing factors Identifying complex human decision making and organisational failures
Sklet (2004)	-	To what degree does the method focus on safety barriers?What kind of accident model has influenced the method?	Does the method provide a graphical description of the event sequence?Is the modeling of the system inductive, deductive, morphological or non-system oriented?	The level of scope of the analysis (referring to Rasmussen's 6 levels)	-	-
Benner (1985; cited in Speziali and Hollnagel, 2008)	-	Consistent - Model must be theoretically consistent with an agency's safety program concepts	-	-	-	-

Underwood (2013) - evaluation framework	A - Model development process		B - Systems approach characteristics			
Hollnagel (1998; cited in Speziali and Hollnagel, 2008)	-	Technical basis - Technical content, as the extent to which models generated from within each approach are grounded in a clear identifiable model of human action	-	How well can the method represent the complexity of the actual situation	-	Analytical capability - The ability 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

Underwood (2013) - evaluation framework	**C - Model usage characteristics**					
	C.1 - Timeline consideration - How does the model incorporate the concept of time in the accident development process?	**C.2 - Avoidance of blame - Does the model direct the analyst towards identifying a root cause?**	**C.3 - Model compatibility - Can the model be used in conjunction with other analysis techniques?**	**C.4 - Recommendation production - Does the model aid the analyst in producing safety recommendations and provide generic insights into accident causation?**	**C.5 - Resources required - What resources and data does the analysist require in order to use the model?**	**C.6 - Usability - What features of the model affect the analysis efficiency and effectiveness?**
Wienen et al. (2017)	Does the method provides a comprehensive and clear picture that paints the narrative of the accident?	-	-	Can produced recommendations persuade management ot take action?	Is the method easy to understand? What time/effort is needed to perform the analysis?	-
Waterson et al. (2015)	-	-	-	-	Many methods prove to be difficult to use, time consuming and require a lot of training	The usability of the method (to be used in a STS context): need to provide support for analysing interactions accross system levels

Underwood (2013) - evaluation framework	C - Model usage characteristics					
Underwood and Waterson (2013)	-	-	-	Does the method provide a useful means of communicating the findings of an analysis with others?	How easy is the method to understand and use? How much usage guidance is available? What resources are required to use the method (e.g. specialist software)?	How reliable is the method? Does the method have a structured application process? Does the method have a taxonomy of factors which contribute to an accident?
Salmon et al. (2011)	-	-	-	Support the development of appropriate, system-wide countermeasures, as opposed to individual operator focused ones	-	Possibility to use/ availability of taxonomies (+/- aspects) Generally applicable (i.e. not sector-specific)
Sklet (2004)	-	-	Is the method a primary or a secondary method?	-	-	-

Underwood (2013) - evaluation framework	**C - Model usage characteristics**					
Benner (1985; cited in Speziali and Hollnagel, 2008)	Realistic - The investigation should result in a realistic description of the events that have actually occurred Comprehensive - There is no confusion about what happened, no unsuspected gaps or holes in the explanation and no conflict of undestanding among those who read the report	Non-causal - Conducted in a non-causal framework and result in an objective description of the accident description of the accident process event; attribution of cause or fault can only be considered seperate from, and after the understanding of the accident process is completed to satisfy the criterion	-	Satisfying - The results should be satisfying for those who initialised the investigation and other individuals that demand results from the investigations Direct - Provide results that do nor require collection of more data before the needed controls can be identified and changes made	-	Definitive - Provide criteria to identify and define the data that is needed to describe what happened Disciplining - 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 Functional - Make the job efficient, e.g. by helping the investigators to determine which events were part of the accident process as well as those events that were unrelated

Underwood (2013) - evaluation framework	**C - Model usage characteristics**					
Hollnagel (1998; cited in Speziali and Hollnagel, 2008)	Audit capabilities - Is it possible to retrace the analysis and reconstruct the choices, decisions, or categorisations made during the analysis Produce an adequate explanation or account of why and adverse event (an accident or an incident) occurred	-	-	-	Practicality - The ease with which each approach can be turned into a practical method or made operational Cost-effectiveness - The relative costs and benefits associated with the method Time to learn - How long time does it take to learn to use the method and to become a proficient user. (H) Resources needed - How difficult/easy is it to use the method. Among the main resources are people (hours of work), time, information and documentation needs, etc.	Relation to existing taxonomies - The extend to which the method is linked to viable systems fro classifying the erroneaous actions that occur in a real-world processing environment

EPILOGUE

The concept of a safety management system (SMS) to control the risks of operational activities has already been introduced in high-risk industries some decades ago. Nevertheless, this SMS is often criticized as burdensome and complex. Through its requirement to formalise all main activities, the SMS is perceived as bureaucratic and as a vehicle for pure compliance and Safety I (one). Furthermore, the SMS is often perceived as detached from an organisation's core and operational activities, going against local practice and it is questioned whether it can deliver the safe performance that was hoped for.

By comparing the model behind SMS with specific requirements for process capability, this research has identified a Safety Fractal that reflects the basic requirements that are needed to control safety related activities at all levels within an organisation, herewith providing an answer to the first research question:

- Q1 – *How can generic SMS requirements be better integrated to improve (the management of) operational performance?*

The Safety Fractal, as a unique unit of analysis, identifies three distinct levels to observe the functioning of a process: A first level of process performance represents the direct functioning of the components that interact during process execution. This is also the level where variation in relation to process specifications and/or expectations can be observed. A second level of process implementation provides the resources and means to ensure the correct functioning of the process components during process execution. And finally, a third level of process control ensures the sustainable control of risks related to all activities of the organisation.

By steering the main part of this research in the direction of accident investigation, no attempt was made to formally validate the Safety Fractal as an instrument to improve safety management at the operational level. This was partly counterbalanced, however, by testing the final outcome against a wide range of models used for auditing SMSs (e.g. Kuusisto, 2000; Cambon, 2007, Peltonen, 2013) and wider business and process management models (e.g. Verweire and Van den Berge, 2004; Hardjono and Bakker, 2006; Verweire, 2014). In addition, the model has been practically used in different operational settings over the last years going from implementing over auditing to investigating processes in an SMS context. Although not to be considered as controlled experiments, none of the above experiences gave reason to question the basic elements of the Safety Fractal. On the contrary, it became clear that attention to the systematic control (and to a lesser extent the implementation) of operational activities is often lacking and would benefit from a more structured approach.

While Dechy et al. (2012) argue that the generic issues of organising work and managing safety are similar, whether analysed before or after an event, and these similarities are the key points that could guide data collection, analysis and interpretation, the possibility to apply the Safety Fractal in such a proactive manner, for example via audits, has not been further elaborated until now. By systematically covering the three layers of looking at performance that were identified in the Safety Fractal (i.e. perform, implement and control), one could hope to overcome the 'eyes wide shut' misguided faith in SMSs that is driven by pure compliance audits as reported in Beausang's (2019) worrying but also for railways recognisable glimpse into the safety management practice of the aviation sector. In the same context, an interesting path for further research could be to analyse the optimal level of "Safety Proceduralisation" (Bourrier and Bieder, 2013) related to the specify-control step in the Safety Fractal for different hierarchical levels in a socio-technical system.

Furthermore, part of the conducted research has given clear indication that the constituent elements of this Safety Fractal, and herewith the concept of SMS, appear to be particularly suitable for organising resilient performance, provided that a strategy that embraces adaptive cultures and performance variability is explicitly identified as the safety strategy to follow and, as such, consequently implemented. While positioning this approach alongside common safety management concepts like management system maturity, leadership and safety culture, the Extended Safety Fractal was developed, leading to a systematic and a more comprehensive view on how to approach and measure safety performance and the basic elements of resilience. This provides an answer to the second research question:

Q2 – *Can the concept of SMS contribute to the new perspective(s) on safety management?*

In general, these findings substantiate the statement made earlier by Pariès and al. (2019) that several safety strategies can fit within an SMS framework, describing the SMS as defining the "piping" of the system, generating safety. This pipework is presented in contrast to the safety strategy, i.e., the models or theories that can help us making sense of the diversity that can be observed in the real world, as the substance that "should flow through the pipes". Traditional SMS standards are certainly based on underlying elements of such a strategy (e.g. the idea of continuous improvement) but without making them explicit and keeping them hidden within more formal requirements.

Measuring the effectiveness of an SMS or its processes is seen by several authors as a way to better capture the true safety state of an evolving organisation (e.g. Hale et al. 1997; Groeneweg, 1992). Cambon (2017) identifies three traditional ways of measuring SMS performance: (1) the analysis of achieved results, (2) the analysis of the approach that is used for setting up the SMS and (3) the comparison of an SMS with an existing reference. The same author also identifies three fundamental attributes of an SMS that need to be captured in order to be able to build a picture of SMS performance: (1) the degree of SMS formalisation, (2) the quality of the implementation and (3) the level of ownership of the SMS by members of the staff in the organisation, taking into account the more informal aspect. Lofquist (2017), on the other hand, when making a case for building resilience into SMSs, proposes two areas that can improve the measurement of effectiveness in an SMS in order to capture the signals of drift (Dekker, 2011) towards and beyond the system’s safe boundaries: (1) the functioning of reporting systems and (2) (improved) safety climate surveys, an idea that also Johnsen (2010) promotes. A similar conclusion is made by Hale et al. (2006), who state that SMS audit tools can provide the hooks to assess resilience, provided that a closer coupling can be made between the traditional SMS structure and safety culture. None of these proposals, however, cover the entire Extended Safety Fractal that summarises a wider set of essential elements needed for an organisation to come to a sustainable, safe and resilient performance and which is believed to be the necessary scope for measuring the effectiveness of the safety management of a complex system. Therefore, the potential of this Extended Safety Fractal and possible matching techniques to paint a broader picture of an organisation's status to manage safety in a sustainable way also seems to be an interesting avenue for future research. An initial experience to develop adapted supervision strategies using the basic ideas of the Extended Safety Fractal, together with some national safety authorities within the European railway sector, promises positive results in that regard (Haug and Accou, 2021).

As expressed by Several authors (e.g. Denyer, 2017; Pariès et al. 2019) such supervision will require explicit focus on an organisation’s safety strategy. While the current research project has taken resilience as the reference strategy, Grant et al. (2018) have identified an interesting set of essential characteristics related to system performance, which may provide a suitable approach for predicting system states and can help in identifying an overall safety strategy. Measuring the effectiveness of safety management will then require assessing how the different elements of the Extended Safety Fractal are aligned to implement that strategy, in order to fit the specific mission and sector. A similar focus on the need for strategic alignment can be found in the integrated performance management framework presented by Verweire (2014) as a prerequisite for excellent performance.

Even though the systems approach to accident analysis is the dominant research paradigm and the concept of SMS has already been mandatory in most high-risk industries for several years, accident investigation practice is still poor at analysing the basic elements that compose an SMS and in embracing system theory. The scope of accident and incident investigations usually stays limited to investigating the immediate causes and decision-making processes related to the accident sequence. Important factors, including design and planning decisions, contributing to accidents are hereby often overlooked and the weaknesses in the SMS are hardly ever analysed. As a direct consequence, the opportunity to use these investigations for introducing sustainable system changes is often missed. The main objective of this research project was therefore expressed in the third research question and the related follow-up questions that arose during the project:

- *Q3 - What accident and incident analysis method can guide investigators to identify those elements of the SMS where interventions might have the greatest impact for improving system safety.*
- Q3.1 – *How can non-human and organisational factors experts be guided to identify HOF elements during accident investigations?*
- Q3.2 – *How can an investigator be guided to analyse the SMS and wider system functions in a structured way?*

In reply to these questions, the SAfety FRactal ANalysis (SAFRAN) method is introduced as a combination of an investigation flow and a graphical representation that is complementing the Safety Fractal. The method offers a structured way to systematically identify human and organisational factors throughout a socio-technical system, more closely aligned to the logic of accident investigation practice than other systemic methods. Starting from the critical variability close to an accident, the application of the method guides investigators in analysing the state of the entire system in its capability to monitor and control this variability. It shows them a structured and iterative way to move from analysing a single event into analysing the wider socio-technical system around it. The essence of using the SAFRAN method for evaluating the performance of the different processes in a socio-technical system, is to approach them in a similar way, building on the generic elements that compose an SMS and systematically looking at the HOF that influenced actions and decision making, regardless of the hierarchical level they are situated at. For investigators, the 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. By doing so, the SAFRAN method is designed not only to allow combining human analysis with a systems-oriented analysis but, in addition, to generate the necessary analytical trail to better communicate the results of such an analysis and to bring forward more demonstrable elements that might convince decision makers to adapt the system.

Rather than following a chain of causal reasoning or trying to reconstruct conditions that may no longer exist, the effort is put in assessing the capability of organisations to manage (critical) variability and thus the actual day-to-day functioning of the socio-technical system. This results in a systemic method for accident analysis that is easily applicable and less resource demanding than the current methods, which often restricts the possibility for in-depth analysis of accidents. This element is reinforced by the relative easiness of learning and using the SAFRAN method and the ability to adapt the method to the scale and scope of the investigation. Moreover, to overcome the practical difficulties several investigation practitioners have encountered in answering the essential third step in the SAFRAN method, additional guidance has been developed to help investigators identify at least the relevant HOF elements and recognise the need to call for further expertise.

It has proven to be very difficult to explicitly validate the developed SAFRAN method with a controlled experiment within the time frame of this project. This would have been possible by teaching investigators to independently apply the method to a large series of occurrences and then analyse whether the resulting recommendations are different from the current investigation practice and address elements that could lead to more sustainable changes of the system under investigation. So far, none of the contacted organisations finally accepted to enter such a project, mostly due to practical and resources constraints. Still, I can't help but feel that often also other known pathogens that stand in the way of learning (ESReDA, 2015) may have played a part in these decisions. Performing an in-depth analysis of HOF and SMS elements in a company or wider socio-technical system requires clearly more than just an analytical tool; it requires understanding and support from involved parties as well as decision-takers at all levels.

As an alternative, to validate the method, a series of practical tests, often involving active accident investigators, made it possible to examine the SAFRAN method against a set of carefully selected and recognised criteria for evaluating systemic accident analysis models and methods. A large set of publicly available investigation reports was ordered in a SAFRAN-logic, identifying paths of further investigation -with concrete questions- that could have been identified when strictly applying the SAFRAN method. This includes also the analysis of the 2007 Grayrigg train derailment, similar to what Underwood and Waterson (2013) did to compare the ATSB, AcciMap and STAMP investigation methods. Inspired by Groeneweg et al. (2010), who asked investigators of the Dutch Safety Board to re-investigate six of their investigations to test an extended version of the Tripod method, two Master students at Cranfield University have applied the SAFRAN method in order to compare the results with the in-company investigation they had performed before. In addition, during the different phases of development of the method, a number of students as well as active investigation practitioners were trained in using the SAFRAN method. Although the received feedback was not consistently gathered in a formal way, this gave good insight in how difficult or easy it is to understand the method and what time and effort is needed to learn to apply the SAFRAN method. Some of these investigators also freely provided useful feedback after first applications of the method. This was especially the case for the Swiss Transportation Safety Investigation Board (STSB) and UK's Rail Accident Investigation Branch (RAIB), with whom separate feedback sessions were organised. Nevertheless, it should be recognized that this way of working clearly has limitations. Due to my own active participation throughout the whole validation process, it often proved difficult to maintain a strict approach and the rigour required for fundamental research. A possible lack of self-criticism in the evaluation and validation of the proposed models and methods is also a pitfall associated with the approach used. I can only hope that the professionalism of the many experts involved as well as the multitude of tests carried out have provided the necessary counterweight to this. In any case, they frequently provided feedback was carefully taken into account in order to continuously adapt the proposed methods to the needs of investigators from the field.

Overall, the performed evaluation gives clear indication that the SAFRAN method, more than other methods, allows not only to link the operational findings of an accident in a logical way to the management processes of an SMS but also to the wider regulatory framework, which obviously satisfies the reason the method was developed.

It was recognised during the development and testing of the SAFRAN method that it 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, 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; Farooqi, 2015) that no single technique can cover the complexity of a system and that it may be better to use different methods alongside each other in an investigator toolkit. In that context, Malone (2020) notes that "STEP and SAFRAN appear to make good partners to support investigators in understanding causal factors in relation to an effective SMS.". Further research could exploit this finding and identify other techniques for the investigator's toolkit.

Staying closer again to the scope of the SAFRAN developments so far, ultimately, the goal of accident investigation is still to come up with recommendations that can improve the system in a sustainable way. In that context, several authors (e.g. Cook, 2000) argue that the traditional views of "cause" and the efforts to prevent individual sub-standard acts limit the effectiveness of defenses against future events. The focus should rather be on the state of the organisation and related error-generating mechanisms (Groeneweg, 1992). The clear parallel between the different levels in a Safety Fractal to evaluate activities, looking for the capability of an organisation to monitor and manage safety critical variability, and the 3 different loops for organisational learning (Argyris and Schön, 1996), as described in chapter 5, may offer an interesting avenue for further research into the effectiveness of recommendations in a domain where little research has been done until now.

Based on the reviewed investigation reports, it's a clear finding that the actual depth of analysis into leadership, safety management, vision and culture is limited. The potential of the SAFRAN method for classifying HOF related elements as well as doing this systematically and traceably for all hierarchical levels in a socio-technical system, as suggested in several of the chapters when analysing real cases, could therefore also be an interesting avenue for future research. Are the same or similar factors influencing decisions and actions at different hierarchical levels and what can we learn from this to support accident investigators in collecting relevant findings?

Furthermore, with the increasing digitalisation of railways and initiatives like Big Data Risk Analysis (e.g. Figueres-Esteban et al., 2018) turning the SMS more and more into a data-driven system, there is a risk that large data collection and analysis efforts create a safety picture that is disconnected from front-line activities (Beausang, 2019). The SAFRAN investigation logic, with the unlimited possibility to iterate the same elements, could offer a simple solution for creating an ontology that can help to extract safety information from accident and incident investigation reports (e.g. Hughues et al., 2019).

Finally, progress can also be made in further testing and promoting the practical application of the SAFRAN method. Different elements of the proposed models and methods would definitely benefit from a more formal empirical evaluation regarding consistency of interpretation and repeatability of analysis. This is in particular true for use of the proposed classification by non-HOF experts. The development of a manual that explains the various underlying concepts and the steps to be followed in a comprehensible manner is undeniably a first initiative that must be taken in that direction. In addition, the continuing demand for practical and realistic examples that illustrate the application of the method in concrete terms should also be taken into account. Finally, a last element suggested by several of the users, is the development of supporting material, possibly via a computer application, to guide the investigators in following and visualising the method.

Although the writing of this overview closes an important chapter in its development, it doesn't feel like the end of the SAFRAN project. The positive reactions to the application of the method and the models developed rather lead to a set of ideas for its continuation.

In addition, as expressed above, a number of topics that were opened in the published articles have so far been underexposed due to lack of time and resources. I hope these will prove to be valid avenues for further research. I am therefore impatiently looking forward to the next steps that will be taken in this dynamic and personally very rewarding project.

ABOUT THE AUTHOR

As a civil engineer in construction, graduated in 1992 from the Vrije Universiteit Brussel, Bart started his career at the Belgian railways (SNCB) in 1993, with the construction of the Eurostar terminal in the Brussels-Midi station. In 1994 he joined SNCB's internal audit team where he reported to the CEO and the Board on procurement and other operational processes. From 2005 on he was responsible for the team that was auditing the safety management systems of both Infrabel (the Belgian infrastructure manager) and SNCB.

Bart joined the European Railway Agency in September 2008 a first time as project officer, working on classifying railway accident causes and guidance for writing accident investigation reports. In October 2009 he became head of the safety certification sector, in charge of the harmonisation of the activities, of National Safety Authorities and National Investigating Bodies, running their European network and developing an assessment scheme for monitoring their activities.

From June 2013 to June 2017 Bart was Head of Methods and Safety at Infrabel, where he was developing and implementing an integrated risk management system. In June 2017, Bart rejoined the European Union Agency for Railways, where he is currently leading the Safety and Operations Unit. The concept of Safety Management Systems, accident and incident analysis, human and organisational factors and safety culture are his main domains of professional interest.

REFERENCES

1. Accident Investigation Board Norway (AIBN). 2018, The AIBN Method – Framework and Analysis Process for Systematic Safety Investigations.
2. Accou, B.; Reniers, G., 2019. Developing a method to improve safety management systems based on accident investigations: The Safety Fractal Analysis. Safety Science 2019, 115, 185–293.
3. Accou, B.; Reniers, G., 2019. Analysing the depth of railway accident investigation reports on over-speeding incidents, using an innovative method called "SAFRAN". In Accident Investigation and Learning to Improve Safety Management in Complex System: Remaining Challenges. Proceedings of the 55th ESReDA, Seminar, Bucharest, Romania, 9–10 October 2018; European Commission: Brussels, Belgium.
4. Accou, B., Reniers. G. 2020, Introducing the Extended Safety Fractal: reusing the concept of Safety Management Systems to organise resilient organisations. International Journal of Environmental Research and Public Health.
5. Accou, B., Carpinelli. F., 2022. Systematically investigating human and organisational factors in complex socio-technical systems by using the "SAfety FRactal ANalysis" method. Applied Ergonomics, 100 (2022) 103662.
6. Accou, B., Reniers. G. 2022, Using the SAfety FRactal ANalysis method to investigate human and organisational factors beyond the sharp end. A critical socio-technical analysis of the Santiago de Compostela train crash investigation. Safety Science xyz, abc-def (to be published).
7. Agnew, J.; Daniels, A., 2010. Safe by Accident? Take the LUCK out of SAFETY: Leadership Practices that Build a Sustainable Safety Culture; Performance Management Publications: Atlanta, GA, USA, 2010.
8. Amalberti, R., 2001. The paradoxes of almost safe transportation systems. Safety Science 2001, 37, 109–126.
9. Amalberti, R., 2013. Piloter la Sécurité–Théories et Pratiques sur les Compromise et les Arbitrages Nécessaires; Springer-Verlag France: Paris, France.
10. Antonsen, S., 2009. Safety Culture: Theory, Method and Improvement; Ashgate Publishing Limited: Farnham, UK.
11. Antonsen, S. 2009, Safety culture and the issue of power. Safety Science 47, 183–191.
12. Antonsen, S., Nilsen, M., Almklov, P.G. 2016, Regulating the Intangible, Searching for safety culture in the Norwegian petroleum industry. *Safety Science,* 92, 232-240.
13. 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.
14. Argyris, C.; Schön, D.A., 1996. Organisational Learning II-Theory, Method, and Practice; Addison-Wesley Publishing Company: Boston, MA, USA.
15. Australian Transport Safety Board (ATSB). 2008, Analysis, Causality and proof in Safety Investigations. Aviation Research and Analysis Report – AR-2007-053.
16. Balfe, N., Geoghegan, S., 2017. Human factors applications of On-Train-Data-Recorders. Sixth International Human Factors Rail Conference, Book of Proceedings, 152-161.
17. Beausang, D., 2019, Eyes Wide Shut: Seeing the Safety Management System as a State. Master thesis, Lund University.

18. Bernard, B. 2014, Safety Culture as a way of Responsive Regulation: proposal for a nuclear safety culture oversight model. *International Nuclear Safety Journal*, vol.3 issue 2, 1-11.
19. Borys, D., Dennis, E., Leggett, S., 2009. The fifth age of safety: the adaptive age. Journal of Health & Safety Research & Practice. Volume 1, issue 1, 2009.
20. Bottani, E.; Monica, L.; Vignali, G., 2009. Safety management systems: Performance differences between adopters and non-adopters. Safety Science, 47, 155–162.
21. Bourrier, M.; Bieder, C. 2013. Trapping Safety into Rules: An Introduction. In Trapping safety into rules: How Desirable or Avoidable is Proceduralization, Bieder, C., Bourrier, M., Eds.; Ashgate Publishing Limited: Farnham, UK, pp. 1–9.
22. Cambon, J., 2007. Vers Une Nouvelle Méthodologie de Mesure de la Performance des Système de Management de la Santé-Sécurité au Travail; École Nationale Supérieure des Mines de Paris: Paris, France.
23. Carpinelli, F., Rebentisch, M., Accou, B., 2021, Training for Investigating Human and Organisational Factors (HOF) in Railways. Communication in preparation for the Seventh International Human Factors Rail Conference, 2021, London.
24. Cook, R. 2000, How Complex Systems Fail. Cognitive technologies Laboratory. University of Chicago.
25. Cooper, M.D. 2000, Towards a model of safety culture. Safety Science 36, 111-136.
26. Cooper, M.D. 2016, The Safety Culture Construct: Theory and Practice. In C. Bieder & B. Journé, H. Laroche, C. Bieder (Ed.), *Safety Cultures, Safety Models, Taking Stock and Moving Forward*. Springer Briefs in Applied Sciences and Technology.
27. Cooper, M.D., 2022. The Emperor has no clothes: A critique of Safety-II. Safety Science 152 (2022), 105047.
28. Costella, M.F.; Abreu Saurin, T.; Buarque de Macedo Guimarães, L., 2009. A method for assessing health and safety management systems from the resilience engineering perspective. Saf. Sci., 47, 1056–1067.
29. Cullen, The Hon. Lord, 1990. The public inquiry into the Piper Alpha disaster. The Department of Energy. Vol 1-2.
30. Czech, B.A., Groff, L., Straunch, B., 2014. Safety cultures and accidents investigation: Lessons learned from a National Transportation Safety Board Forum, Adelaide Australia.
31. Daniellou, F.; Simard, M.; Boissières, I., 2010. Les Cahiers de la Sécurité Industrielle. In Facteurs Humains et Organisationnels de la Sécurité Industrielle: Un État de l'art; Institut pour une Culture de Sécurité Industrielle (ICSI): Toulouse, France.
32. Daumal, S. 2018, Design d'expérience utilisateur, Édition Eyrolles, 3ème édition.
33. Dechy, N., Rousseau, J.-M., Llory, M., 2012. Are organisational audits of safety that different from organisational investigations of accidents? In Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds). Taylor & Francis Group, London.
34. De Cnudde, Ph.; Hindryckx, B.; Bauwens, M.; Carrette, B.; Verweire, K., 2004. Introducing Maturity Alignment: Basic Concepts. In Integrated Performance Management–A Guide to Strategy Implementation, Verweire, K., Van Den Berghe, L., Eds.; Sage Publications: Thousand Oaks, CA, USA; pp. 275–292.
35. 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).

36. Dekker, S. 2006, The Field Guide to Understanding Human Error. Ashgate Publishing.Dekker, S., 2011. Drift into Failure: From Hunting Broken Components to Understanding Complex Systems; Ashgate Publishing: Aldershot, UK.
37. Dekker, S., 2011. Drift into Failure: From Hunting Broken Components to Understanding Complex Systems; Ashgate Publishing: Aldershot, UK.
38. Dekker, S., 2014. The psychology of accident investigation: epistemological, preventive, moral and existential meaning making. Theoretical issues in Ergonomics Science.
39. Dekker, S. Cilliers, P., Hofmeyr, J.-H. 2011, The complexity of failure: Implications of complexity theory for safety investigations. Safety Science 49, 939-945.
40. Del Frate, L., Zwart, S.D., Kroes, P.A., 2011. Root cause as a U-turn. Engineering Failure Analysis 18 (2011), 747-758.
41. Denyer, D., 2017. Organisational Resilience: A Summary of Academic Evidence, Business Insights and New Thinking; BSI and Cranfield School of Management: Bedford, UK.
42. Deschoolmeester, D.; Braet, O., 2004. Strategic Information Systems Alignment. In Integrated Performance Management: A Guide to Strategy Implementation, Verweire, K., Van den Berghe, L., Eds.; Sage Publications: Thousand Oaks, CA, USA, pp. 135–151.
43. Dien, Y., Llory, M., Montmayeul, R., 2004. Organisational accident investigation methodology and lessons learned. Journal of Hazardous Materials, 111 (2004), 147-153.
44. 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.
45. Dul, J., Bruder, R., Buckle, P., Carayon, P., Falzon, P , Marras, W. S., Wilson, J.R., van der Doelen, B. 2012, A strategy for human factors/ergonomics: developing the discipline and profession, Ergonomics, 55:4, 377-395.
46. Dul, J. and Neumann, W.P., 2009. Ergonomics contributions to company strategies. Applied Ergonomics, 40 (4), 745–752.
47. 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.
48. ERAIL, https://data.europa.eu/euodp/fr/data/dataset/erail-safety-indicators
49. EUROCONTROL, European Organisation for the Safety of Air Navigation 2014, Systems Thinking for Safety: Ten Principles. A White Paper. Moving towards Safety-II.
50. EU, 2018, COMMISSION DELEGATED REGULATION (EU) 2018/762 of 8 March 2018 establishing common safety methods on safety management system requirements pursuant to Directive (EU) 2016/798 of the European Parliament and of the Council and repealing Commission Regulations (EU) No 1158/2010 and (EU) No 1169/2010. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0762&from=EN (accessed on 19 August 2021)
51. EU, 2020, COMMISSION IMPLEMENTING REGULATION (EU) 2020/572 of 24 April 2020 on the reporting structure to be followed for railway accident and incident investigation reports. Available online: EUR-Lex - 32020R0572 - EN - EUR-Lex (europa.eu) (accessed on 19 August 2021)
52. EU, DIRECTIVE (EU) 2016/798 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on railway safety (recast). available online at:
53. https://eur-lex.europa.eu/legal-content/fr/TXT/ ?uri=CELEX%3A32016L0798

54. EU, DIRECTIVE 2004/49/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive). - available online at:
55. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32004L0049
56. European Safety, Reliability & Data Association (ESReDA), 2015. Barriers to learning from incidents and accidents. ESReDA Guidelines, http://www.esreda.org/.
57. Farooqi, A.T., 2015. Methods for the Investigation of Work and Human Errors in Rail Engineering Contexts. PhD Thesis, University of Nottingham.
58. Faste, T., Faste, H., (2012). Demystifying "Design Research": Design is not research, research is design. IDSA Education Symposium 2012, Boston.Gelfand, M., 2019. Rule makers, rule breakers: Tight and loose cultures and the secret signals that direct our lives. Scribner
59. Faverge, J.-M., Leplat, J., Guiguet, B. 1958, L'adaptation de la machine à l'homme, Edité par P.U. F, Paris.
60. Figueres-Esteban, M., Hughes, P., El Rashidy, R.A.H., van Gulijk C., 2018. Manifestation of ontologies in graph databases for big data risk analysis. In Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds). Taylor & Francis Group, London.
61. Fitts, P.M. (Ed.) 1951, Human engineering for an effective air-navigation and traffic-control system. NRC Comitte on Aviation Psychology, National Research Council, Washington, D.C.
62. Flovenz, G., 2020. Investigating SMS – A problem of methodology. School of aerospace, transport and manufacture. Safety and Accident Investigation (Air Transport). MSc Thesis.
63. Fowler, D., 2013. Proceduralization of safety Assessment: A Barrier to Rational Thinking. In Trapping Safety into Rules: How Desirable or Avoidable is Proceduralization, Bieder, C.; Bourrier, M., Eds.; Ashgate Publishing Limited: Farnham, UK, pp. 87–106.
64. French, S., Steel, T. 2018, The investigation of Safety Management Systems and Safety Culture. ITF Discussion Paper 2017-20. OECD/ITF 2017.
65. French, S., Steel, T. 2018, Looking beyond the obvious – the investigation of organisational factors following a railway accident. International Railway Safety Conference, Dublin.
66. Geertz, C. 1973, The interpretation of cultures, New-York: Basics Books.
67. Gibson, H., Mills, A., Gregory, J., Harrison, C., Woods, M. 2017, The Role of Human Factors in Supporting Safety Learning from Railway Incidents. International Railway Safety Council, Hong Kong.
68. Grant, E., Salmon, P.M., Stevens, N., Goode, N., Read, G., 2018. Back to the future: What do accident causation models tell us about accident prediction? Safety Science 104, 99-109.
69. Groeneweg, J., 1992. Controlling the Controllable: The Management of Safety; DSWO Press, Leiden University: Leiden, The Netherlands.
70. 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.
71. Grote, G. 2012, Safety management in different high-risk domains - All the same? *Safety Science* 50, 1983-1992.
72. Grote, G. 2014, Adding a strategic edge to human factors/ergonomics: Principles for the management of uncertainty as cornerstones for system design. *Applied Ergonomics*, 45, 33-39.

73. Grote, G. 2019. Leadership in Resilient Organisations. In S. Wiig & B. Fahlbruch (Ed.), *Exploring Resilience, A Scientific Journey from Practice to Theory.* Springer Briefs in Applied Sciences and Technology
74. Grote, G.; Weichbrodt, J., 2013. Why Regulators Should Stay Away from Safety Culture and Stick to Rules Instead. In Trapping Safety into Rules: How Desirable or Avoidable is Proceduralization, Bieder, C., Bourrier, M., Eds.; Ashgate Publishing Limited: Farnham, UK, pp. 225–240.
75. Groupe d'échange ICSI "Analyse d'Événement". 2013, Numéro 2014-04 de *Cahiers de la Sécurité Industrielle*. Institut pour une Culture de Sécurité Industrielle, Toulouse, France (ISSN 2100-3874).
76. Guldenmund, F.W., 2015. Organisational safety culture. In the Wiley-Blackwell Handbook of the Psychology of Occupational Safety and Workplace Health, Clarke, S., Probst, T., Guldenmund, F., Passmore, J., Eds.; John Wiley & Sons Ltd.: Chichester, UK.
77. Haavik, T.K.; Antonsen, S.; Rosness, R.; Hale, A., 2019. HRO and RE: A pragmatic perspective. Safety Science, 117, 479–489.
78. Hale, A.R., 2000. Culture's confusions. Safety Science 34 (2000), 1-14.
79. Hale, A.; Borys, D., 2013. Working to Rule, or Working Safely. In Trapping Safety into Rules: How Desirable or Avoidable is Proceduralization, Bieder, C., Bourrier, M., Eds.; Ashgate Publishing Limited: Farnham, UK, pp. 43–68.
80. Hale, A.R., Heming, B.H.J., Carthey, J., Kirwan, B., 1997. Modelling of Safety Management Systems. Safety Science, Vol. 26, No 1/2, pp. 121-140.
81. Hale, A.; Guldenmund, F.; Goossens, L., 2006. Auditing Resilience in Risk Control and Safety Management Systems. In Resilience Engineering: Concepts and Precepts, Hollnagel, E., Woods, D.D., Leveson, N., Eds.; Ashgate Publishing Limited: Aldershot, UK, pp. 289–314.
82. Hardjono, T.W., Bakker, R.J.M., 2006. Management van Processen: Identificeren, Besturen, Beheersen en Vernieuwen (Derde, Geheel Herziene Druk); Kluwer, Dortdrecht, The Netherlands
83. Haug, M., Accou, B., 2021. Developing a framework for the oversight of safety culture. Proceeding of the Seventh International Human Factors Rail Conference. RSSB.
84. Herrera, I.A.; Hollnagel, E.; Habrekke, S., 2010. Proposing safety performance indicators for helicopter offshore on the Norwegian Continental Shelf. Presented at PSAM, Seattle, WA, USA, 7–11 June 2010.
85. 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.
86. Hollnagel, E., 1998. Cognitive Reliability and Error Analysis Method (CREAM); Elsevier Science Ltd.: Amsterdam, The Netherlands.
87. Hollnagel, E., 2002. Understanding Accidents-From Root Causes to Performance Variability. In Proceedings of the 2002 IEEE 7th Conference on Human Factors and Power Plants, Scottsdale, AZ, USA, 19 September 2002.
88. Hollnagel, E., 2004. Barriers and Accident Prevention. Aldershot, UK, Ashgate.
89. Hollnagel, E., 2008. From protection to resilience: Changing views on how to achieve safety. In Proceedings of 8th International Symposium of the Australian Psychology Association, Sidney, Australia, 8–11 April 2008; p. 7.
90. 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).

91. Hollnagel, E., 2009 The four cornerstones of resilience engineering. In Preparation and Restoration, Nemeth, C.P., Hollnagel, E., Dekker, S., Eds.; Ashgate: Aldershot, UK, pp.117–134.
92. Hollnagel, E., 2009. The ETTO Principle: Efficiency-Thoroughness Trade-Off-Why Things That Go Right Sometimes Go Wrong; Ashgate Publishing: Aldershot, UK.
93. Holnagel, E., 2012. FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems; Ashgate Publishing Ltd.: Aldershot, UK.
94. Hollnagel, E. 2014, Human factors/ergonomics as a systems discipline? "The human use of human beings" revisited. Applied Ergonomics, 45, 40-44.
95. Hollnagel, E., 2014. Safety-I and Safety-II: The Past and Future of Safety Management; Ashgate Publishing: Farnham, UK.
96. Hollnagel, E., 2018. Safety-II in Practice: Developing the Resilience Potentials; Routledge: Abingdon, UK.
97. Hollnagel, E.; Woods, D.D.; Leveson, N., 2006. Resilience Engineering: Concepts and Precepts; Ashgate Publishing Limited: Aldershot, UK.
98. Hollnagel, E., Speziali, J., 2008. Study on Developments in Accident Investigation Methods: A Survey of the "State-of-the-Art". SKI Report 2008:50.
99. Hughes, P., Robinson, R., Figueres-Esteban, M., van Gulijk C., 2019. Extracting safety information from multi-lingual accident reports using an ontology-based approach. Safety Science 118, 288-297.
100. Hutchings, J., 2017. Systemic factors in the investigation of South African railway occurrences. PhD thesis, University of the Witwatersrand, Johannesburg.
101. IBRAI, 2017. Derailment of a SNCB/NMBS passenger train, Buizingen – 10 September 2015. Investigation Body for Railway Accidents and Incidents (IBRAI).
102. ICSI, 2013. Leadership in Safety: Industrial Practice Number 2013-06 of the Cahiers de la Sécurité Industrielle; (ISSN 2100–3874); Institute for an industrial safety culture: Toulouse, France - Available online: http://www.icsi-eu.org/docsi/fr/ (accessed on 15 February 2018).
103. 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): Toulouse, France.
104. International Civil Aviation Organisation (ICAO), 2013. Annex 19 to the Convention on International Civil Aviation: Safety Management; International Standards and Recommended Practices; ICAO: Montreal, Canada.
105. ISASI. Guidelines for Investigation of Human Factors in Accidents or Incidents. International Society of Air Safety Investigators (ISASI). www.isasi.org.
106. ISO, 2004. ISO/IEC 15504-2:2003, Information Technology—Process Assessment—Part 2: Performing an Assessment; International Organisation for Standardisation (ISO): Geneva, Switzerland.
107. Johnsen, S., 2010. Resilience in risk analysis and risk assessment. In Critical Infrastructure Protection IV; IFIP AICT 342; Moore, T., Shenoi, S., Eds.; IFIP: Laxenburg, Austria, 2010; pp. 215–227
108. Johnson., C.W., 2003. Failure in Safety-Critical Systems: A handbook of incident and accident reporting. Glasgow University Press.
109. Johnson, C., 2004. Review of the BFU Überlingen Accident Report - Final report. Eurocontrol Contract C/1.369/HQ/SS/04.
110. Johnson., C.W., 2009. Review of accident investigation methodologies - Final report. European Railway Agency contract ERA/2009/SAF/NP/02

111. 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.

112. Kelly, T., 2017. The Role of the Regulator in SMS. In International Transport Forum Discussion Papers 2017-17; OECD/ITF: Paris, France.

113. Kontogiannis, T. 2012, Modelling patterns of breakdown (or archetypes) of human and organisational processes in accidents using systems dynamics. Safety Science 50, 931-944.

114. Kringen, J., 2013. Proceduralization and Regulation of Culture: Experiments on the Frontiers of Risk Regulation. In Trapping Safety into Rules: How Desirable or Avoidable is Proceduralization, Bieder, C.; Bourrier, M., Eds.; Ashgate Publishing Limited: Farnham, UK, pp. 205–224.

115. Kuusisto, A., 2000. Safety Management Systems – Audit Tools and Reliability of Auditing. Technicle Research Centre of Finland, VTT Publications, Espoo, Finland, Volume 428.

116. Kyriakidis,M., Majumdar, A. and Ochieng, W.Y. 2015, Data based framework to identify the most significant performance shaping factors in railway operations. *Safety Sience*, 78, 60-76.

117. 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.

118. Lappalainen, J., 2017. Overcoming Obstacles to implementing SMS. In International Transport Forum Discussion Papers 2017–20; OECD/ITF: Paris, France - discussion paper is available online at: https://www.itf-oecd.org/overcoming-obstacles-implementing-sms - accessed on 23 November 2017

119. Le Coze, J.C., 2013. What have we learned about learning from accidents? Post-disaster reflections. Safety Science 51, 441-453.

120. Le Coze, J.C. 2019. Resilience, Reliability, Safety: Multilevel Research Challenges. In S. Wiig & B. Fahlbruch (Ed.), *Exploring Resilience, A Scientific Journey from Practice to Theory.* Springer Briefs in Applied Sciences and Technology

121. Le Coze, J.C., 2020. Hopkins' view of structure and culture (one step closer to strategy). Safety Science, 122.

122. Le Coze, J.-C.; Wiig, S., 2013. Beyond Procedures: Can 'Safety Culture' Be Regulated? In Trapping Safety into Rules: How Desirable or Avoidable is Proceduralization, Bieder, C., Bourrier, M., Eds.; Ashgate Publishing Limited: Farnham, UK, pp. 191–203.

123. Leplat, J. 1997, Regards sur l'activité en situation de travail, Contribution à la psychologie ergonomique, Paris, PUF.

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

125. Leveson, N., 2011. The use of safety cases in certification and regulation. J. Sys. Safe.

126. Leveson, N.G., 2011. Engineering a Safer World; MIT Press: Cambridge, MA, USA.

127. Leveson, N.G., 2016. Rasmussen's legacy: A paradigm change in engineering for safety. Appl. Ergonom., 59, 581–591.

128. Leveson, N., 2020. Safety III: A Systems Approach to Safety and Resilience.

129. 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.

130. 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.

131. Lofquist, E.A., 2010. The art of measuring nothing: The paradox of measuring safety in changing civil aviation industry using traditional safety metrics. Safety Science, 48, 1520–1529.
132. Lofquist, E.A., 2017 Jousting with Dragons: A Resilience Engineering approach to manage SMS in the transport sector. In International Transport Forum Discussion Papers 2017-19; OECD/ITF: Paris, France.
133. 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.
134. 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.
135. New York Times, (1918). Malbone Street wreck - The New York Times · Saturday, November 2, 1918. Consulted on 30/08/2018 at: https://www.nycsubway.org/wiki/Malbone_Street_Wreck_(New_York_Times,_1918)
136. Norman, D. 1983, Design Rules Based on Analyses of Human Error, Communication of the ACM, April, 26, 254-258.
137. Norman, D. 2002, The Design of Everyday Things, Ed. 2002, New York: Basic Books.
138. Malone, M., 2020. Do different analysis techniques influence the evaluation of the Safety Management System in an investigation: a case study involving a principal contractor in the rail industry. Cranfield Safety and Accident Investigation Centre Cranfield University. MSc Thesis.
139. Maurino, D., 2017. Why SMS: An introduction and overview of safety management systems. International Transport Forum Discussion Papers 2017-16; OECD/ITF: Paris, France, 2017.
140. Mohammadfam, I.; Komalinia, M.; Momeni, M.; Golmohammadi, R.; Hamidi, Y.; Soltanian, A., 2017. Evaluation of the Quality of Occupational Health and Safety Management Systems Based on Key Performance Indicators in Certified Organisations. Safe. Health Work, 8, 156–161.
141. Nævestad, T.-O., Storesund Hesjevoll, I., Ranestad, K. and Atonsen, S. 2019, Strategies regulatory authorities can use to influence safety culture in organisations: Lessons based on experiences from three sectors, *Safety Science*, 118, 409–423.
142. Pariès, J.; Macchi, L.; Valot, C.; Derhavengt, S., 2019, Comparing HROs and RE in the light of safety management systems. Safety Science, 117, 501–511.
143. Peltonen, J.S., 2013. Review of SMS Audit Techniques and Methods–Final Report; Contract ERA/2012/SAF/S-02; European Union Agency for Railways: Lille, France.
144. RAIB, 2016. Overspeed at Fletton Junction, Peterborough, 11 September 2015 - Report 14/2016. Rail Accident investigation Branch (RAIB), Department for Transport.
145. RAIB, 2017. Overturning of a tram at Sandilands junction, Croydon 9 November 2016 - Report 18/2017. Rail Accident investigation Branch (RAIB), Department for Transport.
146. RAIB, 2019. Runaway at Bradford Interchange / SAFRAN, 8 June 2018, Meeting with Bart Accou (ERA). Private communication.
147. 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.
148. Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Safety Sience, Vol. 27 (182-213).

149. Rasmussen, J. 1980, Notes on Human Error Analysis and Prediction. In G. Apostolakis, S. Garribba, & G. Volta (Eds.), Synthesis and Analysis Methods for Safety and Reliability Studies (357-389), New York: Plenum Publishing Corporation.
150. Rasmussen, J.; Svedung, I., 2000. Proactive Risk Management in a Dynamic Society; Swedish Rescue Services Agency: Karlstad, Sweden.
151. Reason, J., 1997. Managing the risk of organisational accidents. Ashgate Publishing.
152. Reason, J., Hobbs, A., 2003. Managing Maintenance Error: A practical guide. Ashgate Publishing.
153. Reason, J. 2008. The human contribution: Unsafe acts, accidents and heroic recoveries.Farnham: Ashgate.
154. Reiman, T., Viitanen, K., 2019. Modelling the influence of Safety Management Tools on Resilience. In S. Wiig & B. Fahlbruch (Ed.), *Exploring Resilience, A Scientific Journey from Practice to Theory.* Springer Briefs in Applied Sciences and Technology
155. Reinach, S., Viale, A. 2006, Application of a human error framework to conduct train accident/incident investigations. Accident Analysis and Prevention,38, 396-406.
156. Rosness, R., 2013. The Proceduralization of Traffic safety and Safety Management in the Norwegian Rail Administration: A Comparative Case Study. In Trapping Safety into Rules: How Desirable or Avoidable is Proceduralization, Bieder, C., Bourrier, M., Eds.; Ashgate Publishing Limited: Farnham, UK, pp. 173–189.
157. RSSB, 2015. Safety Culture and Behavioural Development: Common Factors for Creating a Culture of Continuous Improvement; RSSB Research and Development: The Helicon, UK - research report is available online at: https://www.sparkrail.org/Lists/Records/DispForm. aspx?ID=22302 – accessed on 16 January 2020
158. RSSB, 2019, Human Factors Awareness Course, Brussels.
159. Ryan, B., Golightly, D., Pickup, L., Reinartz, S., Atkinson, S., Dadashi, N., 2021. Human functions in safety - developing a framework of goals, human functions and safety relevant activities for railway socio-technical systems. Safety Science 140, 105279.
160. Salmon, P.M., Cornelissen, M., Trotter, 2011. Systems-based accident analysis methods: A comparison of Accimap, HFACS and STAMP. Safety Sience 50 (4), 1158-1170.
161. 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.
162. Salmon, P., Read, G., Stanton, N., Lenné, M. 2013, The crash at Kerang: Investigating systemic and psychological factors leading unintentional non-compliance at rail level crossing. Accident Analysis and Prevention 50, 1278-1288.
163. Schröder-Hinrichs, J.-U.; Praetorius, G.; Graziano, A.; Kataria, A.; Baldauf, M., 2015. Introducing the Concept of Resilience into Maritime Safety. Presented at the 6th Resilience Engineering Association's International Symposium, Lisbon, Portugal, 22–25 June 2015.
164. Shappell, S.A., Wiegmann, D.A. 2000, The Human Factors Analysis and Classification System–HFACS, National Technical Information Service, Springfield, Virginia 22161, U.S. Department of Transportation.
165. Shaw, J. 2016, The Memory Illusion: Remembering, Forgetting, and the Science of False Memory. *Penguin Random House*.
166. Singleton, W.T., 1978. The analysis of practical skills. The Study of Real Skills: Volume I, MTP Press Limited.

167. Sklet, S., 2004. Comparison of some selected methods for accident investigation. Journal of Hazardous Materials 111 (2004), 29-37.
168. Speziali, J., Hollnagel, E., 2008. Study on Developments in Accident Investigation Methods: A Survey of the "State-of-the Art". SKI Report 2008:50.
169. Strauch, B. 2015, Can we examine safety culture in accident investigation, or should we? *Safety Science*, Vol. 77, pp. 102-111.
170. Stringfellow, M. Accident analysis and hazard analysis for human and organisational factors. Massachusetts Institute of Technology. Doctoral thesis.
171. STSB, 2019. Test méthode SAFRAN. Feedback intermédiaire à Bart le 22.05.2019. Private communication.
172. Teperi, A.-M., Puro, V., Ratilainen, H. 2017, Applying a new human factor tool in the nuclear energy industry. Safety Science 95, 125-139.
173. 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.
174. Underwood, P.J., 2013. Examining the Systemic Accident Analysis Research-Practice Gap. Doctoral thesis, Loughborough University.
175. Underwood, P., Waterson, P., 2013. Systemic accident analysis: examining the gap between research and practice. Accident Analysis Prevention 55, 154-164.
176. Underwood, P.J., Waterson, P.E., 2013. Accident analysis models and methods: guidance for safety professionals. Loughborough: Loughborough University, 28 pp.
177. Underwood, P., Waterson, P., 2013. Systems Thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models.
178. van Schaardenburgh-Verhoeve, K.N.R.; Corver, S.; Groenweg, J., 2007. Ongevalsonderzoek buiten de grenzen van de organisatie. In Proceedings of the Nederlandse Vereniging Voor Veiligheidskunde (NVVK) Jubileumcongres, Arnhem, The Netherlands, 25–26 April 2007.
179. Vautier, J.-F., Dechy, N., Coye de Brunélis, T., Hernandez, G., Launay, R., Moreno Alarcon, D. 2018, Benefits of systems thinking for a human and organisational factors approach to safety management. *Environment Systems and Decisions*, 38, 353-366.
180. Verweire, K., Van den Berghe, L. Eds., 2004. Integrated performance management: A guide to strategy implementation. Sage Publications: Thousand Oaks, Ca, USA.
181. Verweire, K., 2014. Strategy Implementation; Routledge: New York, NY, USA.
182. Vierendeels, G.; Reniers, G.L.L.; Ale, B.J.M., 2011. Modelling the major accident prevention legislation change process within Europe. Saf. Sci., 49, 513–521.
183. Wahlström, B.; Rollenhagen, C., 2014. Safety management-A multi-level control problem. Safety Science, 69, 3–17.
184. Waterson, P., Robertson, M., M., Cooke, N., J., Militello, L., Roth, E., Stanton, N., A., 2015. Defining the methodological challenges and opportunities for an effective science of sociotechnical systems and safety. Ergonomics.
185. Wikipedia, 2018. Available online: https://en.wikipedia.org/wiki/Fractal (accessed on 05 January 2018).
186. Wikipedia, (2018). Malbone Street Wreck. at: https://en.wikipedia.org/wiki/Malbone_Street_ Wreck (Accessed on 30/08/2018)

187. 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.

188. 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.

189. 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.

190. Young, M., Shorrock, S., Faulkner J., Braithwaite, G. 2004, Who moved my (Swiss) cheese? The (r) evolution of human factors in transport safety investigation. ISASI Seminar - Gold Coast, Australia.

191. Young, M., Steel, T. 2017, Non-technical skills in rail accidents: Panacea or pariah? Sixth International Human Factors Rail Conference, 6-9 November 2017, London.

192. Zwetsloot, G.I.J.M., 2000 Developments and debates on OHSM system standardisation and certification. In Systematic Occupational Safety & Health Management–Perspectives on an International Development, Frick, K., Quinlan, M., Langaa Jensen, P., Wilthagen, T., Eds.; Pergamon-Elsevier Science Ltd.: Amsterdam, The Netherlands, pp. 391–412.