Towards a New Way of Understanding the Resilience of Socio-Technical Systems: The Safety Fractal Analysis Method Evaluated

Bart Accou * and Genserik Reniers

Safety and Security Institute, Delft University of Technology, 2600 Delft, The Netherlands
* Correspondence: bart.accou@era.europa.eu; Tel.: +32-491997718

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 of a systemic method for accident analysis that is easily applicable and less resource demanding than the actual methods, Accou and Reniers (2019) developed the SAfety FRactal ANalysis (SAFRAN) method. The method, which is based on the principles of an 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, which 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.

Keywords: safety management system; accident analysis; resilience; safety fractal

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., [1,2]) 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 [3] 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, Accou and Reniers [4] also considered the lack of in-depth analysis into (elements of) safety management systems (SMS) 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, Accou and Reniers [4] developed the SAfety FRactal ANanalysis (SAFRAN) method, with the main aim of guiding 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 findings close to operations that explain the occurrence are the elements

accident investigators are first confronted with [5]. The SAFRAN method uses these findings as the starting point to further guide investigators also analysing the relevant processes of an SMS (and wider socio-technical system) that should organise and control safety performance. The essence, however, 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. To allow this, the SAFRAN method is built around a unique unit of analysis called the Safety Fractal. This model or unit reflects 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 an SMS with specific requirements for process capability that can represent the management of activities at an operational level [4]. Building on the similarities between both references, a five-step safety management delivery system was identified, with the following logic:

(1) **Specify**: the scope and desired outcome of an activity are 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 conducted 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 conducted).

(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 adequate changes to control, or implementation elements, are introduced.

The above Safety Fractal was then compared with the common accident investigation approach that was distilled by Wienen et al. [6], based on an analysis of state of the art in incident and accident analysis methods while searching for an appropriate accident analysis method that could be used for analysing incidents that cause service unavailability in the Dutch telecommunication sector:

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.

Applying this common accident investigation approach, with the Safety Fractal as a basis, finally resulted in the following investigation logic [4]: five simple steps that help to evaluate the human and organisational factors that influenced actions and decision making, regardless of the hierarchical level at which they are situated.

In short, the consecutive steps for one iteration of the SAFRAN method can be summarised as follows:

- 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 (SPV): 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.

These steps are first completed for the critical events that are identified in the sequence of events that describes the occurrence 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. This is illustrated in Figure 1.
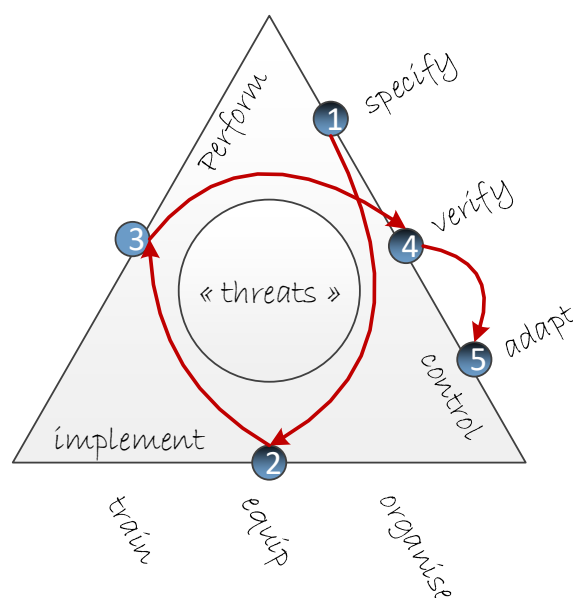
Figure 1. The Safety Fractal.

The investigation logic of the SAFRAN method further suggests two possible ways of identifying a function that should be analysed in a further iteration. Firstly, for each of the identified SPV of the initially investigated function, the process that logically would manage this should be further investigated, with the identified SPV as the outcome of the process performance of this process. In such a case, the investigated new function is graphically represented by a new triangle and an arrow, starting from the bottom of a previously investigated function, indicates the link with the identified SPV. Secondly, the process that represents the capability of the system to verify the variability in the performance of the initially investigated function should be further analysed. The link between both functions is represented by an arrow starting from number 4, on the right-hand side of the triangle representing the initial process, towards the left-hand side of a triangle representing the function that verifies variability in the performance of the initial function or process. This logic can then be repeated for each analysed triangle as the starting point for identifying new implementing or control processes for further analysis. The graphical representation of this logic is illustrated in Figure 2 below.
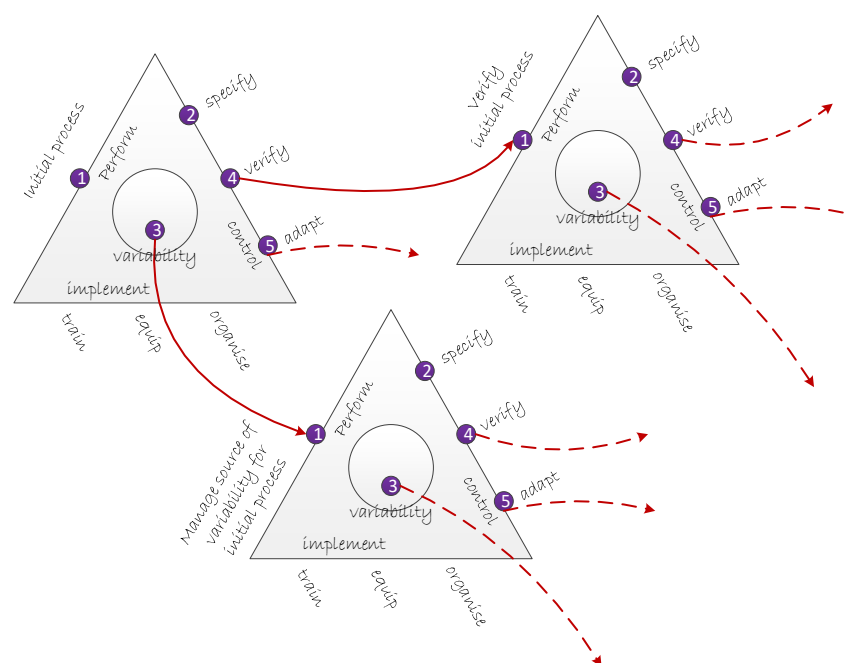
Figure 2. Graphical representation of linked functions following the SAFRAN logic.

The following sections of this paper aim to validate 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. Chapter 2 explains the methodology that was used to achieve this. The systematic analysis of an existing investigation into a major railway accident that provides elements to apply the chosen methodology for validating the SAFRAN method is equally covered in the second chapter. The third chapter reports in detail on the findings of the performed evaluation, while Chapter 4 critically discusses these findings to come to a conclusion in Chapter 5.

2. Methodology

Underwood [7] 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 the validity and reliability of an accident analysis method as a prime evaluation criterion (e.g., [8–10]). Yet, for most of the existing systemic accident analysis methods, proper validation appears to be missing [7]. In that context, practical and resource constraints could be mentioned as the 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 analyst 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.

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 [7] has designed an evaluation framework that allows to assess and compare accident analysis methods. As graphically summarised in Figure 3 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).
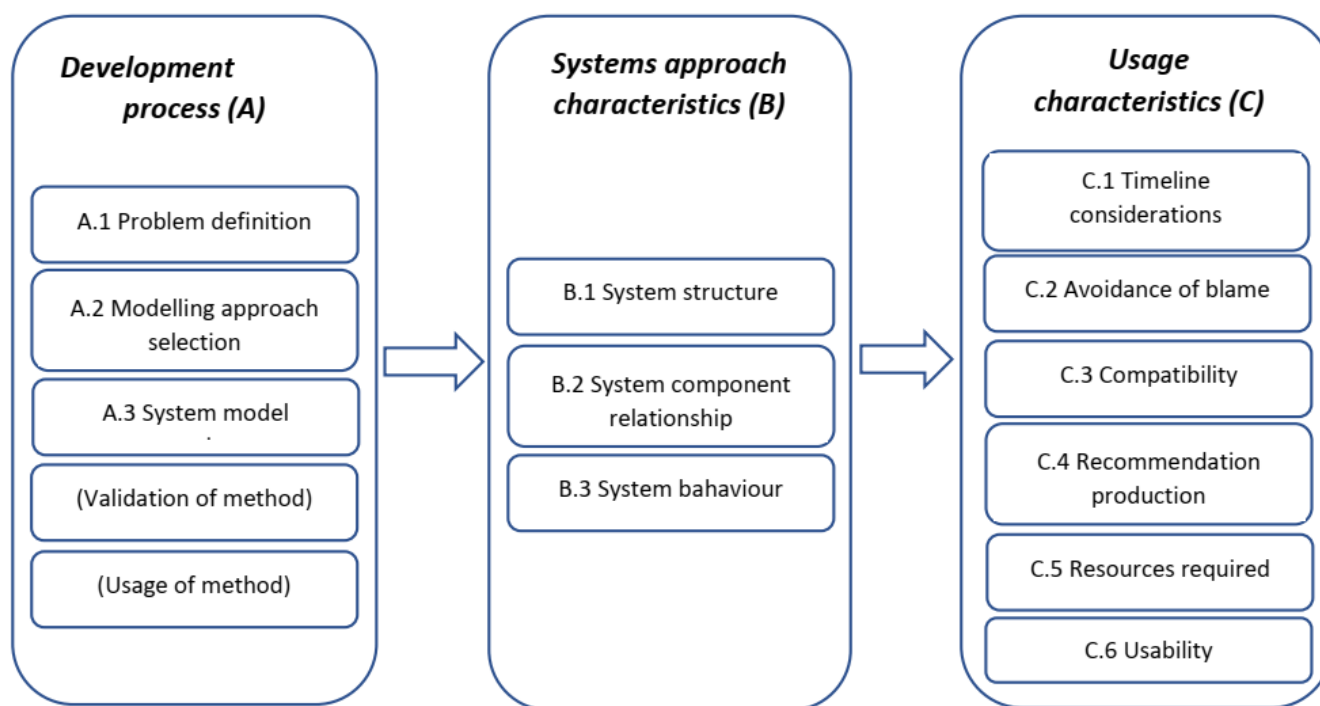
Figure 3. The evaluation framework adapted after Underwood [7].

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 ([8]; Benner (1985) and Hollnagel (1998) in [10]) or provided guidance on the selection of such methods for practitioners [3,6,10–12]. 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, which is part of the usage characteristics, to a 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 Chapter 3 of this paper. A summary of the different elements covered by each of the cited authors is available in Appendix B.

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 one of the authors, two Master's students at Cranfield University 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 [13] 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 [14] 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 [7].

In addition, during the different phases of development of the method, one of the authors also has had the chance, on 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 inside into how easy the method is to understand and what time and effort are needed to learn to apply the SAFRAN method. In addition, some of these investigators also freely provided useful feedback after the 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 [15] conducted to compare the ATSB, AcciMap and STAMP methods, the SAFRAN method was 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 [16]. This allows for 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 [4,17,18].

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 [15] 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 [16] 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. Additionally, several shortcomings in inspection and maintenance practices and, more generally, 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 the next step, in order to facilitate the comparison with the results of Underwood and Waterson [15], the different elements that resulted from this work were put next to their analysis, and when relevant, the code or labelling 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 graphically represented in Appendix A.

In this graphical representation, the boxes with a green lining represent the physical sequence of events. From this sequence, focusing on variability in the 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. Boxes filled with a similar colour present the same or related information, while the boxes 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 [15].

The triangles represent the system functions that, based on the information provided in the investigation report [16], showed critical performance variability. For each of these triangles, information on the actual performance (left-hand side of the triangle and represented by the number 1), the sources of performance variability (bottom of each triangle, and represented by the number 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 the first iteration, describing either an activity that leads to the unsafe state of the switch (i.e., tightening switch bar fasteners and setting the residual switch opening) or 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 initiated to analyse 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 logical continuation of the investigation when applying the SAFRAN method, which 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 of further investigating 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 a nuance that SAFRAN urges to focus this analysis on identifying performance variability and does not require identifying 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 a 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

3. Findings

In the following sections, the combined findings of the gathered experience with applying the SAFRAN method is used to evaluate the method against the different elements of Underwood's evaluation framework [7].

3.1. Development Process (A)

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 [7]). 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

3.1.1. A.1 Problem Definition

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

Several authors (e.g., [19,20]) 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 [21], contributing to the accident are hereby often overlooked and weaknesses in the SMS are hardly ever analysed [22]. 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 by Accou and Reniers [23] 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 [9,24–26] 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 such as SMS as a tool for resolving issues related to human performance or technical failure at the operational level [27].

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 logical way.

3.1.2. A.2 Modelling Approach Selection

A second criterion, linked with the development process of an investigation method, 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 [11] and Katsakiori et al. [8], who explicitly refer to an underlying accident model. Speziali and Hollnagel [10], 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).

As explained in the introduction chapter, 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 control safety-related activities. While the SMS may be considered by some authors as a product of reactive safety management [1], Pariès et al. [28] 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 [29] as well as Denyer's ideas on "paradoxical thinking" [30] 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 [4]. 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 [31]. Furthermore, when grouping the five 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) provides the resources and means to ensure the correct functioning ("doing things right") of the process components during process execution. Finally, a level of **process control**, composed of steps (1), (4) and (5), ensures 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 [32] proposed a way to connect the higher system level management controls with human and technical factors at the lower level. Similarly, Wahlström and Rollenhagen [33] 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 operating systems. They further elaborate on how this control metaphor, which 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. Additionally, Lin [32] 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 humans and hardware. Following this line of thought, we conclude that the Safety Fractal model has the potential to be applied for developing and/or assessing 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 of fractals, also explains the name that was given to the model.

Comparing the above Safety Fractal, the common accident investigation approach that was distilled by Wienen et al. [6] finally resulted in the five-step investigation logic that was presented in the introduction [4]. As also explained in the introduction, this logic, which helps in understanding the performance of one specific process or activity, can then be repeated or iterated with the "next process" that focuses on the implementation of control sides of the previous process.

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 [7] 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 [3] 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 analysis with others. Sklet [11], 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 is 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, as also illustrated in Figures 1 and 2, a triangle was 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: process performance on the left side, process implementation on the bottom and process control on the right

side. The related control processes of specifying, verifying and adapting performance are systematically numbered 2, 4 and 5, respectively. When presenting the results of an investigation, 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 4, zooming in on one of the analysed functions from the Grayrigg accident investigation, illustrates the approach.
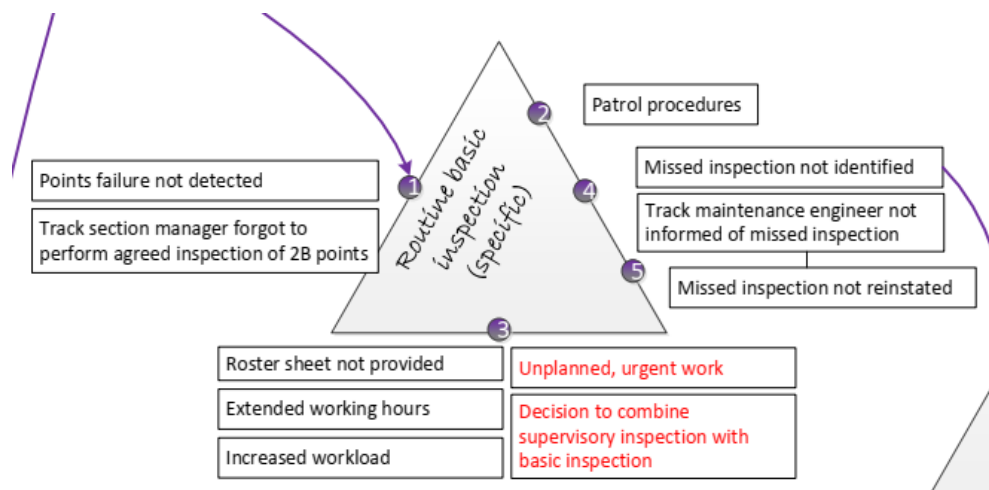
Figure 4. Graphical representation of one analysed function.

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 overcoming the resource-demanding description of the entire system as required by FRAM [34], with its focus on describing in detail how something is performed, or STAMP [35], where step 3 of the method requires documenting 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 [18], 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 a clear focus on what to investigate. A similar logic is equally valid for the functions to verify performance variability.

3.2. Systems Approach Characteristics (B)

The second pillar in the evaluation framework aims at verifying whether a method applies system thinking. To be able to perform this evaluation, Underwood [7] has identified three interrelated themes that broadly reflect the different elements that exist in the 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 [2], 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.

3.2.1. B.1 System Structure

Leveson [2] 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 [3]). Being able to represent a system's hierarchy will therefore be an essential part of any systemic analysis method. Similarly, Salmon et al. [12] require a systemic method to be capable of covering the entire socio-technical system, while Sklet [11] already referred to the possibility of including 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 of 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. [9], 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.
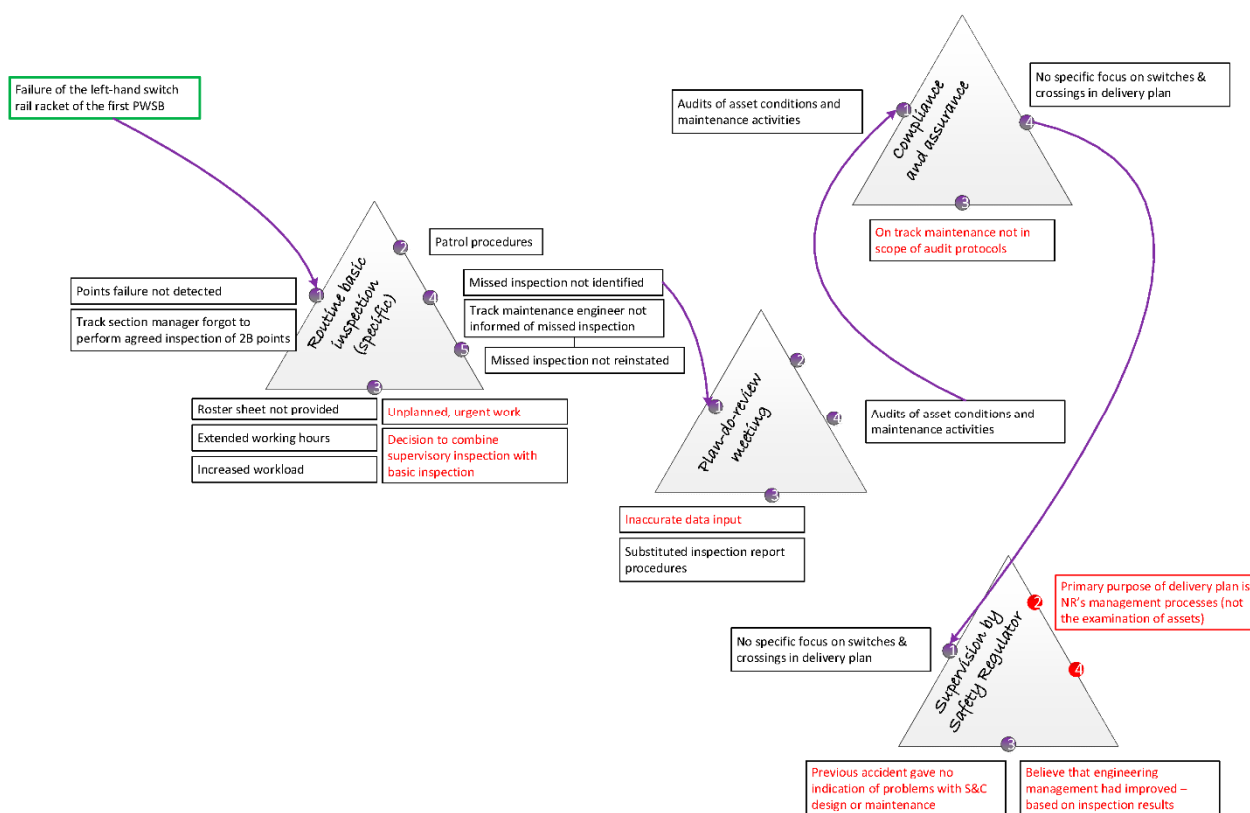
Figure 5. Illustration of hierarchical levels of control with SAFRAN for the Grayrigg accident.

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 [15], characteristic of 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.

3.2.2. B.2 System Component Relationship

Underwood [7] 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 [2] 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 [15] 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. As described above for the system structure criterion and 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 relationships between the various components, as is required for STAMP. The former is conducted 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.

3.2.3. B.3 System Behaviour

The last criterion that is proposed by Underwood [7] 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 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., the same starting point can produce a range of outputs), system adaptation, and the context in which performance takes place. Leveson [2], from a higher system perspective, refers to the possibility of describing the state of a system as a set of relevant properties describing it at any time. Hollnagel (cited in [10]), 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 [7] or the ability to identify contributing factors that can explain complex human decision making and organisational failures [12].

With the SAFRAN method, the output of a function or system —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 are 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 also covers 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.

3.3. Usage Characteristics (C)

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.

3.3.1. C.1 Accident Description

Underwood [7] introduces a timeline consideration criterion by evaluating whether a method incorporates the concept of time in the accident development process. Katsakiori et al. [8], later followed by Wienen et al. [6], 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 [10]) for a method to produce an adequate explanation or account of why an adverse event (accident or incident) occurred. Additionally, Benner (cited in [10]) 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 lead 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 looks 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.

3.3.2. C.2 Avoidance of Blame

Benner (cited in [10]) 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 [10] translated this avoidance of blame into the question of whether a method directs the analyst towards identifying a root cause. Del Frate et al. [36], 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 [37] 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 further argued under the section that reflects on the production of recommendations, the aim of accident investigations should be to teach an organisation to be resilient in order to compensate for structural shortcomings [38] as well as to address the weaknesses in the operating feedback systems that hamper a good understanding of vulnerabilities coming from daily, routine functioning [21]. 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.

3.3.3. C.3 Compatibility of the Method

The next criterion proposed by Underwood [7] 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 [11], providing special input as a supplement to other methods. Contrary to a primary method, that would be a stand-alone investigation technique.

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 countermeasures need to be taken, preferably by changing an organisation's performance in an intended direction. Underwood [7] therefore suggests questioning whether a method aids the analyst in producing safety recommendations and providing generic insights into accident causation. Additionally, Katsakiori et al. [8] put forward a consequential requirement, questioning whether a method generates recommendations for improved safety, while similarly, Salmon et al. [12] require a method to support the development of appropriate countermeasures, as opposed to countermeasures that are focused on individual operators. In the same context, Benner (cited in [10]) 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. [6], 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, Accou and Reniers [4] already argued 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). Additionally, the third type of learning that was identified by Argyris and Schön [39], 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.

3.3.5. C.5 Resources Required

The next criterion proposed by Underwood [7] 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 [10]) 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 such as specialist software. 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 [7,8,12].

In general, learning and applying the SAFRAN method is not considered very time-consuming. Flovenz [13], 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 [40] 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 [41] states that "the method has the particularity of not being complicated to use".

3.3.6. C.6 Usability

The last criterion, put forward by Underwood [7] 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 by Benner (cited in [10]), who requires an investigation method to be disciplining, functional and definitive. The requirement to be disciplining refers to the capability of a method to provide an orderly, systematic framework and a set of procedures to discipline the investigators' tasks in order to focus their efforts on important and necessary tasks. Similar reasoning can be found in Underwood and Waterson's work [3], who suggest questioning whether a method has a structured application process. Benner's functional requirement aims at helping the investigators determine which events were part of the accident process as well as those events that were unrelated. Waterson et al. [9] relate this to the need for a method to support 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 [8]; Hollnagel, cited in [10,42]. The last element that relates to the usability of an investigation method put forward by Salmon et al. [12] is whether the method is generally applicable and not sector specific.

In its feedback on the first application of the SAFRAN method, RAIB [40] reports that systematically following the five steps for each iteration was useful and introduced rigour into the investigation. Malone [14] then reports that applying the SAFRAN methods prevents 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 to be 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 [13], who validated the method for use in the aviation sector using real safety investigation data and concluded 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 an SMS is a legal obligation, the authors are confident that this finding is also valid in other domains where safety risks have to be managed.

4. Discussion

The above evaluation against a well-defined set of structured criteria gives a 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 elements 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 Safty 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 on 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 of a system's approach [7]. 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 a better understanding of management decisions that are contributing to accidents [21], 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., [38]). Still, the authors believe that the iterative aspect of the SAFRAN method, when starting from the identified critical variability closest to the event sequence, will prevent investigators from overlooking the importance of cognitive issues at the sharp end in favour of those organisational and wider systemic issues; a risk identified by Young et al. [43] 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 communicate 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 [40], when providing feedback on an early application of the method for an ongoing 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, the authors relate this to the trade-off that each time needs to be made between showing an overview on a restricted display and keeping the structure in the logic and hierarchy of the findings. This is also reflected in the analysis performed by Flovenz [13], who reports on a "rapid consumption of space" when using 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. Malone [14] also reports on similar difficulties in producing 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 [13] or to integrate the SAFRAN findings into the graphical representation they are currently using and that is fault-tree inspired [40]. The authors acknowledge that more work is needed to achieve a satisfactory result that 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 of the flexibility of the method.

Additionally, the evaluation of the usage characteristics (C) of the SAFRAN method reflects 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 [13], 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 the 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 [40], when providing feedback on an early application of the SAFRAN method for an ongoing investigation, reported that "there were no difficulties transferring the result of the SAFRAN analysis into the RAIB report format". Again Flovenz [13] 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, focusing more on the analytical interpretation of an event rather than 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 [14]: "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 compliment 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 [14] 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 [3,44] 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 [39], 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. [6] that applying systemic methods makes it harder to formulate corrective measures that can be implemented by management. This idea is supported by Flovenz's finding [13] that within a few iterations with the SAFRAN method, he arrived at questions that generated management discomfort, which he considers to be 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 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 to more resilient performance. As such, the 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 [45], 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 [14] 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 into the existing systemic accident analysis methods (e.g., [6]). Based on their practice of training investigators in applying the SAFRAN method, the authors recognise different degrees of complexity in understanding how to apply the method to achieve its maximum potential. 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 the 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 [13] and Malone [14] 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 [40] 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 [31] also identified that the actual practice of railway accident investigation might lack proper knowledge of human and organisational factors to be able to consistently provide an answer to the step 3 of a single SAFRAN iteration. This appears to be even more the case for further iterations. STSB [41], 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 depends not only on the expertise of the investigators in using the method but also on the understanding of stakeholders' need to provide the necessary information in order to improve the system.

The authors believe that the structured approach that is characteristic of the SAFRAN method can help to explain the interaction between the different hierarchical layers in the socio-technical system and how they ultimately contribute to controlling critical system variability. However, to gain full effect, management and other stakeholders would have to be trained in system thinking as well. The last element, related to the use of resources, is the application of a stop rule. Both RAIB [40] and Flovenz [13] report that the SAFRAN would benefit from clear criteria or at least guidance on how far to take the analysis. Additionally, Malone [14] found it difficult to determine when to stop the analysis. The initial investigation logic [4] proposed to stop the analysis when a major specification issue for a 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 [41] 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 [13], "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 also argued above, he 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, the 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 [41]. Performing this type of analysis, which 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 [46]. Like Le Coze [46], the authors believe that this requirement is more likely to be met when several specialists or experts interact on the same accident analysis. A similar reflection was made by Accou and Carpinelli [31] 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 introduce variability in (operational) performance and to recognise what additional expertise can be called upon when needed.

Additionally, Flovenz [13] highlights the possibility of having taxonomies to support the SAFRAN analysis as a 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 [31] that match the SAFRAN investigation logic. Additionally, Flovenz's [13] 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., [47]), (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 [31]) 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. The first results of such a classification of investigation result show 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, training on the methods and corresponding guidance material should also help to gain a better understanding and increase usability. In particular, the development of concrete examples was an idea that was proposed by several of the participants in 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 ongoing accident investigations [40,41] and specifically also by the work of Flovenz [13], 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, the authors would also like to stress that they do not want to give the impression

that high-risk industries are generally unsafe. Consecutive decades of structures 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. Conclusions

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 us 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 an in-depth analysis of accidents. Based on the performed evaluation, the authors 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.

Author Contributions: Conceptualization, B.A.; Writing—original draft, B.A.; Writing—review and editing, G.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A
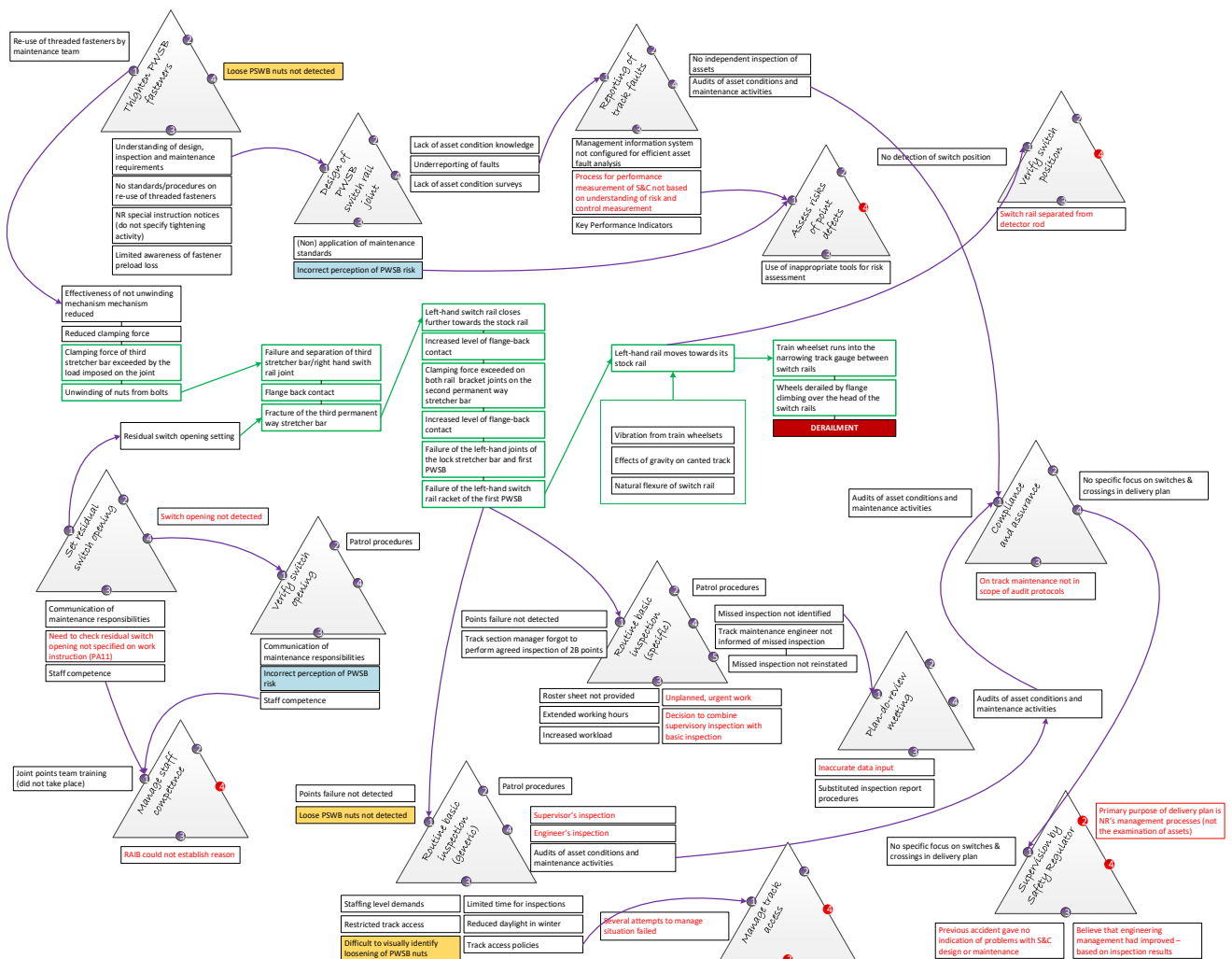
Figure A1. SAFRAN representation of the Grayrigg accident.

Appendix B

Table A1. Comparing Underwood's evaluation framework with other authors.

Underwood (2013)—Evaluation Framework [7]	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) [6]	-	-	-	-	Does the method take into account the socio-technical context?	Does the method allow to describe control-feedback loops at different hierarchical levels?
Waterson et al. (2015) [9]	-	-	-	Defining what is meant by an 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) [15]	-	-	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 analysis with others?	How complex is the system to be analysed? How much of the system will be analysed?	-	-

Table A1. *Cont.*

Underwood (2013)—Evaluation Framework [7]	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?
Salmon et al. (2011) [12]	-	-	-	Coverage of the overall socio-technical system	Linkage of failures within and between levels	Ability to identify (all of the) contributing factors Identifying complex human decision making and organisational failures
Sklet (2004) [11]	-	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) [10]	-	Consistent—Model must be theoretically consistent with an agency's safety program concepts	-	-	-	-

Table A1. *Cont.*

Underwood (2013)—Evaluation Framework [7]	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?
Hollnagel (1998; cited in Speziali and Hollnagel, 2008) [10]	-	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

References

1. Hollnagel, E. *Safety-I and Safety-II: The Past and Future of Safety Management*; Ashgate Publishing: Farnham, UK, 2014.
2. Leveson, N. *Safety III: A Systems Approach to Safety and Resilience*; Department of Aeronautics and Astronautics, MIT: Cambridge, MA, USA, 2020.
3. Underwood, P.J.; Waterson, P.E. *Accident Analysis Models and Methods: Guidance for Safety Professionals*; Loughborough University: Loughborough, UK, 2013; p. 28.
4. Accou, B.; Reniers, G. Developing a method to improve Safety Management Systems based on accident investigations: The Safety Fractal Analysis. *Saf. Sci.* **2019**, *115*, 285–293. [CrossRef]
5. Young, M.; Steel, T. Non-technical skills in rail accidents: Panacea or pariah? In Proceedings of the Sixth International Human Factors Rail Conference, London, UK, 6–9 November 2017.
6. Wienen, H.C.A.; Bukhsh, F.A.; Vriezekolk, E.; Wieringa, R.J. *Accident Analysis Methods and Models—A Systematic Literature Review*; Technical Report No.TR-CTIT-17-04; Centre for Telematics and Information Technology (CTIT): Twente, The Netherlands, 2017.
7. Underwood, P.J. Examining the Systemic Accident Analysis Research-Practice Gap. Doctoral Thesis, Loughborough University, Loughborough, UK, 2013.
8. Katsakiori, P.; Sakellaropoulos, G.; Manatakis, E. Towards an evaluation of accident investigation methods in terms of their alignment with accident causation models. *Saf. Sci.* **2009**, *47*, 1007–1015. [CrossRef]
9. Waterson, P.; Robertson, M.M.; Cooke, N.J.; Militello, L.; Roth, E.; Stanton, N.A. Defining the methodological challenges and opportunities for an effective science of sociotechnical systems and safety. *Ergonomics* **2015**, *58*, 565–599. [CrossRef] [PubMed]

10. Speziali, J.; Hollnagel, E. *Study on Developments in Accident Investigation Methods: A Survey of the "State-of-the Art"*; SKI Report 2008:50; Ecole des Mines de Paris: Paris, France, 2008.

11. Sklet, S. Comparison of some selected methods for accident investigation. *J. Hazard. Mater.* **2004**, *111*, 29–37. [CrossRef] [PubMed]

12. Salmon, P.M.; Cornelissen, M.; Trotter, M.J. Systems-based accident analysis methods: A comparison of Accimap, HFACS and STAMP. *Saf. Sci.* **2011**, *50*, 1158–1170. [CrossRef]

13. Flovenz, G. Investigating SMS—A Problem of Methodology. Master's Thesis, School of Aerospace, Transport and Manufacture, Safety and Accident Investigation (Air Transport), Cranfield University, Cranfield, UK, 2020.

14. Malone, M. 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. Master's Thesis, Cranfield Safety and Accident Investigation Centre Cranfield University, Cranfield, UK, 2020.

15. Underwood, P.; Waterson, P. 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. *Accid. Anal. Prev.* **2013**, *68*, 75–94. [PubMed]

16. RAIB. *Rail Accident Report: Derailment at Grayrigg 23 February 2007*; Report 20/2008 v5 July 2011; Rail Accident Investigation Branch, Department of Transport: Derby, UK, 2011.

17. Accou, B.; Reniers, G. Analysing the depth of railway accident investigation reports on over-speeding incidents, using an innovative method called "SAFRAN". In Proceedings of the 55th European Safety, Reliability & Data Association (ESReDA) Seminar, Bucharest, Romania, 9–10 October 2018.

18. Accou, B.; Reniers, G. 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. *to be published*.

19. Antonsen, S. *Safety Culture: Theory, Method and Improvement*; Ashgate Publishing Limited: Farnham, UK, 2009.

20. Kelly, T. *The Role of the Regulator in SMS*; ITF Discussion Paper 2017-17; OECD/ITF: Paris, France, 2017.

21. Dien, Y.; Dechy, N.; Guillaume, E. Accident Investigation: From Searching Direct Causes to Finding In-Depth Causes. Problem of Analysis or/and of Analyst? In Proceedings of the 33rd ESReDA Seminar, Ispra, Italy, 13–14 November 2007; Dechy, N., Cojazzi, G.G.M., Eds.; European Commision: Luxembourg, 2007; p. 16.

22. Johnson, C. *Review of the BFU Überlingen Accident Report—Final Report*; Eurocontrol Contract C/1.369/HQ/SS/04; Eurocontrol: Brussels, Belgium, 2004.

23. Accou, B.; Reniers, G. Introducing the Extended Safety Fractal: Reusing the concept of Safety Management Systems to organize resilient organizations. *Int. J. Environ. Res. Public Health* **2020**, *17*, 5478. [CrossRef] [PubMed]

24. Reason, J. *Managing the Risk of Organisational Accidents*; Ashgate Publishing: Farnham, UK, 1997.

25. Lundberg, J.; Rollenhagen, C.; Hollnagel, E. What-You-Look-For-Is-What-You-Find—The consequences of underlying accident models in eight accident investigation manuals. *Saf. Sci.* **2009**, *47*, 1297–1311. [CrossRef]

26. Dekker, S. *Drift into Failure: From Hunting Broken Components to Understanding Complex Systems*; Ashgate Publishing: Farnham, UK, 2011.

27. Rasmussen, J. Risk management in a dynamic society: A modelling problem. *Saf. Sci.* **1997**, *27*, 182–213. [CrossRef]

28. Pariès, J.; Macchi, L.; Valot, C.; Derhavengt, S. Comparing HROs and RE in the light of safety management systems. *Saf. Sci.* **2019**, *117*, 501–511. [CrossRef]

29. Hollnagel, E. The Four Cornerstones of Resilience Engineering. In *Resilience Engineering Perspectives, Volume 2: Preparation and Restoration*; Nemeth, C.P., Hollnagel, E., Dekker, S., Eds.; Ashgate: Farnham, UK, 2009; pp. 117–134.

30. Denyer, D. *Organizational Resilience: A Summary of Academic Evidence, Business Insights and New Thinking*; BSI and Cranfield School of Management: Bedford, UK, 2017.

31. Accou, B.; Carpinelli, F. Systematically investigating human and organisational factors in complex socio-technical systems by using the "SAfety FRactal ANalysis" method. *Appl. Ergon.* **2022**, *100*, 103662. [CrossRef] [PubMed]

32. Lin, P.-H. Safety Management and Risk Modelling in Aviation: The Challenge of Quantifying Management Influences. Ph.D. Thesis, Next Generation Infrastructures Foundation, Delft, The Netherlands, 2011.

33. Wahlström, B.; Rollenhagen, C. Safety management—A multi-level control problem. *Saf. Sci.* **2014**, *69*, 3–17. [CrossRef]

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

35. Leveson, N.G. *Engineering A Safer World*; MIT Press: Cambridge, MA, USA, 2011.

36. Del Frate, L.; Zwart, S.D.; Kroes, P.A. Root cause as a U-turn. *Eng. Fail. Anal.* **2011**, *18*, 747–758. [CrossRef]

37. Reason, J. *The Human Contribution: Unsafe Acts, Accidents and Heroic Recoveries*; Ashgate: Farnham, UK, 2008.

38. van Schaardenburgh-Verhoeve, K.N.R.; Corver, S.; Groenweg, J. Ongevalsonderzoek buiten de grenzen van de organisatie. In Proceedings of the Nederlandse Vereniging Voor Veiligheidskunde (NVVK) Jubileumcongres, Arnhem, The Netherlands, 25–26 April 2007.

39. Argyrys, C.; Schön, D.A. *Organizational Learning II-Theory, Method, and Practice*; Addison-Wesley Publishing Company: Boston, MA, USA, 1996.

40. Railway Accident Investigation Branch (RAIB), Derby, United Kingdom. Runaway at Bradford Interchange/SAFRAN, 8 June 2018, Meeting with Bart Accou (ERA). Private Communication. 2019. Available online: https://www.gov.uk/government/organisations/rail-accident-investigation-branch (accessed on 28 March 2022).

41. Swiss Transportation Safety Investigation Board (STSB). Bern, Switzerland Test Méthode SAFRAN. Feedback Intermédiaire à Bart Le 22.05.2019. Private Communication. 2019. Available online: https://www.sust.admin.ch/en/stsb-homepage (accessed on 28 March 2022).

42. Salmon, P.; Read, G.; Stanton, N.; Lenné, M. The crash at Kerang: Investigating systemic and psychological factors leading unintentional non-compliance at rail level crossing. *Accid. Anal. Prev.* **2013**, *50*, 1278–1288. [CrossRef] [PubMed]

43. Young, M.; Shorrock, S.; Faulkner, J.; Braithwaite, G. *Who Moved my (Swiss) Cheese? The (r)evolution of Human Factors in Transport Safety Investigation*; ISASI Seminar: Gold Coast, Australia, 2004.

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

45. Groeneweg, J. *Controlling the Controllable: The Management of Safety*; DSWO Press, Leiden University: Leiden, The Netherlands, 1992.

46. Le Coze, J.C. What have we learned about learning from accidents? Post-disaster reflections. *Saf. Sci.* **2013**, *51*, 441–453. [CrossRef]

47. Ryan, B.; Golightly, D.; Pickup, L.; Reinartz, S.; Atkinson, S.; Dadashi, N. Human functions in safety—Developing a framework of goals, human functions and safety relevant activities for railway socio-technical systems. *Saf. Sci.* **2021**, *140*, 105279. [CrossRef]