Safety and Health at Work 12 (2021) 10–19

Contents lists available at ScienceDirect

Safety and Health at Work

journal homepage: www.e-shaw.net

Review Article

Safety-II and Resilience Engineering in a Nutshell: An Introductory Guide to Their Concepts and Methods

Dong-Han Ham ☆

Department of Industrial Engineering, Chonnam National University, Republic of Korea

ARTICLE INFO

Article history:
Received 5 February 2020
Received in revised form
29 October 2020
Accepted 25 November 2020
Available online 2 December 2020

Keywords:
FRAM
Resilience
Resilience engineering
Safety-I
Safety-II

ABSTRACT

Background: Traditional safety concept, which is called Safety-I, and its relevant methods and models have much contributed toward enhancing the safety of industrial systems. However, they have proved insufficient to be applied to complex socio-technical systems. As an alternative, Safety-II and resilience engineering have emerged and gained much attention for the last two decades. However, it seems that safety professionals have still difficulty understanding their fundamental concepts and methods. Accordingly, it is necessary to offer an introductory guide to them that helps safety professionals grasp them correctly in consideration of their current practices.
Methods: This article firstly explains the limitations of Safety-I and how Safety-II can resolve them from the four points of view. Next, the core concepts of resilience engineering and Functional Resonance Analysis Method are described.
Results: Workers' performance adjustment and performance variability due to it should be the basis for understanding human-related accidents in socio-technical systems. It should be acknowledged that successful and failed work performance have the same causes. However, they are not well considered in the traditional safety concept; in contrast, Safety-II and resilience engineering have conceptual bases and practical approaches to reflect them systematically.
Conclusion: It is necessary to move from a find-and-fix and reactive approach to a proactive approach to safety management. Safety-II and resilience engineering give a set of useful concepts and methods for proactive safety management. However, if necessary, Safety-I methods need to be properly used for situations where they can still be useful as well.

1. Introduction

Much effort has been made in several directions to improve the safety of a system, which include accident analysis, risk assessment, safety culture promotion, and human-centered design of equipment and training systems [1–4]. However, the safe situation that was ultimately intended to be achieved through those research activities was defined as a situation in which as few accidents as possible do happen [5,6]. This is the definition of safety (as few things as possible go wrong) that has traditionally been accepted in the safety community [6]. In line with this definition, most of the accident analysis or risk assessment methods have focused on the failed work outcomes (accident situations), thereby finding or anticipating the causes of accidents and fixing them [7].

Traditional system safety methods are based on the following assumptions and concepts [5–7].

- All accidents are caused by the failed components of a system that are broken or do not work properly as specified. However, those components work well as specified in non-accident situations. That is, failed and successful work outcomes have different causes and processes.
- All accidents have their specific causes (particularly a root cause).
- For an accident, if its related information and evidences are sufficiently obtained, analysts can reasonably designate a set of causes that are directly or indirectly related to the accident.
- If a set of causes concerned with an accident can be eliminated or replaced, the same accident or its similar accidents do not occur again in the future.

Even, the prevalent belief in many industries is that it is possible to count all accidents that can happen in a system and to predict

☆ *E-mail addresses:* donghan.ham@gmail.com; dhham@jnu.ac.kr (D.-H. Ham).
Department of Industrial Engineering, Chonnam National University, 77 Yongbong-ro, Buk-gu, Gwangju, 61186, Republic of Korea.

2093-7911/$ – see front matter
https://doi.org/10.1016/j.shaw.2020.11.004

when they happen [6]. Because of the assumptions and concepts described above, a find-and-fix reactive approach has been widely recognized as the most useful way of maximizing the safety of a system [5]. If analysts can identify a particular set of causes associated with an accident, they can fix them and therefore make it possible that as few things as possible go wrong. The find-and-fix approach can be regarded as reactive approach in that it aims to find and fix the causes of an accident after it happens. Moreover, most of the system safety methods are equipped with a plausible accident model that can explain why and how an accident can happen [9–13]. Thus, accident analysts can understand the processes underlying an accident and identify the causes of an accident more efficiently [12]. In addition, after identifying the causes of an accident, they can consider several ways of mitigating the effects of the causes based on the accident model.

The traditional safety concept defined above is referred to as the Safety-I, which is very useful in a technical system consisting of purely technical elements. However, it has been pointed out that the concepts of Safety-I are limited to deal with safety issues in a complex socio-technical system [6,14–17]. As information and communication technologies are widely used in the industry, most of the industrial systems increasingly show the typical features of complex socio-technical systems [18]. In fact, it is not easy to find a purely technical system in modern industrial systems. In addition, ironically, there is a conceptual contradiction in between Safety-I concepts and its methods. As described above, the safety concept in Safety-I is that failure situations are minimized or do not exist. However, Safety-I methods, which aim to find and fix the causes of an accident, can have their usefulness when failure situations exist [6]. This is an interesting and undesirable conceptual inconsistency.

In this regard, there was a strong motivation to have an alternative new safety concept and its practical methods to supplement the limitations of Safety-I [7,19–21]. Safety-II has been emerged as a new safety concept in response to the motivation [6]. Resilience engineering has also been emerged as a practical safety discipline that aims to proactively manage system safety through a synergistic integration of Safety-I and Safety-II [15,19,21,22]. Safety-II and resilience engineering have attracted much attention in the safety community for the last two decades. However, it seems that not a few safety professionals, who are particularly familiar with traditional safety concepts and methods, still have some misconceptions about Safety-II and resilience engineering [23,24]. Additionally, there seems to be a need for safety professionals unfamiliar with them to have insight on how to integrate their experiences and knowledge with the concepts, principles, and methods related to them. To help them to have a right understanding about Safety-II and resilience engineering, this article aims to offer a simple introductory guide to Safety-II, resilience engineering, and FRAM. It should be noted that this article is not intended to offer a comprehensive literature review on those disciplines. This article also aims to offer some insights on the balanced use of Safety-I and Safety-II and to propose a set of future research issues to advance the state of the art of the disciplines.

2. Materials and methods

To offer a concise and introductory guide to the fundamental concepts and principles underlying Safety-II and resilience engineering, the author has reviewed several types of materials published since 2006 when we met the first book in the field of resilience engineering, which is titled *Resilience Engineering: Concepts and Precepts* [21]. The three search tools were used: Google Search (http://www.google.co.uk), Google Scholar (http://scholar.google.com), and Science Direct (http://www.sciencedirect.com). The following keywords and their combinations were used to look for as many relevant research articles as possible: Safety-I, Safety-II, resilience, resilience engineering, performance variability, accident causation, accident analysis, accident modelling, risk assessment, Functional Resonance Analysis Method (FRAM), human error, safety culture, resilient organization, proactive safety management, etc. Additionally, the search was not specific to a particular work domain; accordingly, the search results contained research articles that addressed system safety issues in a wide range of work domains including nuclear power plants, air traffic control, rail systems, manufacturing systems, healthcare systems, construction industry, etc.

As a result of the search, more than 160 research materials could be firstly found. Looking into the main topics of those materials and judging the relevance of those topics to the fields of Safety-II, resilience engineering, and FRAM, the author selected core research articles that were judged to be the easiest to read as well as the most important in studying Safety-II and resilience engineering. All of the core articles were included in the references of this article. It should be noted that the search and selection process was subjective; they were conducted on the author's personal judgment. However, to corroborate the results of the selection, three other researchers reviewed those results and gave a feedback about their relevance to Safety-II, resilience engineering, and FRAM. All of them had more than 8 years of experience in the field of human factors and system safety engineering and had been studying Safety-II and resilience engineering for more than 3 years. Two researchers had conducted accident analysis based on FRAM at least two times. The three researchers firstly checked the validity of the key words and the list of the questions used for the literature search. Regarding the key words and search strategy, their opinion was that there were no problematic points. Next, they reviewed the initial list of the core articles and suggested five other articles that they think could be core articles. After reviewing five other articles, I added the three of them to the list of core articles.

When searching for research materials by using the combination of keywords stated above (e.g., Safety-II + accident analysis), the author listed up the following topics that need to be answered to get a right understanding of Safety-II and resilience engineering. Most of the topics were generated based on the questions that the author was asked in the lectures and consultations on Safety-II and resilience engineering.

- What are the limitations of Safety-I when they are used in complex socio-technical systems?
- Why and how can the use of Safety-I methods be problematic?
- What are the requirements for dealing with the limitations of Safety-I?
- What are the core concepts and principles of a new safety paradigm?
- What are the conceptual and practical differences between Safety-II and Safety-I?
- What are the practical methods for realizing the concepts of Safety-II?
- What are the essential points of resilience engineering?
- Can we evaluate the degree of resilience of an organization qualitatively or quantitatively?
- How can FRAM be used for accident analysis and risk assessment?
- What are the advantages of using FRAM as a system safety method?

Further, the author has looked for research materials that organized those topics in a logical way. Of the materials investigated, it was found that the recent study of Hollnagel and Macleod [25] gives four useful points of view for understanding those topics

systematically. They include the following: WAI (Work-As-Imagined) vs. WAD (Work-As-Done) [26–30], ETTO (Efficiency-Thoroughness Trade-Off) Principle [31,32], Methods with Accident Models [11–13,33,34], and WYLFIWYF (What You Look For Is What You Find) [35,36]. This article adopts the logical flow and structure used in the study of Hollnagel and Macleod [25]. Referring to the four perspectives and other relevant research articles, this article describes the basic concepts and principles of Safety-II. Then the fundamental concepts and methods of resilience engineering and FRAM are briefly reviewed. Several advantages of using FRAM as a new safety method, which have been demonstrated by previous studies, are summarized as well. And then, this article proposes a set of future research topics in those disciplines.

3. Results

3.1. Safety-II as a new safety paradigm

3.1.1. WAI vs. WAD

WAI means a work procedure or method optimized for a certain work situation. In general, system designers prepare WAI in anticipation of probable work situations. However, as systems are increasingly complex and accordingly the interactions between their functional elements become more complex, it is very impossible to anticipate all work situations and environmental changes [6,27]. It is thus impossible to develop WAI optimized for all the work situations [7]. If this is possible and workers are well trained and have sufficient resources (e.g. time, equipment, materials, etc.), it would be reasonable to argue that not following WAI or not working as specified in WAI is the main cause of all accidents.

However, considering the complexity and variability of work conditions in socio-technical systems, we can agree that this is a very unrealistic argument. In practice, human workers carry out their tasks constantly adapting to their work conditions, taking into account the demands of dynamically changing works and the resources currently available to them [27–29]. Such an adaptation is called performance adjustment [6]. When organizations perform their works, they also exhibit performance adjustment. Thus, we can say that actual work practices (WAD) may not be the same as WAI in a specified work context [30]. Moreover, in an unanticipated work situation where there is no pre-planned WAI, workers' adaptive performance adjustment is absolutely important for the successful work outcomes.

It should be noted, however, that this adaptive performance adjustment results in inconsistent work performance. This means that performance variability is a normal phenomenon that can be found in work systems [7]. It is also worth noting that this adaptive performance adjustment is the cause of many successful work outcomes and at the same time very rare adverse work outcomes (accidents or incidents) [6]. In other words, an accident happens when performance adjustments, which have always been successful in every day work situations, result in unexpected accumulation and combination of performance variability in a certain work condition. This means that the causes of successful work outcomes are not different from those of failed work outcomes. Both of them originate from the same source. It is more reasonable to regard accidents as abnormal results coming from successful work processes in a certain work condition. This is a point of view contradictory to the bi-modality assumption of Safety-I that failures occur due to specific and identifiable causes irrelevant to successes.

This point of view has an important implication in accident analysis. To understand why and how an accident occurred, it is necessary to firstly understand why and how the same work performance adjustments have been successful in many times previously and then why and how the accident happens at this time. This explains why it is important to thoroughly analyze the daily work performance (WAD) having resulted in successful work outcomes in accident investigation. In this sense, it is easily agreed that the assumption that an accident has its specific root causes to be fixed is very unreasonable. In addition, we need to think about again the traditional viewpoint that human beings or human errors can be considered a plausible root cause of accidents in many cases. However, this view needs to be changed. Because performance adjustment and performance variability are the significant concepts to understand the successful human and organizational works as well as the failures, we need to have different viewpoint about human errors. It is necessary to have a viewpoint that human errors are not the root causes of a failed outcome but the symptoms of poor system and task designs. What is important is to examine why we cannot sufficiently support human workers' performance adjustment. To sum up, Safety-I does not well reflect the arguments described above.

3.1.2. ETTO (Efficiency-Thoroughness Trade-Off) principle

As mentioned previously, it is impossible to fully predict every work condition of a system; it is thus necessary to pay attention to and investigate WAD. However, the ETTO principle needs to be the conceptual basis for analysing and understanding WAD in a system [31]. When human workers and organizations adaptively adjust their work process and performance in dynamically changing work situations, ETTO is the fundamental principle guiding their performance adjustment [31,32]. In other words, it is necessary to observe, investigate, and analyze practical work practices with ETTO principles in mind.

Workers and organizations always work with trade-offs in efficiency and thoroughness because all of the resources needed to meet work demands are not always present. Pursuing efficiency means working with the least amount of resources necessary to perform works; in contrast, pursuing thoroughness means conducting works after sufficient resources are available to avoid negative work outcomes. However, in reality, it is difficult to meet both simultaneously. It is, thus, necessary for workers and organizations to make trade-offs between them. For this reason, we need to have ETTO principle as a conceptual basis for understanding and analysing why and how performance adjustments are made and to attempt to understand it more systematically.

3.1.3. Methods with accident models

It was previously described that most of the safety methods based on Safety-I assume a plausible model of how an accident occurs. This means that analysts attempt to interpret the process of accidents in accordance with the model assumed in accident analysis methods that they use [33]. Obviously, the use of such an accident model makes accident analysis process more efficient. However, from the other point of view, it can be said that the process of trying to fit all the accidents into the assumed accident model is not reasonable in that it is likely to ignore the intricate actuality of an accident occurrence [5,6]. From the point of view of ETTO principle, we can say that the use of assumed accident models pursue efficiency more than thoroughness in accident analysis.

Additionally, most of the traditional accident models are based on linear causality (linear cause and effect relationships) [7]. This is the view that a cause leads to a certain result, and that the result is a new cause bringing about another result—the linear chain of causes and effects. In this linear model, forward reasoning from causes to results is no problem in terms of completeness and logic; however, backward reasoning from a result to causes does not guarantee completeness and logic [3]. An outcome in a system can results from several causes. Thus, even if it is known that A leads to B and B happens, we cannot warrant that B always results from A; B

sometimes can be the result of another cause C. In this regard, this shares a logical error and incompleteness in abductive reasoning. Nevertheless, for the efficiency of accident analysis, safety methods assuming an accident model based on such linear causality have been widely used in safety community. However, by relying strongly on linear causality-based accident models, accident analysts are likely to fall into hindsight bias and have too much unjustifiable confidence on a root cause.

In this regard, it can be said that traditional safety methods need to be improved in consideration of the concepts of Safety-II. In addition, since these methods mainly address failure cases such as accidents, they are clearly limited to examine successful performance adjustments and work outcomes that are emphasized in Safety-II [14,24]. First of all, as industrial systems become more complex, it is increasingly difficult and unreasonable to explain all accidents by a linear causal relationship. Since accidents are caused by unforeseen nonlinear combinations of performance variability in routine work processes, it is necessary to develop a system safety method reflecting the concept of performance variability and their diverse combinations [37,38]. One example of such a method is FRAM to be explained later.

3.1.4. WYLFIWYF

The quality of accident analysis is inevitably dependent on the things checked and examined in the analysis process because analysts understand an accident and conclude absolutely based on them [10]. To support analysts in identifying factors that seem to be related to an accident, most of the accident analysis methods provide a plausible set of causal factors and their classifications [33]. The cause factor classification system in the Human Factors Analysis and Classification System (HFACS) is a typical example [12]. In addition, as explained earlier, it has tended to understand accidents based on linear causality and to identify a root cause (especially a person committing human error that can be blamed) for the efficiency of accident investigation, even though they are illogical and inappropriate. Since Safety-I focuses on failure situations to eliminate hazards as the first priority and examines some of the causal factors that can plausibly explain these failures, it is very likely that there exist factors that are related to an accident under investigation but not investigated. It is also likely that there exist failed system elements that are not examined because they are judged not to be relevant to an accident under investigation. This is the problem to be noted when analysts strongly rely on a set of causal factors in accident analysis.

Based on the above four points of view, the following can be summarized. Safety-I defines safety as a condition where failures are minimal or absent, but as systems become more complex, it is practically impossible to predict all failures in advance, find, and eliminate all the causes for them. In contrast, Safety-II defines safety as a condition in which successful work outcomes continue, or in a condition where such successful work outcomes are maximized. Safety-I and Safety-II have the common consequence that reduces the number of adverse work outcomes (accidents or incidents) as a result of their efforts; however, they have fundamentally different safety concepts and approaches [6]. Safety methods based on Safety-II are ultimately concerned with how to ensure a successful work situation rather than focusing on how to minimize failed situations. This requires a thorough and systematic investigation of how successful work outcomes and working conditions are achieved. Based on this, it is necessary to continuously monitor successful work situations in everyday work settings, and to proactively manage the changes (reduction in performance variability) while being aware of large and small changes (performance variability) of these work situations. In other words, Safety-II claims that safety professionals monitor a work system and its surroundings vigilantly and proactively respond to changes in the system and the environment, while always worrying about system safety [25].

3.2. Resilience and resilience engineering

A system operates successfully without any accidents in many cases, and very rarely accidents occur. Nevertheless, it is impossible to fully predict all the accident situations and their likelihood particularly in complex socio-technical systems. As explained previously, a traditional approach for ensuring the system safety was to identify and eliminate the causes of an accident once it happens and to repeat such activities if a new accident occurs [5,14]. In this sense, we can say that a traditional approach is principally reactive [6]. Of course, risk assessment has been done to predict probable accident situations and prepare control measures for mitigating the effects of accidents. A general industrial practice was that risk assessment is conducted during the design process of a system and additional risk assessment is conducted whenever there is a change of a work system or its environmental context (this is called “management of change”). However, a continuous monitoring and active management of changing risks in a system has less been emphasized in traditional risk assessment. This should be conducted even if there is no any significant change in a system. In this regard, traditional risk assessment seems to be more reactive as well [8].

As Safety-II implies, a better way for maximizing the system safety would be a proactive approach ensuring that a system keeps operating successfully and reliably [6,7]. This naturally leads to the

Table 1
Sample questions developed by Australian Radiation Protection and Nuclear Safety Agency [45,46]

No.	Ability to respond
1	Do we frequently identify possible events or scenarios which we may need to respond to, and do we consult with staff to help identify them?
2	How frequently do we test our ability to respond to an incident or event?
3	How do we ensure that our response capability is sufficient to respond appropriately to these possible identified scenarios?
No.	**Ability to monitor**
1	Is there a way we can improve the way we track how our systems or operations are performing to ensure they are performing safely?
2	How do we ensure that our operations are not drifting or deviating from expected performance?
3	What processes or practices do we follow if we find that our operations deviate from expected performance?

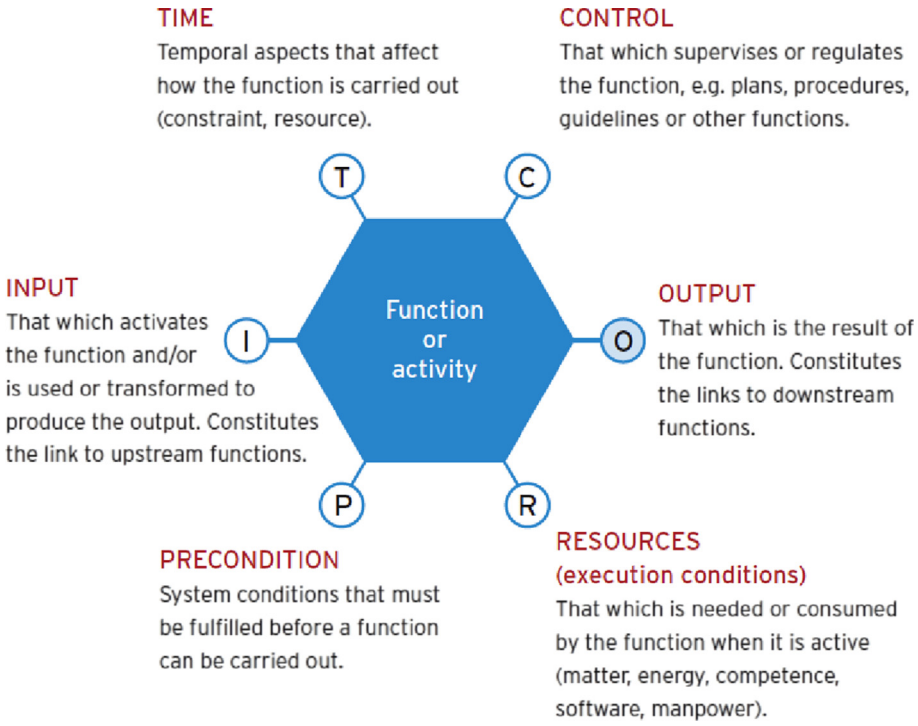

Fig. 1. Six aspects characterizing a function in FRAM (borrowed from [38]).

concept of resilience. In resilience engineering, a system is said to be resilient if it can adjust its functioning prior to, during, or following changes and disturbances, and thereby sustain required operations under both expected and unexpected conditions [7,21,22]. Simply, resilience means the ability of a system that achieves its functional purposes, adapting to unexpected work conditions as well as expected conditions and proactively suppressing the risks in a system [7,39]. Resilience engineering is the scientific discipline that focuses on developing the principles and practical methods that are necessary to enable systems to function in a resilient manner [21,22].

More specifically, how can we make a system have resilient ability? Or what is the basic requirements for a system to be resilient? Regarding this question, resilience engineering claims that a resilient system needs to exhibit the four capabilities: responding, monitoring, learning, and anticipating [40]. Firstly, responding refers to the ability of a system to know what to do in anticipated or unanticipated work situations and the ability to adapt the way a system works to changing work conditions. This capability includes responding at the blunt end (e.g., developing a new safety policy) as well as responding at the sharp end (e.g., handling quickly changing task situations). Secondly, monitoring means the ability to know what to look for attentively or what to identify and monitor things that can seriously affect or actually affect the performance of a system in the near term. This capability includes the ability to monitor what is happening inside a system as well as its surroundings. It includes monitoring at the blunt end (e.g., examining the effectiveness of current training systems) as well as monitoring at the sharp end (e.g., observing critical sensor data indicating current system states). Thirdly, learning refers to the ability of a system to continuously learn from successful as well as failed work outcomes and to accumulate information and knowledge useful for improving the system safety. The ability to review the effects of learning and to reflect the review for a more effective learning is another important aspect of this fourth capability. Lastly, anticipating is the ability to know what to expect in the relatively long term or to predict how a system and its surroundings will change in the future. To this end, it is essential to establish a right model of a system and its surroundings. To sum up, a proactive safety management based on resilience engineering emphasizes that one should be always aware of what changes can occur in a system and its surrounding conditions and should always attempt to secure resources or means to cope with them. However, what is interesting is that there are four foundational principles underlying industrial hygiene, which include anticipating, recognizing, evaluating, and controlling. It is a decision-making framework and process used for identifying and managing risks. Although they show somewhat differences from the four capabilities of a resilient system, it would be interesting to find their connections.

Next, an arising question is about how to assess the degree of resilience of a system or how to discern a resilient system from others. Resilience engineering offers useful methods for this practical issue [40–46]. Of those, Resilience Assessment Grid (RAG) would be the most popular method to assess how well a system is capable of exhibiting the four abilities [40]. RAG evaluates the resilience capabilities of a system by the use of key assessment questions for each ability. The current set of key assessment questions are never a complete one; instead, they need to be customized in consideration of the characteristics of a system, the purposes of assessment, etc. For instance, Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) developed a set of questions for assessing the four resilience abilities, referring to the key assessment questions in RAG [45,46]. The customized questions are a part of the regulatory guide developed by ARPANSA. Table 1 shows the sample questions developed by ARPANSA, which aim to evaluate the ability to respond and monitor.

3.3. *Functional Resonance Analysis Method*

It is necessary to have a right model of a work system, particularly a model describing the actual work practices (WAD), to

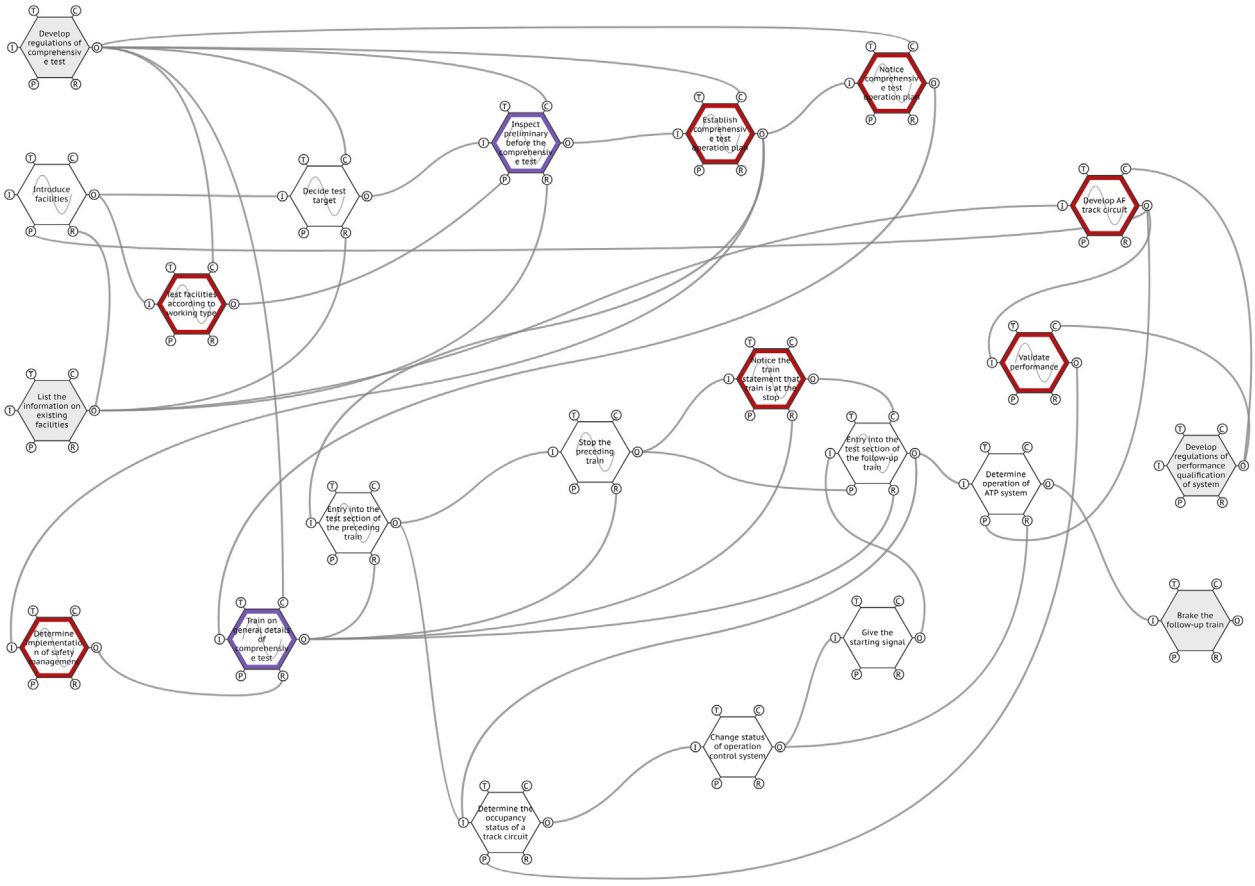

Fig. 2. An example of FRAM model.

analyse accidents and to assess risks based on Safety-II [6,25]. Of course, the use of such a model is an essential activity for enhancing the four core abilities of a resilient system systematically [21]. However, it should be noted that a model needs to reflect the fundamental concepts underlying Safety-II, which include performance adjustment and variability in conducting a task (function), the propagation of variability in a system, the complicated interactions between system elements, etc. [37,38].

FRAM was developed for this purpose and has been widely used in a range of work domains and problem situations [37,38,47–65]. Strictly speaking, FRAM is a method for modelling complex socio-technical systems based on functional resonance that reflects the concept of performance variability and its propagation. Although it is a system modelling method, it can be effectively used for accident investigation and risk assessment from the perspective of Safety-II [47–50]. First of all, one of the big advantages of FRAM is that it enables analysts to understand the process of accidents and to assess probable accident situations without assuming any particular accident model [37]. A model developed by FRAM merely represents actual work practices in a system; it is useful to represent WAD. For this reason, it can also be used for investigating how works can be done successfully [37,38].

The basic unit of the FRAM model is a function (task), which is characterized by six aspects: Input, Output, Time, Control, Precondition, and Resources [37,38]. Fig. 1 shows these six aspects.

Generally, the construction and use of a FRAM model follows the four steps [37]. Firstly, the functions to be represented in a model should be identified and described. For this, task analysis or function analysis needs to be thoroughly conducted. The identified functions are characterized in consideration of the six aspects in Fig. 1. Secondly, the variability of each function needs to be identified. In particular, the main concern is the functions that are conducted by human workers and organizations rather than technical systems such as automation. This is because performance variability is especially meaningful when human workers or organizations do some tasks. Performance variability is represented by several failure mode types such as time and precision. Thirdly, it is necessary to identify how the performance variability of each function can be combined and propagated. For this, it is important to understand the relationships between the functions in a model, which are represented by the connections between the six aspects of one function and those of another function. Lastly, the countermeasures to manage performance variability need to be developed on the basis of the developed model.

Fig. 2 shows an example of a FRAM model. This is the model developed by a graduate student being supervised by the author. This model was developed to understand the situations and process of the train collision accident that occurred in 2017 at central railway line in South Korea. The basic unit of the FRAM model is each function; however, the core of the FRAM model would be the connection between the functions that make up a system. Of the six aspects of each function, the five aspects (Input, Time, Control, Precondition, and Resources), except for Output, are linked to the Output of other functions. For example, the Output of A function can be connected to the Input of B function and to the Control of D function as well as to the Precondition of C function. In this way, the interactions between the functions can be understood using the relationship between these six aspects. Some functions have

Table 2
Summarized comparison between Safety-I and Safety-II [24]

No.	Safety-I (accident analysis methods)	Safety-II (accident analysis methods)
1	They attempt to identify the causes of an accident with a linear and simple cause–effect relationship.	Accident analysis should admit that an accident cannot be sufficiently explained by a linear and simple cause–effect relationship.
2	They generally assume an accident causation model and attempt to explain an accident based on the model.	An accident needs to be investigated without too much relying on an accident causation model.
3	They strive to look for a root cause and tend to neglect other possible causes once a root cause is found.	An accident is not so simple that it can be sufficiently explained only with a root cause.
4	They attempt to understand an accident with a predetermined set of causal factors linked to a presumed accident model.	It should be acknowledged that the currently assumed set of causal factors may not be actual causes of the accident and that other contextual factors assumed not to be problematic may be actual causes.
5	They have a stance that all failed work outcomes have their unique causes.	The causes of successful work outcomes and failed work outcomes are not different but the same.
6	They are inclined to seek human errors and regard them as root causes.	An accident analysis method should focus on performance variability in terms of resource demands and resources available in the situation of an accident, instead of human errors.

performance variability when conducting these functions (as explained above, mainly when workers or organizations perform these functions). In Fig. 2, a function with a wave within it means that there is a possibility of variability in the performance of the function. In addition, the variability of the function spreads to other functions by the connection between the six characteristics, so that the performance variability can be amplified, maintained or reduced. Like this, FRAM models make it possible to understand the occurrence of an accident and to assess risks in terms of performance variability and its propagation.

A FRAM model represents the potential couplings of functions that should have been worked to result in successful outcomes. However, it does not represent the actual couplings that may exist under given situations. In addition, the sequential order of carrying out functions is not represented in a FRAM model. An accident scenario with actual couplings is represented as a type of instantiation based on a model. In the instantiation of an accident, one can construct the event sequence of functions to explain how an accident happens. Such a sequence can be regarded as a cause–effect relationship. Without such a sequence, how an accident happens could not easily be explained. However, there is a significant difference between such a sequence in an instantiation and linear causal relationships speculated in traditional accident analysis methods. While the latter represents an assumed and fixed relationships between system components, the former represents transient relationships between functions. Thus, although a preceding function can be the cause of a following function in an instantiation, the preceding cannot be the cause of the following in

Table 3
Advantages of using Functional Resonance Analysis Method (FRAM) for accident analysis and risk assessment

No.	Advantages of using FRAM	Literature
1	Since FRAM models do not assume any accident model and represent WAD well, it helps understand the process and situation of accidents from a more holistic point of view.	[47,48,55]
2	FRAM models enable analysts to have the view that accidents with the same phenomena can occur by different causes and in different ways.	[55,56]
3	Analysts can look into the whole system as well as its detailed parts at the same time by using FRAM. They lead analysts to consider several systems with different scale collectively and flexibly.	[57,58]
4	With the use of FRAM model, it is possible to consider the structural aspects of a system as well as functional aspects.	[56,59,60]
5	FRAM models enforce analysts to think of the interactions between functional elements of a system as a central focal point of accident analysis and risk assessment.	[56,61,62]
6	Performance variability is the central conceptual basis of FRAM models. Thus, they enable analysts escape from the misconception that the sources of successful work outcomes are different from those of failed work outcomes.	[55,56]
7	FRAM models helps analysts escape from the misconception that there is a specified root cause for an accident.	[55,57]
8	It is possible to represent how things go right, by the use of FRAM models.	[53,55,57,63]
9	FRAM models is useful to represent actual works in practice (WAD).	[52,63]
10	Considering performance variability and its propagation represented in FRAM models, we can explain an accident as an emergent phenomenon rather than outcomes resulting from linear cause–effect relationships.	[50,56,61,62]
11	Several instances can be developed from one FRAM model; thus, it is possible to consider the dynamic state changes of a system with the use of FRAM.	[64]
12	FRAM helps analysts predict how the states of a system can change as a result of the change of a system element	[50,63]
13	It is possible to consider non-technical elements (human and organization) as well as technical ones.	[50,61,64]
14	FRAM models enable analysts to consider workers' performance adjustment and contextual factors influencing the work performance in a systematic manner.	[50,63,64]
15	FRAM helps analysts escape from the misconception that human errors are the root causes of an accident. Instead, FRAM leads them to have the view that human errors are the results of poor system and task designs.	[48,57]

another instantiation. This can be explained by using the concept of functional resonance (performance variability).

4. Discussion

4.1. Balanced use of Safety-I and Safety-II

In comparison with Safety-I, Safety-II, and resilience engineering have surely several different philosophies and principles and show some big advantages over Safety-I in the promotion of system safety. The typical weak points of Safety-I, which were explained previously, have been continuously recognized by safety practitioners and researchers. They have attempted to deal with the weak points, and Safety-II has been proposed as a new paradigm through their efforts. However, it should be noted that they have been developed to supplement the drawbacks of Safety-I instead of wholly replacing it. Accordingly, it is necessary to discern the situations where Safety-I methods are sufficiently meaningful and effective from those where they are insufficient and thus Safety-II methods can be a useful alternative. What is important is to use a proper concept and method from Safety-I and Safety-II synergistically, in consideration of problem situations.

In this regard, it would be helpful to have a summarized comparison between Safety-I and Safety-II, although they were described in the previous section. Their differences would be more clarified when their main features are compared in relation with accident analysis. Table 2 gives a summarized comparison between Safety-I and Safety-II that focuses on their accident analysis methods [24].

Other systematic accident analysis methods, such as AcciMap [17] and STAMP (Systems Theoretic Accident Model and Process) [2], have several features that can supplement the limitations of Safety-I methods. Without doubt, they are useful methods that enable accident analysis to enjoy systems thinking in the accident analysis. However, FRAM would be the currently most useful method that facilitates the use of core concepts and principles of Safety-II. Based on the literature reporting the use of FRAM in several work domains, the advantages of using FRAM for accident analysis and risk assessment can be summarized as shown in Table 3.

4.2. Future research issues

During the last two decades, Safety-II and resilience engineering have much contributed toward promoting system safety from the new perspectives. Nonetheless, there seem to be several points to be improved and further studied to advance the disciplines. Here, the author proposes the following research issues that are considered important in the effective use of Safety-II and resilience engineering methods and in the development of new methods based on Safety-II and resilience engineering. It should be noted that they are never a complete set of future issues; there would be more significant and urgent issues.

- Development of practical and easy-to-use methods for investigating how workers and organization adjust their performance in the field, and development of case studies in a range of work domains.
- Development of methods and case studies for examining the types and patterns of performance variability and the effects of the spread of performance variability.
- Case studies of understanding the differences between current WAI and WAD and establishing strategies for improving them, on the basis of FRAM models.
- Development of guidelines about how to analyze a lot of successful work outcomes, and development of methods that support system designers in developing measures for managing performance variability, based on the understanding of how things go successfully.
- Development of another new system modelling methods like FRAM, which can be used for dealing with the issues above or integration of FRAM and other useful modelling concepts such as abstraction hierarchy [51].
- Development of industry-specific guidelines and case studies for supporting the use of FRAM.
- Development of engineering tools and techniques for strengthening workers' performance adjustment ability in diverse work contexts (particularly unexpected situations) and reducing performance variability.
- Development of ways of integrating Safety-I and Safety-II methods.
- Development of intelligent methods for monitoring and controlling the changes of a system and its surroundings.
- Development of industry-specific key assessment questions for the four abilities of a resilient system.
- Development of industry-specific case studies of using RAG.

However, as regard the effective use and the advancement of FRAM, a recent review article on FRAM [65] needs to be noted. It offers a very comprehensive review of previous studies on FRAM; thus, it is recommended to readers who want to understand the past, present, and future of FRAM-related studies in a comprehensive way. They can find several research directions to modify the FRAM to enhance the effectiveness of FRAM in accident analysis and risk assessment. They include attempts to support the identification of functions represented in a FRAM model and the characterization of functional variability and studies to support the quantification of functional variability and its aggregation in an instantiation of FRAM.

5. Conclusions

This article offered an introductory guide to Safety-II, resilience engineering, and FRAM to help safety professionals, who are still not familiar with their concepts and principles, have a right understanding on them. As pointed out several times earlier, the shift to Safety-II and resilience engineering does not mean that Safety-I methods will not be needed any more. It would be a better strategy to selectively use Safety-I and Safety-II methods in consideration of a type of system, the characteristics of a working condition, etc.

If analysts use Safety-I methods under the recognition of their limitations, they can still be effectively used for promoting system safety in many situations. Even if we do our best to manage system safety proactively, accidents can still happen. Once an accident occurs, we need to understand the processes and situation of the accident thoroughly and to think about various ways of mitigating the negative effects of the accident and preventing its recurrence. For this, if we can use Safety-I methods wisely acknowledging their drawbacks, there is no reason not to use them, alongside the use of Safety-II methods. It is undeniable that the results of accident analysis and risk assessment based on Safety-I methods provide useful insights for improving system and task design, training systems, and safety culture. They are also important information to identify strategies and means for supporting workers' performance adjustment and reducing performance variability.

However, although both Safety-I and Safety-II methods are surely useful, it is true that a lot of safety practitioners still have difficulty in applying them to their industrial safety problems. This is mainly because they have limited resources such as time and financial support. Addressing this issue will also be a big challenge to system safety researchers. They need to develop more simplified and practical methods to leverage the values of Safety-I and Safety-II.

Conflicts of interest

All authors have no conflicts of interest to declare.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (Ministry of Education) (NRF-2020R1I1A3069000).

References

[1] Dekker S. Field guide to human error investigations. Aldershot (UK): Ashgate; 2002.
[2] Leveson N. Engineering a safer world: systems thinking applied to safety. Cambridge: The MIT Press; 2011.
[3] Yoon YS, Ham D-H, Yoon WC. A new approach to analyzing human-related accidents by combined use of HFACS and activity theory-based method. Cognition, Technology & Work 2017;19:759–83.
[4] Yoon YS, Ham D-H, Yoon WC. Application of activity theory to analysis of human-related accidents: method and case studies. Reliability Eng System Safety 2016;150:22–34.
[5] Hollnagel E, Leonhardt J, Licu T, Shorrock S. From Safety-I to Safety-II: a white paper. Brussels (Belgium): EUROCONTROL; 2013.
[6] Hollnagel E. Safety-I and Safety-II: the past and future of safety management. Farnham (UK): Ashgate; 2014.
[7] Hollnagel E. Resilience engineering: a new understanding of safety. J Ergonomics Society of Korea 2016;35:185–91.
[8] Leonhardt J, Hollnagel E, Macchi L, Kirwan B. A white paper on resilience engineering for ATM. Brussels (Belgium): EUROCONTROL; 2009.
[9] Hollnagel E. Understanding accidents-from root causes to performance variability. In: Proceedings of the 2002 IEEE 7th human factors and power plants 2002. p. 1–6.
[10] Underwood P, Waterson P. Systematic accident analysis: examining the gap between research and practice. Accident Analysis Prevention 2013;55:154–64.
[11] 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. Accident Analysis Prevention 2014;68:75–94.
[12] Wiegmann DA, Shappell SA. A human error approach to aviation accident analysis: the Human Factors Analysis and Classification System. Farnham (UK): Ashgate; 2003.
[13] Reinach S, Viale A. Application of a human error framework to conduct train accident/incident investigations. Accident Analysis Prevention 2006;38:396–406.
[14] Sujan MA, Huang H, Braithwaite J. Learning from incidents in health care: critique from a safety-II perspective. Safety Science 2017;99:115–21.
[15] Patterson M, Deutsch E. Safety-I, Safety-II and resilience engineering. Current Problems Pediatric Adolescent Health Care 2015;45:382–9.
[16] Ferjencik M. An integrated approach to the analysis of incident causes. Safety Science 2011;49:886–905.
[17] Svendung I, Rasmussen J. Graphic representation of accident scenarios: mapping system structure and the causation of accidents. Safety Science 2002;40:397–417.
[18] Perrow C. Normal accidents-living with high risk technologies. Princeton: Princeton University Press; 1999.
[19] Patriarca R, Bergström J, Di Gravio G, Costantino F. Resilience engineering: current status of the research and future challenges. Safety Science 2018;102:79–100.
[20] Dekker S. Reconstructing human contributions to accidents: the new view on error and performance. Journal of Safety Research 2002;33:371–85.
[21] Hollnagel E, Woods DD, Leveson N. Resilience engineering: concepts and precepts. Aldershot (UK): Ashgate; 2006.
[22] Hollnagel E, Pariès J, Woods DD, Wreathall J. Resilience engineering in practice: a guidebook. Farnham (UK): Ashgate; 2011.
[23] Shorrock S. What Safety-II isn't; 2016. Available from: http://humanisticsystems.com/2014/06/08/what-safety-ii-isnt/.
[24] Ham D-H, Park J. Use of a big data analysis technique for extracting HRA data from event investigation reports based on the Safety-II concept. Reliability Engineering System Safety 2020;194:106232.
[25] Hollnagel E, Macleod F. The imperfections of accident analysis. Loss Prevention Bulletin 2019;270:2–6.
[26] Havinga J, Dekker S, Rae A. Everyday work investigations for safety. Theoretical Issues Ergonomics Science 2017;19:213–28.
[27] de Carvalho PV, Righi AW, Huber GJ, Lemos C, Jatoba A, Gomes JO. Reflections on work as done (WAD) and work as imagined (WAI) in an emergency response organizations: a study on firefighters training exercises. Applied Ergonomics 2018;68:28–41.
[28] Woltjer R, Pinska-Chauvin E, Laursen T, Josefsson B. Towards understanding work-as-done in air traffic management safety assessment and design. Reliability Engineering System Safety 2015;141:115–30.
[29] Wachs P, Saurin TA, Righi AW, Wears RL. Resilience skills as emergent phenomena: a study of emergency departments in Brazil and the United States. Applied Ergonomics 2016;56:227–37.
[30] Wachs P, Saurin TA. Modelling interactions between procedures and resilience skills. Applied Ergonomics 2018;68:328–37.
[31] Hollnagel E. The ETTO principle: efficiency-thoroughness trade-off. Farnham (UK): Ashgate; 2009.
[32] Xiao T, Sanderson P, Clayton S, Venkatesh B. The ETTO principle and organizational strategies: a field study of ICU bed and staff management. Cognition, Technology & Work 2010;12:143–52.
[33] Salmon PM, Stanton NA, Lenne M, Jenkins DP, Rafferty LA, Walker GH. Human factors methods and accident analysis: practical guidance and case study applications. Farnham (UK): Ashgate; 2011.
[34] Salmon PM, Cornelissen M, Trotter MJ. Systems-based accident analysis methods: a comparison of Accimap, HFACS, and STAMP. Safety Science 2012;50:1158–70.
[35] Hulme A, Stanton NA, Walker GH, Waterson P, Salmon PM. What do applications of systems thinking accident analysis methods tell us about accident causation? A systematic review of applications between 1990 and 2018. Safety Science 2019;117:164–83.
[36] Lundberg J, Rollenhagen C, Hollnagel E. What you find is not always what you fix-how other aspects than causes of accidents decide recommendations for remedial actions. Accident Analysis and Prevention 2010;42:2132–9.
[37] Hollnagel E. FRAM: the functional resonance analysis method. Farnham (UK): Ashgate; 2012.
[38] Hollnagel E, Hounsgaard J, Colligan L. FRAM-the Functional Resonance Analysis Method-a handbook for the practical use of the method. Center for Quality; 2014.
[39] Anderson JE, Ross A, Back J, Duncan M, Snell P, Walsh K, Jaye P. Implementing resilience engineering for healthcare quality improvement using the CARE model: a feasibility study protocol. Pilot Feasibility Studies 2016;2:61.
[40] Hollnagel E. Safety-II in practice: developing the resilience potentials. London (UK): Routledge; 2018.
[41] Patriarca R, Gravio GD, Costantino F, Falegnami A, Bilotta F. An analytic framework to assess organizational resilience. Safety and Health at Work 2018;9:265–76.
[42] Shirali G, Shekari M, Angali KA. Assessing reliability and validity of an instrument for measuring resilience safety culture in sociotechnical systems. Safety Health Work 2018;9:296–307.
[43] Lundberg J, Johansson B. Systemic resilience model. Reliability Engineering System Safety 2015;141:22–32.
[44] Hoffman RR, Hancock PA. Measuring resilience. Human Factors 2017;59:564–81.
[45] Arpansa. Regulatory guide: holistic safety. Australian Radiation Protection and Nuclear Safety Agency; 2017.
[46] Arpansa. Regulatory guide: holistic safety-sample questions. Australian Radiation Protection and Nuclear Safety Agency; 2017.
[47] Raben DC, Viskum B, Mikkelsen KL, Hounsgaard J, Bogh SB, Hollnagel E. Application of a non-linear model to understand healthcare processes: using the functional resonance analysis method on a case study of the early detection of sepsis. Reliability Engineering and System Safety 2018;177:1–11.
[48] Hollnagel E, Pruchnicki S, Woljter R, Etcher S. Analysis of Comair flight 5191 with the functional resonance accident model. In: Proceedings of the 8th international symposium of the Australian aviation psychology association 2008.
[49] Rosa LV, Haddad AN, de Carvalho P. Assessing risk in sustainable construction using the functional resonance analysis method (FRAM). Cognition, Technology & Work 2015;17:559–73.
[50] Patriarca R, Di Gravio G, Costantino F, Tronci M. The functional resonance analysis method for a systemic risk based environmental auditing in a sinter plant: a semi-quantitative approach. Environmental Impact Assessment Rev 2017;63:72–86.
[51] Patriarca R, Bergström J, Di Gravio G, Costantino F. Defining the functional resonance analysis space: combining abstraction hierarchy and FRAM. Reliability Engineering System Safety 2018;165:34–46.
[52] Clay-Williams R, Hounsgaard J, Hollnagel E. Where the rubber meets the road: using FRAM to align work-as-imagined with work-as-done when implementing clinical guidelines. Implementation Science 2015;10:125.
[53] Raben DC, Both SB, Viskum B, Mikkelsen KL, Hollnagel E. Learn from what goes right: a demonstration of a new systematic method for identification of leading indicators in healthcare. Reliability Engineering System Safety 2018;169:187–98.
[54] Aguilera M, da Fronseca B, Ferris T, Vidal M, de Carvalho P. Modelling performance variabilities in oil spill response to improve system resilience. J Loss Prevension Process Industries 2016;41:18–30.
[55] Hounsgaard J. Patient safety in everyday work: learning from thigs that go right. University of Southern Denmakr; 2016.
[56] Herrera IA, Woltjer R. Comparing a multi-linear (STEP) and systemic (FRAM) method for accident analysis. Reliability Engineering System Safety 2010;95:1269–75.
[57] de Carvalho P. The use of Functional Resonance Analysis Method (FRAM) in a mid-air collision to understand some characteristics of the air traffic management system resilience. Reliability Engineering System Safety 2011;96:1482–98.
[58] Woltjer R. Resilience assessment based on models of functional resonance. In: Proceedings of the 3rd symposium on resilience engineering 2008.

[59] Tian J, Wu J, Yang Q, Zhao T. FRAMA: a safety assessment approach based on Functional Resonance Analysis Method. Safety Science 2016;85:41–52.
[60] Furniss D, Curzon P, Blandford A. Using FRAM beyond safety: a case study to explore how sociotechnical systems can flourish or stall. Theoretical Issues Ergonomics Science 2016;17:507–32.
[61] Patriarca R, Di Gravio G, Costantino F. A Monte Carlo evolution of the Functional Resonance Analysis Method (FRAM0 to assess performance variability in complex systems. Safety Science 2017;91:49–60.
[62] Pereira A. Introduction to the use of FRAM on the effectiveness assessment of a radiopharmaceutical dispatches process. In: Proceedings of 2013 international nuclear atlantic conference 2013.
[63] Praetorius G, Hollnagel E, Dahlman J. Modelling vessel traffic service to understand resilience in everyday operations. Reliability Engineering System Safety 2015;141:10–21.
[64] de Vries L. Work as Done? Understanding the practice of sociotechnical work in the maritime domain. J Cognitive Engineering Decision Making 2017;11:270–95.
[65] Patriarca R, Di Gravio G, Woltjer R, Costantino F, Praetorius G, Ferreira P, Hollnagel E. Framing the FRAM: a literature review on the functional resonance analysis method. Safety Science 2020;129:104827.