24

Resilience Engineering for Sociotechnical Safety Management

Riccardo Patriarca

Introduction

It was October 2004, when a pool of experienced researchers sat together in the Swedish city of Soderkoping reflecting on what might have been done to further improve the field of safety management. At that time, it was acknowledged that the nature of work in modern societies called for a reconsideration of what is meant by the terms *risk* and *safety*. Technology was—and is now more than ever—evolving to deal with fast-moving and competing societal requirements. The related dynamic interactions among technical, human, procedural, and organizational aspects of work have contributed to increase the inherent complexity of pure technological systems. These latter have become even more symbiotically interrelated to human agents and organizational aspects with severe implications for safety management.

Safety is generally considered as the characteristic of a system that prevents damage to the health of people (i.e., injury or loss of life), property, or adverse consequences for the environment. Following etymology, the English word *safe* comes from the Latin word *salvus*, which means intact or whole. In organizational processes, the term *safe* refers to something as being without harm or injury or even free from related risks (Hollnagel, 2018). Risk can be considered as a situation or an event where something of human value (including humans themselves) has been put at stake with an uncertain outcome (Rosa, 1998).

Building on this understanding of safety, during the first Resilience Engineering Association Symposium held in Soderkoping in 2004 the notion of resilience and, more specifically, resilience engineering moved from the original state of consensus toward a more structured stage of knowledge generation (Dekker, 2006). To better understand the scientific

Riccardo Patriarca, *Resilience Engineering for Sociotechnical Safety Management* In: *Multisystemic Resilience*. Edited by: Michael Ungar, Oxford University Press (2021). © Oxford University Press. DOI: 10.1093/oso/9780190095888.003.0025

meaning and relevance of resilience in the context of safety management, however, it is necessary to take a conceptual step backward.

Formally speaking, the science of safety was developed to provide the epistemically most warranted and reliable statements on the subject, which reflect the best research across multiple disciplines (Hansson, 2013). As such, safety science can be considered as being constituted by two scientific components: the acquired knowledge about safety-related phenomena and the conceptual tools for understanding, assessing, characterizing, communicating, and managing safety.

The concept of resilience in safety management, meanwhile, has come to refer to the activities taken to understand, assess, communicate, and manage safety of a system, an organization or even a society, based on knowledge products produced at both conceptual and pragmatic levels. Combined, these knowledge products have come to be known as resilience engineering with the explicit aim to consider systemic sociotechnical complexity and to understand how this complexity affects a system's behavior and performance. These systems can range from aircraft to hospitals, vessels, trains, or any system characterized by a symbiotic interaction among technological, human, and social (or even societal) elements.

This chapter will first introduce the notion of complexity for sociotechnical system analysis as a starting point for resilience research that improves system safety. Next, a description of two methods typically used in resilience engineering to improve safety will be presented: the resilience analysis grid (RAG) and the functional resonance analysis method. This chapter includes examples of both methods and their application to engineering problems. The last part of the chapter summarizes the contributions resilience engineering can make to the safety of systems and a possible research agenda.

On Complexity

The word *complex* comes from the Latin *complexus*, which means "what is woven together." In the scientific world, the word *complexity* first appears within the second law of thermodynamics, in relation to the inherent irreversibility of time and a molecule's motion (Morin, 2006). Since then, research on complexity has come to a number of multidisciplinary perspectives which hold a common interest in the analysis of diverse interacting and intertwined elements that are able to adapt or react to processes they are involved in, or which they contribute to (Arthur, 1999). In a sociotechnical system, processes are strictly dependent and interacting, through multiple hardly identifiable patterns that have the potential for dynamic, nonlinear, and unpredictable behaviors. By way of illustration, consider Alaska Airlines Flight 261. In January 2000, the MD-80 taking off from Puerto Vallarta in Mexico and headed to Seattle encountered a serious problem: the horizontal stabilizer, designed to control the aircraft's node attitude during cruise, appeared to be jammed. The problem led to a disaster: 2 pilots, 3 cabin crewmembers, and 83 passengers on board were killed when the airplane was destroyed on impact. Even though an investigation identified a broken part (the jackscrew-nut assembly that held the horizontal stabilizer), the final accident report included a complex intertwined muddle of factors related to organizational practices, strategic decisions, regulatory gaps, and lack of proper redundancy strategies, which over years were

progressively accepted as normal but created patterns that were the basis for the disaster itself. A critical and detailed analysis of the event has been proposed by Dekker (2011).

Epistemologically, *complex* is not a synonym for *complicated* (Dekker, Bergström, Amer-Wåhlin, & Cilliers, 2013): a system is complicated if it is ultimately knowable by a set of rules (more or less difficult to define and understand) that are able to capture its functioning, while a complex system is never fully knowable, with the impossibility to attain a complete fixed or exhaustive description (Cilliers, 2010; Heylighen, Cilliers, & Gershenson, 2007). To Illustrate these differences, Figure 24.1 describes two systems: System A, whose tight links make it a complicated system (under the hypothesis that there are no more hidden links present), and System B, whose complexity is ascribed to multiple degrees of freedom that make it impossible to predict the system's behavior and evolution precisely. In more general terms, System B would be more complex than System A, since some of the degrees of freedom of System A are constrained (Goldratt, 2008). The scientific field of resilience engineering acknowledges that complexity is not considered a thing per se, rather it is a situation to be investigated (Rasmussen, 1979).

Following a broader perspective, a sociotechnical system can be interpreted as a type of complex adaptive system whose analysis might benefit of insights from a complexity management viewpoint. Complexity can be thus managed according to three different perspectives: the algorithmic complexity, the deterministic complexity, and the aggregate complexity (Manson, 2001). Algorithmic complexity refers to computational efforts necessary for solving a problem. Deterministic complexity is grounded in chaos and catastrophe theory for the determination of major effects in output variables coming from minor changes in a set of initial variables, with high potential to become prone to crumble for large systems. Deterministic complexity relies on mathematic equations and strict assumptions of how systems behave to make equations credible.

On the contrary, aggregate complexity aims at gaining a holistic representation of a system, not forcing a strict mathematical correspondence. In this context, a complexity-oriented perspective is more focused on relationships than on constituent elements (Hollnagel, 2012a). Specifying the scope of the aggregate complexity notion, a system analysis needs to acknowledge three dimensions: the world in which the system acts, the involved elements, and the representation utilized in the observation of the system, which contributes

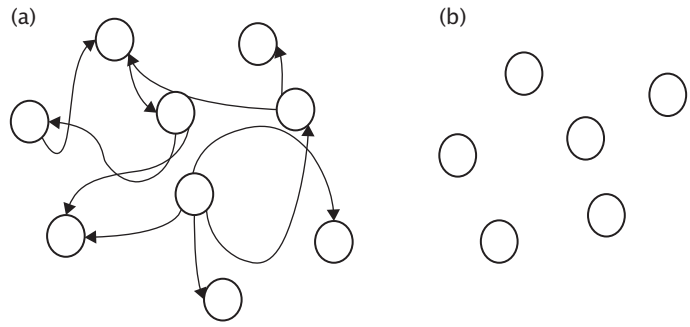

FIGURE 24.1 Complicated System A versus complex System B.

to complexity itself (Woods, 1988). A system representation is a certain model that is developed to offer a representation of a system, which has to inherently capture the dynamicity and intertwined nature of the system at hand.

It is then possible to define a set of common characteristics of complex sociotechnical systems (Pavard & Dugdale, 2006). These include

- *Limited functional decomposability*: The intertwined nature of sociotechnical systems does not ensure that the decomposed system in static stable parts keeps the same properties of the system as a whole.
- *Nondeterminism*: It is hardly possible to anticipate precisely the behavior of a complex system even though the functioning of its constituents is completely known.
- *Distributed nature of information and representation*: Some cognitive properties of the system are distributed among agents rather than assigned individually, leading to uncertain, ambiguous, incomplete, or unavailable data.
- *Emergence and self-organization*: A system property is considered emergent if it cannot be anticipated from knowing the system's components functioning. It may emerge due to local interactions between distributed actions of individual or collective sociotechnical agents.

These assumptions on complexity, as well as the ones on the nature of safety management, have been acknowledged as the theoretical foundation for the definition of the scientific field of resilience engineering (Patriarca, Di Gravio, & Constantino, 2017).

Resilience Engineering as a Paradigm Shift

In Kuhnian terms, resilience engineering constitutes a paradigm shift for safety management. It focuses on systems capability to continuously cope with the complexity arising from balancing productivity with safety in everyday work (i.e., being resilient; Hollnagel, 2006). It was early acknowledged that the discipline of resilience engineering needed to be inherently systemic by nature, focused on the complexity of the system as a whole, rather than summing oversimplified individualistic analyses of a system's constituent parts. The acknowledgement of the need for an explicit complexity-oriented viewpoint in safety science comes from the increasingly larger emphasis on systemic aspects of safety dating back to the 1970s and continuing into the 1980s. An increasing regulatory interest moved the focus from specific technical concerns to decision-making and management issues. Several major accident reports at that time started stressing participatory issues related to human and organizational activities (Hale, Heming, Carthey, & Kirwan, 1997). For example, the Three Mile Island nuclear accident in 1979, the Challenger shuttle explosion in 1986, and the Chernobyl disaster in the same year. By the late 1980s, risk started to be addressed as a structural problem of those systems that are inherently risky due to their tight couplings and non-linear interactions, as suggested by the normal accident theory (Perrow, 1984). Due to the presence of multiple agents and multiple tight, even conflicting, goals, risks can also be considered as a

controllable problem to maintain a system's performance within the metaphorical boundaries of safety, economy, and workload (Rasmussen, 1997).

According to an aggregate complexity perspective, safety in a sociotechnical system cannot be represented as "a product of" or to "reside within" one or more of the social and/or technical perspective of a system (Hettinger, Kirlik, Goh, & Buckle, 2012). Given the dynamic nature of sociotechnical systems, safety is not a constant or permanent property of a system; it rather emerges from the interactive properties of the system and the environment's constituent components (Yang, Tian, & Zhao, 2017).

In this context, resilience has been shown to be related to the concept of adaptation (Amalberti, 2006), summarized as four cornerstones: responding (knowing what to do), monitoring (knowing what to look for), anticipating (knowing what to expect), and learning (knowing what has happened; Hollnagel, 2011). More recently, another theoretical perspective focused on the idea of rebound, robustness, graceful extensibility, and adaptability, has been proposed in line with awareness of the impossibility for addressing some general features of resilience, which are valid for engineering purposes (Woods, 2015).

All these definitions mostly agree with defining resilience as a system feature that allows the system itself to respond to an unanticipated disturbance and then to resume normal operations quickly and with minimum decrement in the system's performance. In formal terms, then, resilience has been defined as the intrinsic ability of a system to adjust its functioning prior to or following changes and disturbances to continue working in the face of continuous stresses or major mishaps (Hollnagel, Woods, & Leveson, 2006; Nemeth, Wears, Woods, Hollnagel, & Cook, 2008). Consequently, Resilience Engineering can be advanced as a complexity-oriented holistic discipline aimed at providing systems with the means for managing, experiencing, and enhancing resilience in response to external and internal perturbations. The discipline acknowledges that managing resilience—and safety—implies managing the dynamics and evolution of risks that may contribute to system breakdowns. In this sense, resilience engineering, like other models of resilience found throughout this volume, requires accounting for risk exposure to fully understand the adaptative capacity of the specific qualities of the mechanisms that enhance a system's resilience.

In traditional safety management, it is usually possible to identify for accident analyses or forecast for risk assessment a typical path to disaster starting from an individual failure, often linked to human actions (i.e., human error). This idea is rooted in an interpretation of risk that is focused on a system's energy (i.e., a dangerous build-up of energy, unintended transfers, or uncontrolled releases). This energy has to be contained by metaphorical and physical barriers that can stop or at least limit its propagation. Examples of barriers are a procedure, an effective management decision, a regulation, an automated feedback system, or a training action (see Figure 24.2).

Energy, however, is not always a threat and barriers can even generate unintended side effects, contributing to increase the complexity, and thus the nonintelligibility of a system and the potential for emergent risks. Such linear perspectives become progressively questionable for modern sociotechnical systems, where identifying the origin of a path's propagation becomes extremely difficult, or even impossible, due to the inherent complexity of the system itself.

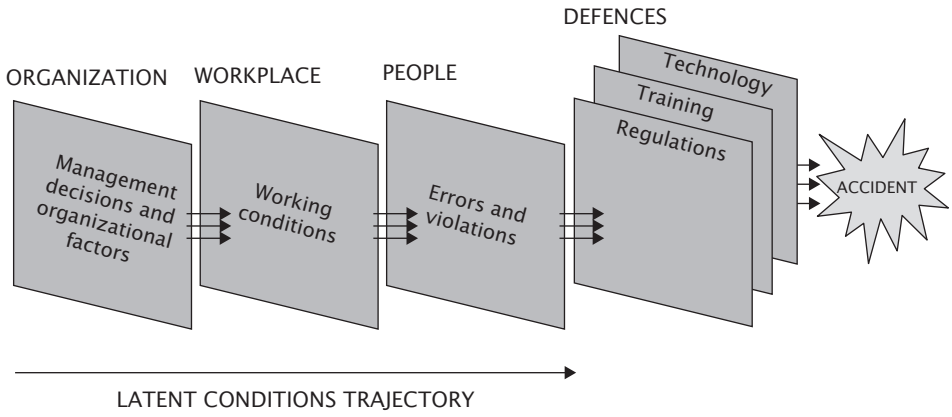

FIGURE 24.2 Swiss cheese model as an example of a barrier-based model Inspired by Reason et al. (2006).

Furthermore, systems generally behave dynamically, and thus their descriptions should be dynamic by nature, rather than oversimplified and only oriented at a constructivist viewpoint (Wrigstad, Bergström, & Gustafson, 2017). This latter refers to the WYLFIWYF principle (What you look for is what you find): causes are not found; they are chosen and selected (Lundberg, Rollenhagen, & Hollnagel, 2009). The organizational perspective cannot give an overall representation of a system's complexity, but it can be integrated with local analyses that account for human–technical interactions. The inherent complexity of systems does not allow defining a static structural cause–effect link among processes and activities that are inherently variable to cope with different operating scenarios.

The theory of resilience engineering, which acknowledges the positive effects of performance variability, is intended to provide the means for safety management of nontrivial sociotechnical systems, encompassing the hypotheses that systems are incompletely understood, descriptions can be complicated and system changes are frequent and irregular rather than infrequent and regular. Such hypotheses lead to the following principles, which are typical of resilience engineering and expressions of complexity science:

1. Systems cannot be decomposed in a meaningful way (highlighted as a main feature of a complex sociotechnical system).
2. System functions are not bimodal (functioning vs. nonfunctioning) but everyday performance is flexible and variable.
3. Human performance variability leads to success as well as failure.
4. Even though some outcomes can be interpreted as a linear consequence of other events, some events are the result of coupled performance variability.

The need to focus on performance variability rather than bimodality motivates the interest of safety for work-as-done (rather than work-as-imagined), looking at how the performance of the whole system varies (Morel, Amalberti, & Chauvin, 2009). Work-as-done represents the inherent adaptation of a system to remain productive under normal circumstances as well as

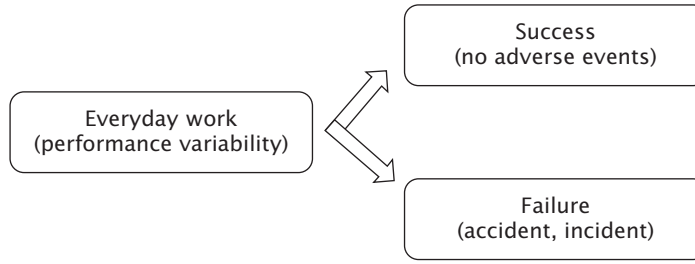

FIGURE 24.3 Resilience engineering point of view, acknowledging the limitedness of bimodal perspective for system functioning: success and failures come from the same source, performance variability.

under hazardous influences (see Figure 24.3). In this sense, the system is engineered to show resilience under the expected conditions in which it is used.

On Methods for Resilience Engineering

Resilience engineering offers a way of viewing processes from different angles, with the purpose of systematically understanding, extracting, or even engineering the potential of a system to self-design to match operational scenarios. In terms of methods, the approaches available in the literature range from individual, process, and systemic modeling to progressively fill the gap between the theoretical aspects of the discipline and its applicability in real contexts. These methods aim at exploring the resilience potential of a system, unveiling its strengths and weaknesses, and refining and enhancing adaptation strategies (if any).

To measure the resilience of sociotechnical systems, there are several ways to assess elements that contribute to resilience at different conceptual levels, organizing them along temporal dimensions, hierarchically (Herrera, Hollnagel, & Håbrekke, 2010; Huber, Gomes, & De Carvalho, 2012). In this context, the RAG (see following discussion) represents one of the most widely used methods for assessing resilience potential through the use of a semistandardized framework based on Hollnagel's (2011) four cornerstones of resilience (i.e., responding, monitoring, anticipating, and learning).

In terms of modeling resilience, system dynamics and causal loop diagrams have been used in several industrial applications (Salzano, Di Nardo, Gallo, Oropallo, & Santillo, 2014). Other specific models have been developed starting from graph theory mainly for technological aspects (Johansson & Hassel, 2010) or through fuzzy cognitive maps (Azadeh, Salehi, Arvan, & Dolatkhah, 2014), or benefit–cost–deficit (BCD) models (Ouedraogo, Enjalbert, & Vanderhaegen, 2013). For qualitative approaches, the functional resonance analysis method (FRAM) has become increasingly popular for modeling complex sociotechnical systems. The FRAM allows for a multidisciplinary analysis of processes, taking into account technical, human, and organizational aspects of work (Hollnagel, 2012b).

The remainder of this section provides more details on RAG and FRAM, both methods of particular interest for assessing and modeling features of sociotechnical systems related to their resilience abilities.

Resilience Analysis Grid

Looking at resilience as the system's ability to adjust its functioning, during, prior to, or after an event (in this case, resilience refers to something the systems does), it follows that the assessment of resilience has to be somewhat different from the traditional measures of safety based on event counts (traditionally referring to something the system has; Hollnagel, 2009). In line with this perspective, the RAG is a question-based tool for assessing resilience potentials aimed at exploiting the system's performance in relation to the four cornerstones of resilience. The RAG is applied through four phases (Hollnagel, 2011):

- *Phase 1. Define and describe a system's structure, boundaries, time horizon, people, and resources*. This phase refers to restricting the application field to the relevant scope of the analysis.
- *Phase 2. Select the relevant questions for correspondent relevant items of the studied system*. Even though there are some standard questions available in standard RAG theory, at this phase it become necessary to adapt them for the context at hand to generate a manageable survey. Such adaption usually consists of an iterative procedure involving subject matter experts (i.e., people with working knowledge of the system).
- *Phase 3. Rate the questions for each cornerstones*. Once the survey is finalized, a pool of people working in the system should be identified as respondents. A preliminary training on the survey and on the nature of the questionnaire is generally advisable to create the proper context for a healthy, nonjudgmental reporting of the system's functioning.
- *Phase 4. Combine the ratings*. Once concluded the data-gathering process, it is generally recommended to present the information in a star plot, where each axis corresponds to the variable used to rate each cornerstone.

The RAG has been applied in several domains, customizing a series of standardized questions depending on the features of the domain itself. For example, it has been applied to rail traffic management (Rigaud & Martin, 2013), air traffic management (Pasquini, Ragosta, Herrera, & Vennesland, 2015; Patriarca, Di Gravio, & Costantino, 2016), and in healthcare settings (Darrow & Eseonu, 2017; Patriarca, Falegnami, Costantino, & Bilotta, 2018). The traditional RAG's star plot does not present a measure of resilience per se; it rather depicts how the resilience abilities of a system have been rated at a specific moment in time (its temporal dimension). The star plot is a snapshot of organizational resilience under specific conditions. Therefore, the RAG can be used to determine what is the initial resilience potential and then to explore the gap between the achieved status and the planned ideal conditions. Finally, it can be used to understand how the system may reach a target status in the future.

Figure 24.3 shows an example of RAG outcomes, combined into a star plot for research conducted in a neuroanesthesiology department (Patriarca, Di Gravio, Costantino, Falegnami, & Bilotta, 2018). The figure shows a distinction between the scores obtained by two classes of respondents, staff and resident neuroanesthetists. Example of questions that were rated on a five-point Likert scale (none, not much, enough, more than enough, completely) include "How frequently have you been involved in a project designed to improve perioperative patient management?" and "How much are you interested and informed about

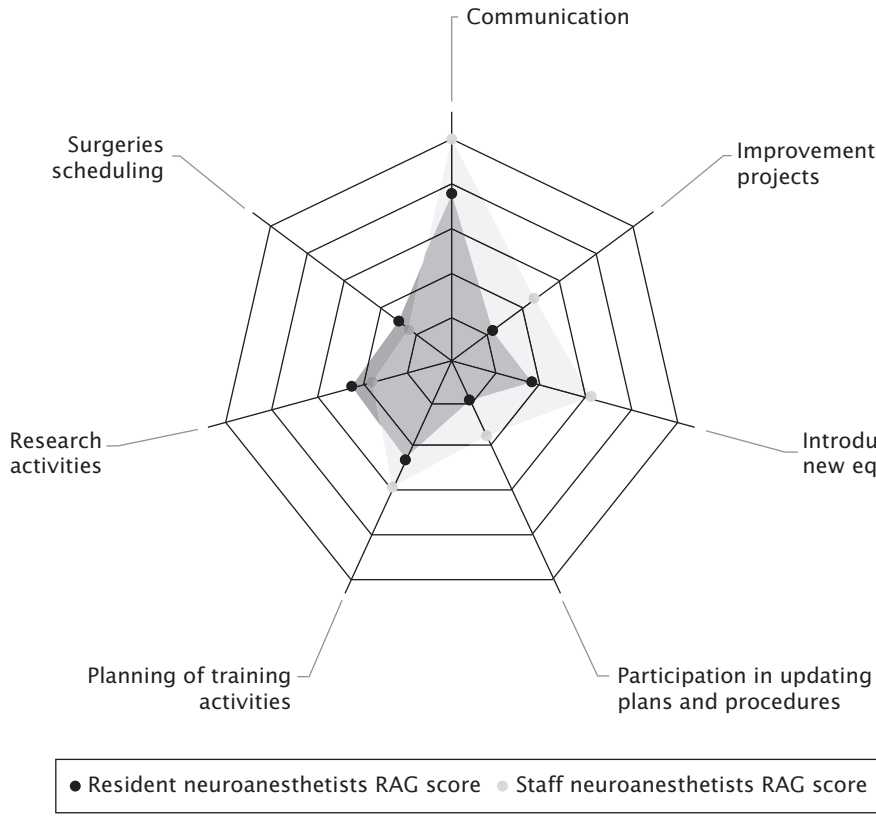

FIGURE 24.4 RAG outcomes with respect to seven questions related to the resilience ability "anticipating" of the system. The radar chat emphasizes different score for two groups of respondents: resident (black) versus staff (grey) neuroanesthesiologists.

research projects in your specific clinical setting?" When used in this way, the RAG provides a meaningful relative assessment, favoring discussions and comparison, to uncover hidden criticalities and motivate the need to acquire best practices among respondents. Exploring Figure 24.4, one can see that the RAG score is higher for resident neuroanesthetists than staff on a question related to involvement in research activities, confirming observations that the neuroanesthetists generally play a major role in trials and experimental projects but that staff do not perceive themselves as often in such functions of the department. This involvement, including an inherent continuous knowledge update on related research, is the cause for the difference. Such knowledge update is inherently considered capable of increasing a medical resident's potential to be resilient (i.e., to anticipate some possible perturbation in the provision of service).

Functional Resonance Analysis Method

The FRAM provides an approach to model complex sociotechnical systems using the concept of functional resonance, as a phenomenon arising from the variability of everyday

performance. Like the RAG, the FRAM is also based on four principles that are aligned with resilience engineering theory (Hollnagel, 2012b):

1. *Equivalence of failures and successes*. Failures and successes both emerge from everyday performance variability. Variability allows things to go both right and wrong, based on complex interactions among tightly coupled processes which overcome a bimodal representation of work.
2. *Approximate adjustments*. At different aggregation levels (individual, group, organization), individuals adjust their performance to deal with the requirements imposed by the operating scenario. These adjustments are usually unavoidable, since sociotechnical work conditions are intractable and underspecified.
3. *Emergence*. It is not necessarily true that every event can be linked to one (or multiple) linear static causes. Events can be emergent rather than result from a specific combination of fixed conditions.
4. *Functional resonance*. A system's functional resonance represents the detectable signal emerging from the unintended interaction of everyday variability for multiple signals. This variability is not random at all, but often depends on recognizable behaviors of the agents involved in the analysis, which act dynamically based on local rationality.

The FRAM incorporates the principles of resilience engineering, especially acknowledging the relevance of work-as-done, rather than work-as-imagined, and its inevitable variability to match working conditions in complex sociotechnical work environments. A strength of the FRAM consists of not adding strict modeling assumptions, thus limiting the bias of the representation. As acknowledged by Hollnagel (2012b), the FRAM is a *method sine model*, rather than a *model cum method*. Such observation implies that a detailed description of everyday system functioning is the necessary foundation for understanding a specific development of actions, actual or hypothetical, and modeling them.

The basic element of a FRAM model is a hexagon, which represents one function characterized by six different aspects (one for every corner; Hollnagel, Hounsgaard, & Colligan, 2014):

- *Input (I)*. What starts the function.
- *Output (O)*. What is the result of the function.
- *Precondition (P)*. What must exist before a function can be carried out.
- *Resource (R)*. What is necessary or consumed while the function is carried out.
- *Time (T)*. The temporal constraints of relationships for the function.
- *Control (C)*. What controls or monitors the function, with the potential for changing its outputs.

The FRAM has been adopted in a large set of sociotechnical system assessments, with a predominant initial focus in aviation. The first FRAM models referred to accident analyses for the study of systemic socio-technical inter-relatedness leading to plane crashes (De Carvalho, 2011; Sawaragi, Horiguchi, & Hina, 2006). Later, interest in using the FRAM

model expanded to other work domains, such as industrial plants (Shirali, Ebrahipour, & Salahi, 2014), maritime operations (Praetorius, Hollnagel, & Dahlman, 2015), and healthcare settings (Sujan & Felici, 2012).

An example of a FRAM model used in a healthcare domain is included in Figure 24.4. To contrast FRAM with RAG, this case example also refers to a context where anesthetics are used, perioperative delivery. The model confirms the complexity of the work domain under analysis, in terms of a high number of links and functions. The FRAM is therefore helpful describing the nature of a work domain and supporting the identification of criticalities in the relationships between functions and processes.

The model in Figure 24.5 refers to the management of a perioperative patient's pathway for a neurosurgery and includes actions performed mainly by anesthetists. The figure highlights as hexagons some upstream and downstream connections of an exemplar function: for example, "Extubate patient" (the act conducted by an anesthetists to remove a tube from patient's airway). This latter generates one output that becomes a precondition for the function "Fill in postsurgery anesthesiology report" (the report can be filled in only after the extubation is completed), as well as other outputs connected to other downstream functions.

As Figure 24.5 shows, the FRAM model is intended to support analysis of how the variability in one function; for example, "Extubate the patient," can generate variability in related functions and how this variability propagates throughout the system, following a tight network of reinforcing or dampening relationships.

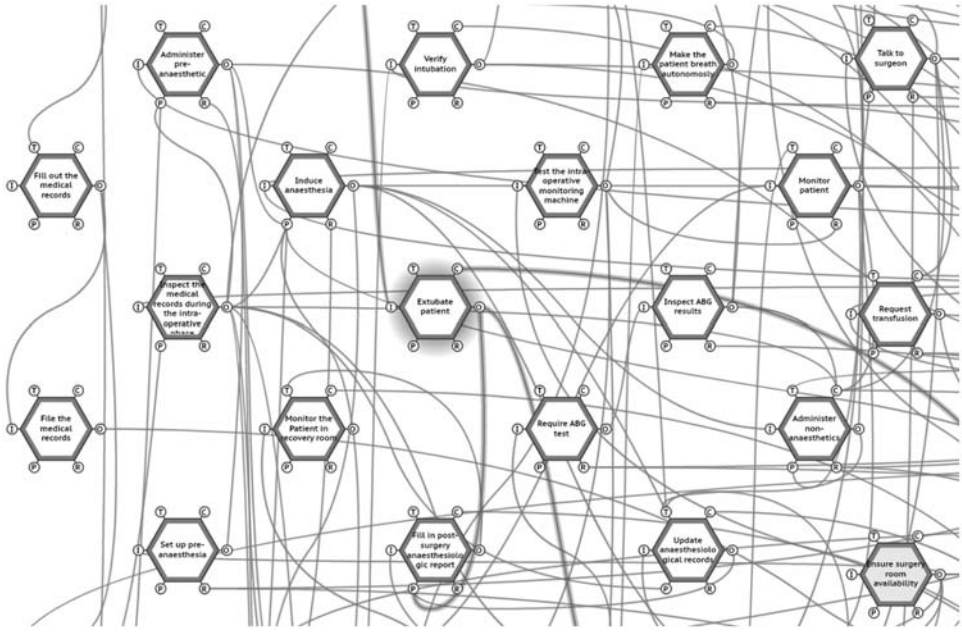

FIGURE 24.5 An excerpt of a FRAM model of a neurosurgery perioperative pathway. Hexagons and edges represent, respectively, functions and functional relationships among functions, following six different aspects (input, output, precondition, resource, control, time).

Therefore, a FRAM model remains consistent with the resilience engineering principles: it inherently supports the analyst to conduct back-and forth analyses, rather than a linear unidirectional focus (like traditional engineering mechanistic approaches). Once built, the FRAM model facilitates analysis that focuses on the couplings among functions rather than on the functions themselves. It thus remains possible to analyze multiple functions that may refer to different activities and multiple intertwined relationships but still maintain the coherence and consistency of a systemic perspective (Patriarca, Di Gravio, & Costantino, 2017).

With reference to both RAG and FRAM, and building on the evidence from research, one could argue that even if both models follow resilience principles, RAG may be more suitable for measuring resilience capabilities, or at least deviations in capabilities at an organizational level, while the FRAM may be a support tool for analyzing the details of a process, its deviance from ideal actions, and the potential source of resilience and brittleness.

Conclusion

Engineering resilience is about nonlinearity and dynamism; for example, understanding how an infinitesimally small change in initial conditions like an assumption in a software line of code can lead to huge consequences for a system as a whole (e.g., an involuntary release of energy that causes a spacecraft to crash; Leveson, 2002). Resilience provides a way of understanding variability and diversity, acknowledging the benefits arising from them and empowering the human component in the system to deal with it. Resilience engineering is, therefore, about dealing with micro–macro connections, and explaining how micro (i.e., local behavior) can produce macro (i.e., global) effects, which usually become unpredictable at a local level in a dynamic environment (Dekker, Hollnagel, Woods, & Cook, 2008).

Exploring micro–macro connections, future research should delve into ethical concerns about the acceptance of danger at the sharp end, and the effects on bureaucracy for a reduced prescriptive dimension at the blunt end (Bergström, Van Winsen, & Henriqson, 2015). A resilience engineering perspective may reduce the disconnection between processes and practices caused by overbureaucracy, empowering humans, and supporting the safer development of systems (Smith, 2018).

The resilience engineering literature argues that current approaches are largely still far from the concept of "knowledge for action" and instead represent academic exercises in a "knowledge for knowledge" sake. It is increasingly recognized, however, that the field is progressively moving toward translating approaches to modeling that are more theory-driven into operational applications (Furniss, Back, Blandford, Hildebrandt, & Broberg, 2011).

With the purpose of setting an agenda for the research in the field, a framework for resilience should be capable of illustrating resilience factors and mechanisms at different levels of analysis (from individual to organizational; Woods, 2006), providing measures and guidelines to improve the overall performance (not necessarily safety) within and across organizational domains (Patriarca, Bergström, Di Gravio, & Costantino, 2018). The framework

should also be flexible enough to be used at different organizational levels, conjugating and coordinating operational and managerial resilience capabilities.

In terms of methods, it is worth noting that the traditional RAG theory can be enhanced by means of advanced analytic aspects aimed at defining more properly the relationships among the abilities, even considering the analytical effects of their interrelatedness. (Patriarca, Di Gravio, et al., 2018).

Traditionally, the FRAM is a pure qualitative method. Its qualitative nature, however, may become soon ineffective for large systems, which do not allow for manual analyses of couplings and interactions. In such contexts, researchers are investigating the possibility to combine the qualitative evaluation with a quantitative assessment through the use of simulation techniques (Patriarca, Falegnami, et al., 2018) and model verification tools (Zheng, Tian, & Zhao, 2016).

In terms of data gathering, for both FRAM and RAG, alternative ways for data gathering are needed, for example, by means of gamified techniques, which may in turn also increase the quality of the knowledge elicitation process.

In this regard, this chapter has shown the scientific progress made in the area of resilience engineering by means of a multidisciplinary perspective.

Key Messages

1. Modern sociotechnical systems are inherently complex and require innovative management approaches.
2. The discipline of resilience engineering is introduced for risk and safety management of complex sociotechnical systems.
3. The analysis of processes in terms of work-as-done is acknowledged of primary interest for sociotechnical safety management.
4. Two methods, the FRAM and the RAG, are discussed at a theoretical level and through two examples.

References

Amalberti, R. (2006). Optimum system safety and optimum system resilience: Agonistic or antagonistic concepts? In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 253–272). Aldershot, UK: Ashgate.

Arthur, W. B. (1999). Complexity and the economy. *Science*, *284*(5411), 107–109. doi:10.1126/science.284.5411.107

Azadeh, A., Salehi, V., Arvan, M., & Dolatkhah, M. (2014). Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: A petrochemical plant. *Safety Science*, *68*, 99–107. doi:10.1016/j.ssci.2014.03.004

Bergström, J., Van Winsen, R., & Henriqson, E. (2015). On the rationale of resilience in the domain of safety: A literature review. *Reliability Engineering & System Safety*, *141*, 131–141. doi:10.1016/j.ress.2015.03.008

Cilliers, P. (2010). Difference, identity and complexity. In P. Cilliers & R. Presiser (Eds.), *Complexity, difference and identity: An ethical perspective* (pp. 3–18). Dordrecht, The Netherlands: Springer. doi:10.1007/978-90-481-9187-1

Darrow, L., & Eseonu, C. I. (2017). Development of a resilience analysis grid survey tool for healthcare. In K. Coperich, H. B. Nembhard, & E. Cudney (Eds.), *Proceedings of the 2017 Industrial and Systems Engineering Conference* (pp. 1163–1168). Pittsburgh, PA: Institute of Industrial Engineers.

De Carvalho, P. V. R. (2011). 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*, *96*(11), 1482–1498. doi:10.1016/j.ress.2011.05.009

Dekker, S. (2006). Resilience engineering: Chronicling the emergence of confused consensus. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 77–94). Aldershot, UK: Ashgate.

Dekker, S. (2011). *Drift into failure: From hunting broken components to understanding complex systems*. Aldershot, UK: Ashgate.

Dekker, S., Bergström, J., Amer-Wåhlin, I., & Cilliers, P. (2013). Complicated, complex, and compliant: Best practice in obstetrics. *Cognition, Technology and Work*, *15*(2). doi:10.1007/s10111-011-0211-6

Dekker, S., Hollnagel, E., Woods, D., & Cook, R. (2008). *Resilience engineering: New directions for measuring and maintaining safety in complex systems*. Lund, Sweden: Lund University School of Aviation.

Furniss, D., Back, J., Blandford, A., Hildebrandt, M., & Broberg, H. (2011). A resilience markers framework for small teams. *Reliability Engineering & System Safety*, *96*(1), 2–10. doi:10.1016/j.ress.2010.06.025

Goldratt, E. M. (2008). *The choice*. Great Barrington, MA: North River Press.

Hale, A. R., Heming, B. H. J., Carthey, J., & Kirwan, B. (1997). Modelling of safety management systems. *Safety Science*, *26*(1–2), 121–140. doi:10.1016/S0925-7535(97)00034-9

Hansson, S. O. (2013). Defining pseudoscience and science. In M. Pagliucci & M. Boundry (Eds.), *Philosophy of pseudoscience: Reconsidering the demarcation problem* (pp. 61–78). Chicago, IL: University of Chicago Press.

Herrera, I. A., Hollnagel, E., & Håbrekke, S. (2010, June). *Proposing safety performance indicators for helicopter offshore on the Norwegian Continental Shelf*. Paper presented at the 10th International Conference on Probabilistic Safety Assessment and Management 2010, Seattle, WA. Retrieved from https://pdfs.semanticscholar.org/3324/c1b89745c0ee1388c2c447f9f77fac4b67b0.pdf

Hettinger, L. J., Kirlik, A., Goh, Y. M., & Buckle, P. (2012). Modeling and simulation of complex sociotechnical systems: Envisioning and analyzing work environments. *Ergonomics*, *58*(4), 1–42. doi:10.1080/00140139.2015.1008586

Heylighen, F., Cilliers, P., & Gershenson, C. (2007). Complexity and philosophy. In J. Bogg & R. Geyer (Eds.), *Complexity, science and society* (pp. 117–134). Oxford, UK: Radcliffe.

Hollnagel, E. (2006). Resilience: The challenge of the unstable. In E. Hollnagel, D. D Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 9–17). Aldersho, UK: Ashgate.

Hollnagel, E. (2009). The four cornerstones of resilience engineering. In C. P. Nemeth, E. Hollnagel, & S. Dekker (Eds.), *Resilience engineering perspectives. Volume 2: Preparation and restoration* (pp. 117–134). Aldershot, UK: Ashgate.

Hollnagel, E. (2011). Epilogue: RAG—Resilience analysis grid. In E. Hollnagel, J. Pariès, D. D. Woods, & J. Wreathall (Eds.), *Resilience engineering in practice: A guidebook* (pp. 275–296). Aldershot, UK: Ashgate.

Hollnagel, E. (2012a). Coping with complexity: Past, present and future. *Cognition, Technology and Work*, *14*(3), 199–205. doi:10.1007/s10111-011-0202-7

Hollnagel, E. (2012b). *FRAM: The functional resonance analysis method—Modelling complex socio-technical systems*. Aldershot, UK: Ashgate.

Hollnagel, E. (2018). *Safety-II in practice—Developing the resilience potentials*. New York, NY: Routledge.

Hollnagel, E., Hounsgaard, J., & Colligan, L. (2014). *FRAM—The functional resonance analysis method: A handbook for the practical use of the method*. Centre for Quality, Southern Region of Denmark.

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

Huber, G. J., Gomes, J. O., & De Carvalho, P. V. R. (2012). A program to support the construction and evaluation of resilience indicators. *Work*, *41*(Suppl. 1), 2810–2816. doi:10.3233/WOR-2012-0528-2810

Johansson, J., & Hassel, H. (2010). An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliability Engineering & System Safety*, *95*(12), 1335–1344. doi:10.1016/j.ress.2010.06.010

Leveson, N. G. (2002). *System safety engineering: Back to the future*. Boston, MA: Massachusetts Institute of Technology.

Lundberg, J., Rollenhagen, C., & Hollnagel, E. (2009). What-you-look-for-is-what-you-find: The consequences of underlying accident models in eight accident investigation manuals. *Safety Science*, *47*(10), 1297–1311. doi:10.1016/j.ssci.2009.01.004

Manson, S. M. (2001). Simplifying complexity: A review of complexity theory. *Geoforum*, *32*, 405–414. doi:10.1016/S0016-7185(00)00035-X

Morel, G., Amalberti, R., & Chauvin, C. (2009). How good micro/macro ergonomics may improve resilience, but not necessarily safety. *Safety Science*, *47*(2), 285–294. doi:10.1016/j.ssci.2008.03.002

Morin, E. (2006). Restricted complexity, general complexity. In C. Gershenson, D. Aerts, & B. Edmonds (Eds.), *Worldviews, science and us* (pp. 5–29). Toh Tuck Link, Singapore: World Scientific. doi:10.1142/9789812707420_0002

Nemeth, C., Wears, R., Woods, D., Hollnagel, E., & Cook, R. (2008). Minding the gaps: Creating resilience in health care. In K. Henriksen, J. B. Battles, M. A. Keyes, & M. L. Grady (Eds.), *Advances in patient safety: New directions and alternative approaches* (pp. 1–13). Rockville, MD: Agency for Healthcare Research and Quality.

Ouedraogo, K. A., Enjalbert, S., & Vanderhaegen, F. (2013). How to learn from the resilience of human-machine systems. *Engineering Applications of Artificial Intelligence*, *26*(1), 24–34. doi:10.1016/j.engappai.2012.03.007

Pasquini, A., Ragosta, M., Herrera, I. A., & Vennesland, A. (2015). Towards a measure of resilience. In *Proceedings of ATACCS 2015—5th International Conference on Application and Theory of Automation in Command and Control Systems* (pp. 121–128). Deep Blue Piazza Buenos Aires 20, Rome, Italy. doi:10.1145/2899361.2899374

Patriarca, R., Bergström, J., Di Gravio, G., & Costantino, F. (2018). Resilience engineering: Current status of the research and future challenges. *Safety Science*, *102*, 79–100. doi:10.1016/j.ssci.2017.10.005

Patriarca, R., Di Gravio, G., & Costantino, F. (2016). Resilience engineering to assess risks for the air traffic management system: A new systemic method. *International Journal of Reliability and Safety*, *10*(4), 323–345. doi:10.1504/IJRS.2016.10005344

Patriarca, R., Di Gravio, G., & Costantino, F. (2017). A Monte Carlo evolution of the functional resonance analysis method (FRAM) to assess performance variability in complex systems. *Safety Science*, *91*, 49–60. doi:10.1016/j.ssci.2016.07.016

Patriarca, R., Di Gravio, G., Costantino, F., Falegnami, A., & Bilotta, F. (2018). An analytic framework to assess organizational resilience. *Safety and Health at Work*, *9*(3), 265–276. doi:10.1016/j.shaw.2017.10.005

Patriarca, R., Falegnami, A., Costantino, F., & Bilotta, F. (2018). Resilience engineering for socio-technical risk analysis: Application in neuro-surgery. *Reliability Engineering & System Safety*, *180*, 321–335. doi:10.1016/j.ress.2018.08.001

Pavard, B., & Dugdale, J. (2006). The contribution of complexity theory to the study of socio-technical cooperative systems. In A. A. Mina & A. M. Y. Bar-Yam (Eds.), *Unifying theories in complex systems* (Volume IIIB, pp. 39–48). Berlin, Germany: Springer.

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

Praetorius, G., Hollnagel, E., & Dahlman, J. (2015). Modelling vessel traffic service to understand resilience in everyday operations. *Reliability Engineering & System Safety*, *141*, 10–21. doi:10.1016/j.ress.2015.03.020.

Rasmussen, J. (1979). *On the structure of knowledge: A morphology of mental models in a man-machine system context*. Roskilde, Denmark: Research Establishment Risoe.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, *27*(2–3), 183–213. doi:10.1016/S0925-7535(97)00052-0

Rigaud, E., & Martin, C. (2013). Considering trade-offs when assessing resilience. In I. Herrera, J. M. Schraaden, J. van der Vorm, & D. Woods (Eds.), *Resilience Engineering Association: 4th international symposium* (pp. 115–120). Soesterberg, The Netherlands: Resilence Engineering Association.

Rosa, E. A. (1998). Metatheoretical foundations for post-normal risk. *Journal of Risk Research*, *1*(1), 15–44. doi:10.1080/136698798377303

Salzano, E., Di Nardo, M., Gallo, M., Oropallo, E., & Santillo, L. C. (2014). The application of system dynamics to industrial plants in the perspective of process resilience engineering. *Chemical Engineering Transactions*, *36*, 457–462. doi:10.3303/CET1436077

Sawaragi, T., Horiguchi, Y., & Hina, A. (2006). Safety analysis of systemic accidents triggered by performance deviation. In *2006 SICE-ICASE International Joint Conference* (pp. 1778–1781). IEEE Xplore. doi:10.1109/SICE.2006.315635

Shirali, G. A., Ebrahipour, V., & Salahi, L. M. (2014). Proactive risk assessment to identify emergent risks using functional resonance analysis method (FRAM): A case study in an oil process unit. *Iran Occupational Health*, *10*(6), 33–46.

Smith, G. (2018). *Paper safe: The triumph of bureaucracy in safety management*. Independently published.

Sujan, M., & Felici, M. (2012). Combining failure mode and functional resonance analyses in healthcare settings. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7612 LNCS*, 364–375. doi:10.1007/978-3-642-33678-2_31

Woods, D. D. (1988). Coping with complexity: The psychology of human behaviour in complex systems. In L. P. Goodstein, H. B. Andersen, & S. E. Olsen (Eds.), *Task, errors and mental models* (pp. 128–148). Bristol, PA: Taylor & Francis.

Woods, D. D. (2006). Engineering organizational resilience to enhance safety: A progress report on the emerging field of resilience engineering. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 50, pp. 2237–2241). doi:10.1177/154193120605001910

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, *141*, 5–9. doi:10.1016/j.ress.2015.03.018

Wrigstad, J., Bergström, J., & Gustafson, P. (2017). One event, three investigations: The reproduction of a safety norm. *Safety Science*, *96*, 75–83. doi:10.1016/j.ssci.2017.03.009

Yang, Q., Tian, J., & Zhao, T. (2017). Safety is an emergent property: Illustrating functional resonance in air traffic management with formal verification. *Safety Science*, *93*, 162–177. doi:10.1016/j.ssci.2016.12.006

Zheng, Z., Tian, J., & Zhao, T. (2016). Refining operation guidelines with model-checking-aided FRAM to improve manufacturing processes: A case study for aeroengine blade forging. *Cognition, Technology and Work*, *18*(4), 777–791. doi:10.1007/s10111-016-0391-1