Safety Science 91 (2017) 49–60

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

A Monte Carlo evolution of the Functional Resonance Analysis Method (FRAM) to assess performance variability in complex systems

Riccardo Patriarca *, Giulio Di Gravio, Francesco Costantino

Department of Mechanical and Aerospace Engineering, University of Rome - La Sapienza, Via Eudossiana, 18, 00184 Rome, Italy

ARTICLE INFO

Article history:
Received 15 March 2016
Received in revised form 27 June 2016
Accepted 20 July 2016

Keywords:
FRAM
Safety-II
Safety assessment
Resilience engineering
Monte Carlo

ABSTRACT

Modern trends of socio-technical systems analysis suggest the development of an integrated view on technological, human and organizational system components. The Air Traffic Management (ATM) system can be taken as an example of one of the most critical socio-technical system, deserving particular attention in managing operational risks and safety. In the ATM system environment, the traditional techniques of risk and safety assessment may become ineffective as they miss in identifying the interactions and couplings between the various functional aspects of the system itself: going over the technical analysis, it is necessary to consider the influences between human factors and organizational structure both in everyday work and in abnormal situations. One of the newly introduced methods for understanding these relations is the Functional Resonance Analysis Method (FRAM) which aims to define the couplings among functions in a dynamic way. This paper evolves the traditional FRAM, proposing an innovative semi-quantitative framework based on Monte Carlo simulation. Highlighting critical functions and critical links between functions, this contribution aims to facilitate the safety analysis, taking account of the system response to different operating conditions and different risk state. The paper presents a walk-through section with a general application to an ATM process.

1. Introduction

Even though the progress in safety management made flying one of the safest way to travel (IATA, 2013), there is a strong consensus that safety in aviation is something that always need to be improved in order not to remain static or become inadequate at system developments. ICAO defines (ICAO, 2013) safety as "the state in which harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management".

This definition complies with the traditional idea of safety as "a condition where nothing goes wrong or where the number of things that go wrong is acceptably small". Safety is then measured by the consequence of its absence rather than a quality itself (EUROCONTROL, 2009). These concepts lead risk governance and safety management to focus, with good reason, on what can go wrong and can lead to unwanted outcomes. Investigations generally rely on the historical approach of listing up adverse events experienced during an accident. These data allow to delve into the negative occurrences in order to propose interventions to eliminate their cause or to define mitigating actions to damp the effects.

This approach, the so-called Safety-I, considers that adverse events happen because something went wrong and ensures that it is possible to find and treat the causes, in line with the "*causality credo*". Several methods and models follow this belief, aiming at individuating the cause-effect link between events. In the Air Traffic Management (ATM) system, starting from the Domino model (Heinrich, 1931), the Reason Swiss Cheese Model (RSCM) (Reason, 1990) acquired a fundamental role and became the base of EUROCONTROL Safety Regulatory requirements (ESARRs) (EUROCONTROL, 2001). All these models promote a bimodal view of the activities, considering acceptable and unacceptable outcomes as two distinct and different modes of functioning: things go right because the system functions as it should and because people work as imagined, things go wrong because something failed. It is then possible to achieve safety only minimizing, or even blocking, the transition from normal to abnormal functioning. In summary, Safety-I, relies on the following assumptions (EUROCONTROL, 2009):

- Systems are decomposable and well-understood.
- System functioning is bimodal.

* Corresponding author.
E-mail address: riccardo.patriarca@uniroma1.it (R. Patriarca).

http://dx.doi.org/10.1016/j.ssci.2016.07.016
0925-7535/

- Systems and places of work are well-designed and correctly maintained.
- Procedures are comprehensive, complete and correct.
- Operators behave as expected and trained.
- Designers have foreseen every contingency and have provided the system with appropriate response capabilities.

Although this conception paved the way to outstanding improvements in safety research, they seem to be ineffective for current needs. The ATM system's work conditions significantly changed over the past decades with a remarkable change in the air traffic volume. Furthermore, the Air Traffic Control (ATC) procedures' complexity dramatically increased, in order to satisfy the performance demand. Nevertheless, the development of technology itself and the IT software capacity determined a significant modification of organization structure, instruments, human activities and human machine interface (HMI). In addition, very few factors are independent from each other and subsequently isolating functions and analyzing them in a one-by-one strategy could be ineffective. Detailing system description is becoming an always more elaborate activity as systems may change before the description process is completed. Thus, only partial understanding of the principles of system functioning is possible. The ATM system, as well as many other present-day socio-technical systems in different industries (e.g. health care, nuclear power plants, space missions), are generally underspecified or intractable. These conditions fail to comply with Safety-I perspective, whose assumptions become inapplicable due to the large complexity and interdependencies among functions.

Safety-II aims to fill this gap, looking at intractable systems' needs. In particular, due to the impossibility of prescribing tasks and actions in every detail, performance must become flexible rather than rigid. This concept is in line with resilience awareness that individuals and organizations habitually adjust their performance to match current demands, resources and constraints in order to compensate the incompleteness of procedures and instructions (Hollnagel et al., 2011). On this path, following Safety-II, the definition of safety shifts to consider not only the adverse outcomes (as in Safety-I), but also positive and negative events, in order to achieve a holistic view of the system and in-depth understand its functioning. Safety-I aims to limit performance variability, Safety-II requires to manage it proactively, rather than simply constrained it. For this purpose, the system functioning is not considered bimodal, i.e. function or malfunction, but strictly related to everyday work and subsequent performance variability, which is the real source of success as well of failures, as shown in Fig. 1.

Safety-II characteristics summarize as follows:

- System components cannot be isolated in a meaningful way.
- System functions are not bimodal but everyday performance is flexible and variable.
- Human performance variability leads to success as well as failures.
- Even though some outcome can be interpreted as a linear consequence of other events, some event results of coupled performance variability.

Since resilience refers (Caralli, 2006; Carlson, 2012; Wood et al., 2006) to something that an organization does (its ability to adjust the way things are done) rather than to something that an organization has (e.g. traffic count, number of accidents/incidents), it is difficult to measure it by counting specific outcomes, such as accidents or incidents.

FRAM (Hollnagel, 2012), as well as other methods (e.g.) STAMP (Leveson, 2004), RAG (Hollnagel, 2015), characterizes complex systems by their functions rather than by their physical structure. It enables capturing dynamics and interactions among functions by modeling non-linear dependencies and performance variability (Hollnagel, 2012). Based on Safety-II principles and traditional FRAM theory for risk assessment, this paper develops an evolution of the method into a semi-quantitative perspective, using a probabilistic approach based on Monte Carlo simulation to define critical functions. A walkthrough application to an ATM system process, i.e. the runway incursion, shows possible advantages and future developments.

The contribution of the paper is as follows. In the first section, it presents a wide literature on FRAM applications. The second section defines the FRAM principles and the FRAM model structure. Based on the FRAM traditional structure, the third section describes the evolution of the method. The fourth explains how to apply the method and validate the results of the analysis. Finally, the conclusions envisage the importance of this semi-quantitative method to assess risk and safety proactively, illustrating the possibility of further research.

2. The FRAM in literature

The main FRAM applications mostly refer to the aviation context. One of the first (Sawaragi et al., 2006) systematically analyzes the automation effects under variable conditions of the pilot cabin. The study aims at understanding any collapses in operating procedures. In particular, the study focuses on the plane crash occurred in Colombia in 1995, flight 965, caused by the dis-coordination between the human and the automated aircraft. Nouvel et al. (2007) conduct an accident analysis about the MD83 aircraft approaching to the Paris Orly airport (ORY) in 23 November 1997. FRAM shows the difference in current risk state perception among the crew, cockpit and ground sector, modeling these interdependent links. With similar targets, Hollnagel et al. (2008) analyze the Comair Airlines flight 5191 accident happened the 27 August 2006 in Lexington (KY) and De Carvalho (2011) focuses on the accident between Gol Transportes Aéreos flight 1907 and an Embraer Legacy 600 in the airspace over the Amazon rainforest.

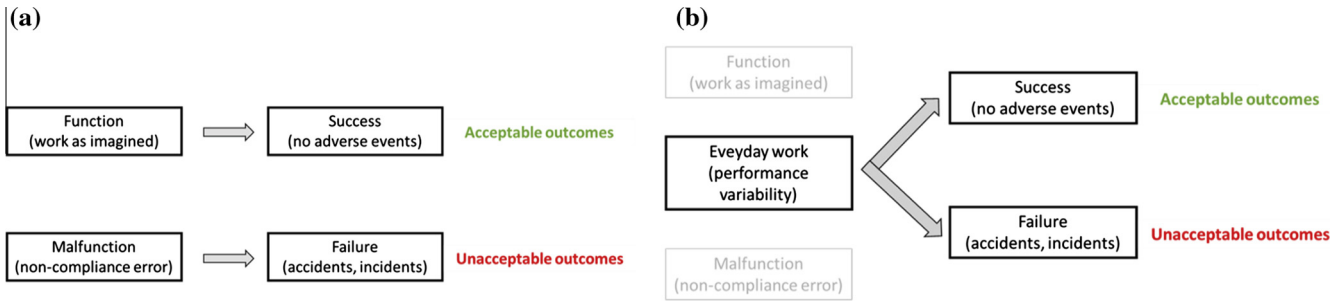

Fig. 1. Different sources of success and failure: Safety-I (a) and Safety-II (b).