Available online at www.sciencedirect.com

ScienceDirect

IFAC-PapersOnLine 49-19 (2016) 432–437

Markers and Patterns of Organizational Resilience for Risk Analysis

A. De Galizia**,*, C. Simon*, P. Weber*, B. Iung*, C. Duval**, E. Serdet**

*Université de Lorraine, CRAN UMR 7039, Bd des Aiguillettes, Vandoeuvre les Nancy, France
(e-mail: christophe.simon;philippe.weber;benoit.iung@univ-lorraine.fr)

**Department of Industrial Risks Management, Electricité de France R&D, Clamart, France
(e-mail: antonello.de-galizia;carole.duval;emmanuel.serdet@edf.fr)

In recent years, the concept of resilience has been introduced in risk analysis and some approaches have been proposed as an alternative (or a complement) to the conventional safety assessment for sociotechnical systems. In that way, Integrated Risk Analysis (IRA) has been developed at EDF to treat different risk causalities linking human, organizational, technical and environmental factors in a unified framework using performance shaping factors (PSF). However, research is still needed to address the issues relating to the modelling of resilience when considering organizational influences on human activities. Thus, this paper aims contributing at the definition and derivation of resilient markers and, consequently, to consider both resilient and pathogenic organizational patterns in a unified risk model. The risk model is initially proposed as a fourth generation method of risk analysis based on probabilistic graphical modelling of causal mechanisms. The model is proposed for safety assessment of technical systems integrating human, environmental and organizational factors. Finally, the feasibility of our proposals is shown on an illustrative case of Integrated Risk Analysis (IRA).

Keywords: Resilience, Markers, Organizational factors, Risk analysis, Sociotechnical systems

1. INTRODUCTION

Historically, many approaches to assess system safety are used to identify pathogenic patterns in order to attribute failures to a component (human or technological). Actually, safety assessment of a sociotechnical system requires a deeper understanding (Back, *et al.*, 2008). In recent studies, as in (Hollnagel & Spezali, 2008), it is found that, although sociotechnical systems continue to develop and become more tightly coupled and complex, risk and safety assessment methods do not change or develop correspondingly. For example, it is widely recognized that the approaches neither can be adopted nor somehow extended to properly treat human and organizational factors if still relying on the same principles that technical safety methods are based on. In particular, it is clear that to address human and organizational factors for risk assessment, methods need to account for not only pathogenic but also resilient patterns that can potentially manifest before, during or after accidental/incidental scenarios. In that way, considerable attention has been devoted to identifying opportunities for modelling *resilience* for risk analysis. Although there is no unique accepted definition across all domains, resilience is widely associated to the ability "to reduce the chances of a shock, to absorb a shock if it occurs and to recover quickly after a shock (restore normal performance)" (Bruneau, *et al.*, 2003). So, resilience can be understood as composed by two distinguished mechanisms:

- *Mitigation,* to reduce negative effects caused by perturbations and shocks;
- *Recovery*, to re-establish a nominal (acceptable) condition.

More recently, researchers working in a field known as resilience engineering (Hollnagel, *et al.*, 2006) have introduced new concepts about how to consider resilience for risk assessment. Along with others, resilience engineering has questioned traditional approaches to safety, especially when trying to account for responses to unexpected events and vulnerabilities that fall outside the scope of formal procedure and design. Nevertheless, it still lacks a clear understanding of what manifestations of resilience look like and how to account for both mitigation and recovery mechanisms in a risk model. Indeed, we need approaches for risk analysis to address the whole complexity neither of modelling resilience nor to consider in a unified model the complex interactions between resilient and pathogenic patterns to assess risks. Thus, it seems still a matter of investigation:

1) Understanding where resilient patterns come from and so whether *markers* exist to track such patterns;
2) Identifying a modelling approach to consider both resilient and pathogenic patterns.

These issues are particularly worthy of investigation at Electricity of France (EDF) where Integrated Risk Analysis (IRA) (Duval, *et al.*, 2012), a global methodology developed by the department of Industrial Risks Management (IRM) and the Nancy Research Center for Automatic Control (CRAN) needs to be reinforced for more reliable safety assessment. In IRA, a human barrier model (Léger, *et al.*, 2009) is used to assess human actions effectiveness, each

2405-8963 © 2016, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2016.10.609

action being defined within its specific organizational context. The causal framework that the model is based on relies on a set of organizational factors (OFs) (Léger, *et al*., 2009). Pathogenic patterns are identified as causal paths linking organizational factors to *items*, *i.e.* team and management related human factors. As pathogenic patterns must be justified when used in the model, a set of markers have been identified for each pattern by analyzing several relevant accidents/incidents occurred across different high-risky domains as nuclear, space and rail transportation. Today, IRA is interested in consolidating the human barrier model by integrating resilience patterns, even if this assimilation is considered only partially, *i.e.* with respect to the *mitigation* mechanism. Reasons behind this restriction are that IRA addresses only pre-accident situations (*recovery* makes sense only after perturbations has led to the accident). Face to these limitations, this paper aims to focus on the development of contributions related to the concept of mitigation by making some proposals on how (1) to identify markers to trace manifestations of organizational resilience in a sociotechnical system and, consequently, (2) to consider both pathogenic and resilient patterns for risk analysis. Based on these considerations, the paper is organized as follows. Section 2 discusses what is done today in order to provide motivation for promoting some contributions. Section 3 offers a formalization of such contributions. Section 4 shows the application of these contributions on an illustrative case in the context of IRA. Finally, conclusions and some perspectives are given in Section 5.

2. RESILIENCE MARKERS AND JOINT CONSIDERATION OF PATHOGENIC AND RESILIENT PATTERNS

A first step towards resilience consideration consists in providing a more precise definition of resilience and understanding how this concept translates when referred to sociotechnical systems.

2.1 *Resilience and sociotechnical systems*

Resilience is a very complex concept difficult to be defined in a unique way. Indeed, generalization is quite impossible as resilience is not a system component but should be understood rather as an emergent property. For risk analysis, a main definition is issued from the resilience engineering (Hollnagel, *et al*., 2006) in which resilience is considered as "the ability of a system or organization to respond and recover after disturbance, with a minimum effect on the dynamic stability of the system". This definition was updated always by (Hollnagel, *et al*., 2010) as it follows: "*a system is resilient if it can adjust its functioning prior to, during, or following events (changes, disturbances, and opportunities), and thereby sustain required operations under both expected and unexpected conditions*." While there is no universally shared definitions of resilience, experts in risk analysis agree on the meaning of resilience when deployed in the context of sociotechnical systems. In fact, four interrelated dimensions, *i.e.* technical, organizational, social and economic, characterize resilience for a sociotechnical system. Understanding whether a technical component rather than the organizational part of a system is resilient, is quite different, as they do not use the same mechanisms to manifest resilience. Therefore, assumptions made by investigating on a particular dimension of resilience cannot be easily generalized as holding for all the other ones.

In that way, this paper is mainly focusing on resilience manifested at the **organizational** level, *i.e.* resilient patterns implicating organizational factors.

2.2 *Identifying markers of resilient patterns*

A first issue arisen in considering resilient patterns is how to derive corresponding markers, *i.e.* all information useful to track manifestations of resilience. With respect to this issue, the resilience engineering (Hollnagel, *et al*., 2010) suggests to analyze all well-ended scenarios to gain information about resilient processes. Unfortunately, this approach hardly applies to risky industries as today most of the available feedback collected after analyzing past accidental/incidental scenarios concerns failures. In risk analysis for nuclear industry, for example, few information is available for unpredictable scenarios. This missing knowledge about potential future scenarios automatically prevent risk assessment methods from investigating markers of resilient patterns by following the approach proposed by the resilience engineering. (Back, *et al*., 2008) have emphasized the importance of identifying contributors to resilience to assess computer systems safety and reliability. In particular, a general framework is proposed based on resilient markers referring to different levels of granularity (individual, small team, plant level, etc.). Nevertheless, the focus is placed mainly on the identification of resilient strategies at the individual and team working situations levels, while no words is given about the approach used to derive their resilient markers.

Today, it is still unclear where and how markers relating to resilient patterns can be systemically obtained, and how they can be employed in reference to predefined organizational factors for risk analysis.

2.3 *Accounting for both pathogenic and resilient organizational patterns in risk analysis*

The second issue addressed in accounting for resilience in risk analysis is how to consider manifested resilient patterns in a modelling approach. This consideration requires a clear understanding of how resilient patterns interact with pathogenic ones in producing consequences in terms of risk. Most conventional methods to assess safety proceed by identifying failure mechanisms related to system components (technical failure rates) as well to human and organizational factors (human error probabilities, etc.). Techniques focusing on human and organizational factors, which are commonly referred to as human reliability analysis (HRA) methods (U.S.N.R.C, 2005), may find difficulties to consider the great complexity hidden behind causal mechanisms leading to a 'human error'. Actually, most of HRA methods make use of the so-called performance shaping factors (PSF) to assess a human error probability (HEP). In general, the analyst attributes to PSFs a weighting-value defined between -1 and