Available online at www.sciencedirect.com

ScienceDirect

IFAC-PapersOnLine 49-12 (2016) 325–330

Modelling Non-Deterministic Causal Mechanisms involving Resilience in Risk Analysis

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

*Nancy Research Center for Automatic Control, Lorraine University, Nancy, France
(e-mail: christophe.simon;philippe.weber;benoit.iung@univ-lorraine.fr)

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

In risk analysis, deterministic propagation of uncertainty as in fault trees models is not sufficient for sociotechnical systems. In recent years some approaches have been developed as Integrated Risk Analysis (IRA) to address different risks causalities linking human, organizational, technical and environmental factors in a unified framework. This framework relies on a Performance Shaping Factors (PSF) based model and constitutes an alternative approach different from that currently adopted at EDF for PSA (Probabilistic Safety Assessment) purposes. The IRA method is supported by Bayesian Networks (BNs) to model non-deterministic causal patterns among system variables. Thus, this paper aims to investigate on how to consider resilient influences in causal probabilistic modelling. In particular, it is focused on how to consider mitigation mechanisms in quantifying organizational influences on a human activity in sociotechnical systems. It leads to propose a formalism to represent a mitigation mechanism in causal interactions between pathogenic and resilient influences in a probabilistic model. Finally, the feasibility of our proposal is shown on an illustrative case declined in the framework of the IRA approach.

Keywords: Resilience, Canonical models, Bayesian networks, Risk analysis, Sociotechnical systems

1. INTRODUCTION

Risk analysis is often called for modelling *complex systems* taken from the real world in order to develop effective assessment. This complexity is related to the modelling with experts of non-deterministic mechanisms that describe causal relationships among interconnected elements, especially in sociotechnical systems, as industrial plants or transportation. In general, sociotechnical systems are characterized by the interaction of technical and social factors (notice the emphasis on *social* rather than on human factors). This type of interactions includes deterministic "causes and effect" relationships but also uncertain relationships involving emergent concepts in risk analysis, as *resilience*. In probabilistic safety assessment (PSA), some approaches have been developed as SoTeRIA (Mohaghegh, *et al*., 2009) for assessing the impact of organizational factors on safety. However, research is still needed to adequately consider the whole complexity due both to risk sources of different nature and uncertainty in non-deterministic causal mechanisms. In recent years, a research in the field of safety management has been carried out by Electricité de France (EDF) and the Nancy Research Center for Automatic Control (CRAN) to develop a unified methodology referred to as Integrated Risk Analysis (IRA) (Duval, *et al*., 2012) which differs from the existing PSA framework currently practiced at EDF. This methodology relies on the idea that in sociotechnical systems conditions for successful system operation are created by the interaction between *organisational, human, technical and environmental* factors. In particular, IRA is based on the so called System-Action-Management (SAM) approach proposed by (Paté-Cornell & Murphy, 1996). According to this approach, the analyst does not simply consider technical but also human and organizational variables to assess, in an integrated framework, possible risk causalities coming from the operation of sociotechnical systems.

In IRA, it led to the 'human barrier' (HB) model (Léger, *et al*., 2008b), a PSF based framework which is adopted to evaluate and rank human actions on the basis of their effectiveness (notice that each action is considered in its environmental and organizational context). The causal framework in the HB model relies on a set of *organizational factors*. These latter are supposed to be the root causes of teams and operators effectiveness when performing their activities. Bayesian Networks (BNs) are the underlying mathematical formalism retained for quantifying the probability of effectiveness of a human action (Weber, *et al*., 2012). In fact, Bayesian Networks are much known as well-adapted modelling formalism to represent complex uncertain relationships among variables, especially thanks to the *Bayesian inference* mechanism used to specify the prior probability for a hypothesis then updated as more evidence or information becomes available. By using BNs, human and organizational variables are specified by means of their *joint probability distribution*, which expresses the probability of each combination of parent and child states. The conditional probability distribution (CPD) allows for deriving the impact

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.2016.07.625

of a subset of parent variables (for example, in IRA a group of organizational factors) on a lower level variables (also in IRA, team and management related factors) through the mechanism of probabilistic conditioning.

In order to reduce the complexity of knowledge elicitation (necessary because of the lack of data), a choice to use the Noisy-OR model (Pearl, 1988) was made for IRA (Léger, *et al.*, 2008a). The Noisy-OR is a *canonical probabilistic model* (Díez & Druzdzel, 2006), *i.e.* an elementary model used in the development of more complicated models, the main advantage of which is that it allows for building probability distributions from a *small number of parameters*. By consequence, this translates in a drastic reduction of the set of questions needed for the expert's elicitation. Others have applied the Noisy-OR model to include organizational factors in probabilistic risk assessment as (Galan, *et al.*, 2007) and (Mohaghegh, *et al.*, 2009). Nevertheless, they have not considered the impact of resilient mechanisms behind the organizational dimension. Indeed in non-deterministic causal relationships, resilient influences can affect and moderate pathogenic influences, *i.e.* influences producing an undesired situation. Thus it is compulsory to consider resilience in the construction of complex models to be used in risk analysis, as defended by the *resilience engineering* (Hollnagel, *et al.*, 2006).

In that way, this paper is addressing, within the general framework of non-deterministic causal mechanisms, the scientific issue of modelling the concept of *resilient influences* and their causal interaction with *pathogenic influences*. In particular, it is focused on how to model their joint effect on the affected variables in the IRA framework for which BNs (and the Noisy-Or model) are used as modelling support. Indeed the representation of such causal mechanisms in the form of conditional probabilistic relationships in BNs introduces some modelling issues, including parameters definition and domain expert elicitation.

With regards to this modelling contribution, Section 2 presents the existing canonical models in order to provide the main differences among these models and reasons for considering the Noisy-Or model in IRA. Then Section 3 proposes a formalisation for modelling resilience in causal mechanisms. Section 4 shows the application of the proposed modelling approach on an illustrative case in the context of IRA. Finally, conclusions and some perspectives are given in Section 5.

2. CANONICAL PROBABILISTIC MODELS

It's useful to remember what *canonical models* consist in and how they can be used when building conditional probability tables (CPT), which correspond to a collection of discrete probability distributions of a variable conditional on its parents in a BNs model. In fact, for a totally free model, the size of CPTs of a variable Y grows exponentially with the number of parents of Y. According to (Díez & Druzdzel, 2006), canonical models can be classified in:

- *Deterministic models*: they do not require any numerical parameters as relations among variables are deterministic. The CPT in this case can be derived from the definition of an algebraic or logical function between parents and child in the network. Examples are the OR, AND, NOT, etc. gates (as in fault trees approaches);
- *ICI models*: they are based on the *independence of causal influence* (ICI) assumption (Henrion, 1989). This means that the number of parameters necessary for building the CPT is proportional to the number of parents. A further distinction is made between:
    - Noisy ICI models,
    - Leaky ICI models,
    - Probabilistic ICI.
- *Simple models*: they need a probability distribution for each link between a parent states combination and the child node, which means that the number of parameters necessary for building the CPT can grow exponentially with the number of parents.

However, there is no evidence that any existing canonical models – whether deterministic (e.g. OR/MAX or AND/MIN), based on the ICI assumption (Noisy OR/MAX, Noisy AND/MIN etc.) or simple – is adapted to model in the CPT resilient influences. When a resilient influence exists, *i.e.* a causal positive mechanism affects the child variable, it could be capable to counteract (at least partially) one or a set of pathogenic influences. The result of such a causal interaction leads to *decrease* the joint probability related to an undesired effect. Then, it should lead to define requirements to be satisfied for taking into account this causal interaction between "conflicting" mechanisms involving resilient and pathogenic influences in probabilistic models, and, specifically for IRA, in the Noisy-Or logic.

3. RESILIENCE MECHANISMS IN PROBABILISTIC MODELLING

The main assumption underlying the Noisy-OR model is independence of causes, which means that there are no interactions between the causal mechanisms by which X_i parent causes produce an undesired effect on a child variable Y (Henrion, 1989). In fact, the Noisy-OR model is useful when modelling independent causes that can produce the undesired effect (Srinivas, 1993). When more causes affect the child variable, this latter has a higher probability to be produced because of the independence assumption itself. However, if resilient and pathogenic influences are supposed to interact with each other – which of course implies dependence – therefore the ICI assumption has to be relaxed in the model.

It is possible to overcome this limitation in order to take into account the possibility of modelling causal interactions that lead to decrease an undesired effect. To support this extension for the Noisy-OR canonical model, some *rules* need to be considered in modelling the interaction between resilient and pathogenic influences. So, it is requested to:

- Comply with a set of *constraint inequalities* in building CPTs of the BNs model. These constraints confine expert judgments within fixed *probability boundaries* so as to