Reliability Engineering and System Safety 94 (2009) 1000–1018

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization

Zahra Mohaghegh *, Reza Kazemi, Ali Mosleh

Center for Risk and Reliability, University of Maryland, College Park, MD 20742, USA

ARTICLE INFO

Article history:
Received 25 July 2008
Received in revised form
16 November 2008
Accepted 21 November 2008
Available online 3 December 2008

Keywords:
Probabilistic Risk Assessment (PRA)
Organizational factors
Safety culture
Socio-technical complex systems
System dynamics
Bayesian Belief Network (BBN)
Safety management
Human Reliability Analysis (HRA)

ABSTRACT

This paper is a result of a research with the primary purpose of extending Probabilistic Risk Assessment (PRA) modeling frameworks to include the effects of organizational factors as the deeper, more fundamental causes of accidents and incidents. There have been significant improvements in the sophistication of quantitative methods of safety and risk assessment, but the progress on techniques most suitable for organizational safety risk frameworks has been limited. The focus of this paper is on the choice of "representational schemes" and "techniques." A methodology for selecting appropriate candidate techniques and their integration in the form of a "hybrid" approach is proposed. Then an example is given through an integration of System Dynamics (SD), Bayesian Belief Network (BBN), Event Sequence Diagram (ESD), and Fault Tree (FT) in order to demonstrate the feasibility and value of hybrid techniques. The proposed hybrid approach integrates deterministic and probabilistic modeling perspectives, and provides a flexible risk management tool for complex socio-technical systems. An application of the hybrid technique is provided in the aviation safety domain, focusing on airline maintenance systems. The example demonstrates how the hybrid method can be used to analyze the dynamic effects of organizational factors on system risk.

1. Introduction

In the past 30 years, we have witnessed significant improvements in safety design concepts, as well as in methods and tools for safety risk analysis of complex technical systems. These improvements can be placed in three distinct phases, evolving from "early" to the "first" and then to the "second" generations of conceptual *theories* and *techniques*, covering "hardware," "human," and "organization" performance. The nature of this development has been similar to the shift in human sciences (e.g. decision research, management, and organizational theory) from "normative," prescriptive models to descriptive models in terms of a "deviation" from rational performance towards modeling the "actual behavior," as described by Rasmussen [1].

The early phase is much more pronounced in the nuclear power industry, where the original safety design philosophy was "defense-in-depth" (use of multiple barriers against accidental release of radioactivity). The corresponding philosophy in aviation was the use of redundancies in critical systems, leading to conservative designs of engineering systems and stringent regulatory oversight, quality control, and inspection. This generation coincided with the phase of "normative" models in human sciences, as mentioned by Rasmussen [1].

The next significant phase (first generation) is characterized by the introduction of formal risk analysis (e.g. Classical PRA (WASH-1400; [2])) into regulatory systems (e.g. risk-informed regulation) and operation (e.g. risk-based maintenance outage planning). Initially, these methods were mostly hardware-driven; however, it was also recognized that major accidents often involved "human error" in addition to the technical system failures. The first generation of Human Reliability Analysis (HRA) methods, such as Technique for Human Error Rate Prediction (THERP) [3], were developed to predict the probability of human error in performing prescribed or procedural tasks, or mainly Error of Omission (EOO).

The interest in extending safety risk models to include organizational behavior was in part motivated by the fact that investigations of major accidents continued to cite management and organizational factors as major root causes of human errors in operating and/or maintaining technical systems [4,5]. Reason's Swiss Cheese Model [4,5] is a well-known example of the use of first-generation organizational accident theories to describe the process of organizational effects on human errors, and, consequently, on the rate of accidents. There are also a number of first-generation quantitative methods and techniques that attempt to quantify the impact of organizational factors on system risk. These include MACHINE [6], WPAM [7,8], SAM [9], Omega Factor Model [10], ASRM [11], and Causal Modeling of Air Safety [12]. The nature

* Corresponding author.
E-mail address: mohagheg@umd.edu (Z. Mohaghegh).

0951-8320/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2008.11.006

of first-generation safety risk analysis theories and techniques can be characterized in terms of "deviations from normative performance" [1].

The emerging second-generation theories and techniques are characterized by more realistic performance models of hardware, humans, and organization. There is a gradual move from classical PRA towards "dynamic PRA" [13,14]. HRA models are becoming increasingly cognition based, and attempt to cover Errors of Commission (EOC) in addition to EOO. Examples are Cognitive Reliability and Error Analysis Method (CREAM; [15]) and Information, Decision, and Action in Crew context (IDAC; [16]). Simulation-based techniques are being introduced to integrate cognition-based *HRA* methods with dynamic models of the technical system behavior. An example is an integration of Accident Dynamics Simulator (ADS; [17]) and IDA [18].

The second generation of safety risk analysis coincided with the phase of models in terms of the "actual behavior" of individuals and organizations, as mentioned by Rasmussen [1]. However, second-generation "organizational models" of safety risk frameworks are still evolving. These models attempt to represent the underlying organizational mechanisms of accidents, focusing on the systemic and collective nature of organizational behavior. On the theoretical side, Rasmussen [1] cites the self-organizing nature of High Reliability Organizations [19] and learning organizations [20,21] as concepts useful in analyzing the managerial and organizational influences on risk. Normal Accident Theory [22], which views accidents caused by interactive complexity and close coupling, can also be considered a second-generation perspective on organizational safety. Meanwhile, second-generation quantitative techniques mostly tackle the dynamic aspects of organizational influences. For example, Biondi [23] uses the qualitative model developed by Bella [24] to describe the changes in the reliability of a system due to organizational dynamics. Other researchers, e.g. Cooke [25] and Leveson [26], have used the System Dynamics approach [27] to describe the dynamics of organizations, but these models do not include detailed, PRA-style models of the technical system. Yu et al. [28] also used the System Dynamics approach to assess the effects of organizational factors on nuclear power plant safety. Their work is an attempt to link System Dynamics and PRA. However, the interconnection between *PRA* and System Dynamics is not clarified.

There are still a number of major challenges in developing second-generation theories and techniques for safety risk analysis in the areas of "organizational models," "human reliability," and "PRA". This paper is a result of a research [29] focused on developing a second-generation "organizational model" of safety risk frameworks. Organizational models often direct the analysis of accidents and incidents to their deeper, more fundamental causes. The key questions in this line of research can be summarized as follows: (1) What are the organizational factors that affect risk, (2) How do these factors influence risk, and (3) How much do they contribute to risk? From a broader perspective, all the efforts and studies in this research domain can be placed under the banner of "Organizational Safety Risk Analysis."

In the absence of a comprehensive theory, or at least a set of principles and modeling guidelines backed by theory, it is hard to assess the validity and quality of the proposed modeling techniques. In a multidisciplinary effort, we focused on improving the theoretical foundations and on introducing of a set of modeling principles into the field of Organizational Safety Risk Analysis. A comprehensive review of relevant theories and technical domains was needed to address the inherently multi-dimensional nature of the problem. Most important among these domains were *quality management* [30], *safety management* [31], *organizational culture and climate* [32], *safety culture* [33,34], *safety climate* [35,36], *human resource systems* [37], *human reliability* (e.g. CREAM; [15] and IDAC; [16]), organizational theory, such as *socio-technical system theory* [38], *Lewinian field theory* [39], *Mintzberg categorical theory* [40], and organizational performance and change models [41], as well the theories of *learning organization* [21].

With a multidisciplinary perspective on the issue, a set of 13 principles for Organizational Safety Risk Analysis was proposed. These principles have been described briefly in Section 2 in order to clarify the scope and goal of the research. More detailed discussions of the principles are given in the corresponding publications [29,42,43]. A new organizatioinal safety risk framework, called Socio-Technical Risk Analysis (SoTeRiA),[1] was then developed, based on these modeling principles. The framework formally integrates the technical system risk model with the social (safety culture and safety climate) and structural (safety practices) aspects of safety prediction models, and provides a theoretical basis for the integration. SoTeRiA is briefly described in Section 3 in order to facilitate the main discussion of the present paper. We refer the reader to [29,42,44] for complete discussion of SoTeRiA.

The next challenge was finding appropriate techniques to operationalize the proposed organizational safety risk theory. This is the main focus of the current paper. Section 4 provides a methodology for assessing and adapting appropriate modeling techniques, building proper interfaces, and creating a hybrid technique consistent with the principles and characteristics of organizational safety risk frameworks. In Section 5, an example of the application of the proposed hybrid technique in the aviation domain is presented through an integration of a system dynamics software, STELLA [45,46], and a hybrid risk analysis software, The Integrated Risk Modeling System (IRIS; [47]).

2. Principles of organizational safety risk analysis—an overview

This section provides an overview of the work by two of the authors on exploring the *theoretical foundations* and a set of principles [29,42] for the field of Organizational Safety Risk Analysis. These principles are a series of testable propositions with supporting rationales, insights from other research efforts, and, in some cases, the integration of different theories from diverse disciplines. Table 1 provides a high-level classification of the 13 principles proposed. They are grouped in four categories and labeled alphabetically. This section only provides a brief description of the proposed principles in order to clarify the scope of the research. One of these principles, Principle M, is the main discussion of the current paper. We refer the interested reader to Mohaghegh and Mosleh [29,42] for more detailed explanation of the rest of the principles.

Principle (A). *Organizational Safety Risk* (*OSR*) *is the unknown of interest or figure of merit in Organizational Safety Risk Theory, and is a measure of the safety performance of the whole, or of some sub-unit of the organization. It is formally expressed as*

$$OSR = f(F_1, F_2, \ldots, F_N)$$

where f stands for an explicit or implicit function or statement, and $F_1, F_2, \ldots, F_N$ *are the predictors* (*independent variables*).

Principle (B). *Safety Risk is one of the organizational outputs that influences and is influenced by other organizational outputs, such as profit and quality.*

[1] Soteria was the Greek goddess of deliverance and preservation from harm.