Journal of Loss Prevention in the Process Industries 33 (2015) 200–212

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Coordinability and consistency: Application of systems theory to accident causation and prevention

Raghvendra V. Cowlagi [a, *], Joseph H. Saleh [b]

[a] Aerospace Engineering Program, Department of Mechanical Engineering, Worcester Polytechnic Institute, Worcester, MA, USA
[b] Guggenheim School of Aerospace Engineering, Georgia Institute of Technology, Atlanta, GA, USA

ARTICLE INFO

Article history:
Received 16 July 2014
Received in revised form
15 October 2014
Accepted 10 December 2014
Available online 17 December 2014

Keywords:
Coordinability
Consistency
Chemical reactor
Accident prevention
System safety

ABSTRACT

Recent works in the safety literature report several fruitful attempts to introduce mathematically rigorous results from systems and control theory to bear upon accident prevention and system safety. Previously, we discussed the implications on safety of the systems theoretic principles of coordinability and consistency, and we identified the lack of coordinability and/or consistency as fundamental failure modes in hierarchical multilevel systems. In this work, we further develop system safety analysis techniques based on these principles. We demonstrate that these principles not only provide a domain-independent vocabulary for expressing the results of post-mortem accident analyses, but they can also be applied to guide design and operational choices for accident prevention and system safety. We develop these ideas with the help of an illustrative case study. This case study represents a broad class of systems where operational policies and procedures of individual stakeholders in the system interact with physical processes such that new system behaviors emerge, and unanticipated safety issues arise. We argue, and illustrate our arguments using this case study, that the coordinability and consistency principles can be developed to deliver a threefold impact on accident analysis and prevention: firstly, these principles provide domain-independent procedural templates and vocabulary for post-mortem accident analysis. Secondly, these principles provide theoretical safety specifications to be met during system design and operation. Finally, these safety specifications can precipitate the formulation of a series of questions directly related to safety-oriented choices in the design, operation, and control of systems.

1. Introduction

Accident prevention and system safety are influenced not only by the reliability and failure behavior of various subsystems and components, but also by the nature of interactions between these components, as well as their interactions with external factors or environmental conditions. For example, large scale systems such as nuclear power plants, air traffic control systems, and offshore oil platforms, exhibit closely interacting technical, managerial, regulatory, and social components. Within the realm of technical systems, emerging cyber-physical systems such as intelligent transportation systems and mobile robots exhibit close interactions between components of fundamentally different nature: namely, computational and physical components (Asare et al., 2012). In the safety literature, the terms *man-made disasters* (Turner, 1978), *organizational accidents* (Reason, 1997), and *system accidents* (Perrow, 1999) have been used to describe adverse events arising due not only to isolated failures in human and technical elements of large systems, but also due to their flawed interactions. These interactions are not properly understood and, when examined, it is often on an ad-hoc basis and without an underlying formal and theoretical foundation. Such a theoretical foundation is nevertheless essential to the study of domain-independent principles of accident prevention and system safety, and the identification of such principles for hierarchical multilevel systems is a crucial area of ongoing research. In this work, we contribute to this research by further developing a previously introduced formal framework (Cowlagi and Saleh, 2013) for accident analysis and system safety. To this end, we briefly review the relevant literature and accordingly contextualize the proposed work. The reader interested is referred to (Saleh et al., 2011) for a thorough review and critical appraisal of the major ideas in accident prevention and system safety.

The literature reports on qualitative ideas and quantitative

* Corresponding author.
E-mail address: rvcowlagi@wpi.edu (R.V. Cowlagi).

http://dx.doi.org/10.1016/j.jlp.2014.12.004
0950-4230/

methods to guide design, operational, and organizational choices for accident prevention and system safety. Notably on the one hand, the High Reliability Organization (HRO) paradigm (Rochlin et al., 1987; Weick and Sutcliffe, 2007) presents a qualitative description of the salient managerial and organizational features of entities that maintain high safety standards and low accident occurrence rates. On the other hand, the method of quantitative risk assessment (QRA) (Apostolakis, 2004) – first introduced as Probabilistic Risk Assessment (PRA) for nuclear power plants (N. Rasmussen, 1975) – provide quantitative bases for making *risk-informed* design and operational decisions related to system safety. QRA and PRA involve technical details of the system configuration and operation, and develop an exhaustive list of possible accident scenarios, along with their potential consequences, and the likelihood of their occurrences. Excellent examples of such analyses for informing risk assessment in the chemical process industries include (Khan and Abbasi, 1999; Kleindorfer et al., 2003, 1999). The recent literature exhibits a thrust to support ideas and methods such as HRO and QRA/PRA with domain-independent design principles to inform technical, managerial, and organizational design choices for system safety (Saleh et al., 2014). Most notably, the defense-in-depth safety principle (NRC, 2000; Sorensen et al., 1999, 2000) emphasizes the implementation of multiple and diverse "barriers" (Hollnagel, 2004) for interrupting potential accident sequences at various stages. The purpose of these "barriers" is to prevent accident sequences from initiating, and/or to prevent them from escalating, and/or to mitigate their eventual consequences. The inherent safety principle (Khan and Amyotte, 2003, 2004) complements defense-in-depth by providing guidelines for choosing in the early design stages the types and locations of safety barriers.

These perspectives on accident prevention and system safety have now culminated in the so-called systems and control theoretic approach to system safety (Saleh et al., 2011), which pursues two complementary objectives: (1) to encapsulate the preceding perspectives on system safety originating from diverse technological domains into a single theoretical and mathematically rigorous framework, and (2) to leverage for accident prevention and system safety the vast arsenal of analytical and algorithmic tools from systems and control theory. The connections between control theory and the implementation and enforcement of safety barriers and safety constraints have been recognized (Leveson, 2004a; J. Rasmussen, 1997), and the role in system safety of the control theoretic notion of observability has been recently highlighted (Bakolas and Saleh, 2011; Favaro and Saleh, 2014). The connections between systems theory (Bertalanffy, 1969; Mesarovic et al., 1970; Weinberg, 1975) and system safety is motivated by the observation that accidents can result "from dysfunctional interactions among system components" (Leveson, 2004a), and that fundamental failure modes resulting due to such dysfunctional interactions are ill-understood (Leveson, 2004b). In a recent work (Cowlagi and Saleh, 2013), we discussed the implications on accident causation and system safety of the systems theoretic principles of coordinability and consistency, hereafter referred to as C&C. Specifically, we identified the lack of coordinability and/or consistency as fundamental failure modes in hierarchical multilevel systems, and we illustrated this claim using relevant accident case studies.

In this work, we further develop system safety analysis techniques based on the coordinability and consistency (C&C) principles. Specifically, the novel contributions of this paper are as follows. Firstly, we demonstrate that the C&C principles provide a theoretical vocabulary for expressing the results of post-mortem accident analyses, which can assist in extracting important lessons to be learned, and in identifying common accident pathogens from epidemiological studies of accidents in diverse technological domains. Secondly, and more importantly, we demonstrate the value of C&C-based system safety analysis for making design and operational choices. In particular, we illustrate the influence of this safety analysis on the choice of measurement equipment and estimation algorithms for various attributes of the system, thereby relating the "systems-" and "control-" theoretic facets of the system safety problem. More generally, we demonstrate that, for system design, the C&C principles can provide theoretical and general "safety specifications" that are more informative than the tautological specification of "the system must be safe", and more concise and domain-independent than specifications consisting of an exhaustive list of potential scenarios that must be avoided. To aid the exposition of these ideas, we present details on the application of the C&C principles for system safety analysis via a detailed illustrative example of a chemical reactor. Although the case study treated here is from the chemical industry, and the analytical model developed is specific to our reactor, this case study represents a broad class of multi-level systems where operational policies and procedures of individual stakeholders in the system interact with physical processes such that new system behaviors emerge, and unanticipated safety issues arise.

The rest of this paper is organized as follows: In Section 2, we provide a brief discussion of the C&C principles for the sake of completeness. The reader interested in further details is referred to (Cowlagi and Saleh, 2013) for a thorough discussion of these principles. In Section 3, we introduce a model of a chemical process plant, and in Section 4, we illustrate the application of the C&C principles for safety analysis of this plant. Finally, in Section 5, we provide conclusions of the proposed analysis, and directions for future research.

2. System theoretic framework for accident analysis and system safety

In this work, we focus on systems involving components interacting over multilevel hierarchies. Hierarchical multilevel structures are omnipresent in systems both in a purely technical context (e.g., cyber-physical systems) and in a sociotechnical context. Hierarchical multilevel structures enable tractable solutions of management and control of systems with ever-increasing technical and organizational complexity. Specifically, these structures support functional specialization, modular design, and multiplicity of decision-making units to break down the overall problem into manageable sub-problems. For simplicity of exposition, we consider a two-level hierarchy as is common practice (Mesarovic et al., 1970; Zhong and Wonham, 1990), with the understanding that the proposed developments can be iteratively applied to multilevel systems by analyzing pairs of components at successive hierarchical levels, and by aggregating components at multiple levels. In this section, we first introduce the formal concepts of coordinability and consistency in hierarchical multilevel systems using the terminology and definitions of (Mesarovic et al., 1970). Then, we summarize the implications of the C&C principles on system safety, which we discussed in detail in (Cowlagi and Saleh, 2013) using illustrative examples. With this background information covered, we will be ready for the analytical model development and the accident analysis using the C&C concepts in Sections 3 and 4.

2.1. Formal definitions of coordinability and consistency

The following description of the C&C principles is a summary of the extended discussion in (Cowlagi and Saleh, 2013). This subsection provides a brief overview of coordinability and consistency.