Safety Science 91 (2017) 154–167

Contents lists available at ScienceDirect

Safety Science

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

Review

Near-miss management systems and observability-in-depth: Handling safety incidents and accident precursors in light of safety principles

Maria Grazia Gnoni [a], Joseph Homer Saleh [b,*]

[a] Department of Innovation Engineering, University of Salento, Lecce, Italy
[b] School of Aerospace Engineering, Georgia Institute of Technology, Atlanta, GA, USA

ARTICLE INFO

Article history:
Received 4 August 2016
Accepted 15 August 2016

Keywords:
Near-miss
Safety management system
Observability-in-depth
Safety principles
Accident precursors

ABSTRACT

Accident precursors and near-miss management systems (NMS) are important safety tools in industries with major accident hazards, such as the airline industry, the nuclear industry, and the chemical industry, and they are increasingly adopted in other sectors such as manufacturing, construction, and health care. The aim of a NMS is to "harvest value" from near-miss data by assessing and prioritizing their risk implications, identifying their failure generating mechanisms, and guiding interventions and safety improvements and awareness. Recognizing that learning from near-misses is less costly than learning from accidents, the main value of a NMS is in the learning loop it provides within and across organizations, in focusing safety resources on addressing unsafe acts, reducing unsafe conditions and procedures, and improving design and operational safety issues. The present study first provides an updated review and synthesis of key ideas and challenges of NMS. It then proposes and examines important synergies between fundamental safety principles adopted in risk management, including defense- and observability- in depth, and NMS. Safety principles offer a new lens by which to view NMS. One important result is that near-miss data can be classified and interpreted in light of safety principles violated, and that safety interventions can be particularly effective when organized around such findings, the objectives being to (re-)establish and strengthen compliance with safety principles through workforce training, system redesign, and/or improved operational procedures. Finally, it is argued that NMS is one of the pillars of the implementation of observability-in-depth, and that the boundaries with the two other pillars (fault detection/online monitoring, and inspection) are likely to be blurred in the future, and that the next generation NMS (2.0) will likely integrate data from multiple sources to improve the efficacy of precursor identification, prioritization, and safety interventions, and ultimately accident prevention.

Contents

* Corresponding author.
E-mail address: jsaleh@gatech.edu (J.H. Saleh).

http://dx.doi.org/10.1016/j.ssci.2016.08.012
0925-7535/© 2016 Elsevier Ltd. All rights reserved.

1. Introduction

This work brings together two strands in the literature on accident prevention and system safety: the development and formalization of general, domain-independent, system safety principles on the one hand, and the examination of near-miss management systems on the other hand. The objectives of the present work are threefold: (i) to review and synthesize the key ideas and challenges of near-miss management systems; (ii) to introduce a set of high-level, domain-independent, safety principles to a broader audience, especially the readership and safety professionals involved in near-miss management systems; and (iii) to examine the relation and synergies between safety principles and near-miss management systems, in particular the observability-in-depth principle, and to explore how safety principles can help inform the design and operation of near-miss management systems and improve their effectiveness.

1.1. Definitions

Before delving into the topic, it is worth clarifying the two related terms of "accident precursor" and "near-miss". Although no generally agreed upon definitions are available, different authors adopt slightly different interpretations of these concepts, their general meaning is intuitive and easily understandable. For example, the National Academy of Engineering defines accident precursors as "conditions, events, and sequences that precede and [can] lead up to an accident" (NAE, 2004), and NASA defines an accident precursor as "an anomaly [off-nominal occurrence or condition] that signals the potential for more severe consequences that may occur in the future, due to causes that are discernible from its occurrence today" (NASA, 2011). And the U.S. Nuclear Regulatory Commission defines an accident precursor as "an observed event and/or condition at a plant, [which] when combined with one or more postulated events (e.g., equipment failures, human errors) could result in core damage" (NRC, 2008). An accident precursor is best understood in relation to the notion of accident sequence, or the sequence of events starting from an off-nominal initiating event, followed by increasingly more hazardous events/states, and leading up to an accident—the uncontrolled release of energy and its adverse consequences (e.g., injuries and loss of life, destruction of property or infrastructure, environmental damage).

An accident precursor can thus be conceived of as any truncation of an accident sequence. Moreover, the precursor can be qualified by its closeness to the complete accident sequence. According to this point of view, a near-miss is a special type of accident precursor for which the truncation of a complete accident sequence is minimal (close to the accident end-state or occurrence). In other words, a near-miss is very similar to an accident sequence with the exception of a few missing elements or ingredients, which translate into a few missing events (truncation) in the accident sequence (Saleh et al., 2013). The further an accident sequence advances before it is interrupted, the more hazardous the situation is, and the more appropriate is its characterization as a near-miss (sometimes referred to casually as a "close call").

In short, a near-miss has many of the ingredients (conditions) and generating mechanisms (causal factors) of an accident sequence with the exception of a few missing ones, which prevent it for further escalating and leading to the accident and its dire consequences. Since near-misses and accidents share some/many common causes, learning from the former (near-misses) and eliminating their causes makes a positive contribution toward preventing the latter (accidents).

As a side note, the severity of consequences is often used as a distinguishing feature between different terms, a disaster for example on one end of the spectrum involves many casualties (severe consequences), and an incident on the other end of the spectrum involving few or none (light adverse consequences). In this view, an accident precursor or near-miss is further out beyond a safety incident on this severity spectrum. This is the aspect favored by the NASA definition, "an anomaly [off-nominal occurrence or condition] that signals the potential for more severe consequences that may occur in the future."

It is worth pointing out that some level of ambiguity exists in the definitions of accident precursors and near-misses, and that the distinction between the two is to some extent subjective (e.g., where to draw the line between one and the other, and with other terms such as "incident"). This semantic wiggle room however is not detrimental to a proper understanding of these terms. When sharper definitions are need for some specific purpose and within a particular organization or context, more ad hoc nuances can be added.

One additional term that is usually subsumed under the definition of accident precursor but deserves some special attention is that of an accident pathogen. An accident pathogen is an adverse latent or pre-existing condition, passive or with no impact on the system output until activated or triggered by other adverse occurrences (see Fig. 1). When compounded with other factors, an (activated) accident pathogen can further advance an accident sequence, precipitate an accident, or aggravate its consequences (Bakolas and Saleh, 2011). For example, a failed emergency power system is an accident pathogen at a nuclear power plant: should the main power system fail, this latent adverse condition will precipitate the accident, or it will cause the sequence to further advance toward a core meltdown (Saleh et al., 2013). In Fig. 1, C_i is an example of an accident pathogen when this accident sequence has not been triggered yet or when it has stopped at the event $e_{3,1}$; the AND gate above C_i does not have the two causes active to allow that the failure logic to propagate up the tree.

1.2. Learning loops and near-miss management systems

Near-miss management systems (NMS), also referred to by other terms such as accident precursor programs, or incident (safety) reporting systems, are concerned with the broadest definition of near-misses and include adverse conditions (accident pathogens), unsafe acts and procedures, and adverse events or sequences of events "that precede and [can] lead up to an accident". All these aspects constitute an important source of knowledge when their safety implications are properly understood. The aim is to learn from collected data about near-misses (broadly