Reliability Engineering and System Safety 136 (2015) 17–34

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

A systems approach to risk management through leading safety indicators ☆

Nancy Leveson *

Aeronautics and Astronautics, Engineering Systems, MIT, Cambridge, MA, USA

ARTICLE INFO

Article history:
Received 22 April 2014
Received in revised form
5 October 2014
Accepted 8 October 2014
Available online 18 October 2014

Keywords:
Leading indicators
System safety
Process safety
STAMP
STPA
Risk management

ABSTRACT

The goal of leading indicators for safety is to identify the potential for an accident before it occurs. Past efforts have focused on identifying general leading indicators, such as maintenance backlog, that apply widely in an industry or even across industries. Other recommendations produce more system-specific leading indicators, but start from system hazard analysis and thus are limited by the causes considered by the traditional hazard analysis techniques. Most rely on quantitative metrics, often based on probabilistic risk assessments. This paper describes a new and different approach to identifying system-specific leading indicators and provides guidance in designing a risk management structure to generate, monitor and use the results. The approach is based on the STAMP (System-Theoretic Accident Model and Processes) model of accident causation and tools that have been designed to build on that model. STAMP extends current accident causality to include more complex causes than simply component failures and chains of failure events or deviations from operational expectations. It incorporates basic principles of systems thinking and is based on systems theory rather than traditional reliability theory.

1. Introduction

There are always warning signs before a major accident, but these signs may only be noticeable or interpretable as a leading indicator in hindsight. In fact, most major accidents have multiple precursors and cues that an accident is likely to happen. Before an accident, such "weak signals" are often perceived only as noise. The problem then becomes how to distinguish the important signals from the noise. Defining effective leading indicators is a way to accomplish this goal by providing specific clues that can be monitored.

There is commonly a belief—or perhaps, hope—that a small number of general "leading indicators" can identify increasing risk of an accident. While some general indicators may be useful, large amounts of effort over decades has not provided much progress [1]. The lack of progress may be a sign that such general, industry-wide indicators do not exist or will not be particularly effective in identifying increasing risk. An alternative, which is the focus of this paper, is to identify leading indicators that are specific to the system being monitored.

Underlying and justifying the use of leading indicators is a belief that most major accidents do not result simply from a unique set of proximal, physical events but from the migration of the organization to a state of heightened risk over time as safeguards and controls are relaxed due to conflicting goals and tradeoffs [2]. If this belief is correct, there should be ways to detect evidence of this migration and intervene before a loss occurs.

As an example, consider the accidental release of methyl isocyanate (MIC) from the Union Carbide plant in Bhopal, India, in 1984, one of the worst industrial accidents in history. Almost all the factors involved at Bhopal existed before the actual triggering event that led directly to the loss. The plant was losing money. In response, Union Carbide had ordered that costs be reduced, without considering how these cuts might conflict with safety. Requirements in the operating manual, such as never filling the tanks more than half their volume, the use of safety equipment for potentially hazardous operations, and the operation of a refrigeration unit to keep the MIC at a safe temperature, were not followed. In fact, when the refrigeration unit was turned off (most likely to save money), the high temperature alarm threshold was raised correspondingly, which eliminated the possibility of an early warning of rising temperatures. Valves leaks and gauges frequently were inaccurate or out of order. Maintenance procedures were severely cutback and critical jobs were left unfilled in shifts when someone called in sick.

☆This research was partially supported by a research grant from BP.
* Correspondence address: Room 33-334, Massachusetts Institute of Technology, 77 Massachusetts Ave, Cambridge, MA 02139, USA. Tel.: +1 617 258 0505.
E-mail address: leveson@mit.edu

http://dx.doi.org/10.1016/j.ress.2014.10.008
0951-8320/

A review and audit two years before had noted that many of the safety devices, such as alarms, the flare tower and the gas scrubber, were inoperable or inadequate. Most of the specific practices leading directly to the accident, such as filter-cleaning operations without using slip blinds, leaking valves, bad pressure gauges, etc., were noted in the report and never fixed. Union Carbide did not follow up to ensure the deficiencies were corrected. Qualifications of personnel went down. Training and oversight were reduced. A similar accident had occurred the year before at the plant but under circumstances where the results were less severe (one person was killed), but nothing was done about fixing the hazardous operation of the plant. Given this state of the plant and its operations, some events were bound to occur that would trigger an accident.

While the events and practices at Bhopal were strikingly bad, in hindsight nearly every major accident has similar migration toward the accident over time that potentially could have been detected and the accident prevented. These changes are often ignored in accident reports, which tend to concentrate on proximal events. The challenge in preventing accidents is to try to prevent and, if unsuccessful, detect migration toward a state of unacceptable risk before an accident occurs.

But detection alone is not enough—there must be a management process in place to act when the leading indicators show that action is necessary. Note that at Bhopal there had been an audit report showing the conditions existed, but they were never adequately addressed.

The process of tracking leading indicators of increasing risk, where that process is embedded within an effective risk management structure, can play an important role in preventing accidents, but a way to derive effective leading indicators is required. The signs are not always as clear as at Bhopal, and, of course, we cannot wait until hindsight shows us what we should have noted before the loss occurred.

This paper proposes an approach to identifying and monitoring system-specific leading indicators and provides guidance in designing a risk management structure to use such indicators effectively. In contrast to the usual ad hoc approach to leading indicators, the paper suggests a formal foundation and structured process for identifying them. It also includes suggestions for operationalizing and managing a leading indicator program.

The approach is based a new model of accident causation called STAMP and on tools that have been designed to build on that model [3,4]. STAMP extends current accident causality models to include more complex causes than simply component failures and chains of failure events. It incorporates basic principles of systems thinking and is based on systems theory rather than traditional reliability theory.

While the subject of the paper is limited to identifying leading indicators related to safety and accidents, the ideas apply to leading indicators and risk management for system properties other than safety.

2. Background

There has been much industrial effort devoted to developing leading indicators as well as academic interest in precursors. The problems in assessing risk, which arise in determining what precursors to check, are also relevant.

2.1. Leading indicators

Much effort has been spent on trying to identify leading indicators, particularly in the petrochemical industry. Almost all of the past effort has involved finding a set of generally applicable metrics or signals that presage an accident. Examples of such identified leading indicators are quality and backlog of maintenance, inspection, and corrective action; minor incidents such as leaks or spills; equipment failure rates, and so on. Some depend on surveys about employee culture and beliefs, with the underlying assumption that all or most accidents are caused by employee misbehavior, and include as leading indicators such culture aspects as safety awareness, mutual trust, empowerment, and promotion of safety [5].

A large number of proposals for leading indicators outside the petrochemical industry focus on occupational safety rather than system safety, and some are simply a listing of potential hazards, such as lack of safety training; whether there is a lock-out, tag-out policy or a stop-work policy; and whether there are medical facilities on site [6]. In fact, the BP Grangemouth Major Incident Investigation Report suggested that industries may have a false sense of safety performance due to their focus on managing personal safety rates rather than process safety[1] [7].

As a result of major accidents in the chemical industry, a concerted and long-term effort has been devoted to identifying leading indicators of risk. Khawaji [1] provides a comprehensive description of these efforts. To summarize Khawaji's analysis, early attempts to develop process safety performance metrics (leading indicators) date from the mid-1900s, but attempts accelerated after the Grangemouth report recommended that "companies should develop key performance indicators for major hazards and ensure that process safety performance is monitored" [7].

A series of documents have been issued since that time by the AICE [8–11], OECD [12,13,], UK HSE [14], OSHA [15], IEC [16], Step Change in Safety [17], and the API [18,19]. Most of these standards recommend that the identification of leading indicators start from the hazard analysis, but they assume that accidents are caused by a linear chain of events and do not address indirect interactions and complex systemic factors in accidents [1]. Most assume that accidents are caused by component failures and that likelihood of failures should be used to reduce the scope of the search for leading indicators despite the fact that likelihood may often be unknown and the practice may result in overlooking low likelihood events.

Beyond these industrial efforts, a large number of research papers have been written about identifying precursors to accidents. The proposals generally can be divided into those that consider technical or organizational precursors.

On the technical side, many people have suggested using incident reporting systems to identify precursors, for example [20–22]. The information could come from a root cause analysis that identifies the events that led up to the specific loss or near miss that occurred. A limitation is that only those events that have occurred will be identified and usually simple chains of failure events are the only precursors identified. Most root cause analysis techniques used widely are limited in the factors they can identify.

Another common suggestion is to use probabilistic risk analysis to detect and analyze precursor events. A leading proponent of this approach is Pate-Cornell [23].

A third general approach to identifying technical precursors is to use Hazard Analysis, for example [24]. The power of the hazard analysis to identify scenarios leading to losses will impact the effectiveness of the approach. Most current hazard analysis techniques focus on component failures and do not handle software requirements flaws, system design errors, the role of operators in accidents very well and usually ignore management and sophisticated errors in decision making.

[1] While the term "system safety" is common in most industries, the same thing is called "process safety" in the process industries. The more general term is used in this paper as the approach being described applies in any industry.