Using STAMP to Develop Leading Indicators

Nancy G. Leveson

Aeronautics and Astronautics Dept.
MIT
77 Massachusetts Ave., Room 33-334
Cambridge, MA 02139
leveson@mit.edu

Abstract: Ths paper describes an approach to using STMP and STPA to derive leading indicators of increasing risk.

There are always warning signs before a major accident, but these signs may only be noticeable or interpretable as a leading indicator in hindsight. 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.

A lot of effort has been spent on trying to identify leading indicators, particularly in the petrochemical industry. Much 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 [Am12]. 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 [HSE03]. 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] [HSE03].

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. 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.

[1] While the term "system safety" is common in most industries, the same thing called "process safety" in the process industries.

Early attempts to develop process safety performance metrics (leading indicators) date from the mid-1900's, 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 [HSE03]. A series of documents have been issued since that time by the American Institute of Chemical Engineering (AICE), the OECD, the U.K. Health and Safety Executive, the U.S. Occupational Safety and Health Agency (OSHA), and the American Petroleum Institute (API). 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 [Kh12, Le04]. Almost all recommend that the 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.

There is commonly a belief—or perhaps, hope—that a small number of such "leading indicators" can identify an increase in risk of an accident. While some general indicators may be useful, large amounts of effort over decades has not provided much progress [Kh12]. 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.

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. It extends the suggestions in the series of standards by the chemical industry, basing them on a different, more comprehensive model of accident causation and, perhaps more important, provides a formal foundation for identifying leading indicators.

The approach is based on the STAMP model of accident causation and tools that have been designed to build on that model [Le04. Le12]. The basic proposal is to base leading indicators and risk management on our assumptions about why accidents occur, which is the essence of STAMP.

The idea of assumptions being the basis for identifying leading indicators is not original but has been proposed for more general risk management programs. RAND developed the methodology of assumption-based planning (ABP) primarily to assist U.S. Army clients with mid- and long-term defense planning and to reduce uncertainty and manage risk [De02].

The process involved uses assumptions and their vulnerability as the basis for identifying leading indicators rather than the classic probabilistic risk methods. The STAMP/STPA process for safety-guided design and hazard analysis provides the framework for a structured leading indicator identification process. System hazards are first identified and used to derive the safety constraints and system safety requirements. Hazards are categorized, if necessary, with respect to potential worst-case severity and vulnerability. The functional safety control structure is designed with safety responsibilities identified for each component, where these control responsibilities are traceable to the system safety constraints. Once the safety control structure is created, STPA is used to identify unsafe control actions and their causes. Elimination of the causes should be first attempted and, if elimination is not possible, to mitigate and control them.

During this process, the information necessary to identify the assumptions being made during design and development is recorded and used to plan operations, to design the data and feedback that must be collected, and to design the overall leading indicator management program. The relative importance of the leading indicators (the consequences of not detecting something) and potential action plans upon their failure is also determinable by the ranking of the severity of the hazards to which they are traceable.

A serious problem that has been well studied in risk assessment is the difficulty in overcoming heuristic biases [e.g., KST82, SFL80]. A structured approach to overcoming common biases that lead to flawed risk assessment can be defined and a process for identifying, monitoring [DFI13] and managing a leading indicators program on this assumption-based approach to risk management can be developed using STPA. Managing such a program should include a process for updating leading indicators as experience is gained and as both the system and its environment change over time.

References

[Am02] American Bureau of Shipping, Safety Culture and Leading Indicators of Safety, January 2012, Houston TX.

[HSE03] The BP Grangemouth Major Incident Investigation Report, UK Health and Safety Executive, August 2003.

[De02] James Dewar, *Assumption-Based Planning*, Cambridge University Press, 2002.

[DFI13] Ioannis M. Dokas, John Feehan, and Syed Imran. EWaSAP: An Early Warning Sign Identification Approach Based on a Systemic Hazard Analysis, Safety Science, Vol. 58, Oct. 2013, pages 11-26.

[KST82] D. Kahneman, P. Slovic, and A. Tversky. *Judgment Under Uncertainty: Heuristics and Biases*. New York: Cambridge University Press, 1982

[Kh12] Ibrahim Khawaji, Developing System-Based Leading Indicators for Proactive Risk Management in the Chemical Processing Industry, SM Thesis, MIT, 2012.

[Le04] Nancy Leveson, A New Accident Model for Engineering Safer Systems, *SafetyScience*, 42(4):237-27, 2004.

[Le05] Nancy Leveson, *Engineering a Safer World: Applying Systems Thinking to Safety*, MIT Press, 2012.

[SFL80] P. Slovic, B. Fischhoff, and S. Lichtenstein, Facts and fears: Understanding perceived risk, *Societal Risk Assessment*, 181-216, 1980