Process safety indicators, how solid is the concept?

Swuste, Paul; van Nunen, Karolien; Schmitz, Peter; Reniers, Genserik

DOI
10.3303/CET1977015

Publication date
2019

Document Version
Final published version

Published in
Chemical Engineering Transactions

CHEMICAL ENGINEERING TRANSACTIONS

VOL. 77, 2019

A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it

Guest Editors: Genserik Reniers, Bruno Fabiano

ISBN 978-88-95608-74-7; **ISSN** 2283-9216

DOI: 10.3303/CET1977015

Process Safety Indicators, How Solid Is the Concept?

Paul Swuste[a,*], Karolien van Nunen[b,c], Peter Schmitz[d], Genserik Reniers[a,b]

[a] Safety Science Group, Delft University of Technology, the Netherlands
[b] Antwerp Research Group on Safety and Security (ARGoSS), Department of Engineering Management (ENM), Faculty of Applied Economics, University of Antwerp, Belgium
[c] Research Chair Vandeputte, University of Antwerp, Belgium [d] OCI-Nitrogen, Geleen, the Netherlands
p.h.j.j.swuste@tudelft.nl

Monitoring progress of accident scenarios, and effectiveness of control measures is a main goal of safety indicators. From an overview of scientific literature one may conclude that indicators do not logically relate to current safety theories and models, their relation with accident processes is far from perfect, and a 'silver bullet' has not been identified yet. Professional literature shows another picture, and divides indicators in leading and lagging. This distinction seems convincing. Not only companies, but also regulations adopted this division. Currently many indicators used in industry generate a number, while the relation with accident processes is questionable at least. In addition, it can be expected that regulators of major hazard companies will ask to identify and implement both lagging and leading indicators, and anchor these indicators in a safety management system. The subject 'safety indicators' will remain in the spotlight in the time to come. This presentation will focus on a review of scientific and professional literature. This article is written in 'praesens historicum', and based upon recent articles (Oostendorp et al., 2016, Swuste et al., 2010, 2014, 2016 a,b, 2018).

1. Introduction

Knowledge and understanding of accident processes is an essential condition for controlling major accidents in process industries. Till now safety science did not produce a unifying theory, or model yet to explain or predict these major accident processes. Most likely this reflects the relatively young age of the scientific domain, which only has become academic from the 1970s onwards. In this context a model is a schematic presentation of reality, not yet validated, or empirically supported, and a theory is a validated model.

Table 1 Unsafe acts as safety indicators (Rockwell, 1959)

	unsafe acts
1	working with loose tools underfoot
2	working without googles when required
3	working under suspended loads
4	failure to use guard as provided
5	working in unsafe postures
6	wearing improper or loose clothing
7	use of shock tools with mushroom hands
8	improvising unsafe ladders and platforms
9	running
10	misuse of air hose

Even nowadays occupational accident rates are seen as an indication of process safety, implicitly referring to Heinrichs' safety pyramid (Heinrich, 1929). In scientific literature this assumption is questioned after World War II. The explosion of the Texas City refinery in 2005 has shaken the dominance of this indicator in the professional press, and the inquiry of Texas City points to the confusion between accident processes in occupational and process safety (Delatour et al., 2014). One of the first publications on safety indicators

Paper Received: 12 January 2019; Revised: 2 April 2019; Accepted: 3 July 2019

Please cite this article as: Swuste P., van Nunen K., Schmitz P., Reniers G., 2019, Process safety indicators, how solid is the concept?, Chemical Engineering Transactions, 77, 85-90 DOI:10.3303/CET1977015

came from the American engineer Thomas Rockwell (1959) (Table 1). He argued an indicator must be reliable, quantifiable, and easy to understand. Occupational accidents with or without lost time are not suitable, failing to account for associated consequences of unsafe behaviour. Rockwell is referring to Heinrichs' domino metaphor, and the 1919 accident proneness theory, which provides a scientific justification for the unsafe act concept, and associated behaviour of workers.

Wold War II had led to an acceleration of technical developments of military machinery and industrial processes, and had created serious control problems. Weaponry and machines were becoming increasingly complex, and created new demands on operators' cognition. It is generally considered that human factors, human reliability analysis, ergonomics, and man-machine systems originates from this period. 'Human factors' is the term used in North America, and 'ergonomics' in Europe; both refer to the study of man's relationship to his work. The domain is concerned with the design of equipment, work operations, and work environment to optimally match the capacities and limitations of the worker population. Beside military applications, also in companies, designers have a natural preference for hardware, and man-machine interfaces can look like 'clock-shops', biased more by designers' interests than machine operators' needs (Singleton, 1969). This upcoming ergonomics also influences the domain of safety science. Authors, like the Dutch physician and psychologist Willem Winsemius, have pointed to the relation between occupational accidents, the occurrence of process disturbances, and the lack of ergonomic design of workplaces (Winsemius 1951). His theory on accident processes is a forerunner for man-machine systems.

In the United States human factors (engineering) had, and still has, a strong emphasis on human efficiency, seeing human error as a main indicator of accidents, like Rockwell. Estimates of human error in man-machine systems are quantifying, including effects on system effectiveness. Databanks of human error probabilities have been set up, but appeared to be less successful. Valves and pumps do have very specific in- and outputs, while humans do not (Kirwan, 1994). There are problems with quantification (Rigby and Swain, 1971), and data collection. Despite these limitations, US human factors specialists remain focussed on human performance, while safety is regarded as a by-product of efficiency.

In Britain the ergonomics domain has been developed in close relations with human biological sciences, and psychology with a focus upon well-being, and health of workers, like the reaction of workers to stress (Singleton, 1967, 1971). In the late 1960s systems theory and systems approach from the United States enters the domain and the term 'system ergonomics' becomes familiar (Singleton, 1974). Human tasks and human information processing and their failures become important, leading to alternative explanations of human failures in industrial environments. The starting point is the assumption that workers are not clumsy, or accident prone when involved in accidents (Hale and Hale, 1970). And secondly, immediate causes of unsafe behaviour are shaped by systematic causes, such as the physical environment and organisations in which people work.

Major accidents, not only in the process industries, but in general in the so-called high-tech-high-hazard sectors continue to occur (Table 2). Complex, partly automated technology requires complex control and therefore situations can occur that cannot be predicted, or when predictable are not changeable.

Table 2 major accidents, a déjà vu (Le Coze, 2013)

high-tech-high-hazard sectors	1970s-1980s	2000s-2010
nuclear	Chernobyl 1986	Fukushima 2011
off-shore drilling	Piper Alpha 1988	Deepwater Horizon 2010
fuel storage	Port Eduard Heriot 1987	Buncefield 2005
aerospace	Challenger 1986	Columbia 2003
aviation	Tenerife 1977	Rio-Paris Air France AF 447 2009
chemical- petrochemical	Flixborough 1977, Bhopal 1985	Toulouse 2001, Texas City 2005
railway	Clapham Junction 1988	Landbroke Grove 1999
maritime I	Zeebrugge 1987	Costa Concordia 2012
maritime II	Exxon Valdez 1987	Erika 2003
air traffic management	Zagreb 1976	Umberlingen 2002

This can be a consequence of a larger distances between operators and controlling processes. Automation limits their task to diagnosis, analysis, and control of process disturbances in high-tech-high-hazard industries. Managements' fixation on occupational accidents plays a role, and automation itself which may insufficiently accounting for tasks of operators. 'We have fifth generation of technology and second generation of minds' (Westrum, 1988). Automation does not decrease the incidence of major accidents, but changes types of accident processes. After BP Texas 2005, governments, professional and international sector organisations have embraced the concept of process safety indicators. Publications show a large variety of definitions, and a focus on 'improving' and 'benchmarking', being buzz-words used in governmental and commercial publications. Examples are given of technical and organisational indicators, either being result indicators (lagging), or activity indicators (leading). And almost all indicators presented are quantifiable.

Obviously a question will rise if, for instance, the number of toolbox meetings, process failures, loss of containments, etc. will provide any information on dominant accident processes. Against this background this article will answer the following question: Which process safety indicators can be deduced from existing safety theories and models, and how 'solid' are these indicators?

2. Safety theories, models, and process safety indicators

Major accidents occurring in high-tech-high-hazard sectors from the 1970s onwards have stimulated various theories and models to understand major accident processes. Knowledge developments on occupational accident processes is soon outplaced by developments in the high-tech-high-hazard sectors. These theories and models are addressing either organisational determinants (disaster incubation theory, safety culture, and Swiss cheese), technical determinants (normal accidents theory and risk concepts), or a combination of both (socio-technical systems, high reliability theory, and bowtie). In the next three paragraphs these determinants are discussed. Their relation to process safety indicators is a topic in the discussion and conclusion paragraph.

2.1 Organisational determinants

The British sociologist Barry Turner is one of the first to address organisational determinants of major accident processes. His theory is known as the 'Disaster Incubation Theory', since this concept of incubation periods of disasters is a central idea of his book 'Man-made disasters' (Turner, 1978). The main question asked at organisations is: 'what has gone wrong in these organizations'. It is assumed that no single human error can be accountable for these major accidents. The causes had to be found in the complex and diverging chains of events and decisions made within those organizations. Various process disturbances make a production system vulnerable, prior to a disaster. Initially, hidden failures and poorly understood events continue to occur, and are presented as poorly structured surprises, not corresponding to the existing beliefs about hazards which the organisation is regarding as normal. According to the author, disasters are a by-product of 'normal' functioning management and technical systems. The collective failure of knowledge of the organisation and misconceptions of risks are caused by a lack of information. These are the ingredients of the incubation period of a disaster, which may take months, or years to result in a disaster. Management has lost contact with the operational reality. The term 'sloppy management' has been introduced in the literature.
The concept of safety culture is introduced in the 1980s. Contemporary accident reports, Chernobyl (1986), Kings Cross (1987) and Piper Alpha (1988), explicitly refer to culture, dealing with safety. It has become popular research, and is still discussed in many articles in the scientific and professional press. Edward Schein, an American social psychologist, proposed an ethnographic description of culture. His approach is social-anthropological to study divisions and differences between groups and societies. In his vision, culture is established during the first major stress test for survival of an organisation. The personal relationships, work patterns and organisational structures, the so-called basic assumptions being successful during the crisis, defines culture for the remainder of its existence. The 'soul' of the organisation is created (Schein, 1992). The culture of an organisation is a neutral concept. 'Good' or 'bad' cultures do not exist. The visible expressions of culture is present in official communications, artefacts, symbols, espoused values and behaviour patterns (Guldenmund, 2000). Culture is defined as shared basic assumptions of a group, or an organisation. This has led to three different approaches. 1/ First the academic approach, which refers to Scheins' work. At the heart of an organisation are basic assumptions, accepted beyond doubt. These assumptions cannot be observed directly, but can be distilled from observable artefacts, and espoused values by investigating work processes, documentation, interviews, etc. Conflicts within or between these cultural elements provide evidence for basic assumptions. The academic analysis of safety culture is qualitative in nature and requires active fieldwork in the organisation or company under study. 2/ The second approach is analytical, also referred to as safety climate. This approach originates from psychology. It creates a snapshot of safety culture, providing a brief insight into the perception, attitude and behaviour towards safety. Psychometric questionnaire surveys quantifies workers' perception towards safety, risks, workers participation in safety decisions, and quality of safety management. Safety climate research is limited to desk-top research, lacking field work and not being able to capture organisational dynamics. 3/ The last approach is a pragmatic, normative one, and not based upon extensive empirical research, but on experience of companies and experts. The approach is normative, because it links safety quality to safety culture. Opposite to an academic approach, a distinction is made between a 'good', and a 'bad' culture. The aim is to improve safety culture in an organisation so the organisation will reach a higher level of safety over all. This normative approach has no relation with basic assumptions. Despite all the research, no conclusive evidence was produced to relate safety culture to a level of safety of a company. There have been few concepts as desired and as poorly understood as safety culture (Hale, 2003). Recently, an integrated model combining safety culture models from different disciplines has been proposed (Vierendeels et al., 2018).

The latent factors, and poorly understood events from Turner, is the central point in the well-known Swiss cheese model, reaching its final version 1997 (Reason, 1997). The origin of latent failures lies in the company's organisation and its decision-making processes. These latent failures can be dormant for a long period of time (incubation period), but are activated in combination with other system failures. Therefore, major accidents are negative outcomes of suboptimal organisational processes. The British psychologist Reason described these latent failures with a medical metaphor: resident pathogens caused by designers, procedure writers, and top managers representing the 'blunt end' of an organisation. Labour conditions leading to major accidents can be reduced to a handful of latent factors, the so-called 'basic risk factors', representing the holes in the barriers of Swiss cheese. Eleven basic risk factors have been identified (Groeneweg, 1992): 1/ poor design of installation, equipment, tools, 2/ hardware, deficiencies in quality of equipment, tools, 3/ error enforcing conditions, 4/ inadequate management of maintenance 5/ absent defences, inadequate protection, 6/ deficiencies in quality, workability of procedures, 7/ poor housekeeping, 8/ training, deficiencies in knowledge and skills, 9/ incompatible goals, conflicting requirements 10/ communication, relevant information not receiving recipients, 11/ organisation, deficiencies in structure.

2.2 Technological determinants

The American sociologist Perrow (1984) is the founder of the Normal Accidents Theory (NAT). This theory is a technologically deterministic approach to major accidents, when an organisation can't control its technology anymore. The theory is based on a meta-analysis of a large number of accident reports from industrial, military, transport, and research sectors. Its naming refers to major accidents occurring in 'normal' organisations. Because of complex, interactive processes and tight coupling of process steps, these accidents became inevitable and are no longer foreseen by designers or understood by operators, engine-drivers, pilots, or managers. The complexity of the technology requires employees deliberately to make mistakes to learn and to understand the technology they control (Rasmussen, 1988). With a tight coupling of the process steps, there is no time to correct errors, which is at odds with the trial and error approach used by operators to understand the technology. Complexity requires decentralised control and decision-making in order to respond appropriately to unexpected events. A tight coupling between process steps, however, requires centralised control and decision-making; these two conflicting demands on control cause problems.

With the introduction of system theory, the risk concept enters the safety domain in the 1970s. This has paved the way for the development of mathematical models for quantitative risk analysis (QRA), based upon experiences in the nuclear sector, the process industries and reliability engineering from operations research. While discussions of risk are conducted in all industrialized countries they are particularly important in The Netherlands due to potential flooding risks of 55% of the country, limited space, and short distances between residential areas and industrial plants and clusters. The so-called 'coloured books' on QRA, developed in the Netherlands have contributed substantially to the Seveso Directives. While methods for quantifying risk are now widely applied and accepted, risk perception and risk in the political decision process are still being debated. Hazards are real, but risks are constructs within social and historical contexts which determine the significance of risks. The technical framing of risk reduces the role of citizens to trust or distrust of experts. For experts, risk is a number, and a technical assessment of the chance of mortality. For non-experts, or citizens, other characteristics of hazards and risk are relevant. In addition to the uneven distribution of risks, benefits and the degree of control, other arguments play a role, like the potential for catastrophes, the uncertainty of the calculation, or the threat to future generations.

2.3 Technical and organisational determinants

Organisations are now conceived as open systems, processing information. Doubts have been expressed related to the formal rationality of organisations. When problems occur in, for instance production, extensive problem analyses and solutions are almost never fully conducted due to time constraints. Rationality is a facade a way in which people in an organisation try to make sense of the flow of information and experience (Weick and Sutcliffe, 2001). In literature this is named 'socio-technical systems' the poorly understood interactions between technical, social and organisational aspects of production. One theory addressing these socio-technical systems is the High Reliability Theory (HRT), based upon extensive observations and field work (Weick, 1989, Roberts, 1989). In high reliability organisations, inherently dangerous and technically complex sophisticated tasks are performed with a very tight man-machine coupling under severe time pressure. Still, accident frequencies are very low, in contrast to predictions from NAT. Work takes place at the boundaries of design and human performances. These organisations do not have a traditional fixation on risk and minimisation of these risks. The keyword is redundancy, both organisationally, technically, and in terms of decision-making. As an example of organisational redundancy, one network, or team takes over, when another team threatens to fail a safety-critical task. Or during peak operations, more teams or more experts are called in. Teams are gathering large amounts of data and information during critical decisions, which are continuously

cross-checked. These organisations functions different from a classical engineering approach, which attaches greater importance to quantifiable, measurable, hard, objective, and formal knowledge and give lower value to knowledge based on experience. Failure reports are rewarded and no blame is laid on operators making mistakes. When problems with daily operations occur, organisational networks, or teams are formed which are self-designed and not formalised. When the problem are solved, the team, or network resolves itself. The organisation could easily switch between centralised and decentralised decision-making, which is carried out at the lowest hierarchical level, where problems arise. Thereby bypassing the main dilemma of the NAT of decentralised and centralised decision-making. The self-designed teams and networks, are only operating locally at the time of danger. The bowtie is a model for accident processes, based on an engineering approach. The model starts with one or more hazards. Several accident scenarios are shown as the arrows from left to right. These can lead to the central event, a situation where hazards have become uncontrollable, leading to consequences, like injury, or damage to material, or the environment. Barriers are physical or technical entities, interrupting an accident scenario. In this model, latent factors are not expressed as holes in barrier, as in Swiss cheese, but in so-called 'management delivery systems': actions of management to ensure and monitor barrier quality, influencing scenarios, or hazards (inherent safe design) directly. These delivery systems are non-technical. Engineers start with hazards. Authors outside the technical domain often disregard the engineering aspects of major accidents and work processes. This is evident in the barrier concept. Engineers define barriers as physical entities stopping or slowing down scenarios. In the Swiss cheese model, the barrier concept is expanded, also including non-technical barriers such as training, procedures, work permits, and other administrative routines. In the bowtie model these non-technical barriers are included as management delivery systems.

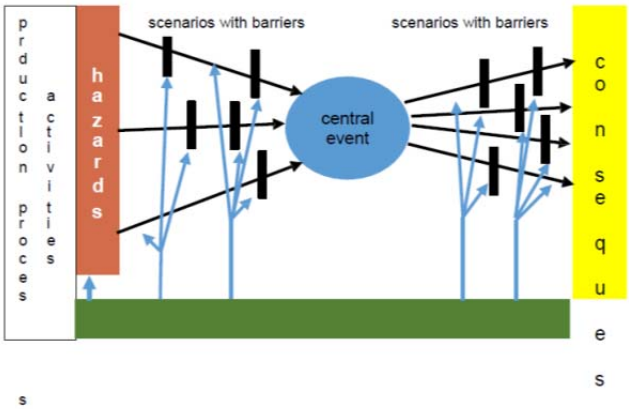

Figure 1: Bowtie metaphor (Visser, 1998)

3. Discussion and conclusion

A lot has been written on process safety indicators (Hopkins and Hale, 2009). Only, on this topic there is little published empirical research. Leading and lagging indicators is a distinction made in professional literature and governmental documents. If there is a difference, one would expect a logical connection between the two. This has not been demonstrated yet. Such a relationship is expected from the bowtie model. After all, a scenario left of the central event, continues its way to the right. A number of authors do not distinguish between leading and lagging anymore, because of this ambiguity a more general terminology is used, like process safety indicators.
Major theories and models of accident processes from previous paragraphs all come from the period between the late 1970s till the late 1990s. The ‘Drift to danger’ model (Rasmussen, 1997) is not discussed, because this model will not fit the topics of the paragraphs. However it is an important system dynamics model, showing the influence of actors, information, and conflicts, affecting process safety and bringing a system beyond its safety envelope. The pace and the dynamics of technological change and market-driven changes to a faster, cheaper and more efficient production, are much greater than the rate of changes of (safety) management structures and safety legislation. This pushes the drift to danger. Another model, resilience engineering (Hollnagel et al., 2006) is not included in this overview, because of its great resemblance with HRT. The discussion on models and theories shows that the formulation of relevant indicators is not an easy task. Most models and theories provide retrospective insights in past major accidents. Only a few may lead to starting points for indicators, like the basic risk factors, complexity and coupling from NAT, organisational, technical and decision making redundancy from HRT, and management delivery systems from the bowtie model. Monitoring progress of accident scenarios, and effectiveness of control measures is more difficult than professional and governmental publications like us to

believe. It is clear a ‘silver bullet’ has not been found yet, and most indicators published in literature are not ‘solid’ enough.

References

Delatour G., Laclémence P., Calcei D., Mazri C., 2014, Safety performance indicators: a questioning diversity, Chemical Engineering Transactions, 36, 55-60

Groeneweg J., 1992), Controlling the controllable, the management of safety, Doctoral thesis, Leyden University, DSWO Press, Leiden

Guldenmund F., 2000, The nature of safety culture: a review of theory and research, Safety Science 34(1-3), 215-257

Hale A., Hale M., 1970. Accidents in perspective, Occupational Psychology, 44, 115-122

Hale A., 2003, Safety Management in Production, Human Factors & Ergonomics 13(3), 85-201 Heinrich H., 1929, The foundation of a major injury, National Safety News, 19(1), 9-11, 59

Hollnagel E., Woods D., Leveson N., 2006, Resilience engineering, concepts and precepts, Ashgate, Aldershot Hopkins A., Hale A., 2009, Process safety indicators, Special issue Safety Science, 47(4), 459-510.

Kirwan B., 1994, A guide to practical human reliability assessment, Taylor & Francis, Bristol

Le Coze J., 2013, New models for new times. An anti-dualist move, Safety Science, 59, 200-218 Perrow C., 1984, Normal accidents, Living with high-risk technologies, BasicBooks, US

Rasmussen J., 1988, Human error mechanisms in complex working environments, Reliability Engineering and System Safety, 22, 155-167

Rasmussen J., 1997, Risk management in a dynamic society: a modelling problem, Safety Science, 27(2-3), 183-213

Reason J., 1997, Manging the risks of organizational accidents, Ashgate, Aldershot

Rigby L., Swain A., 1971, In-flight target reporting –how many is a bunch? Human factors, 13(2), 177-181Roberts K., 1989, New challenges in organizational research: high reliability organizations, Industrial Crisis Quarterly, 3, 111-125

Rockwell T., 1959, Safety Performance measurement, Journal of Industrial Engineering, 10(1), 12-16 Schein E., 1992, Organisational culture and leadership, Jossey-Bass, San Francisco

Singleton W., 1967, Ergonomics in system design, Ergonomics, 10(5), 541-548

Singleton W., 1969, Display design principles and procedures, Ergonomics, 12(4), 519-531 Singleton W., 1971, The ergonomics of information presentation, Applied ergonomics, 2(4), 213-220 Singleton W., 1974. Man machine systems, Penguin Edition, London

Swuste P., Gulijk C. van, Zwaard W., 2010, Safety metaphors and theories, a review of the occupational safety literature of the US UK and The Netherlands till the first part of the 20th century, Safety Science, 48, 1000- 1018

Swuste P., Gulijk C. van, Zwaard W., Oostendorp Y., 2014, Occupational safety theories, models, and metaphors in three decades after WO II, in the United States, Britain, and the Netherlands, Safety Science, 62, 16-27

Swuste P., Theunissen J., Schmitz P., Reniers G., Blokland P., 2016a, Process safety indicators, a review of literature, Journal of Loss Prevention in the Process Industries, 40, 162-173

Swuste P., Gulijk C. van, Zwaard W., Lemkowitz S., Oostendorp Y., Groeneweg J., 2016b, Developments in the safety science domain, in the fields of general and safety management between 1970-1979, the year of the near disaster at Three Mile Island, a literature review, Safety Science, 86, 10-26

Swuste P., Groeneweg J., Gulijk C. van, Zwaard W., Lemkowitz S., 2018, Safety management systems from Three Mile Island to Piper Alpha, a review in English and Dutch literature for the period 1979 to 1988, Safety Science, 107, 224-244

Turner B., 1978, Man-made disasters. Butterworth-Heinemann, Oxford

Vierendeels G, Reniers G, Nunen K. van, Ponnet K., (2018). An integrative conceptual framework for safety culture: the Egg Aggregated Model (TEAM) of safety culture, Safety Science, 103, 323-339

Visser K., 1998, Developments in HSE management in oil and gas exploration and production, in: Hale A., Baram M., (Eds.), Safety management, the challenge of change, p. 43-66. Pergamon, Amsterdam Weick K., 1989, Mental models of high reliability systems, Industrial Crisis Quarterly, 3, 127-142

Weick K., Sutcliffe K., 2001, Manging the unexpected, Resilience performance in the age of uncertainty, John Wiley & Sons

Westrum R., (1988), Organisational and inter-organisational thought, Contribution to the World Bank Conference Safety control and risk management, October

Winsemius W., 1951. De psychologie van het ongevalsgebeuren.(The psychology of accidents, PhD thesis). Kroese, Leiden