Safety Science 101 (2018) 121–134

Contents lists available at ScienceDirect

Safety Science

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

Implications from major accident causation theories to activity-related risk analysis

Xue Yang[a,*], Stein Haugen[b]

[a] Department of Mechanical and Industrial Engineering, Faculty of Engineering, NTNU, Norwegian University of Science and Technology, Norway
[b] Department of Marine Technology, Faculty of Engineering, NTNU, Norwegian University of Science and Technology, Norway

A R T I C L E I N F O

Keywords:
Major accident theories
Activity performance risk
Safety critical parameters
Operational planning decisions

A B S T R A C T

Operational Planning Decisions, which are characterized by short planning time and high frequency in the operational phase, has received little attention in risk and safety research in oil and gas industry. Activity performance risk, as an important part of the input to such decisions, must reflect explicitly the critical factors (Safety Critical Parameters) that determine the risk level involved in the activity. The paper looks into major accident theories that are relevant for the operational phase to find key concepts and implications for activity performance risk analysis. A generic list of Safety Critical Parameters is developed to assist managing both identified and unidentified risk in the activity. The main conclusion is that the different theories are not conflicting but supplementing to get the list that covers the most important factors in a broad sense. This list provides a guide to Operational Planning Decision makers to collect systematically activity-related risk information to ensure a safe activity.

1. Introduction

Experience has shown that decisions that are made in operational settings can have a significant influence on major accident risk. Among them, operational planning decisions, which are characterized by the short time lag between decision and execution, have received little attention in safety and risk research in the oil and gas industry. Most of the planning decisions are related to activities, such as

- Is it safe to allow another job next Monday, in addition to the already scheduled 50 jobs?
- After observing an internal leak from an isolation valve, is it safe to postpone the repair work to next week?
- Is this operation safe under current system constraints (e.g., gas detection systems have not been tested in a year, even though the scheduled test interval is six month)?

As a result, the variation in day-to-day risk of the plant is mainly activity-driven (Haugen and Vinnem, 2015; Knegtering and Pasman, 2013) and added on top of the baseline risk represented by the condition of technical systems. This requires a shift in focus from system-based risk analysis represented by quantitative risk analysis (QRA), to activity-based risk analysis (Haugen et al., 2016; Haugen and Vinnem, 2015).

We have earlier proposed to focus on three aspects of activity risk to generate a more comprehensive risk picture, as input to operational planning decisions. Activity consequence risk (ACR) captures the effect on the baseline risk level of the plant of completing an activity. Activity performance risk (APR) expresses the risk associated with performing an activity, with the system condition as a constraint. Period risk (PR) illustrates variations in risk level in the concerned period taking into account all activities that will be executed in the same period (Yang and Haugen, 2015). Motivated by the desire to better understand what influences these three aspects of risk and effectively plan how to control the risk, a review is conducted of some important accident causation theories relevant for the operational phase. As Leveson (2004) pointed out, "Accident models form the basis for all hazard analysis and risk assessment techniques."

Each theory has its own characteristics based on the causal factors it highlights (Kjellén, 2002). The energy-barrier perspective (Gibson, 1961; Haddon, 1980) emphasizes control of energy flow and mitigation of consequences caused by the release of energy based on the defense-in-depth principle. The Man-made disasters theory (Pidgeon and O'Leary, 2000; Turner, 1978, 1994; Turner and Pidgeon, 1997) highlights the lack of information flow and misperception among individuals and groups during an incubation period leading up to the accident. The conflicting objectives perspective (Rasmussen, 1997) looks at driving forces for unsafe decisions that push systems towards

* Corresponding author.
E-mail address: xue.yang@ntnu.no (X. Yang).

http://dx.doi.org/10.1016/j.ssci.2017.08.020
Received 14 October 2016; Received in revised form 5 May 2017; Accepted 25 August 2017
0925-7535/

the safety boundary. The Normal Accident Theory (Perrow, 1984) is a rather pessimistic perspective stating that major accidents are inevitable in complex systems due to “interactive complexity” and “tight coupling”. The System-Theoretic Accident Model and Processes (STAMP) (Leveson, 2012) perceives accident causation from a systemic viewpoint, indicating that accidents arise from inadequately enforced safety constraints, flawed control processes, and inconsistent, incomplete or incorrect process models. High Reliability Organization (HRO) (Laporte and Consolini, 1991; Roberts, 1990) and Resilience Engineering (RE) (Hollnagel et al., 2008, 2011, 2006) perspectives focus on a series of properties of organizations that can contribute to avoid major accidents. Strictly speaking, HRO and RE are not accident causation models. However, due to their important implications for accident prevention during operation, they are also included in the review.

The purpose of this paper is to demonstrate how these accident causation theories can contribute to activity-related risk analysis, especially activity performance risk (APR), as an input to operational planning decisions. The following questions are discussed in detail in the rest of the paper.

1. What are the main concepts and principles of these perspectives?
2. How can they contribute to activity performance risk analysis?

The work and findings are restricted to the following limitations. First, the work is performed with major accidents risk[1] in mind, which means the findings may not be applicable for occupational risk that stems from day-to-day occupational accidents. Second, the risk to personnel that is caused by major accidents is the main concern in this paper. Other elements of risk such as risk to assets and risk to environments are out of the scope. Third, we mainly focus on decisions from the Norwegian oil and gas industry, even though we believe the work has the potential to be transferred to other industries. Fourth, the decisions considered in this paper are major-accident related, or have major-accident potential. Fifth, the main background of this paper is to improve risk assessment methods to better support decision-making during the operational phase. This means decisions in early phases such as concept selection phase or design phase are out of consideration. Last but not the least, it is acknowledged that risk is only one criterion for decision-making in the operational phase. Other considerations such as availability of resources and cost obviously also play important roles in the decision-making process. In addition, the quality of the decision depends not only on the collected risk information, but also on other factors such as the competence of the decision-maker, information related to other objectives and who are involved in the decision. The paper only focuses on systematically identifying risk information that needs to be considered on an activity level, leaving the other factors out of consideration.

The remainder of this paper is organized as follows. In Section 2, the main principles of the alternative perspectives are summarized with a focus on critical causal factors that they emphasize. In Section 3, we introduce operational planning decisions and typical decision-making arenas for such decisions. We also briefly summarize the three aspects of risk related to the activity. Section 4 discusses briefly process safety indicators that are widely applied in the operational phase, and Section 5 discusses the implications of different perspectives on risk to activity-related risk modeling. Section 6 concludes the work.

[1] A major accident is defined as “an acute incident, such as a major discharge/emission or a fire/explosion, which immediately or subsequently causes several serious injuries and/or loss of human life, serious harm to the environment and/or loss of substantial material assets” PSA (2013). “Major accident”.Petroleum Safety Authority Norway, Retrieved from http://www.ptil.no/articles-in-safety-status-and-signals-2012-2013/focus-major-accidents-article9146-1095.html.

2. Main principles of different perspectives

2.1. Energy-Barrier Perspective (EBP)

The Energy-barrier perspective originates from the energy model introduced by Gibson (1961), and was popularized by Haddon (1980) with ten accident prevention strategies. The barrier perspective is widely applied in the Norwegian oil and gas industry and barrier management plays an increasingly important role in safety management in the industry.

The basic idea of the barrier perspective is that accidents happen due to loss of energy control and no effective barriers present in between energy sources and vulnerable assets Haddon (1980). The key elements in this perspective are therefore:

- Energy source (Hazard): this is the source of harm and losses. Avoiding accidents is about avoiding losing control over energy.
- Vulnerable assets: this is what we want to protect from harm and losses. This may take on a variety of forms although initially associated primarily with humans and avoiding loss of life and health.
- Barriers: this is our means to avoid losses, by “separating” or protecting the vulnerable assets from the hazardous energy. Provided we need energy and as long as there are assets that may be exposed, barriers are the key to maintain system safety.

This may be regarded as a classical interpretation, to treat barriers mostly as physical/technical means to prevent or protect assets from a dangerous energy source. The control strategies are commonly referred as “defense-in-depth” (IAEA, 1999) principle or “layer of protection” (CCPS, 2001) after the hazardous/initiating event. The perspective is further developed by the “Swiss cheese model” (Fig. 1) which shows how an accident emerges due to holes in multiple barriers caused by active failures and latent conditions (Reason, 1997). Active failures are unsafe acts committed by sharp-end personnel and technical failures that trigger unwanted events. They normally have a direct and short-lived impact on defence integrity. Latent conditions are “resident pathogens” within the system that arise from decisions made by designers, procedure writers, and top-level management (Reason, 2000). Latent conditions may lie dormant in the system for years, and when they combine with active failures and local triggers, an accident might occur.

Along with recognition of the important role played by procedures, administrative routines, and human actions, an extended interpretation of barriers has developed. A barrier is interpreted as “a physical and/or nonphysical means planned to prevent, control or mitigate undesired events or accidents (Sklet, 2006b)”. The barrier perspective is not only related to energy flow anymore, but also to other hazards, such as human errors in the process. This extended interpretation of barrier leads to one problem: all kinds of functions, elements, and systems that are associated with safety are given the label “barrier” (Rollenhagen, 2011).

The distinction between barrier system and barrier function needs to be clarified under the extended usage of the barrier. Barrier function is “a function planned to prevent, control, or mitigate undesired events or accidents”, while barrier system is “a system that has been designed and implemented to perform one or more barrier functions” (Sklet, 2006b). This means the barrier function is realized or executed by one or multiple barrier systems.

2.2. Man-Made Disaster Theory (MMD)

The man-made disaster theory suggested by Turner (1978) opened up a new perspective by looking into soft factors that lead to accidents. The theory suggests that rather than viewing disasters as “acts of god” that have nothing in common, they can be systematically analysed by looking into soft factors such as humans and organizations. Turner’s