Safety Science 109 (2018) 201–218

Contents lists available at ScienceDirect

Safety Science

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

Systemic thinking in support of safety management in nuclear power plants☆

Björn Wahlström

Systems Analysis Laboratory, Aalto University, Otakaari 1F, FI-02150 Espoo, Finland

ARTICLE INFO

Keywords:
Systemic thinking
Safety management
Nuclear power
Organisational deficiencies
Decision making
Systems intelligence

ABSTRACT

Systemic thinking is proposed to be applied within safety management. In the article I discuss benefits and content of systemic thinking in connection to safety. Systemic thinking has to do with creating an understanding of systems in an environment. How can macro behaviour be understood as generated by micro interactions of its parts? The article places a focus on nuclear power in Finland, because it avoids dangers of being too abstract. An application of safety principles during design and operation makes it possible to reach acceptable safety and avoid open ended discussions. A definition of necessary and sufficient requirements for safety condensed into claims and evidence can be collected from systems design and operation. The article starts with an account of concepts from systemic thinking and safety management, to discuss how sociotechnical models can be used. A separation between humans, technology, organisation and information provides a system of systems model of the plant. Using this model one may consider safe and dangerous regions of the plant state space. A proper management of design and operation makes it possible to argue that used practices provide mechanisms for early detection and correction of deficiencies in plant systems. Important components are management systems, decision support, performance evaluation, organisational learning, staff proficiency and stakeholders. In the discussion part of the article remaining challenges in ensuring safety are brought forward. The article concludes that systemic thinking and a simultaneous consideration of entirety and details are important components in ensuring nuclear safety.

1. Introduction

Systemic thinking has been proposed to be applied within safety management. In this article I discuss content and benefits of systemic thinking in connection to safety. Systemic thinking has to do with creating an understanding of systems that are functioning in an environment. Systemic thinking involves concurrent views on entirety and details of the object of investigation. How can macro behaviour be understood as generated by micro interactions of its parts? A systemic approach has an important contribution for understanding concepts of risk and safety. Systems designed and operated for production of goods and services may as a by-product carry hazards of incidents and accidents. Traditional safety engineering, where hazards are eliminated, isolated, controlled and mitigated, has largely been successful in minimising risks in both occurrence and severity. In this article I argue that systemic thinking and methods of systems analysis can contribute to an increased safety of industrial systems. In this endeavour recent research activity in system complexity, systems of systems and systems intelligence are highly relevant.

In the article I focus on the nuclear domain in Finland, because it enables me to avoid a too abstract reasoning. This does not belittle the fact that safety oriented organisations in one domain and country can learn from organisations in other domains and countries. I think however that each domain and country have their own characteristics, which have to be taken into account when looking at details of safety precautions. In the nuclear domain, safety thinking has to a large extent been influenced by three major accidents, TMI, Chernobyl and Fukushima. Not going into details, my own simple interpretation of these accidents is that (1) it is necessary to account for humans in building safety, (2) it is necessary to understand organisations and their contributions and (3) when a single plausible event may lead to disaster, this plant should be closed and not be allowed to operate before the risk is removed.

Safety science has in my view gone through a considerable development during the last four decades. Models, methods and tools used today can at least in principle make our systems safe. Incidents and accident still occur, which does not seem to depend on an absence of knowledge, experience and skills, because analyses of incident and

☆ This research did not receive any grant from funding agencies in the public, commercial, or not-for-profit sectors.
E-mail address: bjorn.wahlstrom@aalto.fi.

https://doi.org/10.1016/j.ssci.2018.06.001
Received 21 June 2017; Received in revised form 23 April 2018; Accepted 3 June 2018

accidents regularly point towards simple misses and oversights in safety precautions. Engineered safety nets have not been able to prevent events and aggravating conditions in their moves of plants to unsafe states from which no returns have been found without large damages. These observations pose the question “have we been able to learn?” (Le Coze, 2013a). Articles in Safety Science have argued for the need to see accidents as consequences of system deficiencies and not to assign blame on people (Dekker and Breakey, 2016). I would to a large extent agree with the view that accidents have a systemic cause, but I would still keep senior management accountable at ill-fated plants. They have accepted the task of managing their plants and they have had power to act (Dekker and Nyce, 2014), but have apparently not been able to look after important issues.

For nuclear power plants, but also for other technical systems, it is necessary to separate between design[1] and operation. Deficiencies in design are claimed to cause more than half of problems in the operations phase (Taylor, 2007; Kinnersley and Roelen, 2007). Safety precautions are in the design process built into plants and their management systems to make them acceptable for operation. Plant operation relies on successful design of many systems, some physical and other non-physical, all with their own models, methods and tools (Wynn and Clarkson, 2017). In Finland the process aiming at a new nuclear power plant is governed by three points of approval. The first point is a decision in principle by the parliament, which confirms that a new plant is in line with the overall good of Finland. The second approval is a construction license and the third an operating license, which are awarded by the Radiation and Nuclear Safety Authority in Finland (STUK) after due investigations that applicable safety requirements are fulfilled. These requirements are taken into account by a safety philosophy, which forms the backbone of plant design and operation. By an analogy, one may consider the difference between designing a safe car and driving a car safely. This view of the difference between design and operation is supported by Stoop et al. (2017). For the discussion below, I have in Fig. 1 made a slight modification in their DCP-diagram (design, control, practice).

One problem in the nuclear domain is that, both generally and especially within digital instrumentation and control (I&C), there seems to be an implicit expectation that safety precautions should be complete, consistent and correct (C^3). In the general case this is not possible, which implies that one can only consider what could be seen as sufficient (Wahlström, 2015). A set of requirements placed on a plant can never be complete, because there is always a possibility that some event together with a suitable set of aggravating conditions will form a challenge to safety. Requirements may be incomplete or contradictory, which implies that designers are left indecisive. Computer programs as well as procedures and instructions cannot be considered safe by inspections only, because they have to be run to know the trajectories the plant state will take. This may perhaps be obtained using simulator models provided that they are correct representations of the plant. However, correctness in this sense can only be ensured by comparing simulations with actual plant transients. An assessment of the safety of a plant is restricted to two high level questions, (1) what can be considered necessary for safety and (2) which requirements can be considered sufficient. These questions should be formulated for the entire plant as well as for its subsystems of humans, technology, organisation and information (HTOI).

The intent of the article is threefold. Firstly it brings up a minimal set of concepts from systems theory that is of help in elucidating the discussion in the rest of the article. Secondly it aims at painting a broad picture of safety management to identify important activities, processes and tasks, which should be given proper attention in design and operation. Thirdly it tries to elucidate the need for and use of systemic thinking in creating an understanding of structures, systems and components (SSC) that determine plant responses in different situations. Safety in this article has a focus on complex technical systems, where high consequence low probability events are a specific concern. I have selected this focus as compared to low consequence high probability events, because I think actions for their management differ. In the article I concentrate on incidents and accidents that have an organisational origin, because they typically emerge from unexpected interactions between several systems, i.e. they have a systemic cause. Such incidents and accidents can regardless of their initiating events, in most cases be attributed to shortcomings by senior management in design and/or operation of the plants.

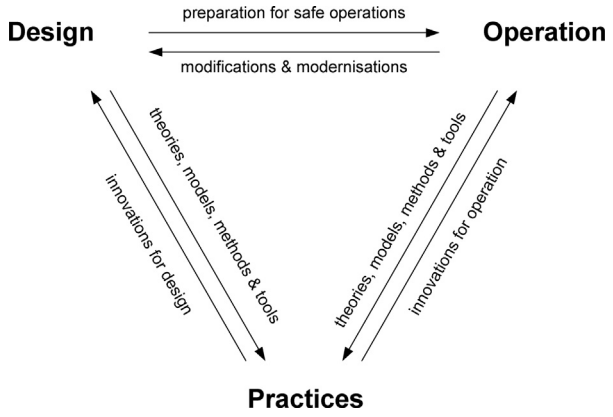

Fig. 1. Interactions between design, operation and practices. For a new system a design and construction project prepares for safe operation. In operation the system is modified and modernised in small projects. Experience from both design and operation is collected to practices that may or may not transfer to later innovations in design and operation.

The first major section of the article introduces systemic thinking in a broad sense. The next section gives a brief overview of major concepts of safety management together with important activities, processes and tasks. The fourth section introduces the concept of sociotechnical systems that serves as a model for understanding how organisations create safety in controls, behaviour and actions. The fifth section starts with a discussion of characteristics of design and operation and continues with a discussion of practices in seven important subdomains of design and operation. In the last section I take a forward look at issues that represent future challenges within safety management. In the summary and conclusions, I reiterate some of the most important issues of the article.

2. Systemic thinking

Systemic thinking has been taken up within safety science as an important component in creating an understanding of contributors to risk and safety. Systemic thinking can be seen as the essence of the development of systems theory and systems science that took place after the Second World War. Systemic thinking incorporates important results from sciences connected to automation, communication, cybernetics, games, information and operational analysis. Important contributors to system sciences have over the years, among many others, been Ludwig von Bertalanffy (1969), Peter Checkland (1999), Norbert Wiener (1961) and Herbert Simon (1996). The development of systems science can be seen as a reaction to an earlier division of science into separate isolated domains.

There have been long discussions whether or not systems engineering has an application for systems, where humans and organisations are integrated parts. They seem to have converged into a division between hard and soft systems practices (Checkland, 1995), where hard practices are associated with classical operational research and soft system practices have to do with action research. However in the

[1] For the sake of simplicity, I use the term design to cover all activities of plant design, construction and commissioning.