VTT TECHNOLOGY 293

Sociotechnical systems theory and the regulation of safety in high-risk industries

White paper

Jean-Christophe Le Coze

Ineris

Kenneth Pettersen, Ole Andreas Engen, Claudia Morsut & Ruth Skotnes

University of Stavanger

Marja Ylönen & Jouko Heikkilä

VTT

Ivanne Merlele-Coze

ISBN 978-951-38-8523-6 (Soft back ed.)
ISBN 978-951-38-8522-9 (URL: http://www.vttresearch.com/impact/publications)

VTT Technology 293

ISSN-L 2242-1211
ISSN 2242-1211 (Print)
ISSN 2242-122X (Online)
http://urn.fi/URN:ISBN:978-951-38-8522-9

JULKAISIJA – UTGIVARE – PUBLISHER

Teknologian tutkimuskeskus VTT Oy
PL 1000 (Tekniikantie 4 A, Espoo)
02044 VTT
Puh. 020 722 111, faksi 020 722 7001

Teknologiska forskningscentralen VTT Ab
PB 1000 (Teknikvägen 4 A, Esbo)
FI-02044 VTT
Tfn +358 20 722 111, telefax +358 20 722 7001

VTT Technical Research Centre of Finland Ltd
P.O. Box 1000 (Tekniikantie 4 A, Espoo)
FI-02044 VTT, Finland
Tel. +358 20 722 111, fax +358 20 722 7001

Cover image: Shutterstock

Juvenes Print, Tampere 2017

Preface

This white paper is a product of the research project on Sociotechnical Safety Assessment within three regulatory regimes (SAF€RA STARS). The project was launched in the end of 2014 and it ended by the end of the year 2016 and it has been carried out by L'institute National de l'Environnement Industriel et des Risques (Ineris), University of Stavanger, and VTT Technical Research Centre of Finland Ltd also as a coordinator. The three regulatory regimes include the Norwegian petroleum industry and the industrial use of hazardous chemicals in Finland and France.

The objectives of the research project were the following:

1) Explore what the shift towards sociotechnical approach entails from a scientific viewpoint and how it affects management of safety
2) Compare the practices in risk regulatory regimes on sociotechnical approaches to safety critical systems
3) Clarify the regulation (limits and possibilities) in ensuring sociotechnical safety in society
4) Develop an evidence-based guide on how to develop regulatory practices towards taking better into account the sociotechnical dimension of safety.

This white paper aims to contribute to the first and third objective. The other objectives of the project will be handled in the other publications of the project.

FONCSI
Fondation pour une culture de sécurité industrielle
safera
The Research Council of Norway
tukes
INERIS
maîtriser le risque pour un développement durable
University of Stavanger

Contents

1. Introduction

This white paper is about the implication of a sociotechnical system approach for regulating safety and disaster prevention in high-risk industries—sectors that are already quite extensively regulated. A sociotechnical system approach to safety is characterised by an orientation toward operational variability and the optimisation of technical–human interactions in industrial systems, including a micro–macro scale for describing system influences on accident risks and safety outcomes.

Sociotechnical developments have contributed towards a wider and multidisciplinary theoretical and methodological scientific field for understanding and managing worker- and organisation-related risks. Across high-risk industries, regulatory theory has incorporated elements of sociotechnical systems thinking. For example, in relation to major accidents and disasters, a sociotechnical understanding of causes embraces the interrelatedness of technical, human and organisational factors in specific contexts (Turner and Pidgeon 1997; Reason 1997). A sociotechnical system approach substitutes individualised and general models of human action and error with descriptions of complex and adaptive realities involving a wide range of individual, technical, organisational and systemic factors. This allows concepts and theories for prevention, such as safety barriers, redundancy and safety management systems, to be developed and studied from different perspectives and across scientific disciplines and practices.

Today, regulators and the industry have a diverse toolbox with standards, concepts and methods for analysing accident risks and evaluating safety measures, including technical specifications, technical risk assessments, best practice, licensing and training standards. The linking of engineering, psychology and organisational perspectives has also produced new models of audit and control, applied in various regulatory and cultural contexts. These are among other meta-rules for risk management systems or functional requirements for safety management systems. Related to rules and established practices, detailed procedures and meta-frameworks developed in nonprescriptive regimes, regulators are mainly engaged in a process of monitoring compliance (Hopkins 2007). This is an important role, but if taking account of a sociotechnical systems approach, safety regulators should find ways to go beyond compliance in improving the management of major accident risks (Hopkins 2007).

Moreover, current regulatory approaches to safety that include sociotechnical factors, such as meta-frameworks for risk management or safety management systems, have a tendency to focus on companies and not relate dynamics of safety to wider systemic trends or institutions in society, such as regulatory culture, labour relations or evolving modes of production that can influence a particular industrial system. Current knowledge and regulatory practice may thus be less relevant in relation to long-term societal shifts or other external challenges that could undermine safety (Pettersen and Schulman 2016; Le Coze 2016a).

As addressed by Pettersen and Schulman (2016) and Le Coze (2016a), systemic changes in societal goals and policies, such as economic stringency goals set by leaders and public officials or the shift in public attention and support for regulation in relation to the demand for cheaper services, can influence the performance and control of technological systems. In recent decades, some critical infrastructures have also been influenced by new public or shareholder pressures to be ''lean and mean" or increased public demand for lower regulatory costs and faster infrastructure speed or capacity (Stephens et al. 2015; Billings 1996).

In addition, globalisation processes are increasing in frequency and speed across industries, shaping new operational constraints on high-risk systems. New interconnected systems following the digitalisation of information and communication technology, the liberalisation of trade and finance, deregulation and privatisation agendas are examples of such supranational processes creating new environments for companies, states and civil society. The implications for major accident risk following these broadly scoped transformations are not straightforward and have to be understood related to their specific context.

In order to address these shifts, accident models and regulatory practices have to be broadened in order to address systemic issues. Human–machine interactions and organisations' contexts are not the only pressing issues of sociotechnical safety development as systems today are networked and globally distributed across regulatory contexts and cultures. How can sociotechnical system theory help us understand, and potentially manage, drivers of system change and systemic risks at macro levels? A sociotechnical system view for regulation beyond compliance must include in the picture the interconnectedness of several dimensions beyond the technical–worker–organisation scale, introducing and then connecting operational variability to systemic structures, institutions and strategic developments.

Aimed at policy makers, regulators, industry managers and other stakeholders, this white paper make explicit some key issues for regulating safety and major accident risk within industries, which derive from including a macro perspective on sociotechnical systems and accidents. Some of the issues raised lead to questions of concern whereas others show future directions towards alternative practices and innovative solutions for regulating high-risk systems. All of the issues have to be explored further in collaboration with a diversity of stakeholders. Do we have sociotechnical system models that enable us to model risk and safety developments at the macro level in relation to micro–meso level implications and change? What are key conceptual and methodological implications of such theorising? What are the implications for regulation when emphasising the relevance of the sociotechnical landscape (Geels 2002) at the macro level?

2. Sociotechnical safety: an overview

2.1 Sociotechnical system thinking in industrial safety: a short history

Sociotechnical system thinking started with work conducted at the U.K. Tavistock Institute of Human Relations (Trist and Bamforth 1951; Emery and Trist 1960; Trist et al. 1963; Trist 1981). Researchers at the institute reflected on the importance of adding to the technical framework of production, the so-called human factor inside a work system (industry or organisation). The idea of the sociotechnical system was designed to cope with the theoretical and practical problems of working conditions in an industry, particularly the introduction of new machines into coal mines.

The researchers argued that technology could not be an independent and autonomous variable as it is strictly related to and influenced by social aspects, such as human working conditions and political and economic structures. Thus, the term sociotechnical was coined to describe the reciprocal interrelations between technology and humans. The term system was taken from general system theory, which describes a system as a set of elements related to each other, with functions that transform the system over time.

These studies provided the foundations for sociotechnical system theory (van Eijnatten 1997), which sought to overcome the challenge of analysing the elements of a system separately by embracing the complexity of industrial systems and the interdependencies between technical (hard or structural) and social (behavioural) aspects. Furthermore, the theory sought to explain adaptations in the workplace in terms of improving ways of organising work, technology and practices (Davis et al. 2014; Klein 2014).

Several disciplines (sociology, psychology, engineering, cognitive engineering, ergonomics, management, and political sciences) have enriched sociotechnical system research, and over the years researchers have formulated different models in order to develop a unifying concept of a "sociotechnical system", such as Smith and Carayon-Sainfort's (1989) work on system model or Wilson's (2000) model of interactions.

In the field of safety, a focus on variabilities at the source and the influence of complex system dynamics is endorsed in the most explicit manner by

Rasmussen's (1997) graphical vertical model (figure 2). Rasmussen's work was part of a growing literature stream, starting in the 1970s, during which "high-risk" (or "safety critical") systems were grouped into an independent category that included industries such as nuclear, aviation, marine and petroleum (Le Coze 2013a). This new category created a sense of common interest for systemic issues linked with the management and governance of such systems, such as the nuclear, aviation, marine, petrochemical or railway systems.

These systems also shared a potential harm to society. Planes can crash, boats can sink, trains can derail, nuclear, petrochemical and chemical plants can explode, and dams, mines and bridges can collapse—all events that threaten the lives of a great number of people at once and/or can endanger generations to come with their long-term radiological or toxicological effects. The rapid increase in size and number of planes or tankers, the concentration of chemical plants, the construction of nuclear power plants, etc., are probably reasons why this interest has intensified over the years.

These trends triggered a mounting social concern: Can our societies master these now ubiquitous dangerous artefacts? Ulrich Beck (1986) in Germany, Barry Turner (1978) in the UK, Patrick Lagadec (1982) in France and Charles Perrow (1984) in the US expressed and shaped, in different ways and through different angles, an academic interest in the topic of high-risk systems and accidents and disasters.

Their message could not be missed, as a first wave of disasters across high-risk industries in the 1980s contributed to justifying the need for a better understanding of the issue of safely operating high-risk systems. Events like Chernobyl (1986), Bhopal (1984), the Challenger disaster (1986), the Piper Alpha disaster (1988) and the MS Herald Free of Enterprise disaster (1987) questioned the ability of modern engineered systems to remain under the control of society.

A host of disciplines including mathematics, engineering, sociology, psychology, ergonomics and cognitive engineering, management, law and political sciences contributed to shaping views of disasters and their prevention and created networks and communities of researchers. An example of the intensity of the debates related to preventing disasters in complex risky systems is the World Bank's workshops held at the end of the 1980s, which gathered a wide range of authors across scientific disciplines and areas of expertise (Rasmussen and Batstone 1989).

Today the relations and influences among technology, human working conditions and organisational structures are part of the principles for managing high-risk systems. Although the relationship between organisations or systems of organisations (i.e., regulatory regimes) and their societal landscape (political, economic, legal, demographic, and cultural dimensions) are key elements of a sociotechnical system view on industrial safety, these have not been as thoroughly researched and acknowledged in relation to regulation. In a sociotechnical system perspective, safety is the dynamic outcome of ongoing implementations of functions which must be understood through technical design and task requirements, as well as structural features of organisations and cognitive, cultural, and power relations at several nested layers of an industrial system (micro–meso–macro) (Le Coze 2013a).

2.2 Sociotechnical system thinking in disaster prevention: current challenges

The repetition of disasters, or the feeling of déjà vu (table 1), has indeed triggered many debates in the field of safety (Le Coze 2013a). Has any progress been made? What about our safety models and theories? Are they still relevant? Have regulations failed in these cases? Should regulations be adapting? Changes are empirical; they concern the daily operating realities of high-risk systems. In this respect, what is the difference, for instance, between the context of the Piper Alpha disaster in 1988 and the Deepwater Horizon disaster in 2010, some 22 years later? What is the difference between the context of Chernobyl in 1986 and Fukushima Daïchi in 2011, 25 years apart?

Table 1. A déjà vu feeling 30 years apart.

Period	
1970s–1980s	**2000–2010**
Chernobyl, 1986	Fukushima Daïchi, 2011
Piper Alpha, 1988	Deepwater Horizon, 2010
Challenger, 1986	Columbia, 2003
Tenerife, 1977	Rio Paris, 2009
Bhopal, 1984	Toulouse, 2001
Exxon Valdez, 1987	Erika, 2003

In fact, a major feature our contemporary situation is globalisation and the rise of a network society—a term coined to describe the changes of the past 20 to 30 years. The following points about the concept of globalisation build a general picture embracing major trends (Le Coze 2016a):

- Despite what could be called (with much simplification) pre-globalised experiences in human history, in the past three decades the world has gone through an intensified stage of transformation characterised by the liberalisation of trade and finance, privatisation, deregulation and technological development, including information and communication technology and transport.

- These transformations created unprecedented flows of money, people, capital, images and data, leading to a host of new problems and challenges such as world governance, multinationals' expansion and power, nation-states' evolving status, civil societies' new struggles and the production of a diversity of identities as a reaction to these processes.
- Far from being a linear, unilateral, homogeneous and monocausal dynamic, globalisation is instead to be understood as a complex, localised, heterogeneous, multilayered and multicausal process where phenomena of both convergence and divergence can be witnessed across technological, cultural, geographical, social, economic and political dimensions, leading to both positive and negative outcomes.
- As these changes take place, a certain number of conceptual developments are produced to try to grasp analytically the new dynamics involved, among which the notion of network stands out. The relevance of the concept rests on its metaphorical power that suggests the possibility of connecting a multiplicity of nodes together, whether these are individuals or other entities (e.g., computers, machines), throughout a range of flows forming complex and polycentric configurations challenging established territories and boundaries.[1]
- In terms of any social science concepts and research, globalisation is both a descriptive and normative topic reflecting a very large number of assumptions and preconceptions of its advocates or opponents, whether from academic, business or civil areas. It indeed has a strong performative value, thereby leading to the much polarised debate over the notion beyond academic circles.

Many accident models and safety theories developed during the 1970s, 1980s and 1990s are related to the notion of a post-industrial society as a central description of Western societies, which saw major transformations in cultural, political, economic and technological areas following the Second World War (Touraine 1969, Bell 1973). In the first decade of the 21st century, the concepts of network society or informational society were suggested, most notably by Manuel Castells (2001), to replace this previous scheme and embrace current transformations.

Information technology, privatisation, deregulation, and financial and trade liberalisation have indeed shaped a new world for industries, leading to new opportunities as well as new challenges (Berger 2005). Incorporating new technological developments into operations, adapting strategies to uncertain global markets, structuring organisations to obtain flexibility through subcontracting and matrix organisations, complying with new demands for accountability through international and intensified standardisation and indicators

[1] Closely associated to it is the notion of complexity. Urry (2005), a theorist of globalisation, qualified it as a complexity turn for the social sciences in this context. See Le Coze (2005, 2008) for a discussion of complexity and safety or Dekker (2011).

(KPI) and negotiating with a risk averse civil society with stronger ecological concerns are some of the new trends of the past two or three decades that have been shaping the environment of high-risk systems.

The Macondo well disaster is a relevant example of the new landscape in which accidents now occur. Intense subcontracting, the creation of autonomous business units (BU) through decentralisation, new technological developments, the intensification of formal audit processes relying on quantitative indicators for compliance to standards, self-regulation and financialisation of strategies under new globalised opportunities are some of the aspects that characterise the orientations that BP's leaders chose and which led to several other incidents and accidents (Bergin 2012; Le Coze 2016a).

Safety adapts to opportunities offered by industries changing environment. Of course, some of the classical explanatory principles of disasters remain relevant across time, including cost reductions or the lack of shared lessons from incidents in companies. However, they now unfold in new terrains, in new dynamics and with new contexts. These empirical novelties, under the heading of network society, are consequently important to reflect on as they represent challenges to regulating safety within high-risk industries. The next section exemplifies these concerns further.

2.3 An example: The Deep Water Horizon (DWH) disaster

There may be no better way to illustrate and understand risk and safety in terms of sociotechnical systems than to immerse oneself in the outcomes of an accident investigation (Le Coze 2016b). In the past thirty years, a wealth of well-documented reports on disasters has been produced. What do they show? The recently investigated Macondo well disaster offers a good illustration (Oil Spill Comission 2011).

In 2010, an offshore drilling platform commissioned by BP and belonging to Transocean exploded in the Gulf of Mexico, killing 15 people and creating one of the biggest oil spills in US history. The accident occurred when high-pressure gas from the geological layer being drilled flowed back up to the platform and exploded, destroying it. Approaching this disaster from a sociotechnical perspective, it is possible to distinguish and decompose the event into several areas, as briefly introduced here with the help of several illustrations extracted from the report (figure 1), while indicating some of the key concepts found in the literature.

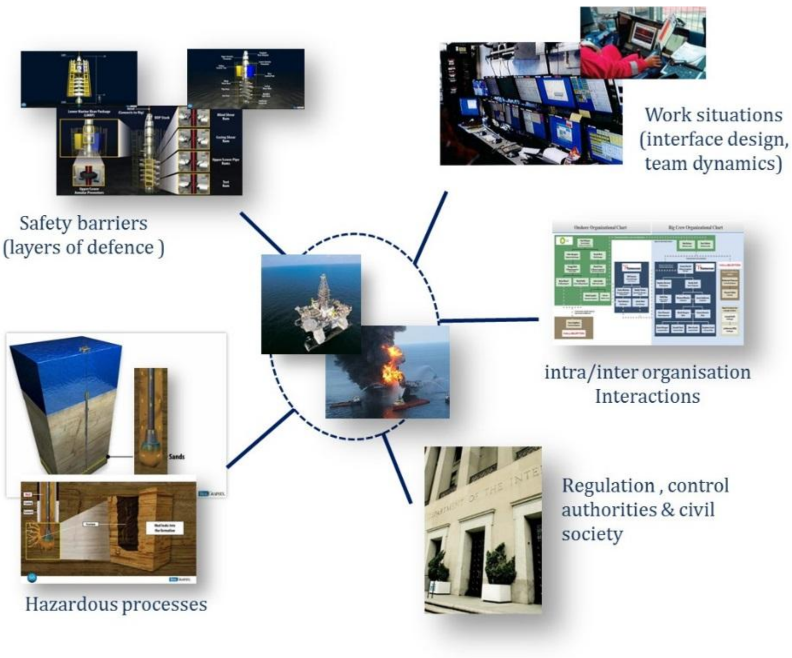

Figure 1. Macondo well disaster: several dimensions to consider.

First, the hazardous processes constitute the source of energy likely to physically cause harm through the natural and artificial phenomena encountered. Deep water exploration entails drilling operations with safety issues including (among others) the loss of containment of gas from the well. One scenario is a ‘kick’ followed by the release of gas on the platform, creating a flammable cloud at the surface. The uncertainties involved in drilling and the likelihood of a ‘kick’ are conditioned by interactions between the tools and the characteristics of geological formations (e.g., temperatures, pressures, nature of sediments). The Macondo well accident was the result of high-pressure gas in a geological formation, the loss of containment of gas and the ignition and then explosion of a flammable cloud which reached the platform.

Second, the technological and engineering-based safety barriers (or layers of defences) prevent and mitigate identified scenarios of potential accidents. In deep water exploration, a blow out preventer (BOP) is for instance one of the key elements of this defence in depth strategy, along with the casing, shoe track cement and cement plugs. In the case of a gas release, a BOP can be activated to stop gas from flowing upwards to the platform. Accidents occur when safety barriers (their redundancies) fail, including the BOP (its functioning, maintenance and design), which introduces issues of reliability and probability as well as the calculation of risks.

Third, operators' (team)work situations (often including human machine–computer interaction) activate or supervise production systems as well as safety barriers. When conducting drilling, an important task is supervising operations from a distance, with the support of computerised technology. Along with this, more visual and manual tasks are also involved on the deck of the platform (e.g., mudlogging). Retrospectively, in light of the DWH events, it appears that the design of human–machine interactions included issues related to the handling of displayed information and the management of alarms in addition to issues related to errors, team dynamics, sensemaking, groupthink and situation awareness in collective situations.

Fourth, inter-/intra-organisational interactions provide resources and constraints to operating actors, whether operators, engineers or managers. Drilling activities involve the interaction of many experts from different organisations, including BP, Transocean, and Halliburton. They require design choices before as well engineering adaptations in the course of operations. This requires coordination among various scientific, engineering and operating backgrounds on a daily basis throughout the lifetime of the operations. The DWH accident involved many issues, including safety management systems and culture(s) as well as potential issues associated with concepts such as drift, deviance or limits of organisations over time, resources and budget pressures.

Fifth, the regulatory and societal aspect of high-risk industries shape specific contexts for companies. Deepwater explorations fall under the regulatory supervision of control authorities who require companies to demonstrate their ability to operate safely and provide access to activities and internal documents in order to perform inspections. In retrospect, issues related to the type of risk regulation regimes have indicated conflicts of interest between safety and industry development as well as technical engineering competences of authorities in the face of evolving technologies. The concepts of robust regulation and regulatory capture indicate important issues to be considered.

2.4 Current related sociotechnical concepts

As highlighted in the previous discussion, since the 1970s, a catalogue or repertoire of concepts associated with a better grasp of sociotechnical systems has slowly been built up and applied in regulations. The concepts span a range of disciplines and industries and have various origins (e.g., safety culture originated in the nuclear industry after Chernobyl). Most of the time, they are not exclusive in the sense that concepts can be approached by many different perspectives and be applied in different ways depending on the contexts. For instance, the topic of safety culture, much like the topic of learning, can be studied through managerial, psychological, anthropological or sociological perspectives. Both concepts can also be introduced in aviation, nuclear or chemical industry regulations, although they may be concretely deployed through different definitions and investigation practices.

Moreover, some of these concepts have migrated from one scientific domain to another, such as the notions of redundancy or barriers, both of which have been translated from the field of engineering into the field of human and social sciences. Identifying and collating some of these more important concepts results in the following list of approximately 20 items (table 2), as long as one follows a broad coverage of the field. In this table, the left column indicates disciplines that would be more related to the concepts introduced and the right column exemplifies implications for regulatory methods and practices.

Yet as already noted above, concepts are not exclusive to one discipline; indeed, they migrate to different disciplines depending on the industrial context. Choices of definition and investigation methods also remain the product of contextual criteria. What becomes regulated in one industry may not be in another. This is particularly true for meta-rules and how they are included in regulations or not. Therefore, table 2 indicates that the concepts identified are to some extent also overlapping, but not always in a straightforward way, across the diversity of industries and disciplines.

Related to their scientific connections, concepts and, therefore, regulatory practices connect to specific ways of understanding and approaching companies and industrial systems, highlighting certain aspects while excluding many others. Table 2 has the virtue of offering a multidisciplinary view in a very vast field—namely, putting together concepts (and/or topics) but without explaining precisely how they can be associated, articulated or coordinated for a sociotechnical system approach to regulating safety.

Table 2. List of sociotechnical concepts (and/or topics) in relation to scientific (and engineering) disciplines (indicative) and regulatory practices and methods.

<table>
<tr><th>Related scientific (& engineering) disciplines (indicative)</th><th>Concepts (and/or topics)</th><th>Regulatory methods and practices</th></tr>
<tr><td>Natural sciences, Mathematics, Engineering</td><td rowspan="4">Explosions, combustion dynamic, flames behaviours, toxic clouds (natural & artificial phenomena)
Probability, failure, reliability & risk
Safety barriers & defence in depth (hardware, software)
Redundancy
Human–machine/computer interaction
Human error
Situation awareness
Expertise
Sensemaking
Teamwork
Resilience
Whistle blowing
Groupthink
Mindfulness
Learning
High reliability organisations
Safety management systems
Safety culture (& climate)
Migration, drift, normalisation of deviance & organisations at the limits
Risk & robust regulation regimes
Regulatory capture
Safety and risk as socially constructed</td><td>Procedures
Technical specifications
Technical risk assessments</td></tr>
<tr><td>Ergonomics, Human Factors and Cognitive Engineering, Naturalistic Decision Making</td><td>Training
Licensing
Team requirements</td></tr>
<tr><td>Work, Organisational Psychology and Social Psychology</td><td>Meta-rules
Risk management systems
Safety management systems</td></tr>
<tr><td>Sociology, Management, Law and Political Sciences</td><td>Safety culture
System monitoring
Risk governance</td></tr>
</table>

3. Sociotechnical system models

One major problem that stands out in establishing regulatory insights into industrial safety is the need to grasp analytically and practically the complexity of operations of high-risk systems across time, space, artefacts and social differentiation (e.g., expertise, hierarchies). Because of the complexity of this problem, graphical contributions play a major role in framing the issues involved in regulating safety and disasters. The importance of figures has been made clear in anthropology and the sociology of science, with for instance the work of Bruno Latour (1986) on the notion of inscriptions. Figures and models materialise and contribute to the intellectual independence of this specific topic because they simplify reality to make it accessible to both practitioners and researchers across disciplines.

In this spirit, psychologists, cognitive engineers and sociologists (Moray 1994; Rasmussen 1997; Evan and Manion 2002; Le Coze 2013a) have suggested some broad frameworks for describing accident risk and safety in sociotechnical systems. These different frameworks demonstrate that there are indeed many different ways of graphically suggesting what constitute sociotechnical safety. As such, they also have their strengths and weaknesses.

Rasmussen's (1997) model is probably one of the most established graphical frameworks in the field of safety. Without a doubt, the greatest influence that Rasmussen's work has had on safety science over the past thirty years lies in its ability to produce imaginative models based on appealing illustrations and a synthesis of different concepts from multiple disciplines in relation to empirical data (figure 2).

One of the most compelling characteristics of this model is certainly its ability to combine different levels together in relation to each other through feedback loops of information, scientific disciplines at different levels, and the dynamics of the environment (including the economy, technology, etc.). Meanwhile, Moray's (1994) version is represented through several layers instead of vertical levels, and it does not explicitly address communication between these layers (figure 3). Technology is at the centre of the figure, which gives the idea of an embedded technology that cannot be understood independently from society.

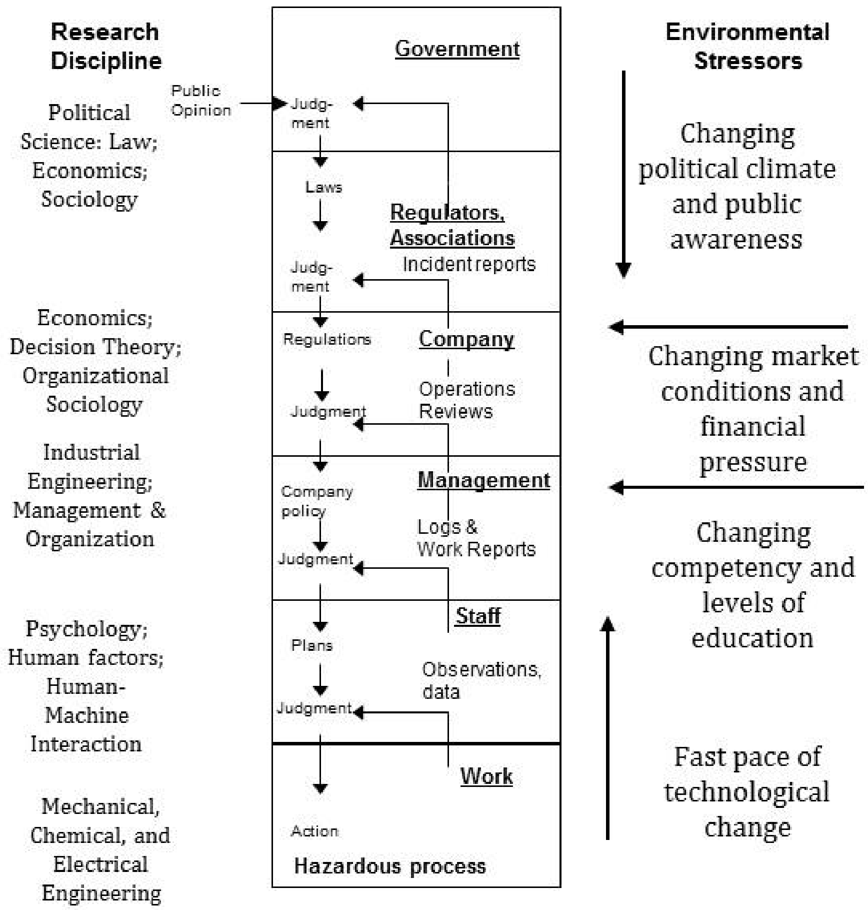

Figure 2. Rasmussen's (1997) sociotechnical model.

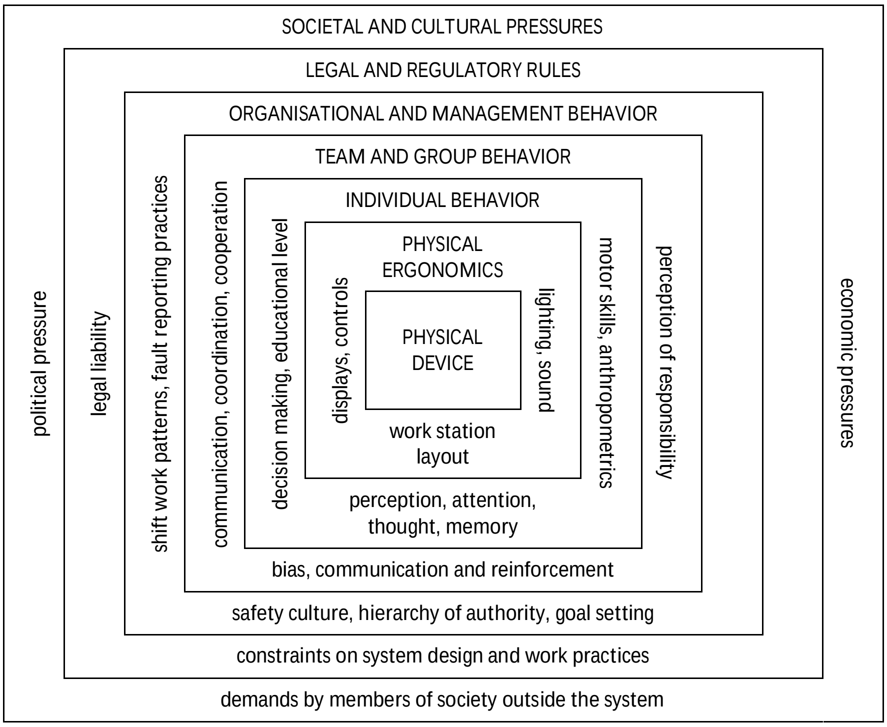

Figure 3. System-oriented approach to design and analysis (Moray 1994).

Evan and Manion (2002) distinguished four quadrants (reminiscent of Parsons' work) in a static manner, without implying the nested layers that Rasmussen and Moray do; instead, they put technological, human, organisational and social dimensions at the same level, avoiding the idea of a hierarchy between levels (figure 4).

	Internal Systemic Factors	External Systemic Factors
Technological Systems	Technical Design Factors	Human Factors Factors
Social Systems	Organizational system Factors	Socio-Cultural System Factors

Figure 4. Parsonian model of Evan and Manion (2002).

Hollnagel's (2004) representation of a joint cognitive system also has a layered approach, but on a horizontal axis, while Roberts (2012) uses circles (figures 5 and 6, respectively).

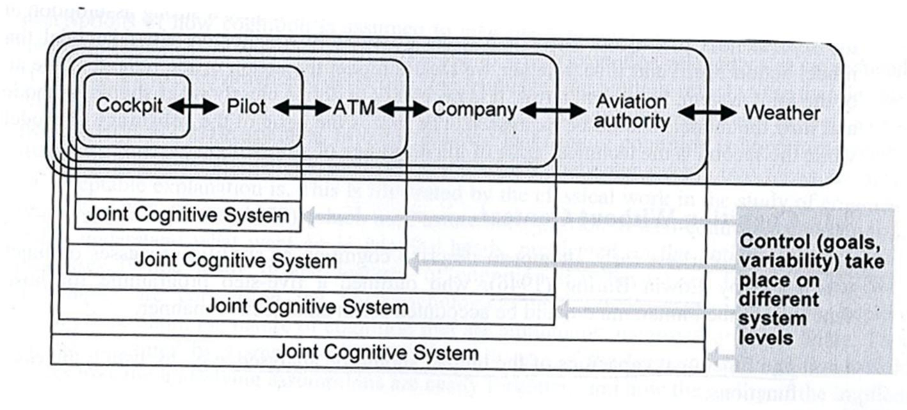

Figure 5. A horizontal view of a sociotechnical system (Hollnagel 2004).

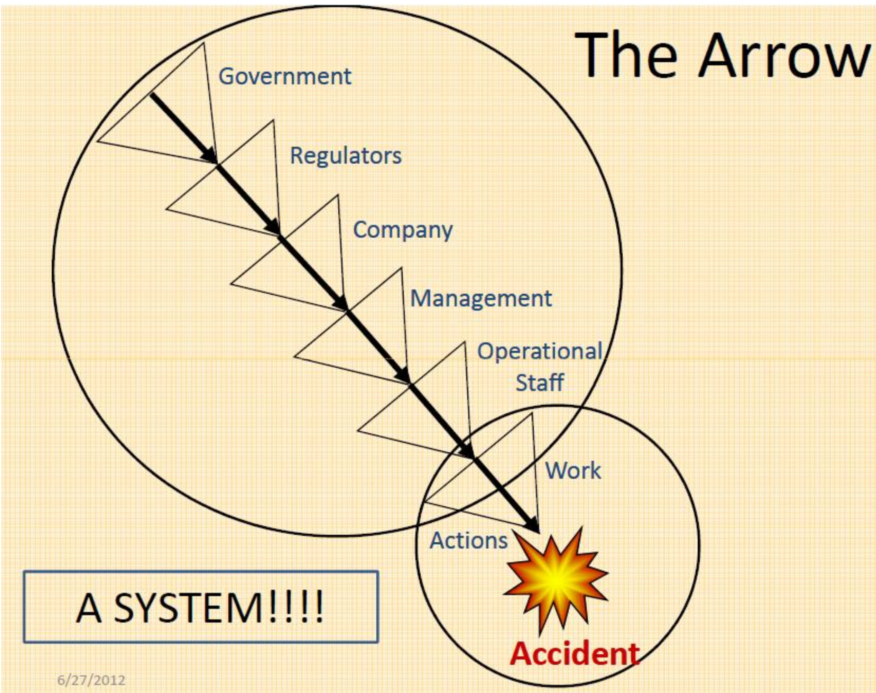

Figure 6. Roberts's view of sociotechnical system (2012).

Also related to accidents, we find the well-known version of defence in depth by James Reason (1997), which he moved from a technological and engineering orientation to a broader organisational orientation (figure 7). Another is Jens Rasmussen's (1997) concept of migration, extended from a cognitive focus to a much broader perspective (figure 8).

Reason's (1997) model is widely popular. It has had various versions throughout the years. Initially created at the end of the 1980s, it evolved throughout the 1990s (one version being named 'Swiss cheese'). The basic idea is that latent failures in management decision-making processes have downward consequences for daily work and create conditions that trigger what is coined as 'active failures'. These are the failures of measures designed to prevent accidents and are represented as holes in barriers (what was initially designated 'planes'). An accident is metaphorically represented by an arrow going through holes that, when aligned, generate an accident (figure 7).

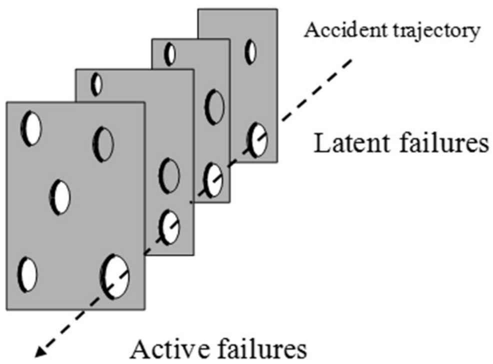

Figure 7. Defence in depth model (adapted from Reason 1997).

Rasmussen's (1997) model captures the notion that systems behave dynamically in what is metaphorically called an envelope. In this envelope, a balance between workload and economic efficiency drive the system within a space of several boundaries, including economic failure, unacceptable workload and what results in acceptable performance. Interactions of the diversity of actors, based on self-organised and adaptive properties, generate processes that are likely, at times, to go beyond this envelope, graphically represented by boundaries. When they do go beyond an acceptable performance, accidents can happen.

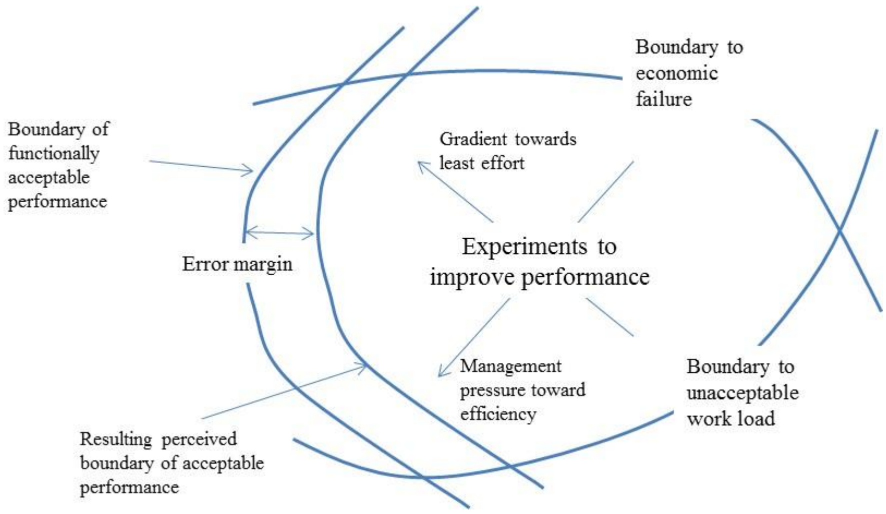

Figure 8. Migration model (adapted from Rasmussen 1997).

Le Coze's (2013a, 2013b) representation explicitly refers to several moves from Rasmussen's (1997) most influential sociotechnical representation (figure 2):

1. Dropping the top-down representation in favour of a polycentric or acentric view.
2. Showing the complexity of the self-organised—negative–positive feedback loops—nature of sociotechnical systems.
3. Socialising and materialising the figure by introducing individuals, technology (techno-science) and nature for interactions.
4. Representing the observers/scientists as part of the system.

The result of this provides a different feel to the complexity of sociotechnical systems (figure 9).

Of course, these figures are all representations and, as such, need to be understood in relation to their empirical and theoretical backgrounds, meaning one should be careful when removing them from their accompanying texts, as contextual factors, such as the discipline of the author, influences which system or view is advocated. This list of figures is not exhaustive. However, it demonstrates the many different ways of representing safety from a global, sociotechnical and complexity perspective.

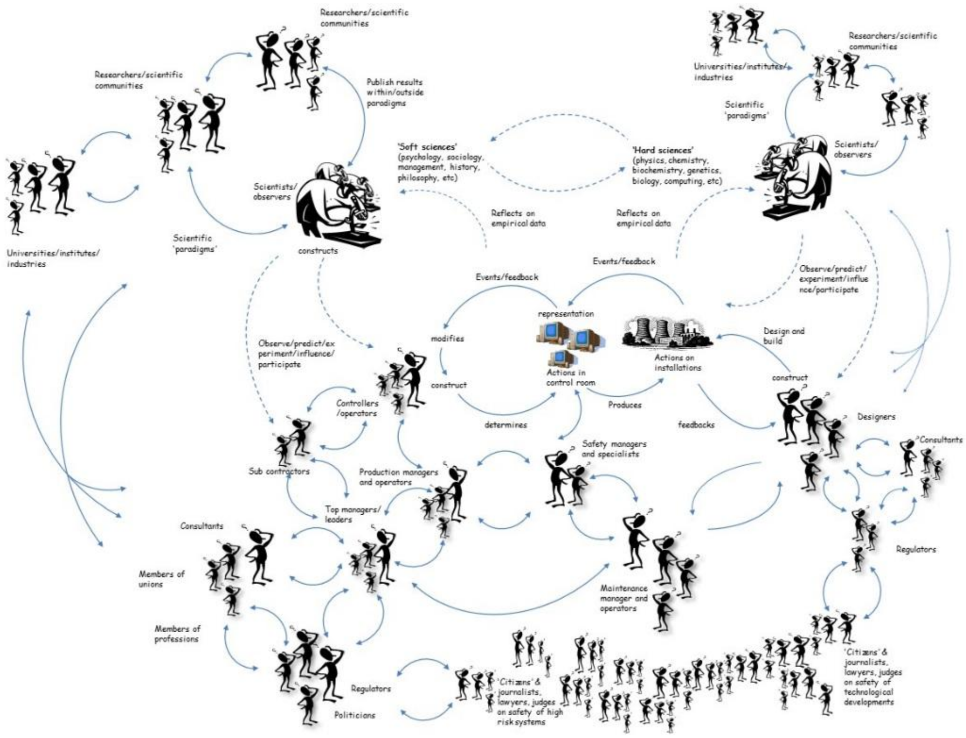

Figure 9. New sociotechnological view (Le Coze 2013a, 2013b).

4. A framework for sociotechnical system safety

4.1 Interwoven domains of knowledge

Sociotechnical system safety implies that safety is a dynamic property of systems and is determined in relation to context. From this perspective, safety is a continuous development. On the one side, it relies on a systems-structured processes and formalised situations, such as accident investigations, audits, inspections and meetings; on the other side, it is symbolic and related to a systems cultures, power relations, trust and human emotions. Consequently, several domains of knowledge interact in complex ways to provide regulators with an understanding of safety and accidents. From the concepts and figures in Sections 1–3, we can identify a knowledge framework consisting of technical and engineered systems, human factors in teams and organisations and management and control within their social and managerial as well as competitive, regulative and governance environments. The following points together capture a framework for knowledge in and about sociotechnical systems (Le Coze 2016c):

- The engineering and technological view corresponds to risk assessments performed to produce quantitative estimates of system performance limits and specifications. It also includes a qualitative analysis of what could possibly happen and estimates the likelihood of these events when taking into account the barriers designed to prevent or mitigate the consequences. Safety-economic studies can help justify choices.

- The human and organisational factor view tackles the problem of designing work situations and task completion, taking into account strengths and weaknesses of humans in specific material, informational and social contexts. Recommendations for display design and functionalities, recommendations for procedures, and team coordination and training are produced to buttress safe performance (in some sectors, behaviour-based safety approaches are included in this human factor perspective).

- The managerial and strategic view concerns the systems and processes delivering support to the management of safety in companies. These include meta-rules and systems for risk assessment, learning from experience, and the management of change—activities constituting the backbone of any systematic approach to safety and often described in regulations and international standards. These processes can be kept track of through indicators reflecting the state of the system and are conveyed by channels of communication producing flows of information throughout and between regulatory environments.

- Finally, high-risk industries are also strongly influenced by interactions with stakeholders (e.g., ministries, civil society). Regulatory strategies are strongly related to such issues, including risk communication, consultation strategies and approaches for system monitoring. This is the governance and political view, looking at the management of high-risk systems from the point of view of the interactions among the media, civil society, justice, regulation and the industry.

This framework for sociotechnical safety has important implications, such as when explaining why accidents keep on happening despite preventive strategies. First, there are limitations in our engineering knowledge of the sociotechnical artefacts that we create, especially when they reach a certain degree of complexity or innovation. As a result, the practice of risk assessment contains methodological limitations and challenges. Second, human cognition still defies our best human factor models. Consequently, predicting human adaptive behaviours across different contexts and increasingly complex technological environments remains a challenge and will be highly problematic for a long time.

Third, managerial decisions influencing safety involve ambiguous, uncertain and imperfect situations and resources, something well documented in the organisational literature. Therefore, a sociotechnical system approach goes against mechanistic and generalised views of organisations and safety management and challenges the idea that any principles can be applied perfectly and idealistically as organisations are messier than their official presentations. Finally, interactions among civil society, the media, justice, regulators and industry can both subvert well-established processes for stakeholder involvement and provide opportunities for managerial and regulatory reform. However, these interactions are not well documented in the literature. To the degree that they are studied and assessed, it is only as part of disaster investigations or special commission reports.

4.2 A systemic sensitising model of safety dynamics

Le Coze (2013a, 2013b) argued that new graphical models are needed considering what we now know about accidents. The graphical model in figure 10 represents a systemic sensitising model of safety dynamics, based on a pattern of six interwoven dimensions within sociotechnical systems:

(1) Strategy change and adaptations (by leaders) in the organisation's environment (economical, political, social and technological) lead to

(2) A number of technological and organisational changes at different levels, which may positively or negatively affect

(3) The new design and/or change of (technical and procedural) safety barriers by those at the operational level (in teams and departments), a situation monitored and controlled by

(4) First, an ability to process signals (possibly conveyed by whistle blowers) about specific safety-related problems or the negative impacts of developments to the new design or change of (technical and procedural) safety barriers, relying on

(5) Second, a safety department which can challenge the organisation about the impacts of changes to the design and implementation of safety barriers and/or to the status of processing of (weak or strong) signals. This department is backed up by

(6) Third, safety (external or internal) reviews which can play a role of organisational redundancy for the internal safety department (or service) on these very same issues.

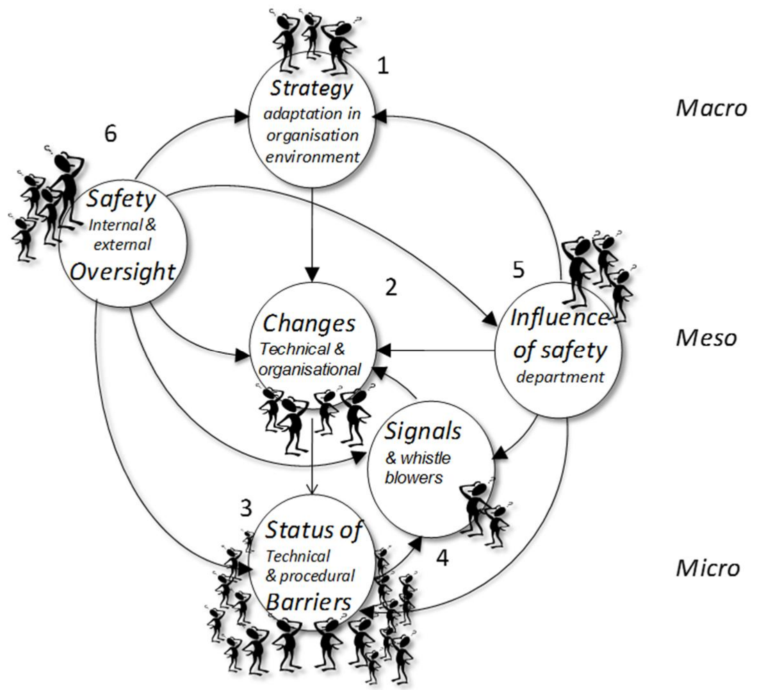

Figure 10. A systemic sensitising model of safety dynamics.

This model is obtained by combining a functional view derived from the safety management system research tradition focusing on structure (Hale 2003) with a grounded, ethnographic one focusing on context and organisational symbolism derived from the sociological tradition (Turner 1978; La Porte and Consolini 1991; Vaughan 1999, 2005). This graphical model has the performative value of naming issues to be systematically kept in mind for an auditor or inspector in order to capture the complex nature of sociotechnical systems in relation to specific safety issues (Le Coze 2013b).

Although such a picture of global structural prerequisites for changes in specific contexts is available in reports of investigations following a major event, these realities are rarely—at least explicitly—discussed beforehand. A sociotechnical system perspective on safety seems only to become meaningful in relation to disasters when the influence of company strategies are described retrospectively. Beyond the practice of audits, there is no equivalent proactive approach built into regulations for assessing safety dynamics in daily operations outside of extraordinary events. Developing such an approach should take inspiration from qualitative methods, among other the methodologies and practices of ethnographic study. It must rely on strong empirical knowledge that relates to the actual working conditions within the system. Therefore, observations of work in daily operations are important.

A proactive approach should also consist of possibilities for regulators openly discussing issues across a diversity of actors and companies involved in activities within the systems, from shop floor (sharp end) to the board of directors. These methods and practices are needed in order to capture the relationship between companies' strategy, organisation and technological transformations linked to the state of installations and practices of workers. At the same time, one must bear in mind the contextual nature of sociotechnical systems. Because of the human and historical nature of every individual system, situations are unique and require an in-depth acquaintance with modes of operation in order to grasp the uniqueness.

One proposition to move regulations towards a sociotechnical system perspective with the help of qualitative and sociological analysis was explicitly formulated by Hopkins (2007). Based on his experience with accident analysis (Hopkins 1999, 2000, 2005, 2008), he identified six strategies to go beyond compliance in order to encompass organisational features, which address many of the aspects of figure 10. The first strategy he proposed is auditing the auditors. The suggestion is to formulate questions to company managers so that they can only be answered with some thinking, not with 'a tick in the box' mentality. Instead of asking, "Is there evidence that hazards have been identified?" one could ask "Have all hazards been identified?" or, more realistically, "How good is the hazard identification methodology?"

The second regulatory strategy identified by Hopkins (2007) is proactive investigations. To wait for accidents to challenge the organisation is not good enough in high-risk systems, and opportunities to learn from small scale events through an investigation are worthwhile. Inspectors could play a role through the external oversight of small events by probing the reasons for their occurrence and challenging companies on safety matters.

The third strategy is supporting the company’s safety staff. Safety-critical organisations have specialised safety departments which act as compliance and safety management agents. Inspectors can support these actors by paying attention to their situation, their constraints and ability to perform their tasks adequately.

Advising on organisational design is a fourth strategy, particularly in terms of promoting the position of safety managers at the top of organisations in order to allow them to exert a certain degree of power over top decision-making processes.

The fifth strategy is exposing performance. By making public the results of companies in terms of safety, top managers are more likely to make efforts to reach expected safety results in order to avoid a bad reputation as a business.

The last strategy proposed by Hopkins (2007) is promoting regulatory crisis. By making public some small events which challenge companies’ practices, bad publicity can be enough to trigger changes in the management of safety. By exposing failures to public scrutiny, regulators can create favourable conditions for improvement in safety practices.

Overall, Hopkins’ propositions address many of the dimensions represented in figure 10, such as the influence of safety departments (supporting company safety staff, advising on organisational design), internal safety oversights (auditing the auditor), status of technical and procedural barriers in relation to change (exposing performance), and amplifying signals (promoting regulatory crisis).

5. Implications for regulation

This section of the white paper focuses on implications of a sociotechnical system perspective on safety for regulation, highlighting some major debates and open/current issues for discussion. A wide range of compliance monitoring tools already exists, as described and applied to regulating major accident risks in various industries. They are part of the safety regulations regardless of whether they are related to technical specifications, competence requirements or meta-rules associated with international management standards or industry best practices. However, as Hopkins (2007) argued, regulators should search for ways to move beyond compliance monitoring as well. In some situations, compliance monitoring can also develop into a ritual that blinds an industry from being aware of developing risks. Analysing the 2010 Gulf of Mexico blowout, Hopkins (2012) claimed that the US regulator at the time lost sight of the safety of the rig operations by focusing on regulatory compliance as an ultimate goal, substituting it for risk awareness within the industry.

5.1 How to grasp the reality of safety

With a bit of a critical bias and slight exaggeration, what regulators usually hear from companies before accidents is more often that they follow procedures, standards or processes defining their ability to produce safely, while in fact leaving aside a host of issues related to real-life situations of their organisations. What we learn afterwards is that procedures, standards or processes are not followed because there is more to high-risk systems than the often very simplistic descriptions of structures offered. Indeed, one clear foundation for the field of safety is that there is always more to practice than the application of procedures and standards or processes. This has become well established in the research on resilience engineering and more generally in human factors and ergonomics for many years—something also described in high-reliability organisations and safety culture research traditions (Pettersen and Schulman 2016; Le Coze, 2016d).

This is of course disturbing because it remains the most common way of approaching safety from an audit and inspection point of view: relying on compliance to procedure, standard or processes to assess situations. This raises the question about what is actually managed and regulated when one relies on the rhetoric of compliance as a guarantee for safety when this is far from the whole picture.

In this respect, it is also obvious that a gap exists between what we know after disasters occur, when investigation reports are produced, and what we know beforehand. Following an accident investigation, the amount of material available linking company strategies, organisational structures, the flow of information and operational practices leading to the events (figure 10) indicates a wide range of risk and safety issues that are not often addressed outside the possibilities offered by these specific events.

There are two reasons for this. First, the resources spent to find out what happened in the aftermath of a disaster consist of collecting a vast amount of data which would not otherwise be available in other contexts. In these exceptional circumstances, the state is empowered to proceed with in-depth investigations, relying on the expertise in a range of scientific disciplines (e.g., engineering, social sciences). Thus, there is a level of depth that is not usually available for a regulator when inspecting or supervising activities during daily operations. Second, it is much easier in retrospect to link a diversity of decisions of operators, engineers and/or managers into processes and view how they occur in relation to organisational structures and cultures combining specific incidents for the accident to happen the way it happened.

5.2 Are accidents normal?

The fact that post-accident situations reveal another side to companies compared to descriptions usually available beforehand in audits or oversights is a key topic in the field of safety and leads to two positions following disasters:

1. A company experiencing a disaster was so badly managed, not following procedures, standards or processes, that the accident was "waiting to happen". In this respect, following the procedures, standards or processes would have prevented the accident.
2. A company experiencing a disaster exceeded its safe envelope because individuals interacting in high-risk systems while dealing with uncertainties in a range of aspects of their operational realities produce evolving actions and associated symbolic expressions which cannot be predicted in detail. Following the procedures, standards or processes would not be a guarantee because reality exceeds them.

The first option maintains a traditional discourse about safety in association with compliance; the second one challenges this discourse and complements it with complex realities involving sociocognitive expertise of a wide range of individuals and groups, including (to put it simply) operators, engineers and managers. This is what Hopkins writes in the context of a shift in regulation from prescriptive to function-based (or management-based) principles: "In short, from this point of view, it is not possible to give a simple answer to the question of whether or not a duty holder is in compliance. The very concept of compliance has to some extent lost its meaning" (Hopkins 2007, p. 7). This second option acknowledges a sociotechnical view. It maintains the importance of procedures, standards and processes but argues for a better appreciation of context and what happens in real-life situations. Note that this does not mean that it is not impossible to have knowledge about any grounded judgement about what is considered an unsafe organisational situation. However, it requires probing realities beyond traditional approaches of inspections relying on compliance, as asserted by Hopkins (2007): "Under a prescriptive regime, the inspector might point to a regulatory violation as the reason for the notice, but in the absence of such a violation the inspector must fall back on subjective judgment of the level of risk" (p. 7).

One problem is indeed that these "beyond compliance" realities are often invisible to a formal and procedure-based approach to organisations. These realities are hidden behind the rational façades safety management systems can create. The discourse about the existence of a formal organisation pretends to reflect the activities behind the scenes. It is supported by auditing techniques which have been criticised precisely for their limitations for looking into complex realities (Power 1997). "Standardized elements, such as the auditable management system (…), represent the rationalizing tendencies of audit to reproduce ever more formal auditable structure, regardless of demonstrable effectiveness" (Power 1997, p. 123) and "images of control over pollution and derivatives (…) get manufactured by an audit process which necessarily insulates itself from organizational complexity in order to make things auditable and to produce certificate of comfort" (p. 140).

A critique of this situation in the context of self-regulation is elaborated by Gunningham and Sinclair (2009): "Only when the formal systems (audits, reporting, monitoring, etc.) are supported by informal (trust, commitment, engagement, means of overcoming conflicting loyalties, etc.) will they be fully effective" (p. 35). If companies are not rational in the sense that they do not neatly follow prescribed or formal paths (e.g., procedures, standard, processes) but have to rely on the expertise of individuals to fill the gaps (and informal world of practices) between expectations and real-life situations through adaptive strategies and virtuous interactions in a constant flow of changes, there are at least two questions for regulation:

- Does it mean that we are left with the impossibility of anticipating high-risk system behaviours and, thus, managing risks? Accidents are normal in Perrow's (1984) original and subsequently extended argument. There will always be surprises no matter what. But then, what is the implication for regulators?

- Does it mean that the conceptual lenses used to frame compliance in regulatory regimes (i.e., procedures, standards or processes) are inadequate for grasping the sociotechnical realities of the daily life of high-risk systems? If so, what is regulated? What else could be done?

The first point is addressed by political scientists who have argued that the state has a strategy to protect itself by exhibiting a voluntaristic approach to regulation despite its lack of resources to effectively control companies (Power 2007; Borraz 2011), something that Haines (2013) characterised as a paradox of regulations. The second aspect raises issues of hindsight bias or retrospective fallacy. Knowing the end of the story makes it much easier to analyse risk and safety afterwards than beforehand. In Norway, writing about the Gullfaks C incident in the continental shelf, Engen (2014) explained that it "revealed challenges within the new organisational structure of Statoil and sounded strong warnings to the top management about the increasing uncertainty of new technologies of well drilling as well as enhanced complexity of the internal organisational safety regime" (p. 360). This analysis exemplifies how we are much better at looking back than looking forward.

Hopkins (2007) also explored how regulation can promote and develop industries to become more risk aware based on his analysis of industrial disasters. As previously discussed, he suggested auditing the auditors, carrying out proactive investigations, supporting company safety staff, advising on organisational design, exposing performance and promoting regulatory crisis as six strategies for moving regulations beyond compliance and improving risk management in companies.

5.3 Sociotechnical systems and regulation beyond compliance

Complementing Hopkins, our sociotechnical system approach raises regulatory implications connected to the potential safety benefit of increasing proactive investigations as well as other regulatory strategies focusing on the strengthening of safety structures and risk-awareness processes within companies. This was previously discussed in relation to the reality of safety. In addition, our approach points to the importance of macro issues. Among other factors, the increasing pace of developments within information technology and automation as well as the extensive organisational changes within many industries following globalisation suggests the need to improve strategies for monitoring systemic trends and finding appropriate ways to regulate safety when systems become globalised. Drawing on the sociotechnical system view of safety as a dynamic and systemic outcome, we suggest that it may also be possible to improve industries' management of risks by encouraging regulatory strategies to (1) audit the regulatory systems, (2) support networks of safety and reliability professionals and (3) monitor precursor conditions in relation to change.

5.3.1 Auditing the regulatory system

As described earlier, what binds more recent high-profile events together (e.g., Fukushima Daïchi in 2011, Deepwater Horizon in 2010, Columbia in 2003) are the empirical transformations which have been taking place in the last twenty to thirty years. It turns out that, when describing these transformations between the 1980s and the 2000s, some key topics take centre stage—namely, globalisation and networks. Again, two questions can be derived from these evolutions for regulations:

- Are high-risk systems more complex due to the changes of operating conditions, consequently making it more likely to create surprises? Should it be considered from the regulatory side as a change in risk profile (as much as changing technology requires updated assessments)?
- What are the implications for regulators' inspections? Should they adapt their practices in order to cope with these evolutions? What sorts of adaptations would these be?

For instance, Quinlan, Hampson and Gregson (2013) established a relationship based on the investigation reports of the National Transportation Safety Bureau (NTSB) between outsourcing the maintenance of aircrafts and the genesis of serious accidents and crashes in the US. In many events during the past decade, problems of maintenance could be directly linked to subcontracting strategies and realities. These authors also provide a critical appraisal of the regulator's (i.e., Federal Aviation Authority [FAA]) oversights for not adapting more quickly to the changing risk profile of the industry. Despite warnings about the established links between these events and the new organisational configurations, regulators were slow to act. As a result, the evolution of organisations towards networks created new possibilities for weaknesses which translated into accidents.

Regulators should be asked questions such as how good their risk profiles of the industry are, whether vulnerabilities exist in the ways they inspect, how they train their inspectors, and how adequate their regulations are. These questions challenge regulators' ways of working, and some can lead to considerable change. If regulation and inspection practices are improved, it may also influence risk management within the industry as a whole.

5.3.2 Supporting networks of safety and reliability professionals

Research on high-reliability organisations (HRO) has identified individuals, generally as part of teams, with special perspectives on reliability, both cognitively and normatively. Termed "reliability professionals", they need not be holders of particular positions, have professional degrees or even any higher degrees at all (Roe and Schulman 2008; Pettersen and Schulman 2016). Reliability professionals often have a long experience with operations in their organisations, generally occupying a variety of jobs throughout their organisational careers.

Their view of systems is larger than those who may focus narrowly on single-case issues or events such as operators who firefight narrowly defined problems or higher-level managers who engage in management by exception. At the same time, reliability professionals see their systems in more concrete, real-time perspectives than those design engineers who conceive of systems abstractly through formal analytic models—a point made by Perin (2004), who contrasted the different logics in organisations running nuclear power plants. These professionals are extremely good at pattern recognition and at the formulation and remembering of action scenarios in relation to new operational problems they may confront (Roe and Schulman 2008; Pettersen 2013)—issues that also have been central in research on natural decision making (Klein 2009) and theories of resilience engineering (Hollnagel et al. 2006). However, reliability professionals rely on support from regulators, and we believe that an unrealised potential exists for regulators seeking out reliability professionals, usually networks of professionals, and taking account of their concerns at the industry level.

5.3.3 Monitoring precursor conditions in relation to change

Recent research on reliability drift in civil aviation has provided empirical descriptions of safety dynamics within the airlines and shown potential drivers that could undermine the effectiveness of adaptations in many organisations (Pettersen and Schulman 2016). Focusing on the dynamics of safety and concepts such as resilience could lead to the development of potential prospective indicators or signals that reveal the presence or loss of adaptive capacities in a variety of organisations relative to their previous capabilities. These indicators could in effect allow regulators to measure the protective capacity of an organisation before the fact is revealed in the actual failure of protective capacities. Such situations of reliability drift may be the result of company transformations and change, which for example entails the questioning of top leaders' strategic choices in competitive global markets as part of safety assessments (see figure 10). From research on HROs and resilience engineering, the potential signals of loss of protective capacity in organisations could be a decline in cross-organisational work planning and interdepartmental problem-solving, resulting in the creation of information silos and the loss of organisation-wide perspectives. In addition, a decline in experiential knowledge and system perspectives among operators and analysts may be signals warranting concern.

6. Concluding remarks

This exploration of sociotechnical system theory and safety indicates several areas of concern for regulators and provides conceptual, methodological, and practical implications. As a general remark, we conclude that regulators should explore the possibility of going beyond compliance to approach the realities of sociotechnical systems.

Conceptually, this involves moving safety regulation from ideas of top-down control, proceduralisation and compliance toward the establishment of links among companies' strategies, technological changes, organisational structure, the work of safety departments and oversight, including their own regulatory activities, in order for each specific industrial case to be understood as a whole (e.g., figure 10).

To support such developments, regulatory capabilities are required to gather and interpret data at several layers of functioning of high-risk systems. Depending on systems' characteristics, such monitoring methods will require resources for collecting and analysing data from a diversity of observations and interviews of a broad range of actors in practical, managerial and engineering positions, implying the need to investigate multiple organisations and probably often, considering current trends in operating constraints. Thus, it involves keeping track of changing the risk profiles of complex sociotechnical systems under evolving markets as well as technological and organisational transformations, particularly by using empirical investigation to build some ideas of how evolutions are taking place in order to anticipate their consequences within the industry.

However, to create such capacities, we believe a number of constraints and challenges require further research and development. These include regulations' contents in terms of human and organisational factors, inspectors' knowledge and backgrounds, method and data access, industries' reception to new types of oversight, legal issues and how to share responsibility between regulators and the industry and the status of inspectors if authorities become an “insider”.

Acknowledgements

The activity and interest of the Finnish Safety and Chemicals Agency (Tukes) in Finland, Petroleum Safety Authority Norway (PSA) and French Safety Authorities have made the STARS project possible. The SAF€RA network has had a significant role in the building of this project which has been funded by the Fondation pour une culture de sécurité industrielle (FonCSI), L'institute National de l'Environnement Industriel et des Risques (Ineris), Ministère chargé de l'écologigie (MEDDE), The Research Council of Norway, University of Stavanger, VTT Technical Research Centre of Finland Ltd and the Finnish Safety and Chemicals Agency (Tukes). The steering board consisting of renowned safety professionals Prof. Juhan Sanne (IVL Svenska Miljöinstitutet), Prof. Gudela Grote (ETH Zürich), and Todd La Porte (Berkeley University) has given us invaluable insight. We greatly thank them all.

References

Beck, U. 1986. Risk Society: Towards a New Modernity. London. Sage.

Bell, D. 1973. The Coming of Post-Industrial Society: A Venture in Social Forecasting. Basic Books.

Berger, S. 2005. How we compete. What companies around the world are doing to make it in today's global economy. Doubleday broadway.

Bergin, T. 2012. Spills and spin: The Inside Story of BP London. Random House Business.

Billings, G. 1996. Aviation automation. New York. CRC Press.

Borraz, O. 2011. Les politiques du risque. Paris. Presse de Sciences Po.

Castells, M. 2001. La société en réseaux. Nouvelle édition. L'ère de l'information, 1. Paris. Fayard.

Davis, M.C., Challenger, R., Jayewardene, D.N.W., & Clegg, C.W. 2014. Advancing socio-technical systems thinking: A call for bravery. Applied Ergonomics, 45, 171–180.

Dekker, S. 2011. Drift into failure. From hunting broken components to understanding complex systems. Ashgate.

Emery, F.E., & Trist, E. 1960. Socio-technical systems. In Management Sciences, Models and Techniques, vol. 2. London. Pergamon Press.

Engen, O.A. 2014. Near major accidents. A challenge for the regulator and the regulated. In Preben, H. l., Baram, M., & Renn, O. (Eds.) Risk governance of offshore oil and gas operations. New York. Cambridge University Press.

Evan, W.M., & Manion, M. 2002. Minding the machines: Preventing technological disasters. Upper Saddle River, NJ. Prentice Hall Professional.

Geels, F.W. 2002. Technological transitions as evolutionary reconfiguration processes: a multi-level perspective and a case-study. Research policy, 31(8), 1257–1274.

Gunningham, N., & Sinclair, D. 2009. Organizational Trust and the Limits of Management-Based Regulation. Law and Society Review, 43(4), 865–900.

Haines, F. 2013. Three Risks, One Solution? Exploring the Relationship between Risk and Regulation. The ANNALS of the American Academy of Political and Social Science, 649(1), 35–51.

Hale, A.R. 2003. Safety management in production. Human Factors and Ergonomics in Manufacturing & Service Industries, 13(3), 185–201.

Hollnagel, E. 2004. Automation and Human Work. In Sandom C., & Harvey, R.S. (Eds.) Human factors for engineers (pp. 113–150). London. The Institution of Electrical Engineers.

Hollnagel, E., Woods, D., & Leveson, N. 2006. Resilience Engineering. Concepts and Precepts. Ashgate.

Hopkins, A. 1999. Managing Major Hazards: The Lessons of the Moura Mine Disaster. Sydney. Allen & Unwin.

Hopkins, A. 2000. Lessons from Longford: The ESSO Gas Plant Explosion. Sydney. CCH Australia.

Hopkins, A. 2005. Safety, culture and risk. The organizational causes of accidents. Sydney. CCH Australia.

Hopkins, A. 2007. Beyond compliance monitoring: new strategies for safety regulators. Law & Policy, 29(2), 210–225.

Hopkins, A. 2008. Failure to learn: the BP Texas City refinery disaster. Sydney, NSW. CCH.

Hopkins, A. 2012. Disastrous Decisions: The Human and Organisational Causes of the Gulf of Mexico Blowout. Sydney, NSW. CCH.

Klein, G. 2009. Streetlights and shadows: searching for the keys to adaptive decision making. A Bradford book.

Klein, L. 2014. What do we actually mean by ‘sociotechnical’? On values, boundaries and the problems of language. Applied Ergonomics, 45, 137–145.

Lagadec, P. 1982. Major technological risk – an assessment of industrial disasters. London. Pergamon Press.

La Porte, T.R., & Consolini, P.M. 1991. Working in practice but not in theory: theoretical challenges of high-reliability organizations. Journal of Public Administration Res and Theory, 1(1), 19–47.

Latour, B. 1986. Visualization and cognition: thinking with eyes and hands. Knowledge and society: studies in the sociology of culture past and present, 6, 1–40.

Le Coze, JC. 2008. Complexity and learning from accidents. In Swedish Rescue Services Agency (ed) Learning from accidents. An anthology based on thoughts and ideas from young research fellows. Räddnings Verket. NCO 2008:5.

Le Coze, JC. 2005. Are organisations too complex to be integrated in technical risk assessments and current safety auditing? Safety Science, 43, 613–638.

Le Coze, J.C. 2013a. New models for new times. An anti dualist move. Safety Science, 59, 200–218.

Le Coze, J.C. 2013b. Outlines of a sensitising model for industrial safety assessment. Safety Science, 51, 187–201.

Le Coze, J.C. 2016a. Trente and d'accidents. Le nouveau visage des risques sociotechnologiques. Toulouse. Octarès.

Le Coze, J.C. 2016b. Risk management: sociotechnological risks and disasters. In Burgess, A., & Zin, O. (Eds.) Handbook of risk studies. London. Taylor and Francis.

Le Coze, J.C. 2016c. Managing the unexpected. In Moller, N., & Hanson, S. (Eds.) Handbook of safety principles. London. Routledge.

Le Coze, J.C. 2016d. Vive la diversité! High Reliability Organisation (HRO) and Resilience Engineering (RE). Safety Science. doi:10.1016/j.ssci.2016.04.006

Moray, N. 1994. Error reduction as a systems problem. In Bogner, M. (Ed.) Human error in medicine (pp. 67–91). Hillsdale, NJ. Lawrence Erlbaum Associates.

Oil Spill Comission. 2011. Deep Water. The Gulf Oil Disaster and the Future of Offshore Drilling. Report to the President. National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling.

Perin, C. 2004. Shouldering risks. The culture of control in the nuclear power industry. Princeton, NJ. Princeton University Press.

Perrow, C. 1984. Normal Accidents, living with high risk technologies. New York. Basic Books.

Pettersen, K. 2013 Acknowledging the Role of Abductive Thinking: A Way Out of Proceduralization for Safety Management and Oversight? In Bieder, C., & Bourrier, M. (Eds.) Trapping Safety into Rules. Farnham. Ashgate.

Pettersen, K., & Schulman, P. 2016. Drift, adaptation, resilience and reliability: Toward an empirical clarification. Safety Science. http://dx.doi.org/10.1016/j.ssci.2016.03.004

Power, M. 1997. The audit society. Rituals of verification. Oxford. Oxford University Press.

Power, M. 2007. Organized Uncertainty: Designing a World of Risk Management. Oxford University Press, Oxford, UK.

Quinlan, M., Hampson, I., & Gregson, S. 2013. Outsourcing and offshoring aircraft maintenance in the US: Implications for safety. Safety Science, 57, 283–292.

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

Rasmussen, J., & Batstone, R. 1989. Why do complex organizational systems fail? The world bank policy planning and research staff. Environment working paper N°20. Washington, DC. World Bank.

Reason, J. 1997. Managing the risks of organizational accidents. Routledge.

Roberts, K.H. 2012. The Deep Water Horizon disaster from a systemic and management of the unexpected perspective. Presented during the E & T on Systemic Approach to Safety and Human and Organizational Factors MANAGING THE UNEXPECTED. From the Perspective of the Interaction between Individuals, Technology and Organization Vienna, 25–27 June 2012.

Roe, E., & Schulman P. 2008. High Reliability Management – Operating on the Edge. Stanford, CA. Stanford University Press.

Smith, M.J., & Carayon-Sainfort, P. 1989. A balance theory of job design for stress reduction. International Journal Industrial Ergonomics, 4, 67–79.

Stephens, J.C., Wilson, E.J., & Peterson, T.R. 2015. Smart Grid (R) Evolution. Cambridge University Press.

Trist, E.L. 1981. The Evolution of Socio Technical Systems. Occasional Paper, 2, 1–67.

Trist, E.L., & Bamforth, K.W. 1951. Some social and psychological consequences of the longwall method of coal-getting: an examination of the psychological situation and defences of a work group in relation to the social structure and technological content of the work system. Human Relations, 4(1), 3–38.

Trist, E.L., Higgin, G.W., Murray, H., & Pollock, A.B. 1963. Organizational Choice. London. Tavistock.

Touraine, A. 1969. La société post-industrielle. Naissance d'une société. Paris. Denoël.

Turner, B.A. 1978. Man-Made Disasters. London. Wykeman.

Turner, B.A., & Pidgeon, N.F. 1997. Man-made disasters (Vol. 2). Oxford. Butterworth-Heinemann

Urry, J. 2005. The complexity turn. Special Issue of Theory Culture & Society, 22(1), 1–14.

van Eijnatten, F.M. 1997. Development in socio-technical systems design (STSD). In Drenth, P.J.D., Thierry, H., & de Wolff, C.J. (Eds.) Handbook of Work and Organizational Psychology. Organizational Psychology (vol. 4). Sussex, UK. Lawrence.

Vaughan, D. 1999. The dark side of organizations: mistake, misconduct and disaster. Annual Review of Sociology, 25, 271–305.

Vaughan, D. 2005. System Effects: On Slippery Slopes, Repeating Negative Patterns, and Learning from Mistakes? In Starbuck, H.W., & Farjoun, M. (Eds.) Organization at the Limit. Lessons from the Columbia disaster. Blackwell Publishing.

Wilson, J.R. 2000. Fundamentals of ergonomics in theory and practice. Applied Ergonomics, 31(6), 557–567.

Series title and number

VTT Technology 293

Title	**Sociotechnical systems theory and the regulation of safety in high-risk industries – White paper**
Author(s)	Jean-Christophe Le Coze, Kenneth Pettersen, Ole Andreas Engen, Claudia Morsut, Ruth Skotnes, Marja Ylönen, Jouko Heikkilä & Ivanne Merlele-Coze
Abstract	Aimed at policy makers, regulators, industry managers and other stakeholders, this white paper makes explicit some key issues for regulating safety and major accident risk within industries. Based on a sociotechnical system approach, we recommend that safety regulators shall be oriented towards operational variability and the optimisation of technical–human interactions in industrial systems, including a micro–macro scale for describing system influences on accident risks and safety outcomes. In the paper, we discuss how and why current regulatory approaches to safety lack focus on the dynamics of safety within industries and the relationships between safety outcomes and systemic factors, such as regulatory culture, labour relations and evolving modes of production. For example, globalisation processes are increasing in frequency and speed across industries, shaping new operational constraints on high-risk systems. New interconnected systems following the digitalisation of information and communication technology, the liberalisation of trade and finance, deregulation and privatisation agendas are other examples of supranational processes creating new environments for high-risk companies, responsible states and civil society. The implications for major accident risk following such wide-scoped transformations are not straightforward and have to be understood in relation to their industrial contexts. In order to address changes in society, accident models and regulatory practices have to be broadened and developed beyond today's focus of monitoring compliance. This paper gives an overview of how sociotechnical system ideas have developed in association with industrial safety and maps the conceptual foundations for current regulatory methods and practices. Sociotechnical system models are also described, demonstrating different ways of representing major accident risks and safety from sociotechnical system perspectives. Safety is explained as a dynamic property of systems determined in relation to industrial contexts. Safety is situational and a property in continuous development, on the one side relying on a systems structured processes and formalised situations such as accident investigations, audits, inspection and meetings while on the other side being symbolic and related to a systems culture, power relations, trust and human emotions. Consequently, several domains of knowledge interact, and we present a framework for knowledge about safety that includes 1) engineering and technology, 2) human and organisational factors, 3) strategy and management and 4) politics and governance. The implications of such a framework for proactive approaches to regulation are discussed in the paper, focusing on possible regulatory strategies for moving forward. Our approach raises regulatory implications that connect to the potential safety benefit of increasing proactive investigations as well as strategies focusing on the strengthening of safety structures and risk awareness processes within companies. In addition, we highlight the importance of systemic issues for regulation. Among other areas, the increasing pace of developments within information technology and automation as well as the extensive organisational changes within many industries following globalisation suggests the need to improve strategies for monitoring systemic trends and finding appropriate ways to regulate safety when systems become globalised. We suggest that it may also be possible to improve industries' management of major accident risks by encouraging strategies for 1) auditing the regulatory systems, 2) supporting networks of safety and reliability professionals and 3) monitoring precursor conditions in relation to change.
ISBN, ISSN, URN	ISBN 978-951-38-8523-6 (Soft back ed.) ISBN 978-951-38-8522-9 (URL: http://www.vttresearch.com/impact/publications) ISSN-L 2242-1211 ISSN 2242-1211 (Print) ISSN 2242-122X (Online) http://urn.fi/URN:ISBN:978-951-38-8522-9
Date	March 2017
Language	English, Finnish abstract
Pages	40 p.
Name of the project	Sociotechnical Safety Assessment within three risk regulation regimes
Commissioned by	
Keywords	sociotechnical, regulation, compliance, safety, high-risk industries
Publisher	VTT Technical Research Centre of Finland Ltd P.O. Box 1000, FI-02044 VTT, Finland, Tel. 020 722 111

Julkaisun sarja ja numero

VTT Technology 293

Nimeke	**Sosioteknisyyden haasteet turvallisuuskriittisen teollisuuden valvonnalle** White paper
Tekijä(t)	Jean-Christophe Le Coze, Kenneth Pettersen, Ole Andreas Engen, Claudia Morsut, Ruth Skotnes, Marja Ylönen, Jouko Heikkilä & Ivanne Merlele-Coze
Tiivistelmä	White paper tarkastelee sosioteknistä turvallisuuden arviointia historiallisista, teoreettisista ja turvallisuustutkimuksen lähtökohdista. Turvallisuuskriittisten organisaatioiden, kuten ilmailun, öljy- ja kaasuteollisuuden, kemianteollisuuden ja ydinvoimateollisuuden, onnettomuudet ovat seurausta useiden toisiinsa kytkeytyneiden systeemien – niin teknisten kuin sosiaalistenkin – keskinäisvuorovaikutuksesta. Onnettomuuksien sosiotekninen luonne edellyttää myös turvallisuuden näkemistä sosioteknisenä, jännitteisenä ja alati syntyvänä ominaisuutena. Raportissa todetaan, että sosioteknisyys on mukana onnettomuuksien hahmottamisessa, mutta sitä ei ole vielä riittävästi sisällytetty turvallisuuskriittisten organisaatioiden valvontaan. Perinteisesti teollisuuden valvonta on perustunut riskien analyysiin ja sääntöjen noudattamisen valvontaan. Sääntöjen noudattaminen ei kuitenkaan yksin riitä takaamaan turvallisuutta. Monimutkaisessa sosioteknisessä tilanteessa tarvittaisiin kykyä tarkastella turvallisuutta kokonaisvaltaisesti. Sosioteknisyyden huomioiminen valvonnassa edellyttäisi organisaation toimintaan vaikuttavan todellisuuden ymmärtämistä tarkkailemalla muutostekijöitä, kuten toimintojen ulkoistamisia ja niiden vaikutuksia turvallisuuden kannalta tärkeisiin toimintoihin. Muutostekijöihin lukeutuvat teknologiset, yhteiskunnalliset, taloudelliset ja poliittiset tekijät. Sosioteknistä ymmärrystä voivat edistää teollisuuden kokeneet, useammassa tehtävässä olleet asiantuntijat, joilla on laaja ymmärrys oman organisaationsa toiminnasta. Valvontajärjestelmän auditointiakin on ehdotettu keinoksi edistää sosioteknistä lähestymistapaa. Sosioteknisyyden sisällyttäminen valvontaan edellyttää paitsi osaamista, henkilö- ja taloudellisia resursseja myös valvojan ja valvottavan suhteen uudelleen pohdintaa. Raportti ei ole lopullinen vastaus sosioteknisyyden haasteeseen valvonnalle vaan paremminkin lähtökohta keskustelulle valvonnan sosioteknisyydestä.
ISBN, ISSN, URN	ISBN 978-951-38-8523-6 (nid.) ISBN 978-951-38-8522-9 (URL: http://www.vtt.fi/julkaisut) ISSN-L 2242-1211 ISSN 2242-1211 (Painettu) ISSN 2242-122X (Verkkojulkaisu) http://urn.fi/URN:ISBN:978-951-38-8522-9
Julkaisuaika	Maaliskuu 2017
Kieli	Englanti, suomenkielinen tiivistelmä
Sivumäärä	40 s.
Projektin nimi	Sosiotekninen turvallisuuden arviointi kolmessa riskienhallinnan regiimissä
Rahoittajat	
Avainsanat	Sosioteknisyys, valvonta, noudattaminen, turvallisuus, turvallisuuskriittinen teollisuus
Julkaisija	Teknologian tutkimuskeskus VTT Oy PL 1000, 02044 VTT, puh. 020 722 111