*Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference*
*Edited by* Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P4059-cd

# From organisational culture to communities of practice: Organisational culture and resilience in a context of co-emerging safety and security challenges

Torgeir Kolstø Haavik

*Studio Apertura, NTNU Samfunnsforskning, Norway. Email: torgeir.haavik@samforsk.no*

Tor Olav Grøtan

*Software Engineering, Safety and Security (SESS), SINTEF Digital, Norway. Email: tor.o.grotan@sintef.no*

Susanne Therese Hansen

*Studio Apertura, NTNU Samfunnsforskning, Norway. Email: susanne.hansen@samforsk.no*

Sissel Haugdal Jore

*Department of Safety, Economics and Planning, University of Stavanger, Norway. E-mail: sissel.h.jore@uis.no*

Ruth Østgaard Skotnes

*Department of Safety, Economics and Planning, University of Stavanger, Norway. E-mail: ruth.skotnes@uis.no*

**Abstract**
This paper reports from an early phase of a research effort engaging with organisations' response to emerging security threats in the oil and gas sector, combined with theoretical advances in cyber resilience. The ambition of the paper is to scrutinise the multi-dimensional appropriation of the term 'culture' to guide behavioural change and compliance with management expectations, rules, and procedures. In addition, we direct attention towards the mechanism of fostering professional culture in communities of practice. We argue that culture is not first and foremost a (pre-)condition for practice, but rather a pattern resulting from practice over time. This implies a 'practice approach' and a 'work-as-done approach' to organisational culture, that facilitates communication between scholarly literatures that rarely meet: the safety and security culture literature, and the resilience literature. The discussion will use cyber resilience as a case, as it is widely recognized across industries that the state-of-the-art cyber security approaches urgently need to be reinforced by resilience principles. There is a risk that the cultural condition may be "lost in translation" of auditability, so that the way we operationalise safety culture/security culture as a management concept implies a risk of running the errand of compliance rather than facilitating resilience. We argue for more focus on communities of practice in organisations to develop an understanding of contextual conditions, professional competence, and discretionary space in organisations. We also suggest how this focus can be inscribed into a further development of theories about resilience in a cyber-/hybrid threat context.

*Keywords*: Safety culture, Security culture, IT/OT culture, Communities of practice, Resilience

## 1. Introduction

Traditionally, industrial safety and cyber security have been distinct academic approaches as well as practices. The very bedrock for their cultural expressions is also different. Safety is founded on an awareness that own activities may inflict harm. In contrast, security is founded on the awareness that some adversaries may deliberately inflict harm. However, in today's interconnected world, safety and security are intrinsically interwoven; they must be seen as a nexus (Hansen & Antonsen, 2024). A telling example of this is the emergency shutdown systems on offshore oil and gas platforms; from once being offline, protected operational control systems, such systems can now increasingly be accessed remotely over the Internet, also by hostile actors. The modernization of critical infrastructures during the last decades has led to the incorporation of information and communication technologies (ICT) in industrial control systems. This has resulted in increased vulnerabilities and threats.

Broadly speaking, resilience thinking offers a reorientation, a focus on *inter alia* endurance, absorption, rebound and adaptive capacity in the face of both expected and unexpected events and conditions. This way, resilience thinking may be relevant for both safety and security individually. However, for our purpose, resilience as a concept is first and foremost interesting in the nexus between safety and security. Nevertheless, there is no readymade cultural concept available that addresses this, but there is an academic vein of safety culture. Despite the foundational difference between safety and security, safety culture has also to some extent, been used as blueprint for security culture. However, some key differences inevitably surface in the combination of information technology (IT) and operation technology (OT) (see 3.2.1). Finally, the literature that combines perspectives on resilience and culture is very scarce. As our endeavour aims at cultural foundations to straddle the nexus by means of resilience, we must however establish the cultural heritage from safety as a starting point.

The introduction of the concept of safety culture to the practice field and to academic circles – and with that the very 'invention' of the concept – is traceable to the aftermath of the Chernobyl catastrophe in 1986, when the International Atomic Energy Agency (IAEA) stated in its investigation report that the (root) cause of the accident was 'poor safety culture' (Antonsen, 2009).

Today one may find culture as a central concept to achieve safe and reliable operations and services through the whole value chain in companies that operate safety-critical processes and critical infrastructures. Specific technical domains within organisations have also been subject to cultural governance, such as when differences between IT work and OT work in the industrial cyber domain are addressed in terms of IT culture and OT culture. But the proliferation of cultural references in the field of safety does not stop there. As the focus on security has increased significantly during the later years, both in safety-critical industries and within scholarship, many of the key parameters of safety have been adapted to contexts of security. This is also the case with culture. Hence, references to security culture can be found at all levels and domains where we are already used to talk about safety culture.

In this paper, we want to deepen the understanding of how safety and security relate to culture. Based on document and interview studies, we discuss challenges that arise when concepts of culture meet organisational realities of safety and security work. The objective of the paper is to discuss how organisational cultures, including safety culture and security culture, can inform the development of cyber resilience in organisations in the aftermath of organisational stress and shock.

## 2. Culture and practice in organisations

### 2.1 *The development of organisational cultures*

Anthropology has inspired different approaches to studies of culture in organisations. Traditionally, anthropology seeks to describe generic cultures in societies – their norms, semantic systems, values, artefacts, etc. – based on thorough studies of practice. One of the most influential theorists on organisational culture is Edgar Schein, who has proposed an approach to organisational culture that builds on the anthropological definition of culture. Considering organisations exist in a larger society – a parent culture – they will bear traits from this society: *"Organizations exist in a parent culture, and much of what we find in them is derivative from the assumptions of the parent culture" (Schein, 1983, p. 17)*. However, organisations develop their own distinct cultures through encounters with internal processes and the external environment.

With reference to what shapes organisational culture, Schein distinguishes between young (newly established) organisations, and older ones. For young organisations, he states that "*leadership is the fundamental process by which organizational cultures are formed and changed*" (Schein, 1983). He underscores, however, that organisations develop over time, and that the influence of leadership diminishes with time.

### 2.2 *Particular aspects of culture in organisations*

Safety culture is defined in many ways, but most refer to the notion of shared basic assumptions, and a shared understanding of reality (Antonsen, 2009). The abundant references in the field of safety science to safety culture, and in later years also to security culture, implies an attempt to

decompose and reverse the cultural logic of traditional anthropology. The decomposition of organizational culture into the narrower aspects of safety and security, respectively, and then approaching and using these cultural aspects as targets for organisational change, is a tempting management approach to behaviour-based safety and security (McSween, 2003).

Concentrating on a particular facet of organisational culture that is deeply imbued with values, normative in nature, yet also subject to debate—namely, safety—elicits intriguing theoretical and practical inquiries about the factors that shape culture, the impact of culture on various elements, and the role of culture in deliberately changing organisations. In later years, the interest in safety culture has been parallelled with an emerging focus on security culture. The concept of security culture largely builds upon the principles of safety culture, with numerous organizations striving to establish a cohesive safety and security culture that incorporates both safety and security aspects (Jore, 2020).

Although the actors in the petroleum industry are individual actors, they are also part of a larger organisational or industrial field, whose extra-organisational governance can be characterised by specific political features. For our undertaking, also the concept of political culture is relevant in several ways. For instance, national features such as the Norwegian tripartite collaboration are connected to political culture (Rosness et al., 2013). Further, as international organizations such as NATO and the EU develop policy blueprints targeted at societal security (and within this mix, industrial resilience, safety and security of critical systems), the work of the oil and gas sector may be influenced by differentiated institutional cultures (NATO, EU) as well as the political cultures of other countries.

The safety literature often distinguishes between a functionalist and an interpretative approach to culture (Reiman & Rollenhagen, 2014; Reason, 1997). The functionalist approach views culture as something an organisation "has" and emphasizes that organisations' management has the power to change culture through the introduction of new measures and practices. The interpretative approach, on the other hand, views culture as something an organisation "is" (Reason, 1997) and sees culture as the meanings and beliefs that the members of an organisation assign to organisational elements (structures, systems, and tools) and how these assigned meanings influence behaviour (Reiman and Rollenhagen, 2014).

#### *2.2.1 IT culture and OT culture*

A subcategory of the distinction between security culture and safety culture is the distinction between IT culture and OT culture. OT practitioners are mainly concerned with human safety, equipment damage, and continuous supply of essential services, and IT practitioners are concerned with cyber security and damage to data, lost revenue, customer trust, and reputation. However, with the evolution of cyber-physical systems the requirement for (cyber) security can no longer be separated from safety (Skotnes & Gould, 2025; Pettersen & Grøtan, 2024).

Nevertheless, Ylönen et al. (2022) found that cyber security in high-risk process industries using industrial control systems were often handled in a separate IT-department, and the communication with the process-safety (OT) department and the environment, health, safety, and security department was often inadequate. Experts from these different departments sometimes used similar terms that had different connotations in their respective fields, or different terms and definitions that the others did not understand.

Several studies have found cultural differences between IT and OT, such as varying degrees of professionalism, and the claim that OT engineers have a safety culture and IT practitioners an innovation culture (Guldenmund, 2000). Different logics of risk assessment feature between safety and security engineers. In legacy OT systems, safety risk has traditionally been understood probabilistically as a "failure rate". On the other hand, (cyber) security incidents in the OT space are a function of anticipating malicious behaviour and relying on sparce historical data.

### 2.3 *Where culture is cultivated: communities of practice and work-as-done*

Practice theories and workplace studies (Dreyfus & Dreyfus, 1980; Lave & Wenger, 1991) which can be seen as part of the larger shift towards practice that characterized the organizational

discipline in the 1990s (Brown & Duguid, 2000; Suchman, 1987) have had very limited influence on safety culture literature (but see e.g. Gherardi, 2018). Practice theories emphasize the social dimensions of learning, such as professional networks and social interaction, and by that elaborate on the local arenas for identity and culture development.

Lave and Wenger developed the theoretical concept 'communities of practice' (CoP) related to learning. In Wenger's words, *"Communities of practice are formed by people who engage in a process of collective learning in a shared domain of human endeavor: (...) In a nutshell: Communities of practice are groups of people who share a concern or a passion for something they do and learn how to do it better as they interact regularly."* (Wenger, 2011, p. 1)

Gherardi has 'translated' and introduced the ideas of communities of practice to the field of organization and safety, also linking it to safety culture. In an elegant manner, Gherardi manages to capture in only one sentence the relation between safety, the community safety is practiced within, and the culture it is embedded in: *"Safety is an emergent competence which is realized in practice, which is socially constructed, innovated and transmitted to new members of the community of practices, and which is embedded in values, norms and social institutions."* (Gherardi, 2018, p. 12)

Besides defining safety in terms of emerging competencies and their cultural embeddedness, Gherardi also associates safety and safety culture with communities of practice, hence, delimited professional networks in the organisations. A focus on practice associates the CoP perspective with resilience perspectives; the resilience literature offers a framework for describing strategies, methods, and heuristics, and indeed, recent contributions have explicitly made the coupling between communities of practice and resilience (Delgado, de Groot, et al., 2021). The efficiency-thoroughness trade-off (ETTO) principle is one such strategy. It is well documented in the resilience literature how ETTO exerts a significant influence on the relation between work-as-imagined/work-as-done. Also, ETTO practices that are shared among participants in communities of practice can help us understand the gap between *culture-as-imagined* and *culture-as-done*. This is a reminder of how organisational culture programs initiated by management may often be disconnected from the underlying factors that drive the development of organisational culture within the workforce.

## 3 Method

This paper draws on findings from two conceptually related research projects. While the paper is mainly conceptual, we draw on insights from review of governing documentation from three case companies from the international oil and gas sector. We also draw on insights from early interviews. The ideas presented in the paper are not directly induced or scaffolded by this data, but we use excerpts from this material for the purpose of illustration. The perspectives developed is an integral part of the ongoing analysis of aspects relating to safety and security culture in a sector experiencing both stronger integration of safety and security challenges, and a new geopolitical situation expanding the threat menu facing industry. Hence, methods and analytical work in the paper is also a part of the ongoing sensemaking process in the projects, that will inform future empirical project work – including extensive interviewing about cultural references, communities of practice and adaptive strategies for resilience.

## 4 Limits to culture

### 4.1 *Organising safety and security work*

The case companies have organised their security work in different functional or thematic areas. All companies address physical security, cyber/digital/information security and personnel security under security management. Different departments or groups are responsible for different security areas. Safety work in the companies is also organised in different departments or groups. Some companies include the areas safety, major accidents and personal injuries (SMP) and health and working environment (HVE), while others use terms such as health, safety, and environment (HSE), emergency preparedness, and emergency response (ER), health, safety, security, and environment (HSSE) management, health, safety, security, environment, and quality (HSSEQ) management, technical safety, barrier management, and external environment.

Several of the companies have organized both safety and security work under one executive vice president. The reasoning behind this is to ensure an aligned cross-company approach. However, in some of our interviews, employees responsible for security work talk about a holistic approach, coordination and cooperation between the different security groups, but not between the different safety and security groups. Others talk about common meeting arenas between the leaders of groups responsible safety and security. Our impression from the preliminary interviews, however, is that the companies mostly focus on cooperation within the safety management area and the security management area, respectively, rather than holistically across the two domains.

Furthermore, we found differing views on culture within the companies. During interviews with managers and employees in one of the companies, representatives from the cyber security department/group agreed that there were clear differences in cultures between professionals working with IT and professionals working with OT. However, a security manager in the same company did not perceive any differences in culture and mindsets between IT and OT professionals.

### *4.2 Top-down culture development*

A central functional requirement for one of the case companies states that a proactive safety culture shall be based on a number of expectations to the employees. These expectations target how the workforces relate to safety and risk: that the employees understand and manage risk; that they look after their colleagues; that they openly report and learn from all incidents; and that they are visible and engaged in their team's safety and security. Such expectations are articulated in other governing documents as requirements for compliance. *Values* are an important aspect of culture according to most definitions, and the connection between culture and values is underscored by the companies by stating that the safety culture shall incorporate very specific company values (e.g., *being courageous*).

These ways of thinking about and shaping culture rest on ideas of culture being *engineered*, and leaders are identified as responsible for establishing the desired culture. Further, the desired 'culture of compliance' shall ensure that procedures are not deviated from.

### *4.3 Can there be one holistic safety and security culture?*

The notion of culture is in the companies' governing documentation treated in a largely generic manner. Culture is addressed in a holistic manner, to permeate the organisation from top to bottom, and through all the different organisational departments and lines. Examples of this include statements defining how a proactive safety and security culture *shall* be, and that it is the top-level leadership's responsibility to establish the desired culture.

This view finds resonance in some parts of the safety and security culture literature, particularly that which supports a functionalistic view on organisational culture. There is, however, a more dominating literature where ambiguity, differentiation and fragmentation describe the existence of subcultures (Antonsen, 2009). We find significant resonance to this literature in the inner life of the case organisations, where safety culture work and security culture work are largely separated activities.

### *4.4 Safety/security culture and communities of practice*

In parallel with the 'cultural expectations' and the ambitions of many organisations to develop a compliant safety culture, the case organisations also acknowledge insights that challenge the eligibility of a uniform, engineered safety and security culture. For example, it is our interpretation that one of the organisations explicitly encourages a variety of perspectives. This gives connotations to the complexity and variety that resilience theory wants us to embrace, with reference to the requisite imagination to manage variability in operative contexts (Adamski & Westrum, 2003). From a resilience perspective, thus, a culture of strict compliance has clear limitations for managing variability and the unforeseen.

HOP (human and organisational performance) (Conklin, 2019) has become a popular reference for safety and security in the industry the recent years. In the pseudo-scientific literature on HOP, insights from safety culture research, resilience, and high reliability organisations (HRO) have been operationalised into a set of core principles for safety. HOP

underscores that compliance is a strategy only in predictable environments. In complex organisations, operating in complex environments, however, variability is the rule, and procedures will always be underspecified. In those environments, one must adjust: "*Compliance is paramount when we can anticipate events. [Safety as] capacity becomes paramount for the unforeseen*" (The Federation of Norwegian Industries, 2023, p. 9).

HOP borrows inspiration from the resilience literature, where one of the central safety and security resources acknowledged is adaptability. A characteristic of adaptive practices is tacit and situated knowledge. That means that this type of knowledge resists formalisation and documentation but lends itself more readily to the shared knowledge reservoir of professional *communities of practice*.

In contrast to a functionalistic premise for organisational safety and security culture programs, cultural frames of reference in the 'practice tradition' are much more subtle, and available first and foremost through social interaction, through engaging with others in ongoing practices (Gherardi & Nicolini, 2002). Lave and Wenger describe communities of practice as *"... a set of relations among persons, activity and world, over time and in relation with other tangential and overlapping communities of practice. A community of practice is an intrinsic condition for the existence of knowledge (...)"* (Lave & Wenger, 1991, p. 98)

By interacting with more experienced colleagues within the community of practice, individuals acquire knowledge that extends beyond what is available through formal descriptions and procedures (Hollnagel, 2015). It is through this interaction that one gains an understanding of the cultural practices that evolve over time as a result of the work. Tricks of the trade, efficiency-thoroughness trade-offs, adaptations, articulation work – all that makes it possible to get the work done safely, securely and effectively. The pattern emerging from these conditions and these practices is indeed a cultural pattern: *"What we call 'safety' is the result of a set of practices shaped by a system of symbols and meanings which orient action, but which consist of something more.*" (Gherardi, 2018)

This way of talking about safety culture differs conceptually from the programmatic and normative view on safety culture that dominates in many organisations. Instead of a culture-oriented approach determining what a desired culture would look like, and trying to alter the workforces accordingly, a practice-oriented approach asks "what are the conditions for work and which strategies, heuristics, and trade-offs do the professionals apply to cope with these conditions and produce the desired results"? Paraphrasing the well-known distinction between work-as-imagined and work-as-done from the resilience literature, one can say that the former approach highlights culture-as-imagined, while the latter engages with culture-as-done.

### 4.5 *A resilience perspective on safety and security culture: closing the gap between culture-as-imagined and culture-as-done?*

'How people work' is an intriguing question. Not only is it a well-kept secret in many instances (Suchman, 1997), but the possible form and level of detail of the answer to this question depends a lot on the frame of reference. If the frame of reference is one of an 'ideal' or 'imagined' safety and security culture or if it is the culture according to Schein's (1983, pp 10-11) definition, makes a significant difference. While safety and security culture often connote to normative descriptions of organisational practices, with reference to value standards such as "*a sound safety culture*" (The Petroleum Safety Authority Norway) or "*just culture*" (Dekker, 2016), the way culture is treated in the tradition of workplace studies is far more pragmatic when it comes to acknowledging the nature of work as it is carried out in often unique settings, by 'competent practitioners'. To the degree that this represents a gap between culture-as-imagined and culture-as-done, there is a need to shrink this gap both in practice and in theory.

### *4.6 The (Cyber) Resilience ABC model*

As digital systems become more complex, the concept of 'resilience' is gaining prominence. It is commonly understood as the inherent necessity to facilitate a managed recovery and resurgence from incidents that surpass the capabilities of risk management. This understanding is predicated on the assumption that preparedness, which is designed for foreseeable events based on the current comprehension of system operations, will

also prove beneficial in the face of unforeseen occurrences.

The Resilience Engineering (RE) approach challenges these presumptions and advocates a different approach, rooted in complexity theory. Complexity implies that fundamental surprise is inherent, thus common basic assumptions of order, rational choice and intent in organizational decision-support and strategy are challenged (Kurtz & Snowden, 2003). RE aims to *engineer* an *adaptive capacity* that precludes organizations from becoming stuck and stale when encountering complexity and deviations from normal operations. Arguably, by embracing change and being poised to adapt, organizations will avoid becoming "robust, yet fragile", and enable what Woods (2018) denotes "graceful extensibility"; a system's ability and capacity to stretch beyond set and perceived boundaries.

Recognizing that different resilience perspectives may be useful on their own terms, Grøtan, Antonsen and Haavik (2022) propose the "Resilience ABC"; comprising three different theories along two dimensions: resilient outcome and attribution of its origin. In Theory A and B, resilience as outcome (e.g., rebound, robustness) is considered something one *has*, corresponding to a functionalist perspective of culture. In Theory C, commensurate with RE principles, resilience (adaptive capacity) is considered something one *does*, a distinct process and practice to achieve and maintain adaptive capacity in the system. This may be paraphrased in an interpretive (CoP) cultural perspective as something the organization *is*, and that requires continuous *cultivation* to persist and sustain.

While Theory A is limited to technical instrumentality, we can argue that Theory B, encompassing an HTO instrumentality, resonates with the tendency to stretch cultural references "upwards" to international and political culture. On the other side, Theory C is supportive of stretching the cultural references "downwards", envisaging different cultural conditions for adaptive capacity in the IT/OT domains. That OT engineers have a safety culture while IT practitioners have an innovation culture, can be interpreted as an OT cultural preference for Theory B, and an IT preference for Theory C. However, Gherardi's (2018) description of safety as "an emergent competence" is so to say straight from the RE textbook, and thus more attached to Theory C. This also supports the more intuitive position that Theory C is the most adequate perspective for this paper's interest in organizational shocks due to new geopolitical situation and the new threat landscapes.

In our empirical material we find both that there are cultural IT/OT differences, and the opposite view. Adding to this apparent "cultural fog", we observe that safety culture is expected to be holistic and incorporate company values of being "courageous" (Theory C), while at the same time observing the expectation that organization culture shall be engineered through management and compliance culture (Theory B). This apparent confusion is however accompanied by acknowledgements of the shortcoming of a uniform, engineered safety and security culture. Hence, we sense an atmosphere of doubt and appetite for more insight and openness for composite approaches. An example of this is the HOP recognition of the limits of compliance, and that in relation to the unforeseen, "*safety is a capacity*". From a Theory C perspective, we just might add "*adaptive*". These observations are commensurate with the findings of Pettersen and Grøtan (2024): while both perspectives are needed, Theory C must be implemented "in the context of Theory B". Such a combination also needs to engage with "culture-as-done".

## 5. Conclusion

There is a need to facilitate arenas where communities of practice can thrive and their members can exchange experiences, where novices can learn about situated adaptation and the aptitude and limitations of rules and procedures from experts in realistic contexts. The safety and security culture approach would also gain from orienting more towards these culture shaping arenas and practices, and literatures of those, which allow for far thicker anthropological insights into organisational cultures than studies of management-initiated culture statements and campaigns.

## 6 Acknowledgements

This research is funded by the Research Council of Norway, Grant No. 303489 and 344332.

## References


Adamski, A., & Westrum, R. (2003). Requisite imagination. The fine art of anticipating what might go wrong. Handbook of cognitive task design, 193-220.

Antonsen, S. (2009). Safety culture: theory, method and improvement. CRC Press.

Conklin, T. (2019). The 5 principles of human performance: Independently Published.

Dekker, S. (2016). Just culture: Balancing safety and accountability. CRC Press.

Delgado, J., de Groot, J., McCaffrey, G., Dimitropoulos, G., Sitter, K. C., & Austin, W. (2021). Communities of practice: acknowledging vulnerability to improve resilience in healthcare teams. Journal of Medical Ethics, 47(7), 488-493.

Gherardi, S. (2018). A practice-based approach to safety as an emergent competence. Beyond safety training: Embedding safety in professional skills, 11-21.

Gherardi, S., & Nicolini, D. (2002). Learning the trade: A culture of safety in practice. Organization, 9(2), 191-223.

Grøtan, T. O., Antonsen, S., & Haavik, T. K. (2022). Cyber resilience: a pre-understanding for an abductive research agenda. In Resilience in a Digital Age: Global Challenges in Organisations and Society (pp. 205-229): Springer.

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

Hansen, S. T., & Antonsen, S. (2024) Taking connectedness seriously. A research agenda for holistic safety and security risk governance. *Safety Science*, Vol. 173.

Hollnagel, E. (2015). Why is Work-as-Imagined different from Work-as-Done? In R. L. Wears, E. Hollnagel, & J. Braithwaite (Eds.), Resilient Health Care, Volume 2: The Resilience of Everyday Clinical Work. Ashgate.

Jaatun, M.G., Albrechtsen, E., Line, M.B., Tøndel, I.A. & Longva, O.H. (2009). A Framework for Incident Response Management in the Petroleum Industry, International Journal of Critical Infrastructure Protection, Vol. 2, No. 1, 26-37.

Johnsen, S.O. (2012). Resilience at interfaces. Information Management & Computer Security, 20(2), 71-87.

Jore, S. H. (2020). Security and Safety Culture—Dual or Distinct Phenomena? The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice, 43-51.

Kurtz, C. F., & Snowden, D. J. (2003). The new dynamics of strategy: Sense-making in a complex and complicated world. *IBM systems journal, 42*(3), 462-483.

Lave, J., & Wenger, E. (1991). Situated learning: legitimate peripheral participation. Cambridge University Press.

McSween, T. E. (2003). Values-based safety process: Improving your safety culture with behavior-based safety. John Wiley & Sons.

Pettersen, S., & Grøtan, T. O. (2024). Exploring the grounds for cyber resilience in the hyper-connected oil and gas industry. Safety Science.

Reason, J. (1997), Managing the Risks of Organizational Accidents, Ashgate Publishing Limited, Aldershot.

Reiman, T. & Rollenhagen, C. (2014). Does the concept of safety culture help or hinder systems thinking in safety? Accident Analysis and Prevention (68), 5-15.

Rosness, R., Forseth, U., Lindøe, P., Baram, M., & Renn, O. (2013). Tripartite Collaboration as an Integral Part of a Regulatory Regime. Risk Governance of Offshore Oil and Gas Operations, New York, 309.

Schein, E. H. (1983). Organizational culture: A dynamic model.

Suchman, L. (1987). Plans and Situated Actions: The Problem of Human-Machine Communication. In: Cambridge University Press.

Skotnes, R. Ø. & Gould, K. P. (2025). Addressing cyber-physical challenges for critical infrastructures in smart cities through integrating organizational processes for safety and security management, in B. M. Sageidet, D. Müller-Eie & K. Lindland (2025), A Nordic Smart Sustainable City: Lessons From Theory and Practice. Routledge.

Skotnes, R. Ø, Holte K. A., and Kines, P. (2018), Translation of a safety culture training program from one industry context to another, in Bernatik, et al. (Eds.), Prevention of Accidents at Work, Taylor and Francis Group, London, pp. 179-185

The Fed of Norwegian Indust. (2023). Safety, leadership and learning -A practical guide to HOP.

The Petroleum Safety Authority Norway. HSE and culture.

Wenger, E. (2011). Communities of practice: A brief introduction.

Woods, D. D. (2018). The theory of graceful extensibility: basic rules that govern adaptive systems. Environment Systems and Decisions, 38(4), 433-457.

Wolf, M & Serpanos, D. (2018). Safety and security in cyber-physical systems and internet of things systems. Proceedings of the IEEE, Vol. 106.

Ylönen, M., Tugnoli, A., Oliva, G., Heikkilä, J., Nissilä, M., Iaiani, M., Cozzani, V., Setola, R., Assenza, G., vd Beek, D., Steijn, W., Gotcheva, N. & Del Prete, E. (2022). Integrated managm of safety and security in Seveso sites - sociotechnical perspectives. Safety Science (151), 1-14.