Hindawi
Complexity
Volume 2019, Article ID 2089763, 13 pages
https://doi.org/10.1155/2019/2089763

Review Article

Emerging Risk Management in Industry 4.0: An Approach to Improve Organizational and Human Performance in the Complex Systems

F. Brocal,[1,2] **C. González**,[3] **D. Komljenovic**,[4] **P. F. Katina**,[5] **and Miguel A. Sebastián**[3]

[1] *Department of Physics, Systems Engineering and Signal Theory, Escuela Politécnica Superior, Universidad de Alicante, Campus de Sant Vicent del Raspeig s/n, 03690, Sant Vicent del Raspeig, Alicante, Spain*
[2] *University Institute of Physics Applied to Sciences and Technologies, Universidad de Alicante, Alicante, Spain*
[3] *Manufacturing and Construction Engineering Department, ETS de Ingenieros Industriales, Universidad Nacional de Educación a Distancia, Calle Juan del Rosal, 12, 28040 Madrid, Spain*
[4] *Institut de Recherche d'Hydro-Québec (IREQ), 1800, boul. Lionel-Boulet, Varennes, Canada J3X 1S1*
[5] *Department of Informatics and Engineering Systems, University of South Carolina Upstate, 800 University Way, Media 211, Spartanburg, SC 29303, USA*

Correspondence should be addressed to F. Brocal; francisco.brocal@ua.es

Received 5 March 2019; Accepted 20 May 2019; Published 19 June 2019

Guest Editor: Jorge Luis García-Alcaraz

Industry 4.0 in the contemporary operating context carries important sources of complexity. This context generates both traditional risks and emerging risks that must be managed. The management of these risks includes both industrial risks and occupational risks, since they are heavily interlinked. The human factor can be considered the main link between both types of risks. Thus, understanding risks originating from human errors and organizational weaknesses as causes of accidents and other disruptions in complex systems requires elaborating sophisticated modeling approaches. Therefore, the objective of this paper is to propose an organizational and human performance approach to improve the emerging risk management linked to the complex systems, like as Human-Machine Interactions (HMI) and Human-Robot Interaction (HRI). To fulfill this objective, we first introduce the concept of emerging risk linked to human factor. Then, we introduce the concept of emerging risk management in the Industry 4.0 context. Under this complex context, we expose the concept considering the current models of risk management. Finally, we discuss how enhancing human and organizational performance can be achieved through risk management in complex systems linked to Industry 4.0. Therefore, we conclude that while Industry 4.0 brings numerous advantages, it must contend with emerging risks and challenges associated with organizational and human factors. These emerging risks include industrial risks as well as occupational risks. Moreover, the human factor aspect of Industry 4.0 is directly linked to industrial emerging and occupational emerging via context of operations. To cope with these new challenges, it is necessary to develop new approaches. One of such approaches is Complex System Governance. This approach is discussed along with the need for adequate organizational and human performance models dealing with, for example, experience from other domains such as nuclear, space, aviation, and petrochemical.

1. Introduction

The concept "Industry 4.0" has its origin in a "strategic initiative" of the German government in 2011 [1]. In its simplest form, this concept is a name given to the current trend of automation and data exchange in manufacturing technologies. Industry 4.0 encompasses elements of cyber-physical systems (CPS), Internet of Things (IoT), cloud computing, and cognitive computing [2]. Industry 4.0 and its synonyms, such as Smart Manufacturing, Smart Production, Internet of Things, or the 4th Industrial Revolution [3], have been identified as major contributors in the context of digital and automated manufacturing environment [4]. Kagermann et al. [1] note that such concepts are linked to smart manufacturing systems configured with digital networking of production. In addition, the concept “advanced manufacturing” is related to a greater interval of industrial modernization. The scientific interest around these terms is clearly increasing during the last years [5].

In contrast to conventional forecast based production planning, Industry 4.0 enables real-time planning of production plans as well as dynamic self-optimisation [6]. The productive model based on Industry 4.0, in addition to improving processes in terms of efficiency and quality, can help improve safety as well as sustainability and the industry image [7]. However, industrial processes configured for advanced manufacturing processes and technologies can increase levels of complexity of production processes and introduce high dynamism into processes creating the so-called smart working environments [8, 9]. Taking the context of critical infrastructures as a reference, Zio [10] suggests that the industrial processes under the Industry 4.0 paradigm can be considered complex, made up of many components interacting in a network structure. These components can be physical and cyber-physical, functioning heterogeneously, organized in a hierarchy of subsystems, and contributing to system as a whole.

However, there is scarcity of literature discussing issue of complexity in the context of Industry 4.0. Table 1 is developed to support this thesis. The first scientific publications emerged in 2012. Thereafter, there has been increased interest in the concept of Industry 4.0.

In relation to enterprise production and operation, Industry 4.0 has four objectives [11]: environmental sustainability, safety, agility, and high efficiency. It has been suggested that Industry 4.0 environment will lead to a new revolution in the domains of safety management practices with “out of the box” thinking [4]. However, this suggests that the management of those organizations brings new challenges given significant uncertainties associated with increasing complexity [12].

Suffice to say that traditional industry has its own problems. When these problems are coupled with emerging paradigm of Industry 4.0 along with emerging complex, there emerges a need for development of rigorous and sophisticated approaches for risk management (i.e., traditional and emerging risk management). Roig and Brocal [13] suggest management of emerging risks through combination of different approaches to provide more enlightened decision-making.

Interestingly, despite an increase in number of scientific publications on the subject of “Industry 4.0” (Table 1) the number of publications addressing “risk” and “Industry 4.0” is very low. Table 2 highlights this concern with the following search in “Web of Science” (search standards used in Tables 1–3; the results are null for the following queries: TS=(“Industry 4.0” and “risk management”); TS=(“Industry 4.0” “emerging risk”)).

The management of these emerging risks includes both industrial risks and occupational risks, since they are heavily linked [14]. The human factor can be considered the main link between both types of risks. In such cases, concepts of Human-Machine Interactions (HMI), Human-Computer Interaction (HCI), and Human-Robot Interaction (HRI) can be considered among the most important [4, 7, 15]. In an equivalent way to the results shown in Table 2, the number of scientific publications that integrate the concepts Industry 4.0, safety, and occupational safety is still very scarce, as shown in Table 3. In this way, Badri et al. [8] indicate that published research on the integration of occupational health and safety (OH&S) in the Industry 4.0 context is rarely cited.

Table 1: Number of scientific publications on complexity and Industry 4.0 (Results from the Web of Science. Timespan: 2010-2018; All databases; Field tag: Topic).

Year	Complexity	Industry 4.0	Industry 4.0 and complexity
2018	70810	1555	69
2017	73548	1136	63
2016	82644	561	48
2015	67325	191	9
2014	59552	69	4
2013	55519	23	3
2012	51013	4	0
2011	48151	0	0
2010	46884	0	0

Thus, understanding risks originating from human errors and organizational weaknesses as causes of accidents and other disruptions in complex systems requires elaborating sophisticated modeling approaches. Therefore, the objective of the present research is to define an approach for organizational and human performance that can be used to improve the emerging risk management linked to the complex systems under paradigm of Industry 4.0. To obtain this objective, the rest of this paper is organized as follows:

(i) Section 2 introduces the concept of emerging risk linked to human factor in Industry 4.0 context.

(ii) Section 3 introduces the concept of emerging risk management in the Industry 4.0 context. Under this complex context, authors expose the concept considering the current models of risk management.

(iii) Section 4 is organized to provide ways to improve organizational performance with the goal of improving safety in the complex systems linked to Industry 4.0

2. Emerging Risks

The definitions and risk models used in the professional and scientific fields are numerous. In this regard, Aven [16] has made a classification of definitions on risk most commonly used. Said author considers that the definitions collected in Table 4 are the most relevant. Aven [16] argues that the definition or model (3) is the most appropriate.

From a standardized perspective, ISO 31000:2018 standard indicates that a risk is usually expressed in terms of risk sources, potential events, their consequences, and their likelihood [20]. In OH&S field, the ISO 45001:2018 standard defines an OH&S risk (the terms “OH&S risk” and

Table 2: Number of scientific publications on risk and emerging risk in the Industry 4.0 (Results from the Web of Science. Timespan: 2010-2018; All databases; Field tag: Topic).

Year	Risk	Risk management	Industry 4.0 and risk	Emerging risk	Management and emerging risk
2018	335.842	7155	66	84	19
2017	324.537	8226	55	88	21
2016	310.952	7762	27	90	17
2015	289.990	7210	7	71	19
2014	265.015	6461	1	81	20
2013	247.840	6173	0	74	17
2012	224.108	5884	0	66	16
2011	207.076	6050	0	62	14
2010	193.041	6092	0	79	11

Table 3: Number of scientific publications on safety and occupational safety in the Industry 4.0 (Results from the Web of Science. Timespan: 2010-2018; All databases; Field tag: Topic).

Year	Safety	Industry and safety	Industry 4.0 and safety	Occupational safety	Industry 4.0 and occupational safety
2018	291.426	13.270	81	1940	7
2017	262.601	14.352	58	2248	7
2016	246.359	11.658	23	1858	1
2015	228.041	11.239	7	1536	1
2014	216.289	10.651	3	1606	0
2013	182.296	10.390	1	1596	0
2012	154.996	9.189	0	1690	0
2011	124.767	8.616	0	1343	0
2010	109.836	7.259	0	1229	0

“occupational risks” are used as equivalent in this paper) as the combination of the likelihood of occurrence of a work-related hazardous event or exposure (s) and the severity of injury and ill health that can be caused by the event or exposure(s) [21]. These definitions are among the models on risk collected in Table 4, highlighting the adaptation of model (2) to the definition of occupational risk.

The application of these definitions and models needs adaptations and new approaches when dealing with emerging risks, which are discussed in the following sections.

2.1. Emerging Risk Concept. Generally, when the term “emerging risk” is mentioned, this term refers to any risk that is new and/or increasing. However, other perspectives do exist. For example, the International Risk Governance Council [22, 23] suggests that emerging risk should be viewed from a “systemic” perspective. A systemic perspective of risk includes both (i) emerging and (ii) new conditions. First, the risk is emerging when it is new in a broad sense, as, for example, in the case of new technologies, new materials, etc. Second, the risk is emerging when being familiar or traditional; it is presented under new or unfamiliar conditions (e.g., the reemergence of the poliovirus). In both cases, uncertainty is the main characteristic of emerging risk [24]. From this perspective, the emerging risk adapts especially well to model (4) (R=U). However, the IRGC [24] notes that this uncertainty is related to the probabilities and/or consequences of the emerging risk. In this way, model (2) would also be applicable.

Brocal et al. [17] have proposed a theoretical framework through which the new and emerging risk (NER) concept has been modeled, especially in industrial processes. The risk model used as a reference is the following: a risk (R) is a structure consisting of five components: the source of risk (SR), causes (C), events (E), consequences (CO), and the likelihood (L); this set may be expressed as (8):

(8) R = (SR, C, E, CO, L)

From this framework, Brocal et al. [25] have developed TICHNER (Technique to Identify and Characterize NERs) technique that aims to identify and characterize the NERs generated by a manufacturing system. TICHNER is based in the definition of NER considered in the reports published by EU-OSHA [26–29]. This definition has been codified by Brocal et al. [17] through the so-called conditions that define an NER (C1, C2, C3, C4, C5, and C6), which are collected in Table 5.

Given that a NER is any risk that is new and/or increasing, Brocal et al. [17] consider that a risk is new (NR, new risk) when it can be associated with conditions C1, C2, and C3. Considering model (8), condition C1 is linked to new SR and new C. The novel aspect can be both technological and organizational. C2 and C3 are linked to new SR, C, E, and CO. In this case, the novel aspect of C2 is associated with changes in social perceptions and the novel aspect of condition C3 to new scientific knowledge about risk. These authors consider that a risk is increasing (IR, increasing risk) when it can be associated with conditions C4, C5, and C6. Condition

Table 4: Main models on risk used in the professional and scientific fields (adapted from [16]).

Model		Description
(1)	R=E	Risk=Expected value (loss)
(2)	R=P&C	Risk=Probability and scenarios/Consequences/severity of consequences
(3)	R=C&U	Risk=Consequences/damage/severity of these + Uncertainty
(4)	R=U	Risk=Uncertainty
(5)	R=OU	Risk=Objective Uncertainty
(6)	R=C	Risk=Event or consequence
(7)	R=ISO	Risk=Event or consequence

Table 5: Possible combinations between the Ci conditions and the risk components (model (8)) that can form a NER: NR and/or IR (adapted from [17]).

	Conditions	Risk Components (model 8)				
		Source of Risk (SR)	Causes (C)	Events (E)	Consequences (CO)	Likelihood (L)
NEW	C1: New technological or organizational variable	(SR,C1)	(C,C1)	—	—	—
	C2: New social perception	(SR,C2)	(C,C2)	(E,C2)	(CO,C2)	—
	C3: New scientific knowledge	(SR,C3)	(C,C3)	(E,C3)	(CO,C3)	—
INCREASING	C4: Increase in the number of sources of risk	(SR,C4)	—	—	—	—
	C5: Increase in the likelihood of exposure	—	—	—	—	(L,C5)
	C6: Increase health consequences	—	—	—	(CO,C6)	—

C4 is linked to the increase of SR, C5 to the increase of L (exposure level and/or the number of people exposed), and C6 to the increase of CO (seriousness of health effects and/or the number of people affected).

Considering the above aspects, Table 5 shows the different possible combinations between the Ci conditions and the risk components that can form an NER (NR and/or IR). Thus, depending on the combination in each case of interest, that is, the characterization of emerging risk according to Brocal et al. [25], the risk could be analyzed with one of the models in Table 4.

The terms "new and emerging risks (NERs)" and "emerging risks" are used as equivalent in this paper. However, some significant differences can be found in the technical and scientific literature. These differences, according to Brocal [30] and Cantonnet et al. [31], point at a clear problem of consensus on terminology and interpretation around emerging risk. The works of Brocal et al. [17, 25] propose approaches and models to reduce the associated uncertainty.

It would be desirable that the terminology regarding these risks (i.e., "new and emerging risks," "emerging risks") is standardized. In this case, the CWA 16649: 2013 document may prove to be the first step. Currently, International Organization for Standardization (ISO) is developing the ISO 31050 standard—Guidance for managing emerging risks to enhance resilience [32].

2.2. Emerging Risks Linked to Human Factor. The effects of Industry 4.0 on OH&S generate advantages and drawbacks that could generate emerging risks [8]. These emerging risks include both industrial risks and occupational risks, since they are heavily related [14]. Arguably, human factor is the main link between industrial emerging risks and occupational emerging risks in advanced manufacturing processes. This may as well be the case, given the complexity of operational and the shifting business environment that continues to overwhelm human cognitive capacities [8, 33–37].

Consequently, one often tries to use mental and intellectual "shortcuts" in finding "easy" explanations or solutions taking into account directly visible parts of the whole context only. The complexity of modern systems generates the opacity where some significant risks become systemic and may be well hidden and lurking beneath until conditions reunite for their full display. One of direct consequences of those changes is the nature of the risks which continue to occur. While undesirable events such as industrial accidents, process and supply chain disruptions, or bankruptcies formerly occurred from known causes and factors, contemporary events usually originate from unanticipated interactions between elements with no visible links [12, 38–40]. In tightly connected complex systems and their environment, it creates conditions for cascading events throughout them [10, 38, 41–49] due to increased interdependencies [50, 51]. Several authors argue that analyzing the performance of complex systems should also imply a careful examination of low level events as well as organizational factors such as safety culture and the incentive system, which shape human performance and affect the risk of errors [37, 39, 52–56].

2.3. Emerging Risks Linked to Complex Systems. The technological evolution, including the introduction of the concept of Industry 4.0, and the contemporary operating context significantly contribute to increasing complexity [12]. Some authors categorize it as a "structural complexity" issued from the heterogeneity of system components across different technological domains. It is a result of increased integration of various technological systems. There is also the “dynamic complexity” which is revealed by an emergent (usually unanticipated) system behavior as a reaction to local perturbations and stimuli in its environment [10]. For example, the integration of modern technologies and new control rules (Industry 4.0) creates additional opacity in systems.

In this regard, concepts such as Human-Machine Interactions (HMI) and Human-Robot Interaction (HRI) can be considered among the most important [4, 7, 15]. HMI and HRI can be considered sources of risk (SR). From this perspective, Brocal et al. [25] have applied the TICHNER in order to identify and characterize emerging risks linked to HMI and HRI. These risks are heavily linked to conditions C1, C4, and C5. In this regard, tasks that involve human control of automated equipment are increasing [57], including the expansion of HRI [58]. With the increase and development of the cobots, these emerging risks are evolving towards scenarios with greater uncertainty, due to (i) the greater flexibility and mobility of the cobots as well as their greater interaction with the workers [8, 57] and (ii) the challenge of increasing the sophistication of the tasks carried out by this type of robots [58].

The increase of this intelligent equipment can lead to connecting the causes of human error with the “smart machine error” [8]. Likewise, the increase in the number of degrees of freedom of the robots also increases their complexity, increasing the risk of entrapment and the difficulty for humans to predict their movements [15]. As the manufacturing tasks become more individualized and more flexible, the machines in smart factory are required to do variable tasks collaboratively without reprogramming [59]. The reliability of such devices is more difficult to predict as the complexity of these systems increases [8].

Brocal et al. [5] have classified the above emerging risks into two groups, in light of their consequences (CO): accidents risks and psychosocial and musculoskeletal risks. The accidents risks in automated environments are closely linked by human errors [60]. Among other causes, it highlights human monitoring and control of processes through control systems, instead of direct control [61], which can lead to a reduction of the practical knowledge of the process [62] and therefore result in over-reliance on automated safety systems [60]. In relation to psychosocial risks and musculoskeletal risks, they can be studied independently or jointly, since they are interrelated, especially in automated contexts. In these contexts, considering the work of Flaspöler et al. [60], the main interrelated causes (C) are low physical activity; static postures; high mental workload, for example, during the monitoring and control of the processes indicated by Chidambaram [61]; reduced privacy at work (mainly because new technologies allow closer and more intrusive supervision); and increase of problems in decision-making.

3. Emerging Risk Management

The increase in organizational complexity in manufacturing processes is changing from centralized decision-making towards decentralized instances. In decentralized instances, decision-making can be taken by workers or by equipment where artificial intelligence is integrated [57]. This increase in the complexity of Industry 4.0 affects the OH&S especially in terms of work content, management, and other organizational factors [8].

Based on the work of Brocal et al. [5], risk management systems in the context of Industry 4.0 can be classified into four hierarchically interrelated types: risk governance, risk management, OH&S management system, and emerging risk management. The main models, according to this classification, are discussed in the following section below.

3.1. Risk Management Models. From a global level, IRGC [63] proposes a framework for risk governance. This framework provides a guide for the design and application of comprehensive assessment and management strategies to deal with these risks. SRA [64] defines risk governance as the application of governance principles to the identification, assessment, management, and communication of risk. Thus, the process of risk management may be considered integrated into the overall process of risk governance.

In relation to risk management, ISO 31000:2018 standard provides guidelines and a common approach to managing any type of risk. This standard defines risk management as coordinated activities to direct and control an organization with regard to risk. SRA [64] defines risk management as those activities to handle risk such as prevention, mitigation, adaptation, or sharing.

In OH&S field, the ISO 45001:2018 standard defines management system as a set or interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives; and OH&S management system is a management system or part of a management system used to achieve the OH&S policy.

3.2. Emerging Risk Management Models. IRGC [65] addresses emerging risks linked to technology and industrial processes. The methodological aspects for early identification and management of emerging risks are described by the IRGC Guidelines for Emerging Risk Governance [24]. These methodological aspects are flexible and adaptable, especially in complex and uncertain contexts [24].

The IRGC [24] has reviewed emerging risk governance frameworks, and it has selected five:

(i) ENISA: European Union Agency for Network and Information Security

(ii) EFSA: European Food Safety Authority

(iii) Swiss Re SONAR system

(iv) Dutch framework (emerging risks related to the use of chemicals)

(v) CEN workshop agreement (CWA) 16649:2013 (emerging risks related to technology)

CWA 16649:2013 proposes the Emerging Risk Management Framework (ERMF). The whole process is based on the concept that emerging risks go through a maturation process [24]. This ERMF is based on the risk management frameworks defined by IRGC [63] and ISO 31000: 2009. Currently, International Organization for Standardization (ISO) is developing the ISO 31050 standard—Guidance for managing emerging risks to enhance resilience [32]. This new standard has taken CWA 16649: 2013 as one of its references [66].

4. Ways to Improve Organizational Performance to Improve Safety in the Complex Systems

As discussed above, the introduction of the concept of Industry 4.0 brings numerous advantages, but also some new issues. It includes, among other things, emerging risks related to rising complexity of technological systems. One has limited knowledge upon them due to lack of long-term observation data. This situation is fairly challenging for management, organizations, and individual workers as a whole.

This section presents a discussion on how to enhance human and organizational performance aiming at improving risk management in complex systems linked to Industry 4.0.

4.1. Challenges Related to Organizational and Human Performance. Komljenovic et al. [12] provide a comprehensive review of research works regarding organizational and human performance in analysis of industrial accidents where complexities, systemic risks as well as organizational and human performance, are seriously involved.

A constant deviation toward danger or failure seems to be one of their key characteristics. The latter is practically impossible to grasp in traditional of chain-of-event analyses.

All this requires overcoming the traditional static approach to risk, through the development of dynamic risk management models oriented towards the organizational and human performance, which is strongly linked to the complex systems characteristic of Industry 4.0.

4.1.1. Dynamic Management. Industry 4.0 provides digital management of operations in new technological devices, improves working conditions, and generates a safe manufacturing environment for workers [4, 8]. In this way, this technological development allows the integration of advanced safety systems. Among them, the use of Virtual Reality (VR) stands out to create a risk-free virtual learning and training environment, applications for the use with mobile devices or wearable computing, and the use of RFID technology [7]. Among the main applications of RFID technology is the Workforce Management and the Enhancing Safety, which allows, for example, real-time control of access to dangerous areas, as well as emergencies [67].

In the work environment of Industry 4.0, a wide range of examples of smart materials, smart personal protective equipment, and other advances technological applications is improving the OSH [9]. Such context production workers provide immediate feedback of production conditions via real-time data through their own smart phones and tablets [6]. In this context, the safety management is one of the most important issues [7], where Podgorski et al. [9] have proposed a framework based on new dynamic risk management paradigm. In this way, one of the challenges of Industry 4.0 is the difficulty of managing dynamic risk, as well as the availability and presence of experts in OSH [8].

Thus, during the last few years, new approaches and methodologies have been developed for risk assessment and management considering the dynamic evolution of risk [68]. The main objective of the dynamic risk assessment is to provide an estimate of the risk over time that reflects the current condition of the system, considering for it the integration of the effective aggregation of heterogeneous information [69].

4.1.2. Organizational Performance. It seems that the understanding of events is changing given that one of the main sources of risks (SR) nowadays is the organization [12]. Majority of undesirable events (E) has essentially organizational components. One considers "organizational" factors that understand a collective behavior (e.g., centralization and decentralization and organizational clarity). These characteristics come from the evolution of two factors: (i) the category of fences (physical or nonphysical) insuring a safe operating environment and (ii) the new couplings between factors that were formerly nearly independent. The latter is even pushed further with Industry 4.0.

Barriers that allow normal operation progressed with both the complication of work and the more involved persons. Therefore, this new context complicates the detection of flaws in these barriers, leading to undesirable events and failures. Such situations bring degradation of operational and safety margins. They may be locally and individually acceptable, but the sum of effects may have important unanticipated consequences that are not captured by a local analysis. The complexity of the operating environment involves a solution at the organizational level in order to cope with new challenges [12, 34, 39, 45, 70–74].

There are also studies investigating the hypothesis that modern enterprises depend on the deployment of cognitive capacities [70]. The authors argue that there are severe limitations on these capacities in a phenomenon they identify as "functional stupidity." "Functional stupidity" represents a lack of critical thinking, a deliberate condition of ignorance evading defiance to the status quo. This type of pathology is usually widespread in settings ruled by economy in persuading [75, 76]. Such a situation may lead to types of administration curbing or marginalizing suspicion and suppress effective communications. On the other hand, this context brings a structure of interior discussions in such ways favoring positive storylines and marginalizing undesirable ones. Thus, those situations may lead to reducing capacities of the innovation and creativity creating more fragile organizational structures that are vulnerable to both internal and external threats and perturbations, particularly in complex modern enterprises.

4.1.3. Human Performance. The behavior of people is basically shaped by their milieu. Marais et al. [77] analyze situations where one does not always anticipate inadequate behavior. It seems that autonomous decisions across organization may lead to unexpected combination with harmful, often surprising, impacts on both the performance and safety. Additionally, Katina [75, 78] using a synthesis of literature suggests that decision-making and actions are influences by norms and personal attitudes, organizational structures, knowledge base, and social context, degree of connectivity, race and ethnicity, mass media, and national ideology. This suggests a need for consideration of cognition, system, and environment as well as their interplay. Furthermore, a tangible reduction of undesirable events, such as accidents, major process interruptions, or bankruptcies, involves a deep understanding of human and organizational performance issues.

Some research works propose the framework of complexity leadership theory which may help getting a better human and organizational performance [79, 80].

As far as the rationality of decision-making is concerned, several research works indicate that one cannot assume that it is always rational [12, 35, 72]. Cognitive and motivational biases are usually part of the decision-making process. Cognitive bias is defined as "a systematic discrepancy between the "correct" answer in a judgmental task, initiated through a formal normative rule, and the decision maker's actual response to such a task." Motivational biases describe a distortion in decision-making regarding outcomes, results, or choices [72]. Those biases usually have a negative impact on the wanted outcomes and performance of organizations.

4.1.4. Complex Systems. The complexity and the opacity of modern systems bring difficulties to the staff to predict its overall behavior as a function of its individual components. The complexity is a system property and results from interactions between its components/subsystems, humans, HMI, HRI, etc. It generates unanticipated and emergent comportment of the system, often intensified by ill adapted operator's actions to those situations.

HRI can be a paradigmatic industrial and occupational example of this complex and challenging context, where Vasic and Billard [15] propose the design of new sensing technology and of fast sensor fusion algorithms (i) to track multiple moving targets in real time, (ii) to achieve robust detection of human motion in order to build good predictive systems, (iii) to ensure robust detection of contact between robots and surrounding living agents in multiple points, and (iv) to develop fast responsive controllers that can replant trajectories in complex, cluttered environment in real time.

Several research works highlight the importance of detecting and cautiously analyzing warning flags, precursors, near-misses, and "low-level" events in order to avoid system level break-downs, process interruptions, and/or major accidents. Therefore, organization should have enough organizational, economic, and technological resilience and flexibility applicable in a large number of different and (un)anticipated situations [12, 36, 37, 39, 55, 81].

As far as human performance is concerned, it is important to understand the error itself. Some research works have shown that both success and failure pathways apply the same intellectual processes, and only the consequence changes. So, the undesired outcome qualifies an action as an error, and it is essential to find its cause. Analyses shall find out why an event occurred ("direct cause" related to preventive and mitigating barriers as well as error precursors) and why it was not stopped ("fundamental cause"). It also has to investigate the organization and its performance (expanded fundamental causes). Considering that it is almost impossible to determine a true causality in complex systems, those analyses become a difficult undertaking in a modern industrial setting. Stock and Seliger [57] propose approaches to address the human factor and social change in Industry 4.0. For this, these authors propose through new technologies increasing the efficiency of the training of the workers, as well as increasing their intrinsic and extrinsic motivation.

4.2. Potential Approaches for Improving Human and Organizational Performance. As discussed above, the introduction of the concept of Industry 4.0 brings numerous challenges. To cope with those new challenges, it is necessary to implement both a systematic return of experience (internal and external) and a continuous improvement process and to increase organizational resilience and robustness to unexpected events. However, increasing resilience shall be thought about wisely in order to preserve competiveness, further development, sustainability, and economic viability of an organization.

The organizational resilience is a developing concept. It will not be discussed in detail here, but there are some suggested references upon the topic [10, 34, 45, 70, 71, 82–84]. This section presents suggestions regarding key elements which may reinforce the organizational resilience in the context of Industry 4.0.

4.2.1. Modeling and Measuring Human and Organizational Performance. Understanding impacts and risks of humans and organizations as contributors to mishaps, disruptions, and accidents in complex systems requires an adequate model. The model has to go further than the "simple" approach of linearly analyzing preventive and mitigating barriers, which provides quite narrow insights of the events.

Although some models exist [12, 39, 52, 53], these models are not necessarily adaptive to the context of Industry 4.0 risks. Therefore, suggesting the development of methods which will enable modeling and measuring human and organizational performance in the context of Industry 4.0 is a novel approach.

In this regard, it is necessary to adequately take account of the complexity of today's organizations as well as their operating context. This complexity necessitates a new way of reasoning and managing contemporary organizations. The traditional approaches in modeling, analyzing, and management are not entirely adequate to do it, and new methods are necessary [12, 36].

Actually, there are numerous research works suggesting that contemporary organizations should be considered, analyzed, modeled, and managed as Complex Adaptive Systems (CAS) or Complex Adaptive Systems of Systems (CASoS) [12, 36, 73, 85]. This claim is particularly relevant with the introduction of the concept of Industry 4.0. The theory of the complexity and characteristics of CASoS are not discussed

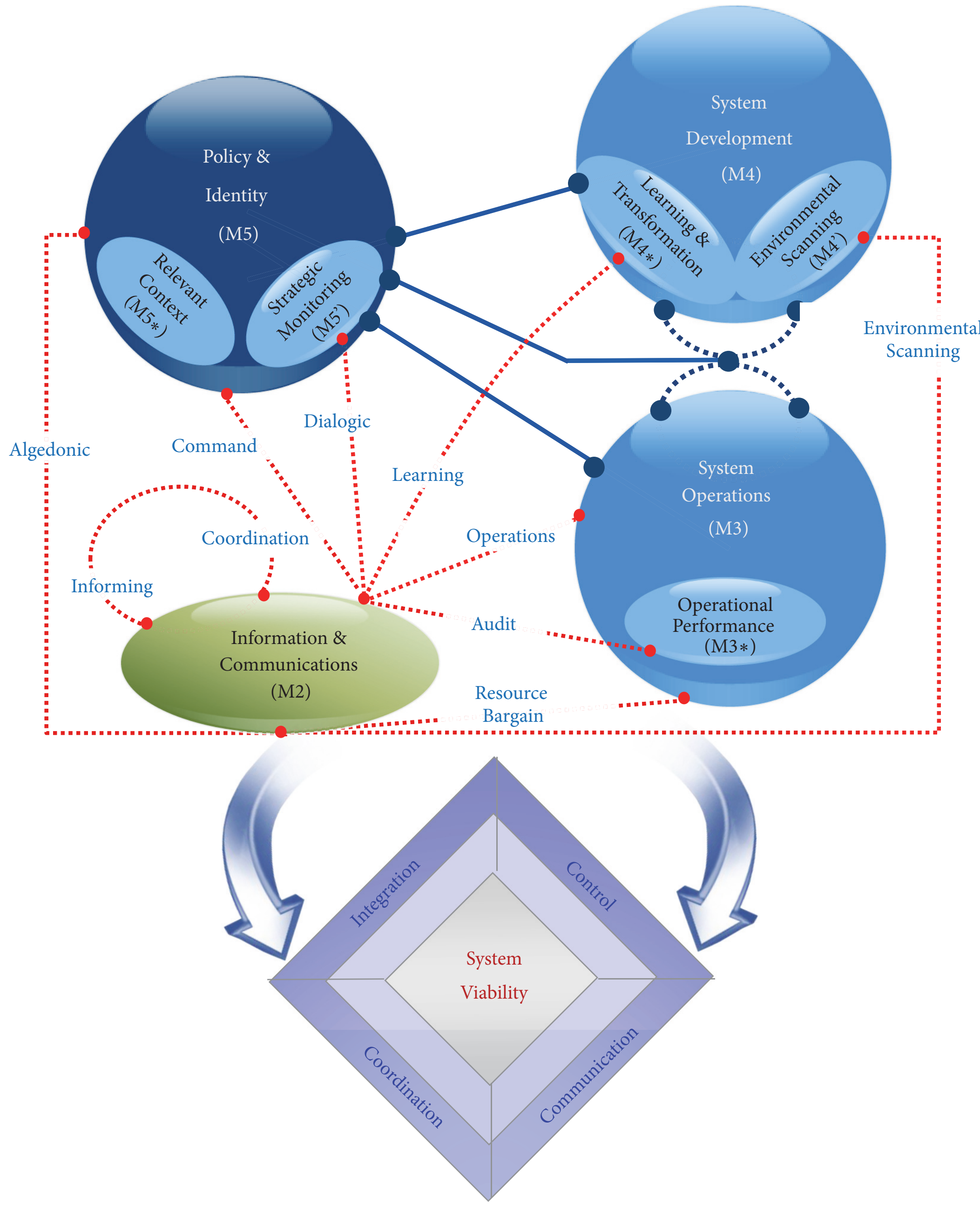

Figure 1: CSG metasystem functions (modified from [19]).

here in detail. It is suggested to consult relevant references on the topic [10, 12, 36, 40, 43, 45, 49, 71, 74, 86, 87].

4.2.2. Adaptation and Introduction of the Concept of Complex System Governance (CSG) for Industry 4.0. A possible approach for dealing with complexity in organizational setting is the application of emerging research of Complex System Governance. Complex System Governance is an emerging field, representing an approach to improve system performance through purposeful execution of design for and evolution of important metasystem roles [19, 88–90]. In this emerging field of CSG, the main roles include evolving and improving system performance essential functions enabling control, communication, coordination, and integration [19]. Figure 1 is based on the research of Keating et al. [19] and provides the overall description of the SG approach (Table 6 provides elaboration of the different functions in the CSG model as suggested by Keating and Bradley's [18] research). In CSG, the "metasystem" is deliberately used to imply functions and roles beyond the purview of individual systems in the "system of systems" cluster [91–93]. In Table 6, individual systems can be represented as M1. However, M1 is not listed as the concern for CSG is as the control and communication beyond individual systems (i.e., the metasystem level).

Keating and Bradley [18] provide the systemic representation of CSG indicated in Table 6 in which the purpose

Table 6: CSG's overall description based on Keating and Bradley's [18].

Areas of concern	Metasystem function	Primary role
System identity	M5: Policy and identity	Focusing on overall steering and trajectory for the Industry 4.0 systems in the fulfillment of their missions. Maintaining identity and balance between current and future focus.
	M5∗: System context	Focusing on the specific context within which the metasystem of an industry is embedded. Context is the set of circumstances, factors, conditions, or patterns that enable or constrain execution of systems in Industry 4.0 setting.
	M5': Strategic system monitoring	Focusing on oversight of the Industry 4.0 performance indicators at a strategic level. This includes identification of performances that exceed as well as those the fail to meet the established expectations.
System development	M4: System development	Developing and maintaining current and future models of systems in question within the Industry 4.0 schema as well as concentrating on the long-range development for the industry to enable the realization of future feasibilities.
	M4∗: Learning and transformation	Focusing on facilitation of learning based on correction of design errors (first order learning) in the metasystem roles of the industry as well as planning for revolution of the industry (second order learning).
	M4': Environmental scanning	Focusing on designs, and monitoring systems that can be used to sense operating environment of the industry to detect environmental trends, patterns, or events that can have implications on the current and future state of the industry.
System operations	M3: System operations (M3)	Focusing on the day to day execution of industry functions (operations)
	M3∗: Operational performance	Monitoring system performance to identify and assess aberrant conditions, exceeded thresholds, and/or irregularities.
System information	M2: Information and communications	Creating designs and mechanisms that enable the information flow and consistent interpretation of exchanges information and data necessary to execute industry functions.

is to provide an organizing construct for the interrelated functions necessary to perform CSG. In CSG approach, the center of any systemic intervention is people with their strengths and weaknesses. In essence, this is recognition that design, execution, and evolution of a systemic intervention are accomplished by people. As such, people become the central driving force behind systemic intervention including challenges related to machine-human interfaces. The effectiveness in intervention must be a function of those who design, conduct, and have participatory roles in the intervention effort [94]. The CSG approach includes a system mapping followed by an investigation to uncover causes of weaknesses (i.e., pathologies) in the governance structure. Pathology acts inhibiting system performance. While CSG is focused on functions enabling viability of the system, it also calls for systemic identification and assessment of system pathologies affecting governance [75]. Interestingly, present research suggests that solutions in the CSG paradigm might involve going beyond technology “fixes” to include “socio” policy, context, and environment.

Pyne et al. [85] further explore concepts, methods, and tools that may help managers to cope with constantly increasing complexity issues. Furthermore, it is suggested that effective problem solving in complex domains (i.e., Industry 4.0) may need different level of “more systemic” approaches capable of matching the uncertain, complex, and dynamic behavior characterize today’s industries. Proponents of CSG approach suggest exploring the challenges in moving the CSG from the theoretical/conceptual formulation to practice.

A potential area of practice is Industry 4.0. Again, if one takes Industry 4.0 to mean the current trend of automation and data exchange in manufacturing technologies and encompassing CPS, IoT, cloud computing, and cognitive computing, there remains a case to be made for the utility of CSG in the various areas of Industry 4.0. At the onset, it appears CSG might be used to address issues related to themes of viability, governance, control, communication, coordination, and integration, as well as malfunctions (pathology) that may emerge in the different facets of Industry 4.0.

4.2.3. Benefiting from Experience of Other Industries at Risk. Main industries at risk such as nuclear, space, aviation, and petrochemical have developed different ways of coping with human and organizational performance issues. Their return of experience may be beneficial for analyzing ways to improve it within the context of Industry 4.0. Some experience and practices from the nuclear power industry are depicted below.

The Institute of Nuclear Power Operations (INPO) identifies key aspects to accomplish the quality in the integrated risk management [81]. Some attributes are enumerated below:

(i) Behaviors: the expected actions for the stages of risk management are suggested for all organizational levels from individuals to corporate executives.

(ii) Organizational characteristics for effective integrated risk management: a set of principles, policies, practices, oversight, and training are recommended for achieving an all-inclusive risk management process which is elaborated and implemented.

(iii) Integrated risk management warning flags: the warning flags aim at helping the staff and managers to detect undesirable conditions affecting an integrated risk management. The former are categorized by defenses aiming at minimizing risky events. The staff and managers should analyze them for stimulating discussions and draw lessons.

Such an approach may help reinforcing the overall resilience and robustness. This activity also involves a cautious analysis of organizational factors such as incentive systems that influence human performance and impact the risk of errors [37]. This feature is also termed “Antifragility” by some researchers [42, 95]. The antifragility puts forward an idea of adaptive organizations with regard to complex and continuously altering internal and external operating context. In this case, one can suggest that internal and external complexification is also partly due to the introduction of the concept of Industry 4.0 which sometimes may overwhelm human capacity to grasp relevant factors in acting and decision-making. This implies that the paradigm of “only” technological solutions to emerging risks may be misleading especially without consideration of role of the human and organizational factor. For example, one becomes inclined to more risk taking by putting undue confidence into the technology without knowing its limits and vulnerabilities.

Therefore, improving and managing human performance risks (including those coming from machine-human interfaces) based on the experience from the nuclear power industry may also include other elements such as the following [48]:

(i) Frequently discuss risks, complexity, and their interdependence

(ii) Perform gap analysis between outlooks and observations of behavior

(iii) Enthusiastically lobby different opinion to avoid deliberate carelessness (reduce cognitive and motivational biases)

(iv) Analyze and discuss past behaviors, including informal messages at the corporate level

(v) Doubt and uncertainty should not go unchallenged

(vi) Ask to demonstrate that a system is appropriately safe to function or not sufficiently unsafe to be shut down

(vii) Be cautious regarding findings from a root cause investigation that one points out to the negligence; in this case, only part of the story has been exposed

(viii) Enlarge the scope of defense-in-depth concept to embrace the concept of complex systems and their intrinsic nonlinearity

5. Conclusions

Undoubtedly, Industry 4.0 brings numerous advantages. However, this paradigm also carries emerging risks and challenges related to organizational and human performance. These emerging risks include both industrial risks and occupational risks. Arguably, human factor is the main link between industrial emerging risks and occupational emerging risks in the Industry 4.0 context.

Addressing these issues calls for effectiveness in dealing with traditional static approach to risk, for example, through the development of dynamic risk management models oriented towards the organizational and human performance. However, there is also a need to develop robust approaches capable of dealing with emerging risks associated with Industry 4.0. In this research, Complex System Governance is suggested.

However, there remains a need for case applications, clearly articulating the potential of such approaches. Moreover, there is no need to be limited to such approaches as Complex System Governance. This research can be extended to include technological approaches such as Blockchain Technology and the discovery of deep systemic pathological issues affecting Industry 4.0.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was funded by the Spanish Ministry of Economy and Competitiveness, with the title "Analysis and Assessment of technological requirements for the design of a New and Emerging Risks standardized management SYStem (A2NERSYS)" with reference DPI2016-79824-R.

References

[1] H. Kagermann, W. Wahlster, and J. Helbig, *Recommendations for Implementing the Strategic Iniciative Industrie 4.0*, Acatech e National Academy of Science and Engineering, 2013.

[2] A. J. C. Trappey, C. V. Trappey, U. Hareesh Govindarajan, A. C. Chuang, and J. J. Sun, "A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0," *Advanced Engineering Informatics*, vol. 33, pp. 208–229, 2017.

[3] B. Marr, "Why everyone must get ready for the 4th industrial revolution," 2016, https://www.forbes.com/sites/bernardmarr/2016/04/05/why-everyone-must-get-ready-for-4th-industrial-revolution/.

[4] S. S. Kamble, A. Gunasekaran, and S. A. Gawankar, "Sustainable Industry 4.0 framework: a systematic literature review identifying the current trends and future perspectives," *Process Safety and Environmental Protection*, vol. 117, pp. 408–425, 2018.

[5] F. Brocal, M. A. Sebastián, and C. González, "Advanced manufacturing processes and technologies," in *Management of Emerging Public Health Issues and Risks*, B. Roig, K. Weiss, and V. Thireau, Eds., Chapter 2, pp. 31–64, Academic Press, 2019.

[6] A. Sanders, C. Elangeswaran, and J. Wulfsberg, "Industry 4.0 implies lean manufacturing: research activities in industry 4.0 function as enablers for lean manufacturing," *Journal of Industrial Engineering and Management*, vol. 9, no. 3, pp. 811–833, 2016.

[7] T. D. Oesterreich and F. Teuteberg, "Understanding the implications of digitisation and automation in the context of Industry 4.0: a triangulation approach and elements of a research agenda for the construction industry," *Computers in Industry*, vol. 83, pp. 121–139, 2016.

[8] A. Badri, B. Boudreau-Trudel, and A. S. Souissi, "Occupational health and safety in the industry 4.0 era: A cause for major concern?" *Safety Science*, vol. 109, pp. 403–411, 2018.

[9] D. Podgórski, K. Majchrzycka, A. Dąbrowska, G. Gralewicz, and M. Okrasa, "Towards a conceptual framework of OSH risk management in smart working environments based on smart PPE, ambient intelligence and the Internet of Things technologies," *International Journal of Occupational Safety and Ergonomics*, vol. 23, no. 1, pp. 1–20, 2017.

[10] E. Zio, "Challenges in the vulnerability and risk analysis of critical infrastructures," *Reliability Engineering & System Safety*, vol. 152, pp. 137–150, 2016.

[11] F. Qian, W. Zhong, and W. Du, "Smart process manufacturing—perspective fundamental theories and key technologies for smart and optimal manufacturing in the process industry," *Engineering Journal*, vol. 3, no. 2, pp. 154–160, 2017.

[12] D. Komljenovic, G. Loiselle, and M. Kumral, "Organization: a new focus on mine safety improvement in a complex operational and business environment," *International Journal of Mining Science and Technology*, vol. 27, no. 4, pp. 617–625, 2017.

[13] B. Roig and F. Brocal, "Introduction: needs on emerging risk and management," in *Management of Emerging Public Health Issues and Risks*, B. Roig, K. Weiss, and V. Thireau, Eds., pp. 17–21, Academic Press, 2019.

[14] F. Brocal, C. González, G. Reniers, V. Cozzani, and M. A. Sebastián, "Risk management of hazardous materials in manufacturing processes: links and transitional spaces between occupational accidents and major accidents," *Materials*, vol. 11, no. 1915, pp. 1–23, 2018.

[15] M. Vasic and A. Billard, "Safety issues in human–robot interaction," in *Proceedings of the IEEE International Conference on Robotics and Automation*, pp. 197–204, IEEE, Piscataway, New Jersey, NJ, USA, 2013.

[16] T. Aven, "The risk concept-historical and recent development trends," *Reliability Engineering & System Safety*, vol. 99, pp. 33–44, 2012.

[17] F. Brocal, M. A. Sebastián, and C. González, "Theoretical framework for the new and emerging occupational risk modeling and its monitoring through technology lifecycle of industrial processes," *Safety Science*, vol. 99, pp. 178–186, 2017.

[18] C. B. Keating and J. M. Bradley, "Complex system governance reference model," *International Journal of System of Systems Engineering*, vol. 6, no. 1-2, pp. 33–52, 2015.

[19] C. B. Keating, P. F. Katina, and J. M. Bradley, "Complex system governance: Concept, challenges, and emerging research," *International Journal of System of Systems Engineering*, vol. 5, no. 3, pp. 263–288, 2014.

[20] International Organization for Standardization (ISO), "Risk management –guidelines," ISO 31000:2018, Geneva, 2018.

[21] International Organization for Standardization (ISO), "Occupational health and safety management systems-Requirements with guidance for use," ISO 45001:2018, Geneva, 2018.

[22] International Risk Governance Council (IRGC), *The Emergence of Risks*, Contributing Factors, IRGC, Geneva, Switzerland, 2010.

[23] International Risk Governance Council (IRGC), *Emerging Risks Sources, Drivers and Governance Issues*, IRGC, Geneva, Switzerland, 2010.

[24] International Risk Governance Council (IRGC), *Guidelines for Emerging Risk Governance*, International Risk Governance Council (IRGC), Lausann, Switzerland, 2015.

[25] F. Brocal, C. González, and M. A. Sebastián, "Technique to identify and characterize new and emerging risks: a new tool for application in manufacturing processes," *Safety Science*, vol. 109, pp. 144–156, 2018.

[26] E. Flaspöler, D. Reinert, and E. Brun, *Expert Forecast on Emerging Physical Risks Related to Occupational Safety and Health*, EU-OSHA (European Agency for Safety and Health at Work), Luxembourg., 2005.

[27] E. Brun, R. O. Beeck, S. Van Herpe et al., *Expert Forecast on Emerging Biological Risks Related to Occupational Safety and Health*, EU-OSHA (European Agency for Safety and Health at Work), Luxembourg, 2007.

[28] E. Brun, M. Milczarek, N. Roskams et al., *Expert Forecast on Emerging Psychosocial Risks Related to Occupational Safety and Health*, Office for Official Publications of the European Communities, Luxembourg, 2007.

[29] E. Brun, R. Op de Beeck, S. Van Herpe et al., *Expert Forecast on Emerging Chemical Risks Related to Occupational Safety and Health*, EU-OSHA (European Agency for Safety and Health at Work), Luxembourg, 2009.

[30] F. Brocal, "Uncertainties and challenges when facing new and emerging occupational risks," *Archivos de Prevención de Riesgos Laborales*, vol. 19, no. 1, pp. 6–9, 2016.

[31] M. L. Cantonnet, J. C. Aldasoro, and J. Iradi, "New and emerging risks management in small and medium-sized Spanish enterprises," *Safety Science*, vol. 113, pp. 257–263, 2019.

[32] International Organization for Standardization (ISO), "Guidance for managing emerging risks to enhance resilience," ISO/NP 31050, Geneva, 2019, ISO/NP 31050, https://www.iso.org/standard/54224.html.

[33] S. Arbesman, *Overcomplicated: Technology at the Limits of Comprehension*, Current, New York, NY, USA, 2016.

[34] J. Bourgon, *A New Synthesis of Public Administration, Servicing in the 21st Century*, The School of Public Studies, McGill-Queen's University Press, 2011.

[35] D. Kahneman, *Thinking, Fast and Slow, Farrar, Straus and Giroux*, New York, NY, USA, 2012.

[36] D. Komljenovic, M. Gaha, G. Abdul-Nour, C. Langheit, and M. Bourgeois, "Risks of extreme and rare events in Asset Management," *Safety Science*, vol. 88, pp. 129–145, 2016.

[37] M. E. Paté-Cornell, "On 'black swans' and 'perfect storms', risk analysis and management when statistics are not enough," *Risk Analysis*, vol. 32, no. 11, pp. 1823–1833, 2012.

[38] S. Dekker, P. Cilliers, and J.-H. Hofmeyr, "The complexity of failure: Implications of complexity theory for safety investigations," *Safety Science*, vol. 49, no. 6, pp. 939–945, 2011.

[39] K. Grigoriou, A. Labib, and S. Hadleigh-Dunn, "Learning from rare events: An analysis of ValuJet Flight 592 and Swissair Flight SR 111 crashes," *Engineering Failure Analysis*, vol. 96, pp. 311–319, 2019.

[40] G. Rzevski and P. Skobelev, *Managing Complexity*, WIT Press, Massachusetts, Mass, USA, 2014.

[41] T. Aven and M. Ylönen, "A risk interpretation of sociotechnical safety perspectives," *Reliability Engineering & System Safety*, vol. 175, pp. 13–18, 2018.

[42] T. Aven, "Implications of black swans to the foundations and practice of risk assessment and management," *Reliability Engineering & System Safety*, vol. 134, pp. 83–91, 2015.

[43] L. Bukowski, "System of systems dependability – Theoretical models and applications examples," *Reliability Engineering & System Safety*, vol. 151, pp. 76–92, 2016.

[44] L. A. Cox, "Confronting deep uncertainties in risk analysis," *Risk Analysis*, vol. 32, no. 10, pp. 1607–1629, 2012.

[45] D. Helbing, "Globally networked risks and how to respond," *Nature*, vol. 497, no. 7447, pp. 51–59, 2013.

[46] N. G. Leveson, *Engineering a Safer World, Systems Thinking Applied to Safety*, The MIT Press, Cambridge, Massachusetts, Matt, USA, 2011, http://mitpress.mit.edu/books/engineering-safer-world.

[47] N. G. Leveson, "Applying system thinking to analyze and learn from events," *Safety Science*, vol. 49, pp. 55–64, 2011.

[48] D. Mosey, "Looking beyond operator – putting people in the mix, nei magazine," collaboration with Ken Ellis, Managing Direction of World Association of Nuclear Power Operators (WANO), 2014, http://www.neimagazine.com/features/feature-looking-beyond-the-operator-4447549/, http://www.neimagazine.com/features/featureputting-people-in-the-mix-4321534/.

[49] O. Renn, K. Lucas, A. Haas, and C. Jaeger, "Things are different today: the challenge of global systemic risks," *Journal of Risk Research*, pp. 1–16, 2017.

[50] P. F. Katina, C. Ariel Pinto, J. M. Bradley, and P. T. Hester, "Interdependency-induced risk with applications to healthcare," *International Journal of Critical Infrastructure Protection*, vol. 7, no. 1, pp. 12–26, 2014.

[51] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 11–25, 2001.

[52] Department of Energy, *Human Performance Improvement Handbook*, vol. 1, DOE Standard, Washington, Wash, DC, USA, 2009, https://www.standards.doe.gov/standards-documents/1000/1028-BHdbk-2009-v1.

[53] IAEA, *Managing Human Performance to Improve Nuclear Facility Operation*, Vienna, Austria, 2013.

[54] R. Moura, M. Beer, E. Patelli, J. Lewis, and F. Knoll, "Learning from accidents: Interactions between human factors, technology and organisations as a central element to validate risk studies," *Safety Science*, vol. 99, pp. 196–214, 2017.

[55] US NRC, *Safety Culture Communicator, Case Study 4: April 2010 Upper Big Branch Mine Explosion – 29 Lives Lost*, Washington, Wash, D.C., USA, 2012, http://pbadupws.nrc.gov/docs/ML1206/ML12069A003.pdf.

[56] B. Wahlström, "Organisational learning - reflections from the nuclear industry," *Safety Science*, vol. 49, no. 1, pp. 65–74, 2011.

[57] T. Stock and G. Seliger, "Opportunities of sustainable manufacturing in industry 4.0," *Procedia CIRP*, vol. 40, pp. 536–541, 2016.

[58] T. B. Sheridan, "Human–robot interaction: status and challenges," *Human Factors*, vol. 58, no. 4, pp. 525–532, 2016.

[59] W. Wang, X. Zhu, L. Wang, Q. Qiu, and Q. Cao, "Ubiquitous robotic technology for smart manufacturing system," *Computational Intelligence and Neuroscience*, vol. 2016, Article ID 6018686, 14 pages, 2016.

[60] E. Flaspöler, A. Hauke, P. Pappachan et al., *The Human Machine Interface as an Emerging Risk*, Office for Official Publications of the European Communities, Luxembourg, 2010.

[61] P. Chidambaram, "Perspectives on human factors in a shifting operational environment," *Journal of Loss Prevention in the Process Industries*, vol. 44, pp. 112–118, 2016.

[62] N. Stacey, P. Ellwood, S. Bradbrook, J. Reynolds, and H. Williams, "Key trends and drivers of change in information and communication technologies and work location," Foresight on new and emerging risks in OSH. Working report, European Agency for Safety and Health at Work (EU-OSHA), 2017.

[63] International Risk Governance Council (IRGC), *White Paper on Risk Governance. Towards an Integrative Approach*, IRGC, Geneva, 2005.

[64] Society for Risk Analysis (SRA), SRA glossary, SRA, 2015.

[65] International Risk Governance Council (IRGC), *Improving the Management of Emerging Risks*, IRGC, Geneva, Switzerland, 2011.

[66] International Organization for Standardization (ISO), "ISO 31050 guidance for managing emerging risks to enhance resilience: thriving in a world growing in uncertainty," ISO 31050-Leaflet_v09aj14082018, 2018, https://www.eu-vri.eu/filehandler.ashx?file=16526.

[67] M. Roberti, "How is RFID being used in the construction industry? ask experts forum 6," 2013.

[68] N. Paltrinieri and G. Scarponi, "Addressing dynamic risk in the petroleum industry by means of innovative analysis solutions," *Chemical Engineering Transactions*, vol. 36, pp. 451–456, 2014.

[69] X. Yang, S. Haugen, and N. Paltrinieri, "Clarifying the concept of operational risk assessment in the oil and gas industry," *Safety Science*, vol. 108, pp. 259–268, 2018.

[70] M. Alvesson and A. Spicer, "Stupidity based theory of organizations," *Journal of Management Studies*, vol. 49, no. 7, pp. 1194–1220, 2012.

[71] T. Homer-Dixon, "Complexity science, shifting the trajectory of civilization," *Oxford Leadership Journal*, vol. 2, no. 1, pp. 2–15, 2011.

[72] G. Montibeller and D. Winterfeldt, "Cognitive and motivational biases in decision and risk analysis," *Risk Analysis*, vol. 35, no. 7, pp. 1230–1251, 2015.

[73] R. D. Stacey and C. Mowles, "Strategic management and organisational dynamic," in *The Challenge of Complexity to Ways of Thinking about Organizations*, Pearson, London, UK, 7th edition, 2016.

[74] M.-C. Therrien, A. Valiquette-L'Heureux, and J.-M. Normandin, "Tightly coupled governance for loosely coupled wicked problems: the train explosion in Lac-Mégantic case," *International Journal of Risk Assessment and Management*, vol. 19, no. 4, pp. 260–277, 2016.

[75] P. F. Katina, "Metasystem pathologies (M-Path) method: phases and procedures," *Journal of Management Development*, vol. 35, no. 10, pp. 1287–1301, 2016.

[76] C. I. Barnard, "Functions and pathology of status systems in formal organizations," in *Industry and Society*, W. F. Whyte, Ed., pp. 46–83, McGraw-Hill, New York, NY, USA, 1946.

[77] K. Marais, J. H. Saleh, and N. G. Leveson, "Archetypes for organizational safety," *Safety Science*, vol. 44, no. 7, pp. 565–582, 2006.

[78] P. F. Katina, "Individual and societal risk (RiskIS): beyond probability and consequence during hurricane katrina," in *Disaster Forensics: Understanding Root Cause and Complex Causality*, A. J. Masys, Ed., pp. 1–23, Springer International Publishing, Geneva, Switzerland, 2016.

[79] M. Schneider and M. Somers, "Organizations as complex adaptive systems: implications of Complexity Theory for leadership research," *The Leadership Quarterly*, vol. 17, no. 4, pp. 351–365, 2006.

[80] M. Uhl-Bien, R. Marion, and B. McKelvey, "Complexity leadership theory: shifting leadership from the industrial age to the knowledge era," *The Leadership Quarterly*, vol. 18, no. 4, pp. 298–318, 2007.

[81] Institute of Nuclear Power Operations (INPO), "Excellence in integrated risk management; the elements, attributes, and behaviors that exemplify excellence in integrated risk management INPO 12-008," 2013, http://nuclearsafety.info/wp-content/uploads/2017/03/INPO-12-008-Excellence-in-Integrated-Risk-Management.pdf.

[82] F. Bouaziz and Z. S. Hachicha, "Strategic human resource management practices and organizational resilience," *Journal of Management Development*, vol. 37, no. 7, pp. 537–551, 2018.

[83] A. De Galizia, C. Simon, P. Weber, B. Iung, C. Duval, and E. Serdet, "Markers and petterns of organizational resilience for risk analysis," *IFAC-PapersOnLine*, vol. 49, no. 19, pp. 432–437, 2016.

[84] D. Mendonça and W. A. Wallace, "Factors underlying organizational resilience: The case of electric power restoration in New York City after 11 September 2001," *Reliability Engineering & System Safety*, vol. 141, pp. 83–91, 2015.

[85] J. C. Pyne, C. B. Keating, and P. F. Katina, "Enhancing utility manager's capability for dealing with complex issues," in *Proceedings of the Water Environment Federation Technical Exhibition and Conference (WEFTEC '16)*, vol. 2016, New Orleans.

[86] B. Johnson and A. Hernandez, "Exploring engineered complex adaptive systems of systems," *Procedia Computer Science*, vol. 95, pp. 58–65, 2016.

[87] A. Stirling, "Keep it complex," *Nature*, vol. 468, no. 7327, pp. 1029–1031, 2010.

[88] D. Baugh, "Environmental scanning implications in the governance of complex systems," *International Journal of System of Systems Engineering*, vol. 6, no. 1-2, pp. 127–143, 2015.

[89] C. B. Keating and V. Ireland, "Editorial: complex systems governance - issues and applications," *International Journal of System of Systems Engineering*, vol. 7, no. 1-3, pp. 1–21, 2016.

[90] C. B. Keating and P. F. Katina, "Complex system governance development: a first generation methodology," *International Journal of System of Systems Engineering*, vol. 7, no. 1-3, pp. 43–74, 2016.

[91] B. Carter, "A metasystem perspective and implications for governance," *International Journal of System of Systems Engineering*, vol. 6, no. 1-2, pp. 90–100, 2015.

[92] K. D. Palmer, "Meta-systems engineering," in *Proceedings of the 10th Annual International Symposium of the International Council on Systems Engineering*, 2000, http://www.archonic.net/MSE04.PDF.

[93] G. R. Djavanshir, R. Khorramshahgol, and J. Novitzki, "Critical characteristics of metasystems: Toward defining metasystems' governance mechanism," *IT Professional*, vol. 11, no. 3, pp. 46–49, 2009.

[94] J. C. Pyne, C. B. Keating, P. F. Katina, and J. M. Bradley, "Systemic intervention methods supporting complex system governance initiatives," *International Journal of System of Systems Engineering*, vol. 8, no. 3, pp. 285–309, 2018.

[95] N. N. Taleb, *Antifragile, Things that Gain from Disorder*, Random House, New York, NY, USA, 2012.