UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

Ensuring Industrial Safety and Security

HANDBOOK

- United Nations Industrial Development Organization
- Russian Federal Environmental, Industrial and Nuclear Supervision Service
- British Standards Institution

ENGLISH

INCLUSIVE AND SUSTAINABLE INDUSTRIAL DEVELOPMENT

Ensuring Industrial Safety and Security

Handbook

United Nations Industrial Development Organization

Russian Federal Environmental, Industrial and Nuclear Supervision Service

British Standards Institution

Vienna, Austria
August 2021

UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

www.unido.org

ACKNOWLEDGMENTS

This handbook was prepared as part of the UNIDO project "Ensuring Industrial Safety and Security" funded by the Russian Federation, and emerged as a product of collaboration between the United Nations Industrial Development Organization (UNIDO); Rostechnadzor, the Russian Federal Environmental, Industrial, and Nuclear Supervision Service; BSI (British Standards Institution), that worked under the overall guidance of Farrukhbek Alimdjanov, UNIDO Industrial Development Officer. Kate Field, Global Head Health, Safety and Well-being, BSI provided the models and valuable writing inputs, additional inputs were provided by JC Sekar, Acuizen Technologies and Michael Tooma, Managing Partner, Clyde&Co, Australia. Oliver Authried and Yana Roessl, UNIDO Project Associates provided supplementary inputs and contents to this handbook.

A special thanks goes to Irina Sokolova, Head of the International Cooperation Department, Rostechnadzor, for her continued support, valuable feedback and guidance throughout the project, together with Dmitry Chachelov, Deputy Head of the International Cooperation Department.

In addition, words of thanks and appreciation are extended to Kate Field for her continued support and provision of expert assessment during the project activities and Michael Tooma, JC Sekar and many others, who have contributed to a webinar series and conference activities. The results of this project, such as the Report on the Conference on Ensuring Industrial Safety and Security, theoretical models and studies were extensively referred to and used as the basis for development of this handbook.

Contents

INTRODUCTION 6

1. ORGANIZATIONAL RESILIENCE 10

2. THE 3C-3P MODEL FOR A RESILIENT INDUSTRIAL SAFETY SYSTEM 16

Resilience and Industrial Safety 18

Safety and the 3-Cs 18

Operationalizing the 3-Cs 23

3. SAFETY CULTURE 26

4. INDUSTRIAL SAFETY INSPECTIONS 32

5. SAFETY ENHANCING TECHNOLOGIES 36

6. CYBERSECURITY 42

CONCLUSSION AND OUTCOME 48

FURTHER READING 50

REFERENCES 50

Introduction

Raising awareness about industrial safety, in particular occupational health and safety (OHS), at the local (firm), national, regional and international levels is the first step towards achieving it. Many firms and national governments, even those in industrially developed regions, are either unaware of the vital importance of industrial safety or tend to ignore it.

The UNIDO project on Ensuring Industrial Safety and Security has been implemented in cooperation between UNIDO and Rostechnadzor (Russian Federal Environmental, Industrial, and Nuclear Supervision Service) and brought forward a range of issues relevant to safety. As part of an awareness raising campaign and to help spread best practices in industrial safety, the first International Conference on Ensuring Industrial Safety, held in Vienna at the end of May 2019, was an example of investments into efforts which achieve industrial safety in all countries, so that no one is left behind. Subsequently and in response to the COVID-19 pandemic, UNIDO and Rostechnadzor moved to organise webinars touching upon issues related to aspects of safety – particularly those that are relevant to the changing conditions brought by the pandemic. As another milestone, this handbook will give some insights into some requirements to ensure a safe working environment and draws on state-of-the-art international expertise.

Raising awareness about industrial safety, in particular occupational health and safety (OHS), at the local (firm), national, regional and international levels is the first step towards achieving it. Many firms and national governments, even those in industrially developed regions, are either unaware of the vital importance of industrial safety or tend to ignore it.

According to the ILO, more than 6,500 people around the world die every day of work-related illnesses and over 1,000 people a day from occupational accidents[1]. The number of annual work-related deaths rose from 2.33 million in 2014 to 2.78 million in 2017[2]. Of the 2.78 million work-related deaths in 2017, 2.4 million were associated with occupational diseases[3]. Fatal occupational accidents were highest in Asia, at 71.5 percent in 2014, followed by Africa (18.9 percent), America (6.5 percent) and Europe (2.9 percent)[4]. The accident fatality rate per 100,000 persons was highest in Africa (17.4) and Asia (13.0), reflecting the global distribution of the working population and hazardous work, as well as differing levels of economic development.

Industrial hazards, occupational accidents and work-related illnesses may originate in technological or industrial conditions, dangerous procedures, infrastructure failures or specific human activities.[5] They have a major impact not only on workers,

1) ILO 2019
2) Hämäläinen, Takala and Boon Kiat 2017.
3) Hämäläinen, Takala and Boon Kiat 2017.
4) Hämäläinen, Takala and Boon Kiat 2017
5) ILO 2019

but also on their families and society at large, in both the short and the long run, through injury or loss of life, deterioration in physical, cognitive and emotional well-being, social and economic disruption, property damage and environmental degradation. Furthermore, such hazards can reduce the productivity and efficiency of enterprises, potentially disrupting production, hampering competitiveness and diminishing the reputation of enterprises along supply chains, affecting the economy and society more widely.

Industrial safety encompasses the prevention of a wide variety of industrial hazards, occupational accidents and work-related illnesses in order to create a “zero-risk” environment. While this is a challenging task, effective prevention strategies at the enterprise, national, regional and international levels can eliminate, or at least minimize risk.

Because industrial activities will never be entirely free of risk from natural and human-caused hazards, it is essential to understand these risks as thoroughly as possible to inform supervisory authorities and to take suitable risk-mitigation measures based on best practices and best available technologies[6].

To ensure meaningful environmental protection and to address potential industrial risks, accidents and hazards, collective action is imperative at the international level as well as the national level. At the international level, protocols, conventions and agreements have been used to manage the negative impacts of industrial accidents. Partnerships among companies, civil society and government agencies are also critical to share vital information and ensure a commitment to common goals[7].

This handbook will provide an overview of essential concepts for ensuring safety and security, and helps to inform on modern trends in industrial safety management, encompassing organizational aspects, especially in light of the COVID-19 pandemic and its disruptions, technological safety, and important implications for cybersecurity.

Cybersecurity plays a key role in modern work environments and needs to be taken seriously from the beginning. Remote working has exposed vulnerabilities in organizations and companies. Other digitalization trends and the connection of production equipment will show an ever-increasing importance of cybersecurity and looking at safety and security in a holistic manner, as this handbook will undertake.

6) UNIDO 2019
7) UNIDO 2019

Organizational Resilience

Even where organizations had business continuity plans that considered pandemic risk, the severity of the impact from COVID-19 was simply not foreseen and existing risk management approaches were often inadequate. This was seen very clearly in industrial safety where there was an increase in industrial safety accidents, particularly during plant start-ups after periods of compulsory ‘lockdown’ (stay at home requirements to control the spread of COVID-19). It has also been seen in occupational health and safety as organizations have struggled to manage the psychosocial risks associated with the pandemic, such as the isolation of working from home.

At the heart of industrial safety is effective risk management; a coordinated set of activities carried out by people in a defined way to manage uncertainty[8]. Risk management also governs any number of other business process including finance and quality. These risk management approaches are predominately 'defensive' - focussed on stopping 'bad things' happening, and are broadly effective at achieving this. The challenge arises when agility and flexibility is needed due to unexpected change.

This was brought sharply into focus during 2020, as a new coronavirus "COVID-19" swept across the globe. Even where organizations had business continuity plans that considered pandemic risk, the severity of the impact from COVID-19 was simply not foreseen and existing risk management approaches were often inadequate. This was seen very clearly in industrial safety where there was an increase in industrial safety accidents, particularly during plant start-ups after periods of compulsory 'lockdown' (stay at home requirements to control the spread of COVID-19). It has also been seen

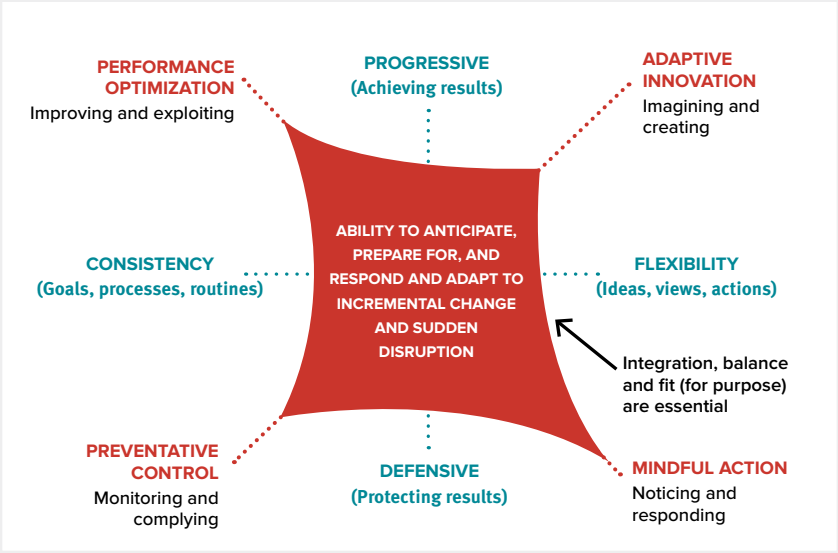


Figure 1: The Organizational Resilience 'Tension Quadrant'

8) Adapted from BS 31100:2011

in occupational health and safety as organizations have struggled to manage the psychosocial risks associated with the pandemic, such as the isolation of working from home.

In response to the pandemic, the concept of organizational resilience has had renewed focus. Organizational resilience is the "ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper"[9]. Organizational resilience takes a more holistic and proactive approach to risk management, through identifying different aspects of leadership behaviour and organisational capacity that are required to navigate through disruptive periods. The Strategic Tensions Assessment Tool (illustrated on opposite page[10]) recognizes the balance between both defensive (stopping bad things happening) and progressive behaviours (achieving desired results) to deliver results, whilst agility is achieved through the balance between consistency and flexibility.

Leaders wishing to build resilience need to determine the most appropriate balance of the four types of behaviour and sometimes this may involve counter-intuitive decisions.

The defensive perspective which is focussed on loss avoidance and preserving value. This is preventative control (being defensive and consistent) and mindful action (being defensive and flexible). Risk management and business continuity planning fits in that camp.

The agile perspective which is focussed on opportunity and growth. This is performance optimization (being progressive and consistent) and adaptive innovation (being progressive and flexible). This is the essence of organisational resilience.

9) Definition from BS 65000:2014 Guidance on organizational resilience

10) Denyer, D. (2017). Organizational Resilience: A summary of academic evidence, business insights and new thinking. BSI and Cranfield School of Management

Organizational resilience is not a one-off exercise and requires continual assessment and monitoring of both internal and external factors to build and strengthen resilience. Mastering organizational resilience requires the adoption of best practice to deliver ongoing business improvement by building competence and capability across all parts of an organization. In order to help organizations better understand organizational resilience, BSI developed a best practice framework which guides organizations through the key elements required to enable improved resilience.

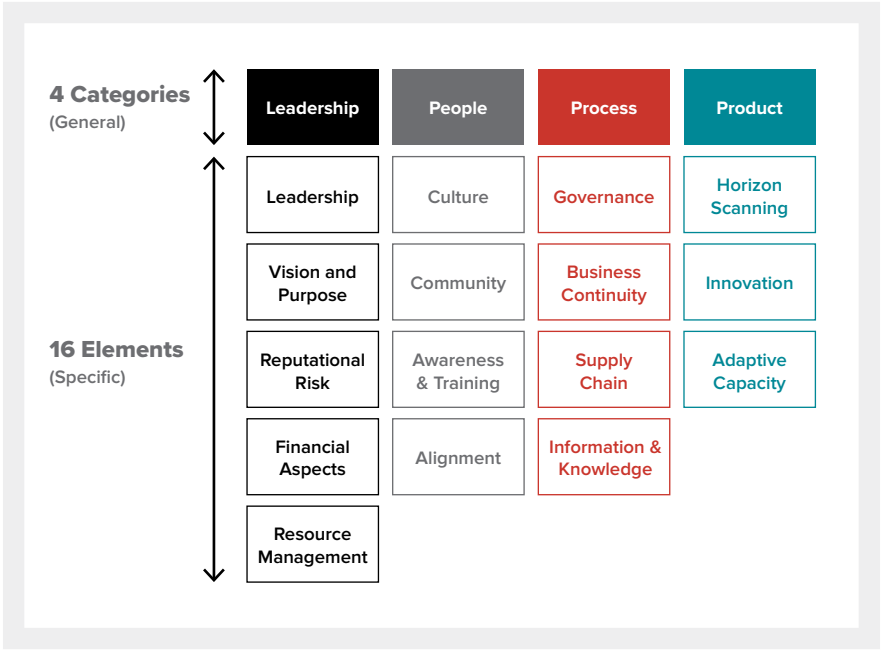


Figure 2: BSI Organizational Resilience Framework

The framework is made up four key categories, under which sixteen specific elements sit. Leadership is accountable and responsible to stakeholders for ensuring the organization remains resilient and thrives over time. It is leadership that determines how the other categories interact and perform and so effective leadership is a critical success factor.

LEADERSHIP

1 Leadership	The culture, visibility and performance of senior business leaders.
2 Vision and Purpose	How purpose is defined, communicated and related to strategic resource allocation.
3 Reputational Risk	The business's approach to managing and limiting reputational risk.
4 Financial Aspects	The quality of the management of financial aspects of the business.
5 Resource Management	The extent to which resources such as people and technology are managed effectively to be deployed where they are needed.

PEOPLE

6 Culture	The extent to which values and behaviours are shared, trust is established and employees are engaged
7 Community	The business's community relations, stewardship credentials and social responsibility
8 Awareness, Training and Testing	The levels of awareness, training and testing of Organizational Resilience
9 Alignment	The extent to which all aspects of the organization, including disciplines such as quality, health and safety and information security, are aligned to realizing its strategy

PROCESS

10 Governance	The extent to which governance policies are clearly defined and senior business leaders are accountable to all stakeholders
11 Business Continuity	The quality of the business continuity framework, policies and procedures
12 Supply Chain	The quality of supply chain governance, security and management
13 Information and Knowledge	The quality of information assets and knowledge sharing

PRODUCT

14 Horizon Scanning	The extent to which the business systematically examines information to identify change, threats, risks and opportunities
15 Innovation	The extent to which the business's culture encourages and promotes innovation
16 Adaptive Capacity	The ability to identify change and uncertainty and to take swift and effective action

2

The 3C-3P Model for a Resilient Industrial Safety System

The Covid-19 pandemic is by no means the last time industry will be subject to disruption. It is increasingly clear that we live in a world where there are going to be “shocks” time and time again. The fact that we live in an interconnected and interdependent world means these shocks can originate from anywhere in the world, can take multiple forms and disrupt activities that may be seemingly unconnected. “Resilience” is not a question of our ability to recover if there is a shock but rather whenever there is a shock.

RESILIENCE AND INDUSTRIAL SAFETY

Resilience in the context of Industrial Safety, an immediate reaction is to define it as our ability to rebound "safely". We typically perceive "safe" here to refer to the absence of any untoward incident. However, it is important to recognize that the absence of an incident is only a lagging indicator. It does not necessarily credit the aspects that make the system safe in the first place and allow for it to be resilient.

These "aspects" that make the system safe and resilient ought to be included in any definition of the term safety. This way, the focus is not on the "absence" of incidents but rather the "presence" of these checks.

SAFETY AND THE 3-Cs

Three aspects are important and can lead to a better definition of safety. It can be explained by the 3-Cs:

Capacity

Undoubtedly, a primary requirement for any resilient system is the "capacity" to withstand a shock. This can be further broken down into two categories:

HARD CAPACITY

These pertain to the existence of adequate resources within the organization, ranging from financial resources and equipment to materials and methods. It is, however, not just about the existence of these resources but about the changes that each of these factors could be subject to in the event of a shock. Accidents and incidents are the result of some form of hazardous energy and the presence of **hard capacity** ensures that this energy is absorbed such that it does not result in a negative impact.

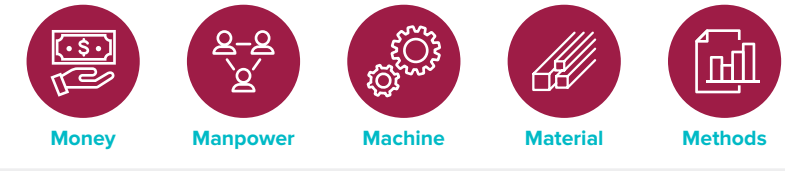


Figure 3: © Acuizen Technologies

SOFT CAPACITY

While the "hard" capacity may be essential for facilitating the recovery of any organization, the importance of "soft" capacity cannot be understated. Soft here refers to aspects such as the culture of the organization. This includes the extent of trust and mutual respect that has been established between the leadership and the operative teams. Situations, such as the current pandemic, have provided a great opportunity for leadership to display the needed compassion towards its workforce and build the trust needed for harmonious long-term relationships.

Yet another indicator of soft capacity is the extent to which the organization has created a "learning" environment among its employees. It is given that we live in a world that is increasingly volatile, uncertain, complex and ambiguous. Organizations need to take this unpredictability as their new normal and prepare its workforce to stay aligned with such a scenario. This means creating an environment where learning is dynamic and ongoing - another indicator of resiliency.

Organizations will need to make conscious efforts to measure and manage the "hard" and "soft" capacity that exist internally. There could be various means- including but not limited to- design reviews, simulation studies, table-top exercises and surveys. This is an evolving area of research and more needs to be done to come up with suitable indicators.

Controls

From our basic understanding of Risk Management, we know it as the existence of a hazard and a trigger- such as an exposure or an uncalled-for action that "could" result in an incident. It is important to assign a probability for this, since the mere presence of a hazard does not necessarily mean it will translate to an incident or accident. The accompanied consequence of this incident could be something minor or potentially major - leading to, e.g., a fatality. This is measured by severity.

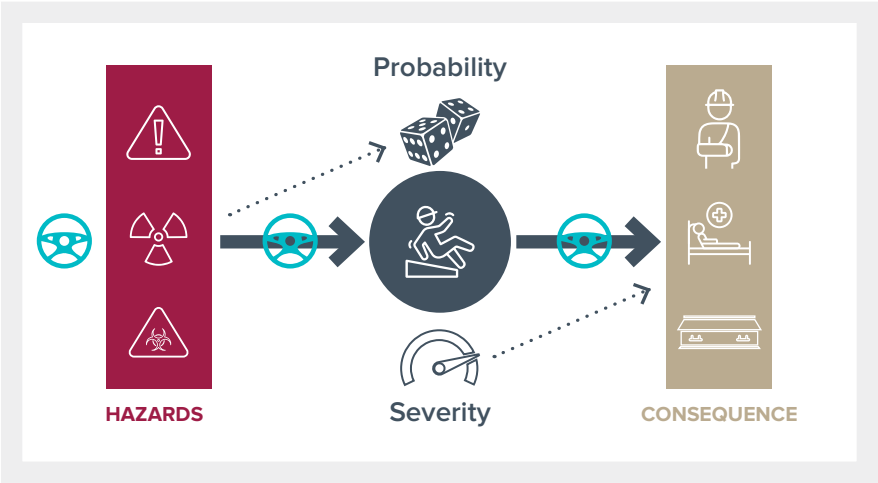


Figure 4: © Acuizen Technologies

We typically perceive risk by looking at events from a combination of probability and severity, which are measured through various quantitative and qualitative means.

While an ideal situation would be to completely eliminate hazards, the reality is that there are several practical considerations and unknowns that make it inevitable for us to live with some degree of risk. However, we can mitigate these effectively by introducing controls at various stages. These are the typical hierarchy of controls and could range from elimination, substitution, engineering, administration to personal protection equipment (PPE). The intent of these controls are to (ideally) eliminate the hazard, but at the very least, protect the individual from harm should the hazard manifest into a risk event.

Organizations need to recognize the need for and the presence of controls for all identified potential hazards.

Competency

At the center of any activity is the human being. It is this human knowledge and skill that facilitates the execution of an activity. Even with an automated activity, it is eventually the skill of the human that programs and designs the process that determines how well the activity is performed.

Training individuals to perform tasks- either formally or informally (in a classroom or otherwise) is definitely one of the first steps. However, one-time training, by itself, is no guarantee that an individual has the necessary expertise to perform the assigned task.

Expertise is built over time and through experience. For instance, a framework to articulate the various steps in an individual's working life is important for the employee to grow. Central to this, is of course, the need for the individual to be motivated and possess the right attitude and aptitude to continually re-skill and up-skill themselves.

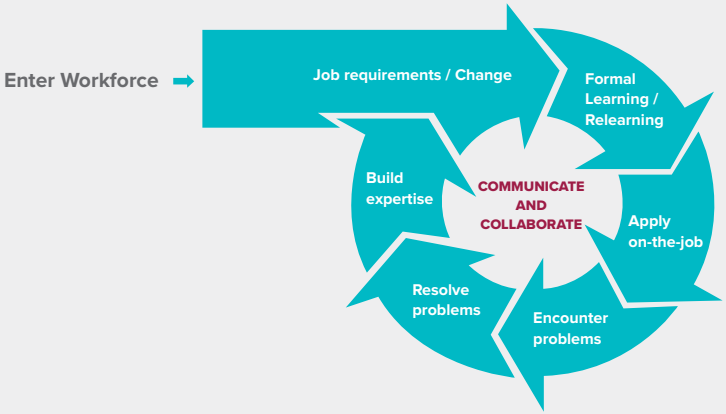


Figure 5: The AcuiZen Spiral of Expertise

RISK COMPETENCE

When specifically looking at "Competency" in the context of Safety, there is a need to measure "Risk Competency" across operational as well as on the individual level. The existence of Risk Competency is an indication of the extent to which the organization and its individuals are in a position to recognize risks and react to them.

There are algorithm-generated mechanisms that evaluate the risk competency of an individual and larger operational units within the organization. Based on the responses to a set of questions, the index scopes and intelligently classifies an individual's risk profile.

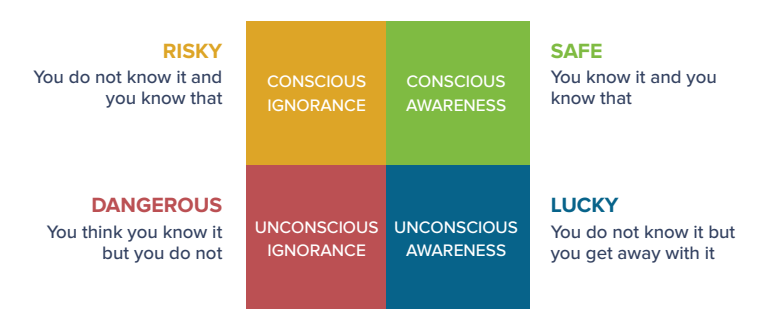
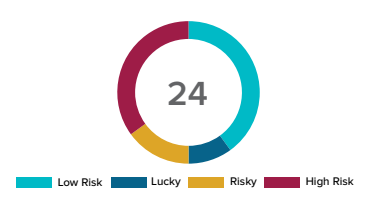


Figure 6: © Acuizen Technologies

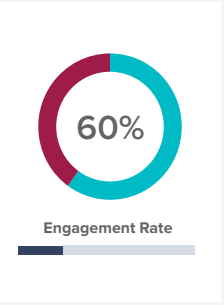


The algorithm computes a Risk Profile for the individual, the operational unit and the entire enterprise. An example is provided on the left.

REACTIVITATION

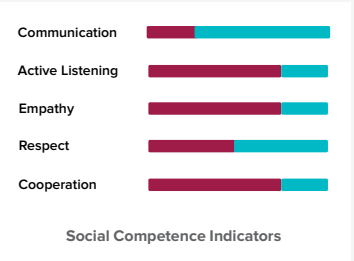
In a dynamic world with multiple sources of information (and misinformation), it is not very difficult for individuals to lose sight of some cardinal safety principles. This oversight could result in a situation where these turn out to be costly from a perspective of safety outcomes. The importance of reinforcing these basic principles time and again is a critical step in competency assurance.

For instance, AcuiZen has identified the importance of technology to measure the competency of an individual through how well they have internalized core safety concepts. The index also measures the engagement level of the individual, paving the way for human intervention where needed.



SOCIAL COMPETENCE

In a world where technology is increasingly taking over manual roles, the need for humans to develop more social skills as they interact with each other cannot be overstated. From a safety perspective, it is also important to have a mechanism for the early detection of psychosocial hazards that could impact the safety of people and processes. Serious incidents can occur when psychological stress and other factors contributing to the well-being of employees remain undetected.



OPERATIONALIZING THE 3-Cs

The 3Cs form the basis of a definition and the requirements for a resilient industrial safety system. How does one go about operationalizing these in practical terms? The belief of the Vision Zero Movement could be the basis under which the question can be answered.

Vision Zero Movement

The Vision Zero Movement is a global initiative launched in 2015. This ongoing movement calls for the commitment of everyone – employers, workers, unions and the government – to embrace a mindset that all injuries and ill-health incidents at work are preventable. A true commitment to the belief that zero harm is possible.

Vision Zero requires a concerted and holistic approach to ensure that all kinds of hazards are taken into consideration and actions taken to mitigate the risks. The nature of hazards may differ based on the context of each organization, however, broadly speaking, we could address these by looking at safety systems from the perspective of: People, Process and Product.

PEOPLE SAFETY

People Safety is addressed through Occupational Health and Safety (OHSH) - a multidisciplinary field concerning the safety, health and welfare of **people** in occupation. A good starting point would be for organizations to look at standards such as ISO 45001, occupational health and safety management and the supporting standard, ISO 45003, psychological health and safety management, that provides a framework for creating physically and mentally healthier, safer working conditions for people.

PROCESS SAFETY

Process safety is generally associated with facilities dealing with hazardous materials such as refineries, oil and gas production installations and chemical process facilities. Their focus is on prevention of fires, explosions or accidental chemical releases.

Process safety, in many cases, is a regulatory requirement and various jurisdictions have their own approach towards regulating process safety. An example would be the Process Safety Management (PSM) system- a regulation promulgated by the U.S. Occupational Safety and Health Administration (OSHA).

The general concepts of PSM may be designed for a facility dealing with hazardous materials. However, arguably, the basic concepts of PSM could be contextualized and applied to all kinds of industrial activities.

PRODUCT SAFETY

Product safety is a term used to describe policies designed to protect people from risks associated with thousands of consumer products they buy and use every day. In an industrial context, this would include equipment used as part of the processes.

Product safety, in most cases, is also regulated. As an example, in Europe, the Electrical Equipment (Safety) Regulations and Low Voltage Directive (LVD) 2014/35/EU applies to the majority of electrical equipment in use at home, the office or industry. The LVD / Electrical Equipment (Safety) Regulations require that electrical equipment can only be placed on the market if it does not endanger the safety of persons, property or domestic animals.

Assurance towards product safety is provided by compliance with applicable regulatory requirements and homologation / certification marks such as CE Mark, UKCA mark, BSI's Kitemark or the UL Safety Mark.

When looking at a resilient and safe system, there is a need to look at all these three broad areas of safety. Realistically, all of these areas have a certain degree of overlap and are not independent of each other. A visual representation of such an overlapping system would be as shown below.

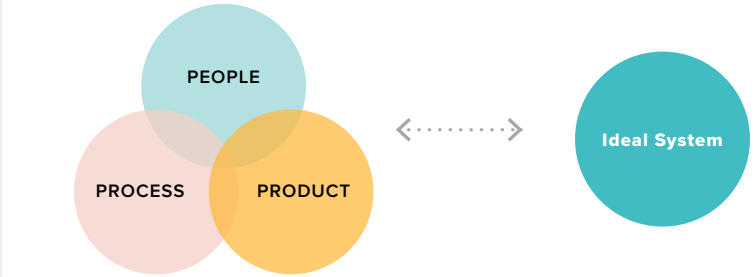


Figure 6: Visual representation of the three areas of safety of a resilient and safe system

The areas of overlap indicate those areas where there needs to be robust systems covering all three aspects (the central zone). There are also overlapping areas representing coverage of two aspects. In the other zones, it represents strength of one aspect but perhaps inadequate focus on the other two aspects.

An ideal system would be one in which all these three aspects are well integrated and comprehensively covered. They would therefore overlap as one circle (see Figure 6 above, on the right).

This represents a Zero and is a reminder that Vision Zero is possible when a holistic view is taken with focus on all the 3-Ps.

Given the dynamic nature of today's work, the quest for "Zero" is ongoing and there are bound to be new disruptions that expose vulnerabilities in either People or Process or Product safety. Organizations need to make a conscious effort to track these disruptions and patch up the vulnerabilities with suitable technical or administrative actions. This ought to be an ongoing and dynamic process.

In this context, one of the key determinants of a resilient organization would be the ability to rapidly communicate with stakeholders during such disruptions and to collaborate and respond to the scenario.

Safety Culture

3

Organizational culture is concerned with “individual and group values, attitudes, managerial practices, perceptions, competencies and patterns of activities” and therefore impacts every aspect of an organization, this is why culture comes under ‘People’ in the resilience framework. It is often referred to as the ‘way things are done here’ or the organization’s “DNA”.

The term 'Safety Culture' first came into prominence when it was cited as a primary cause of the Chernobyl disaster. The safety advisory group within the International Atomic Energy Agency defined it as:

"... the product of individual and group values, attitudes, competencies and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organization's health and safety programmes."

Whilst this definition was driven by industrial safety, if organizations simply focus on one aspect of culture, such as safety, they are missing the point. Organizational culture is concerned with "individual and group values, attitudes, managerial practices, perceptions, competencies and patterns of activities"[11] and therefore impacts every aspect of an organization, this is why culture comes under 'People' in the resilience framework. It is often referred to as the 'way things are done here' or the organization's "DNA".

There may be several identifiable cultures in an organization, typically associated with, for example, different departments, hierarchical layers, or roles. If one culture is risk adverse and another is highly risk tolerant, such as if often found between industrial safety teams and innovation teams, tensions arise. This is why leadership needs to drive the culture of the organization consistently across the whole organization.

What underpins the culture of an organization is trust. During the fifth episode of the webinar series 'Ensuring Industrial Safety and Security in times of COVID-19 and beyond'[12] John Marshall, from the World Ethical Data Foundation, noted that trust is always present but it can be misplaced, or abused – and we know that once trust is lost it is very hard to regain. Where trust is present it is very powerful and creates a culture where individuals are empowered and bring their very best to work – this brings significant benefits across the whole organization, enhancing:

- INDUSTRIAL SAFETY
- OCCUPATIONAL HEALTH AND SAFETY

11) ISO 45001:2018 Annex A
12) https://www.unido.org/ensuring-industrial-safety-and-security-times-covid-19-and-beyond

- LEGAL COMPLIANCE
- QUALITY
- PRODUCTIVITY
- JOB SATISFACTION AND MORALE
- RECRUITMENT AND RETENTION
- REPUTATION
- AND OF COURSE, ORGANIZATIONAL RESILIENCE

Creating a culture of trust does not happen overnight, it takes time and continual commitment, this is termed cultural maturity. Caroline Pike, a consultant at the International Atomic Energy used the analogy of a garden during the same webinar; to make a garden beautiful takes a lot of hard work and then you need to tend the garden on an ongoing basis otherwise the weeds will take over. Key aspects that need to be in place to create a positive culture include:

COLLABORATIVE, COMMUNICATIVE, EMOTIONALLY INTELLIGENT LEADERSHIP

In industrial safety this includes concepts around 'just', 'restorative' or 'learning' cultures where individuals are not blamed for failures, where these failures are the result of systemic organizational issues, often referred to as performance influencing factors (PIFs)[13] .The opposite of this is a culture of fear, where individuals are scared to report concerns for fear reprisals such as losing their job.

VISION AND VALUES

There needs to be a clear alignment between an organizations vision and values and its day-to-day operations. A powerful example of this in industrial safety and occupational health and safety, is "zero harm" or "zero accident". It may be a powerful statement of intent from leadership, yet how does that translate to the workforce and actual operations? What concrete changes are implemented on a day-to-day basis to improve safety? It is often a long-term aspiration of intent, rather than a practical series of tangible actions but this is not communicated clearly, so when day to day operational decisions conflict with "zero harm" aspiration, the message loses its authenticity and trust is broken. There is a then a mismatch between the vision and the practice, which erodes trust leading to disengagement and resentment.

INCLUSIVE CONSULTATION AND PARTICIPATION

Evidence clearly shows that where workers are involved in decision making about safety and health issues within the workplace, the safety and health performance of the organization is greatly improved. This is because workers are often best placed to identify the problems and solutions; and where they are involved, they feel respected and valued and, this in turn drives positive (safety) behaviours. In every respect, workers are a resource to harness and not a problem to control. The more the system is designed for achieving that, the greater the trust and the more effective it will be.

13) https://www.hse.gov.uk/humanfactors/topics/pifs.pdf

COMPETENCY AND RESOURCES

This is a critical part of organizational culture. If individuals don't have the rights skills and capabilities, then they will never be able to perform optimally. Likewise, if the resources are not in place in order to deliver the work, then sub-optimal performance and safety are the only predictable outcomes. In terms of industrial safety and occupational health and safety, understanding risk competency is essential. Do individuals (at all levels of the organization) understand risks and how to protect and mitigate those risks? Indeed, this is an essential component of an often forgotten, critical part of safety culture – "flexible culture". That is, the empowerment of competent and knowledgeable individuals to make decisions at the 'coal face' to achieve the objective of safety even if that requires an adaption of approach. That adaptive capacity is the point of intersection of safety culture and resilience. Harnessing that requires investment in the capacity of workers and leaders.

Whilst COVID-19 has brought many challenges, it has also created an opportunity to enhance trust in a way that is unprecedented. Prior to COVID-19 many organizations were reluctant to allow flexible or home working. Whilst plausible sounding business reasons were given (IT infrastructure; customer service), the real reason was simply that organizations did not trust their people. It was assumed that if people worked from home, they would not deliver. Research and direct evidence have shown this is simply not the case, in fact for many organizations productivity went up. Whilst flexible and home working is not an option for many roles, particularly in industrial safety; and not everyone who can potentially work from home wants to; organizations must re-evaluate their perceptions of trust in their workforce. Organizations that fail to do this will simply experience a rapid deterioration in culture and resilience plus a sharp exodus of talent. To help organizations create the right culture, BSI has developed the Prioritizing People Model©. The model maps out what best practice in creating a culture of trust really looks likes, one that will create the right conditions for individual fulfilment (well-being) and organizational resilience.

Industrial Safety Inspections

4

COVID-19 pandemic was also a challenge for industrial safety authorities. The legislation requires inspections of plants and enterprises to be carried out in order to check compliance with safety rules but 2020 showed that the legislation should be flexible in order to set a special control and supervision regime in case of unforeseen circumstances.

COVID-19 pandemic was also a challenge for industrial safety authorities. The legislation requires inspections of plants and enterprises to be carried out in order to check compliance with safety rules but 2020 showed that the legislation should be flexible in order to set a special control and supervision regime in case of unforeseen circumstances.

On the one hand it is obvious that the number of inspections should be reduced in order to minimize face-to-face contacts but on the other hand safety issues shouldn't be overlooked as they can lead to unpleasant consequences such as incidents and accidents.

That is why in such conditions it is crucial to define which hazardous facilities should be supervised by state authorities on site taking into account the hazards and risks and also compliance with the sanitary rules which oblige inspectors to mind social distancing and wear personal protection equipment such as medical masks and gloves.

For low hazard facilities, inspections could be carried out through audio or video communication and remote interaction tools. For this purpose, there should be a special information centre which accumulates document analyses and data coming from facilities' information systems.

Industrial safety authorities in such conditions as COVID-19 pandemic should take special measures to ensure the safe operation of enterprises and use different methods of remote interaction, minimizing the number of required documents, and extending the validity period of the previously released documents based on the results of previous inspections.

Safety Enhancing Technologies

Technology has been able to provide continued assurance for industrial safety and occupational health and safety, principally through the use of remote audits and inspections. The audits mainly cover document and record review, tours of premises, evidence of implementation and interviews with workers, using a range of digital tools.

Technology has been an important component in COVID-19 safe working practices to keep people safe: the ability to work from home, or attend training on-line has minimized the risks of infection; the use of touch free access and operations has limited transmission risk; and mobile apps have kept record of where we've been, allowing rapid 'track and trace'. Technology has also been able to provide continued assurance for industrial safety and occupational health and safety, principally through the use of remote audits and inspections.

Remote audit and immersive audits (and inspections) are approached in a similar way to on-site audits, but the auditor engages via technology. The audits cover document and record review, tours of premises, evidence of implementation, interviews with workers etc. using a range of digital tools including:

Live web streaming technology such as Webex, Zoom, MS Teams, GotoWebinar.

Live streaming paired with mobile technology such as a smartphone or tablet with video capabilities (e.g. WhatsApp, WeChat, Skype or Facetime).

Live streaming paired with smartphone, tablet, smartglass technology and video headsets.

As well as continuing to offer assurance, the use of immersive auditing has other benefits. It can reduce travel which has positive environmental impacts; it can allow more frequent and targeted interventions; allow more effective evaluation of non-compliance resolution; and allow blended expertise. Immersive audits also allow for greater audit or inspection participation providing broader transparency of nonconformity, best practice and overall observations.

There are also some challenges to remote auditing. Using 'live' digital tools is not always possible due to issues with connectivity. In these circumstances, other approaches can be used, such as video; a specific process can be videoed by someone on site and then the video can be sent by email (or other sharing tool) and reviewed separately. There are also situations where digital tools introduce risk such as in explosive atmospheres. In these scenarios, intrinsically safe technology can eliminate exposures in those environments and enables the immersive audit to continue. All parties participating in the audit also need to have the competency to use and deliver an immersive audit; and understand the impacts of mental fatigue – delivering audits remotely can be exhausting.

An additional challenge is that some standards, accreditation bodies and legislature are not keeping up with the appetite for remote auditing. A really good example of this was seen in the automotive sector, where the International Automotive Task Force (IATF) would not allow remote auditing for their quality management system certification, and it took several months of lobbying by industry and certification bodies to make allowances. A similar issue also occurred in the food sector with a reluctance to adopt a blended approach to audit and food inspections. In contrast the aerospace industry responded rapidly with the International Aerospace Quality Group (IAQG) producing clear guidance on remote auditing, allowing assurance to continue during the pandemic.

Immersive audits clearly have value but there is consensus that they cannot fully replace physical audits, particularly in industrial safety and occupational health and safety, so a blended approach will be required. What is now needed is a rapid and collaborative approach between all the stakeholders to agree what that blended model will look like. Up until now, we have simply lifted a traditional physical audit approach into a virtual one. Regulators, standards makers and accreditation bodies need to think differently; if they continue to measure the new blended approach by the metrics of the old approach they will get left behind as industry is racing ahead to sieze the benefits of digitization. Indeed, there is a real opportunity for these bodies to better utilize the digital footprint of organizations for their auditing and

enforcement activities, through tools such as continuous monitoring.

The area of remote and continuous monitoring systems is developing rapidly and shows great potential for both compliance and enforcement. This is an area that is particularly being explored within industrial safety. Industrial safety is already using a huge array of operational technology; what we are now seeing is this technology being linked with analytical and digital tools to create predictive risk models. The same is also being seen in construction and the use of building information modelling (BIM) for occupational health and safety. The ability to predict safety, quality or security incidents before they happen is clearly a powerful proposition, especially in industrial safety, where an incident can have tragic and long-lasting human and environmental implications. However, we need to take a precautionary approach to the opportunities that digitization and industry 4.0 is bringing. We cannot delegate the responsibility for safety to technology, especially as the technology is often flawed. If we look at artificial intelligence for example; the algorithms that underpin this powerful tool are written by humans and humans bring conscious and unconscious bias and the risks of human error that come from poor management of human performance indicators (see culture section), all of which can lead to the technology increasing risks, not reducing them.

It is also critical that we do not lose sight of basic safety issues. On the 4th of August 2020, the Middle East was rocked by an explosion which is considered one of the most powerful artificial non-nuclear explosions in history. A huge amount of ammonium nitrate stored at the port city of Beirut exploded, killing at least 210 people and destroying the port and a large part of the city. The investigation into the causes is ongoing but it is clear that this highly hazardous chemical had been stored without the correct safety measures for several years. The explosion was preceded by a fire which may be connected with ‘hot works’. Chemical storage and hot works are basic safety issues, and we need to ensure that we are effectively managing these basic safety risks, as the consequences can be tragic.

Finally, industry 4.0 has introduced a new safety issue which we ought to consider as a ‘basic’ safety issue within our risk management strategies– cybersecurity.

Cybersecurity

6

Risk management is at the heart of cybersecurity and industrial safety and yet these two functions rarely work together in a meaningful way, breaking down these barriers is essential to overall safety (cyber and industrial).

As mentioned, industrial safety has been using a huge array of operational technology in industrial control systems for many years, what is interesting however is that whilst safety risks have been identified, assessed and mitigated, the cybersecurity risks of these systems have often been neglected. This highlights one of the fundamental aspects of culture that was covered earlier – is there the right level of risk competency within an organization? It also highlights another area of culture that was also alluded to; the ability of cross-functional teams to work effectively together. Risk management is at the heart of cybersecurity and industrial safety and yet these two functions rarely work together in a meaningful way, breaking down these barriers is essential to overall safety (cyber and industrial).

A number of the barriers and issues that exists between industrial safety and cybersecurity have been brought into sharp focus by the recent cyber-attack on Florida's water treatment plant, which saw a bad actor try to poison the water supply[14].

NOT INSTALLING PATCHES AND SYSTEM UPDATES

Industrial control systems may have been in place for a number of years and there is often a nervousness in allowing information technology updates for fear of breaking critical operational (and sometimes safety) systems. Therefore, rather than install updates that are designed to improve cybersecurity, the updates simply aren't installed. This was the case in Florida which was running an outdated Window 7 operating system. It is therefore essential that updates are installed. If there are genuine operational or industrial safety issues with doing this, then then the safety teams (cyber/industrial) must work with the operational teams to identify effective alternatives, such as properly designed network segmentation and deploying a zero-trust architecture.

14) https://us-cert.cisa.gov/ncas/alerts/aa21-042a

ASSET TRACKING AND SEGMENTATION

Industrial controls systems have become byzantine. As a result there may not be a clear understanding of what assets actually exist, and from a cybersecurity point of view, if and how they are connected to each other, or the internet. This means that they may be much easier targets for bad actors to gain access to; and then because they are not segmented (separated from each other/the overall IT system), the bad actor can navigate through systems to a more attractive target.

In the Florida incident, the plant's computers appeared to be connected directly to the Internet without any firewall protection. Organizations therefore need to have an up-to-date asset registry and understand how they are connected to the internet and other IT infrastructure. These (and many) other best practises are addressed in the International Standard for Information Security Management, ISO 27001.

COMPETENCY AND SOCIAL ENGINEERING

It appears that the same password was used across all of the Florida water treatment plant computers and for remotely accessing a desktop sharing application. This is the password that the bad actor used to gain access to the system. Whilst there are many technological controls that can, and should, be used such as multiple-factor authentication and random password generators; more often than not, penetration into systems is by means of social engineering such as phishing, so employees, at all levels of the business need to be trained in understanding cybersecurity risks and what steps to take to eliminate or mitigate that risk.

THIRD PARTIES

Whilst not an identified issue in the Florida water treatment incident; another significant risk is that posed by third parties. Third parties (contractors, suppliers, customers) may have access to any number of systems. Original Equipment Manufacturer's (OEMs) will often mandate that they have to install updates and patches into their own equipment, and leave access points to do this easily. These access points can then be used by bad actors. The key is to have suitable access control mechanisms in place which will vary from system to system.

LEGISLATIVE CHANGES

Many jurisdictions have started to mandate cybersecurity requirements: from the European Union Agency for Cybersecurity (ENISA) NIS (network and information systems) directive, to the United States Department of Defense (DOD) requirements in the Cybersecurity Maturity Model Certification (CMMC) framework, to specific legislative requirements in California.

For example, the NIS requirements address critical sectors (energy, transport, water, health, digital infrastructure and finance sector) while addressing the need for member states to ensure they define their national strategy on the security of network and information systems. This addresses: cooperation methods between the public and private sectors, awareness raising, training and education, research and development plans related to NIS strategy as well as risk assessment plans.

The Cybersecurity Act introduces European Union (EU) wide rules for the cybersecurity certification of products, processes, and services. In addition, the Cybersecurity Act sets a new permanent mandate for ENISA, as well as more resources allocated to the Agency to enable it to fulfil its goals.

All these new requirements have implications on nearly every organization, especially manufacturing companies with their vast array of Industrial Control Systems which in many cases are (still) using IT technology from the 1980s – and therefore are extremely difficult – if not impossible – to upgrade to state-of-the art Information Security requirements. The long lifecycle of manufacturing facilities and the tendency to "not fix until broken" leads to an increased risk over time as known vulnerabilities will be exploited by more and more bad actors over time. After all from an operational perspective that control system is still working, so why would someone replace an apparently perfectly working piece of equipment with a new one? Indeed, a more proactive approach may be required where organisations are required to ensure, so far as reasonably practicable, the cybersecurity of their operations. This will allow organizations to proactively assess their cyber risk and put in place appropriate controls that fit their needs and circumstances. Such a performance based approach will strike the right balance between public safety, accountability and efficiency.

Many modern organizations rely on large supply chains and their digital connection with these. Ranging from shared design files, to order processing, inventory management to financial systems. Security in the digital supply chain is often ignored or at the very least not addressed with the seriousness required. While many organizations have recognised the supplier's impact on the quality of their product, many have ignored the supply chain impact on both their own information security as well as their business continuity resilience.

Conclusion and Outcome

As this handbook tries to demonstrate, there are sometimes simple solutions to complex problems. However, they all need to start and consistently execute these simple steps, which eventually results in a safer world and work environment which improves not only personal well-being, but eliminates costs associated from serious incidents. Cutting corners in safety may result in serious harm and eventually serious costs, often, ultimately being borne by public authorities.

It is therefore notable that this handbook has brought together an overview of where to start these simple steps and ensure a safe, secure and healthy work environment across sectors. There are various models to be considered and it depends on the actual circumstances on which will work best – the importance being that proactive safety management and adequate control measures are in place.

Over the course of the UNIDO project, Ensuring Industrial Safety and Security, the pool of experts and the network created to the cause - to improve safety and security globally - has managed to raise attention across the board. It has been emphasized that safety is not the sole responsibility of regulators, nor the company, nor the worker – it's important to see the dynamic nature of these relations and learn the necessary lessons for each. For this purpose the major Conference in May 2019 on Ensuring Industrial Safety and Security convened over 80 leading experts in Safety, representatives of Government, safety regulators and safety technology providers.

As a follow up and based on the extensive and positive feedback to the Conference, and in response to the COVID-19 pandemic, a series of webinars was quickly established to find solutions to a crisis that was yet unfolding and is still keeping hold in many countries. The response to COVID-19 challenged both advanced and already struggling safety regimes, highlighting how important it is to ensure long-term planning when it comes to safety.

Learning from experience has brought us to know the best practices in safety and how to avoid harmful incidents. Yet, we still see them happening in the world. Lockdowns and the pandemic has cut off vital information flow in some cases, but provided new opportunities, such as remote inspection and monitoring, which can lead to a better information flow to regulators and safety authorities. This could help build back safer and more securely. Moreover, the quick innovation shown in monitoring, inspection and assessment could continue to help inform optimisation processes, be it in industry or for regulators. The potential for collaboration has been demonstrated and this fruitful spirit should continue to be applied going forward.

In the near future, the topic and the collaboration established in the course of this project will continue to be placed in all international forums and any dialogue settings, to ensure that safety is improved globally and that our economies will become more resilient, tailored more to people and to realise the vision of Inclusive and Sustainable Industrial Development.

Further Reading

[1] Agnew, J., 2013. Building the Foundation for a Sustainable Safety Culture. Available at: https://www.ehstoday.com/ sustainable-safety-culture.

[2] Bauer, A., Wollherr, D. and Buss, M., 2008. Human-Robot Collaboration: A Survey. International Journal of Humanoid Robotics, 5, 47–66. 10.1142/ S0219843608001303

[3] Bridgestone, n.d. Safety, Industrial Hygiene. Available at: https://www.bridgestone.com/responsibilities/safety_health/index.html.

[4] British Safety Council, 2017. Five Star Occupational Health and Safety Audit. Available at: https://www.britsafe.org/media/3388/ma176-fsa-hs-spec-v6–2507.pdf

[5] Estimates of the Cancer Burden in Europe from Radioactive Fallout from the Chernobyl Accident. International Journal of Cancer. Cardis et al. (2006).

[6] Frick, K. and Zwetsloot, G.I.J.M., 2007. From Safety Management to Corporate Citizenship: An Overview of Approaches to Health Management. In: U. Johansson, G. Ahonen & R. Roslander (editors), Work Health and Management Control, Thomson Fakta, Stockholm,pp. 99–134.

[7] Haimes, Y.Y., 2009. Risk Modeling, Assessment, and Management. New York, NY: John Wiley & Sons, pp. 154–196.

[8] HSE (Health and Safety Executive), 2000. Safety Culture Maturity Model: Offshore Technology Report 2000/049. Keil Centre for the Health and Safety Executive.

[9] 2005. A Review of Safety Culture and Safety Climate Literature for the Development of the Safety Culture Inspection Toolkit. Research Report 367. Crown Publishers. Available at: http://www.hse.gov. uk/research/rrpdf/rr367.pdf.

[10] HSL (Health and Safety Laboratory), 2002. Safety Culture: A Review of the Literature. Crown Publishers. Available at: http://www.hse.gov.uk/research/hsl_pdf/2002/ hsl02-25.pdf

[11] ICSI (Institut pour une Culture de Securite Industrielle) Safety Culture Working Group, 2017. Safety Culture: From Understanding to Action. Issue 2018-01 of the Cahiers de la Securite Industrielle collection. Toulouse, France: ICSI. https://www.icsi-eu.org/documents/88/csi_1801-_ safety_culture_from_understanding_to_action.pdf

[12] ISO (International Organization for Standardization), n.d. ISO 45001 Occupational Health and Safety. Geneva: ISO. Available at: https://www.iso.org/iso-45001 -occupational-health-and-safety.html

[13] Building a Safety Culture: Improving Safety and Health Management in the Construction Industry SmartMarket Report. Centre for Construction Research & Training. Dodge Data & Analytics. DuPont, The DuPont™ Bradley Curve™. Available at: https://www.consultdss.com/bradley-curve/Jones et al. 2016.

[14] OSG (Occupational Safety Group), n.d. Six Tips to Help you Build a Positive Safety Culture. Available at: https://osg.ca/six-tips-to-help-you-build-a-positive -safety-culture-in-your-workplace/

[15] UN (United Nations), n.d. Global Indicator Framework for the Sustainable Development Goals and Targets of the 2030 Agenda for Sustainable Development. New York: United Nations. Available at: https://unstats.un.org/sdgs/indicators/Global%20Indicator%20Framework%20after%202019%20refinement_Eng.pdf

[16] University of Cambridge. 2019a. Managing Cyber Risk in the Fourth Industrial Revolution: Characterizing Cyber Threats, Vulnerabilities and Potential Losses.

[17] 2019b. OK Computer? The Safety and Security Dimension of Industry 4.0.

[18] 2019c. Safety Assurance of Autonomy to Support the Fourth Industrial Revolution.

References

[1] Hämäläinen, P., Takala, J. and Boon Kiat, T., 2017. Global Estimates of Occupational Accidents and Work-related Illnesses 2017. XXI World Congress on Safety and Health at Work. Singapore: Workplace Safety and Health Institute. Available at: http://www.icohweb. org/site/images/news/pdf/Report%20Global%20 Estimates%20of%20Occupational%20Accidents%20 and%20Work-related%20Illnesses%202017%20rev1.pdf.

[2] ILO (International Labour Organization), 2019. Safety and Health at the Heart of the Future of Work: Building on 100 Years of Experience. Geneva: ILO, p. 3. Available at: https://www.ilo.org/wcmsp5/ groups/public/---dgreports/---

[3] United Nations Industrial Development Organization, 2019. International Conference on Ensuring Industrial Safety: The Role of Government, Regulations, Standards and New Technologies. Vienna.

www.unido.org

The project is funded by the
Russian Federation

UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

Vienna International Centre · P.O. Box 300 · 1400 Vienna · Austria
Telephone (+43-1) 26026-0 · unido@unido.org
www.unido.org