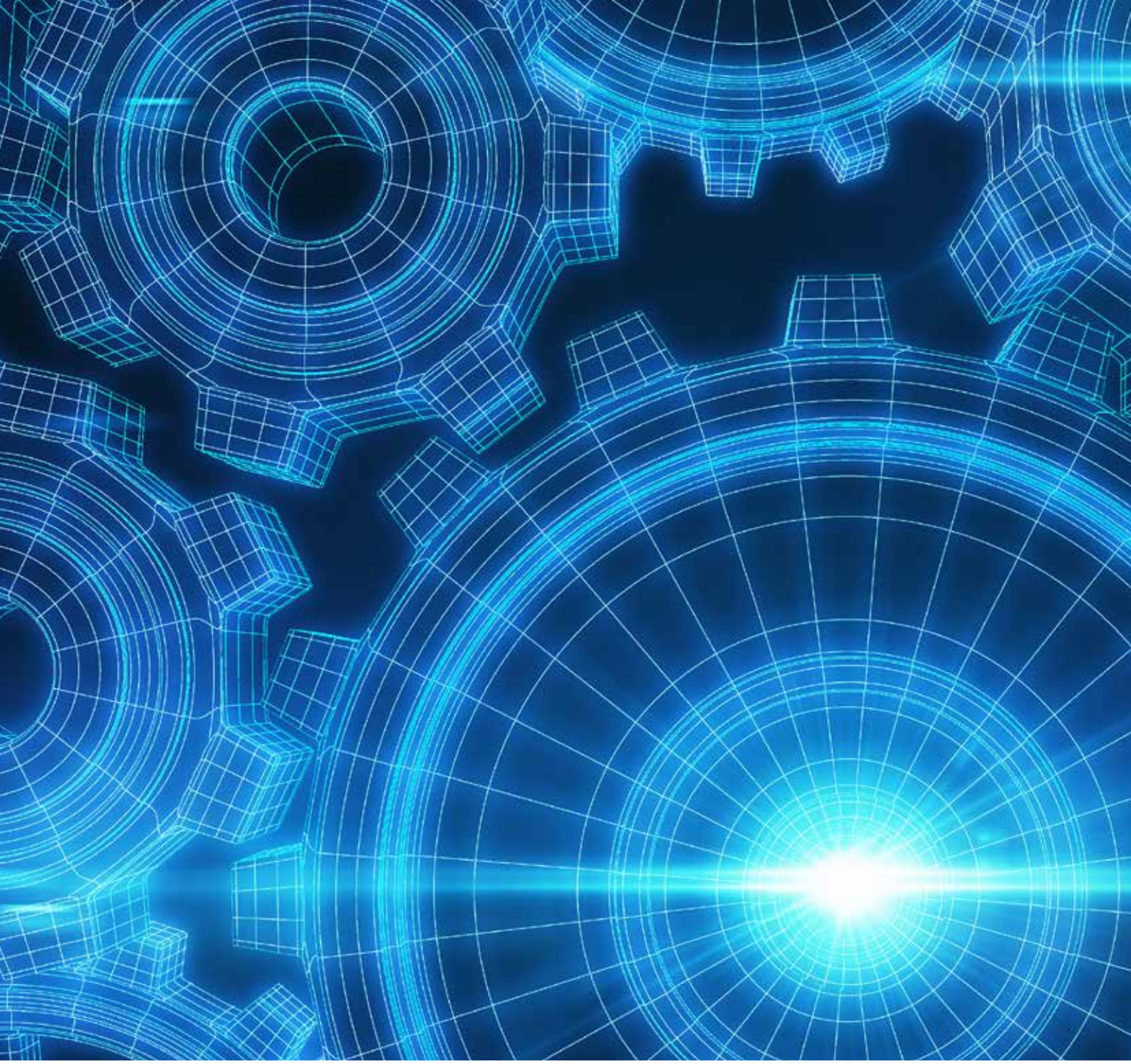


White Paper

Safety in the future

Executive summary

As more and more machines are integrated into the factory automation and logistic automation, mobility and healthcare processes, the need to ensure safe procedures for people working with machines is increasing. The Internet of Things (IoT), big data, advanced robotics and especially artificial intelligence (AI) are all transforming the connection between electrotechnical systems and people. While AI can dramatically improve efficiency in the workplace and can augment the capacity of human performance, the question arises: will machines become super-intelligent, leading humans eventually to lose control? Though the probability of such a scenario with possible additional risks is subject to debate, we do know that unforeseen consequences for humans always emerge when new technology is introduced. Consequently, more than at any moment in the past, it is critical to ensure that human safety be placed at the centre of the new human-machine relationship.

According to recent estimates released by the International Labour Organization (ILO), 2,78 million workers die each year from occupational accidents and work-related diseases. Millions more are injured on the job. Aside from the economic costs engendered by such factors, a further intangible human toll exists in terms of the immeasurable human suffering produced. Such outcomes are both tragic and regrettable, because, as research and practice over the past century have repeatedly demonstrated, the casualties involved are largely preventable.

As humans continue to play a major role in causing workplace accidents, whether at the design and planning stages or during execution of the work, any efforts to improve safety in human-machine collaboration must focus specifically on human/worker behaviour. And while the future can hardly be predicted with precision, technological, societal and legislative megatrends will clearly impact the future of work and safety.

Using real life examples, this white paper addresses safety in the future by referencing current social trends and initiatives such as the UN Sustainable Development Goals and various real-life examples of projects, works and companies that are pioneering innovative safety solutions for the future. Common to such solutions is the underlying realization that the concept of safety will be delivered in an integrated system in which humans, machines and the environment collaborate. The paper also introduces a collaborative framework called the *tripartite system for safety*. This concept facilitates a systematic approach to examining key elements of safety in the future.

Bringing the ambitious visions connected with the tripartite system for safety to fruition will require significant efforts in standardization, with a view, for example, to mitigate some of the most pressing challenges related to decision-making between machines and humans, as well as expanding holistic approaches to safety. Thus the white paper presents an anticipated safety-in-the-future framework to address those needs.

The white paper concludes by formulating recommendations both of a general nature as well as specifically addressed to the IEC and its committees. The principal recommendations proposed include:

- Social goals should be established that aim to achieve both safety and efficiency, by shifting from a safety model based on separation of

man and machine to one in which safety is achieved through man-machine cooperation.

- Consideration should be given to the possibility that humans may not be the smartest component in a new human-machine collaborative system. A new concept of safety should be elaborated through the development of technology and the reconfiguration of man's place in the system.
- Measuring safety outcomes has formed a key part of safety management systems for many years, with a focus on incident statistics. However, a more forward-looking, proactive approach could be adopted by introducing “leading” indicators into the calculation.
- Standards bodies need to expand and deepen their holistic approach to safety. This will require incorporating not only traditional technical expertise but also insights gathered in the fields of safety psychology, sociology and human behaviour. In other words, it is recommended that in the development of future safety standards, clear attention be paid to non-technical factors.

Acknowledgments

This white paper was developed by the IEC Market Strategy Board (MSB) safety in the future project team, directed by Dr Kazuhiko Tsutsumi, MSB Convenor, Mitsubishi Electric Corporation, with major contributions from the lead project partner, Dr Coen van Gulijk, TNO, the Netherlands.

The management team is listed below, followed by the project team in alphabetical order:

Dr Kazuhiko Tsutsumi, Mitsubishi Electric Corporation, Project Director, IEC Vice President, MSB Convenor

Dr Coen van Gulijk, TNO, Lead Project Partner

Dr Atsushi Miyoshi, Mitsubishi Electric Corporation, Project Manager

Mr Dragi Trifunovich, Mitsubishi Electric Corporation, Project Manager

Mr Masao Dohi, IDEC, Project Manager

Mr Shawn Paulsen, CSA Group, IEC Vice President, CAB Chair

Dr Tommi Alanko, Finnish Institute of Occupational Health

Mr Tadashi Ezaki, Sony, SMB member

Dr Toshihiro Fujita, IGSAP

Mrs Jillian Hamilton, Manage Damage

Ms Rieko Hojo, JNIOSH

Mr Yun Chao Hu, Huawei

Mr Philippe Juhel, Schneider Electric, ACOS Chair

Dr Jens Jühling, BG ETEM

Mr Toshiyuki Kajiya, IGSAP, CAB Alternate

Mr Hiroo Kanamaru, Mitsubishi Electric

Dr Nobuyasu Kanekawa, Hitachi Ltd

Mr Pete Kines, National Research Centre for the Working Environment (NRCWE) (DEN)

Ms Tomoko Konya, NARO

Mr. Peter J Lanctot, IEC, MSB Secretary

Mr Vimal Mahendru, Legrand-India, SMB member

Mr Steve Margis, UL

Mr Hirokazu Nakano, METI

Mr Alan Sellers, Dyson Technology Ltd

Mr Shimizu Shoken, JNIOSH

Ms Thu Thủy Tran, NARO

Mr Bernd Treichel, ISSA

Mr Andy (Di) Wang, Huawei

Mr Joeri Willemsen, TNO

Mr Tsutomu Yamada, Hitachi Ltd

Dr Gerard Zwetsloot, TNO, Gerard Zwetsloot Research & Consultancy

Table of contents

Executive summary 3

List of abbreviations 9

Glossary 13

Section 1 Safety in the future: challenges, opportunities and the role of standardization 15

1.1 Scope 15

1.2 Workplace casualties and electricity 16

1.3 Safety as a concept, system and paradigm 16

1.3.1 Socioeconomic factors 17

1.3.2 Safety frameworks 19

1.3.3 Safety outcomes 19

1.4 Behaviour-based safety – humans at the centre 20

1.4.1 Safety risk management: risk analysis and assessment 20

1.5 IEC role in ensuring safety 22

1.6 Implications for standardization 23

Section 2 Trends, initiatives and challenges impacting safety in the future 25

2.1 Introduction 25

2.2 Advanced technologies opening new safety perspectives 25

2.3 Societal and legislative trends 28

2.4 Additional trends, concepts and options 29

2.4.1 Innovating to zero 29

2.4.2 Collaborative safety 31

2.4.3 Prescriptive legislation and the standardization/conformity assessment option 33

2.4.4 Megatrends and their impact on work 34

2.5 Risk management, risk governance and standardization challenges 35

2.6 Standards challenges 38

Section 3 The tripartite system for safety 41

3.1 Humans, machines and the work environment 41

3.2 Information flows in the tripartite system 42

3.3 System boundaries and linkages in the tripartite system 43

3.4 Levels of sophistication in the tripartite system 44
3.5 Key enabling technologies of tripartite systems 45
3.5.1 IoE 45
3.5.2 Ontology and semantic interoperability 46
3.5.3 Assurance algorithms 48
3.6 New technologies for tripartite systems 50
3.6.1 Digital twins 50
3.6.2 Real-time collision avoidance 51
3.6.3 AI-assisted behavioural analysis 52
3.7 Technological necessity: cyber security 54
3.8 Implications of standardization and conformity assessment for the tripartite model 54

Section 4 Application areas of the tripartite system 57
4.1 Human-machine collaboration in manufacturing 57
4.2 Intelligent machines in construction 58
4.3 Intelligent networks in the environment facilitating farming safety 59
4.4 Electrical power distribution systems with automated safety features 61
4.5 Smart monitoring maintenance of power distribution networks 61
4.6 Public safety in cities 62
4.7 Access to electricity 64
4.8 Implications for standardization 65

Section 5 Conclusions 67
5.1 Working with machines that are smarter than humans 67
5.2 Putting humans first 67
5.3 What are the challenges for ensuring safety in the future? 67
5.3.1 A pillar of trust for social responsibility 67
5.3.2 Standardization toward an ecosystem of intelligent systems 68
5.4 Conformity assessment with intelligent agents 69
5.5 Achieving global safety excellence 70

Section 6 Recommendations 71
6.1 Recommendations to governmental regulators, industry drivers and standards bodies 71
6.2 Recommendations to the IEC community 72

Bibliography 73

List of abbreviations

Technical and scientific terms

AGV	automated guided vehicle
AI	artificial intelligence
API	application programming interface
ATEX	equipment for potentially explosive atmospheres
BBS	behaviour-based safety
BIS	building information system
BSP	basic safety publication (IEC)
CA	conformity assessment
CAD	computer-aided design
CAM	computer-aided manufacturing
CCPA	California Consumer Privacy Act
CDD	common data dictionary (IEC)
CSL	collaborative safety level
DC	direct current
DL	deep learning
EMI	electromagnetic interference
GDP	gross domestic product
GDPR	General Data Protection Regulation
GPS	global positioning system
GSP	group safety publication (IEC)
HPC	high performance computing
HV	hybrid vehicle
IC	information communication
ICS	industrial control system
ICT	information and communication technology
IoE	Internet of Everything
IoH	Internet of Humans
IoT	Internet of Things

ISMS	information security management system
JTC	joint technical committee
LGPD	General Data Protection (*Lei Geral de Proteção de Dados* in Portuguese)
LTE	long term evolution
LVDC	low voltage direct current
OSH	occupational safety and health
PSS	product safety standard (IEC)
PV	photovoltaic
RAMS	reliability, availability, maintainability and safety
RFID	radio frequency identification
SBA	Safety Basic Assessor (qualification)
SC	subcommittee (IEC)
SCADA	supervisory control and data acquisition
SDG	sustainable development goal (UN)
SEG	standardization evaluation group (IEC)
SELV	safety extra-low voltage
TC	technical committee (IEC)
UAV	unmanned aerial vehicle
UWB	ultra-wideband

Organizations, institutions and companies

ACOS	Advisory Committee on safety (IEC)
CAB	Conformity Assessment Board (IEC)
CASCO	Committee on Conformity Assessment (ISO)
EU-OSHA	European Agency for Safety and Health at Work
IGSAP	Institute of Global Safety Promotion
ILO	International Labour Organization
IRGC	International Risk Governance Council
ISSA	International Social Security Association
JISHA	Japanese Industrial Safety and Health Association

MSB	Market Strategy Board (IEC)
NARO	National Agriculture and Food Research Organization (Japan)
NECA	Nippon Electric Control Equipment Industries Association
SMB	Standardization Management Board (IEC)
WHO	World Health Organization

Glossary

autonomous mobility

system that partners in-vehicle artificial intelligence (AI) with remote human support to help driverless autonomous vehicles make decisions in unpredictable situations

basic safety publication
BSP

IEC publication focussing on a specific safety-related matter, applicable to many electrotechnical products

behaviour-based safety
BBS

process creating a safety partnership between management and employees that continually focuses the attention and actions of workers on their own and others' daily safety behaviour

circular economy

economic system aimed at eliminating waste and the continual use of resources

digital transformation

use of new, fast and frequently changing digital technology to solve problems by transforming previously non-digital or manual processes to digital processes

NOTE An example of digital transformation is cloud computing.

digital twin

digital replica of a living or non-living physical entity

entanglement

physical phenomenon that occurs when a pair or group of particles is generated, interacts or shares spatial proximity in such a way that the quantum state of each particle of the pair or group cannot be described independently of the state of the others

group safety publication
GSP

IEC publication covering all safety aspects of a specific group of products within the scope of two or more product technical committees

International Labour Organization
ILO

United Nations agency whose mandate is to advance social and economic justice through setting international labour standards

Internet of Things
IoT

infrastructure of interconnected entities, people, systems, information resources and services which processes and reacts to information from the physical and virtual worlds

ISO/IEC Guide 51

joint ISO/IEC publication providing requirements and recommendations to the drafters of standards for the inclusion of safety aspects in standards

NOTE ISO/IEC Guide 51 is applicable to any safety aspect related to people, property or the environment, or to a combination of these.

superposition

feature of a quantum system whereby the system exists in several separate quantum states simultaneously

NOTE Superposition is a fundamental principle of quantum mechanics.

UN Sustainable Development Goals
SDGs

collection of 17 global goals designed by the United Nations to serve as a "blueprint to achieve a better and more sustainable future for all"

NOTE The SDGs, elaborated in 2015 by the United Nations General Assembly and intended to be achieved by the year 2030, form part of UN Resolution 70/1, *Transforming our world: the 2030 Agenda for Sustainable Development*.

Wi-Fi 6

next generation standard in Wi-Fi technology

NOTE Wi-Fi 6 is also known as “AX Wi-Fi" or "802.11ax Wi-Fi”.

Section 1

Safety in the future: challenges, opportunities and the role of standardization

1.1 Scope

By 2030 almost every electrotechnical system in the world will be equipped with some degree of digital intelligence (i.e. smart objects, machinery and devices). Yet there seems to be relatively little understanding of how intelligent systems affect safety, health, and human well-being. Requirements concerning the safety of workplace machinery have changed rapidly with the increasing use of automation. Innovative technology has enabled protective devices to be integrated into the work process, and as a result, such devices no longer pose a hindrance for operators but instead contribute to increased productivity.

Nevertheless, new and complex safety requirements have emerged with the vast expansion of intelligent systems. At the same time, technological developments and digital advances are providing the tools for innovative responses to such challenges.

This white paper focuses on developments affecting safety in electrotechnical systems but also considers the wider socio-economic environment in which such developments are taking place. It outlines the challenges involved in integrating digital devices and robotics into the workplace and considers the particular needs posed by increased human-machine cooperation. However, beyond this, the paper examines trends affecting societal values, cultural differences, the specifics of workplace safety and trends in regulation. The wider relationship of such factors to the important framework of the United Nations Sustainable Development Goals (SDGs) [1] is also considered, as well as the contribution of standardization to the concrete realization of such goals as regards the safety, health and well-being of workers in the future.

The aim of this white paper is to exert a positive impact on the role of global standards developing organizations in designing a version of human-centred intelligent electrotechnical systems focused on promoting the health and safety of the public operating within the new technological environments. Responsibility for ensuring such safety is incumbent on a variety of stakeholders, including policymakers and regulators, industry partners and insurers, academic experts and research organizations, the UN and non-governmental organizations, and a variety of global foundations and development agencies.

As a prelude to presenting a discussion of trends, initiatives and challenges impacting safety in the future (see Section 2), identifying key elements and approaches aimed at addressing those challenges (see Section 3), and defining areas for the application of the tripartite framework elaborated in Section 4, this section examines current workplace casualties due to electricity, socio-economic factors and existing safety frameworks, as well as the need to place human safety at the centre of efforts to ensure the safe functioning of human-machine cooperation. The section concludes with an outline of the IEC role in such efforts and the implications for standardization.

1.2 Workplace casualties and electricity

According to recent estimates released by the International Labour Organization (ILO), 2,78 million workers die each year from occupational accidents and work-related diseases [2]. Millions more are injured on the job. Aside from the economic costs engendered by such factors, a further intangible human toll exists in terms of the immeasurable human suffering produced. Such results are both tragic and regrettable, because, as research and practice over the past century have repeatedly demonstrated, the casualties involved are largely preventable. Furthermore, the loss of morale, damage to camaraderie and feelings of helplessness that set in following an accident also impact economic performance. No type of development, measured on any dimension or using any set of metrics, can justify this kind of loss of life and loss in quality of life.

With electricity being intrinsically unsafe, it comes as no surprise that casualties occur when people work with it. Yet determining the exact number of such accidents globally and identifying how many of these accidents are fatal, as well as the specific cause(s) of death or injury involved, is no easy task. As a rule, countries around the world maintain mandatory workplace casualty registration systems. Unfortunately, workplace casualties are recorded differently in various parts of the world. But even without considering the intricacies of accident reporting systems, we can still gain some insight into the proportion of electrical accidents by determining their relative frequencies. This white paper adheres to two kinds of reporting when discussing human-machine injury and death frequency rates: 1) workplace and 2) non-workplace reporting.

Categories of reported accidents include:

- consumer product use-related incidents
- accidents related to product design defects
- production defects and accidents at work not related to product defects

Standard definitions of an electrical incident or accident relate to direct electric currents and an injury, incident or accident. The electrotechnical environment has changed. Today, computer-related, IoT-connected and numerous other industrial plant items rely much more than before on electrical and cyber methods for power, operation and automation. The exact definition of an electrotechnical incident/accident should be reconsidered, and metrics should be designed to measure such events. In most developed countries the percentage of fatalities due to accidents with electrical systems ranges between 1-4% (Japan [3]), and 3,5% (New Zealand [4]); e.g. in Australia [5] and the United Kingdom [6] the figure is 2,7%, in the United States [7], 3,0%.

It is important to remember that the above numbers are only indicative, as they include neither non-workplace incidents nor non-fatal accidents and only cover economically developed countries, whereas fatal accident rates in developing countries are assumed to be generally much higher. Yet even these numbers show a relatively small but nevertheless persistent presence of electricity-related workplace fatalities of at least 370 000 per year. One can easily imagine that the real number of deaths is substantially higher.

1.3 Safety as a concept, system and paradigm

Safety as a concept encompasses the behaviour of people in the presence of hazards, modified or influenced by socioeconomic factors; safety frameworks, including regulations, standards, and industry best practices; and individual or specific behaviours, interventions and tactics. This system results in specific outcomes that can be measured in frequency of loss, injury or death and near-miss incidents, see Figure 1-1.

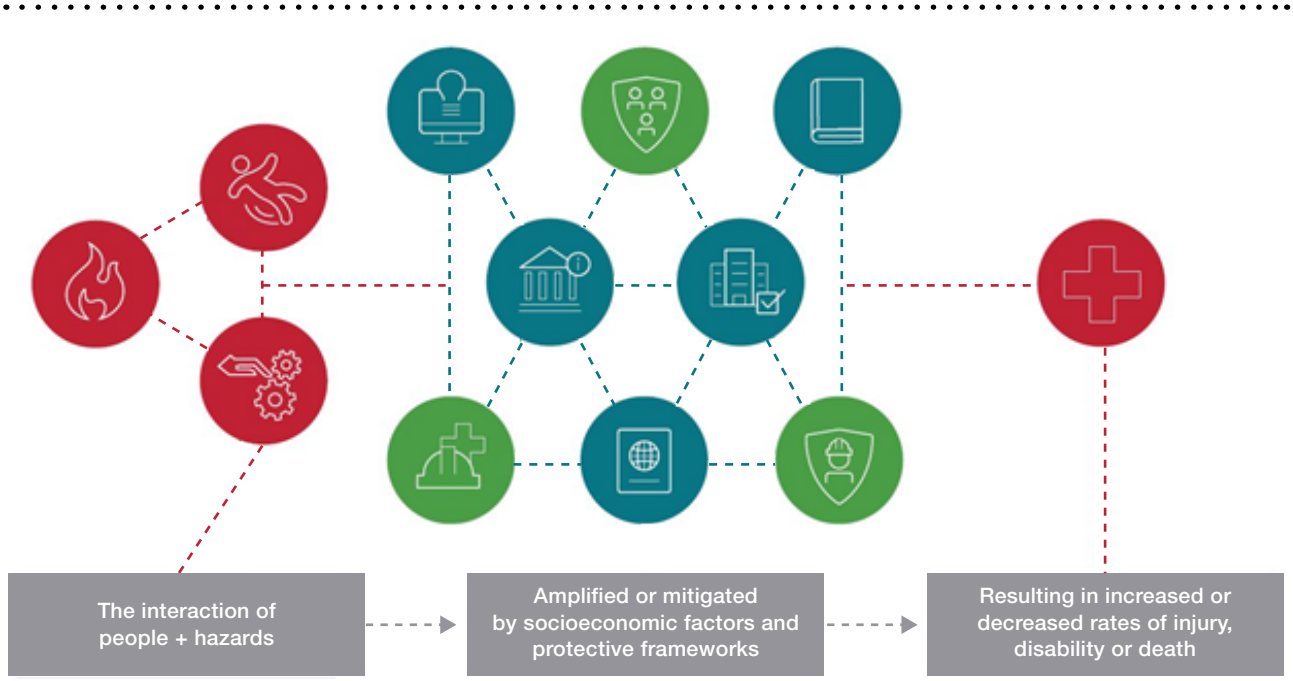


Figure 1-1 | System of safety

Our conception of hazards is also expanding to include chronic hazards, such as psychological stresses and exposure to low levels of chemicals, which can manifest as reduced health and well-being.

Socioeconomic conditions, safety frameworks and specific interventions all interact to enhance or reduce safety. At the broadest level, societal and socioeconomic forces materialize slowly, such that their influence on safety may be difficult to isolate from other factors. However, such forces work powerful effects over time and cannot be ignored. Elaborating sustainable development goals and increasing the efficacy of safety standards affords positive conditions for the enhancement of safety and should be integrated in the overall safety measurement paradigm.

1.3.1 Socioeconomic factors

While most societies aspire to provide a safe and secure environment for their people, the availability of resources is always a limiting factor in that effort. A country's gross domestic product (GDP) per person is one measure of the resources available to that society. Simply stated, GDP provides a measure of the financial resources that can potentially be allocated to address safety and other societal needs.

In developed economies, a greater amount of "discretionary" resources is potentially available for allocation to specific safety programmes, including safer infrastructures, governmental spending on consumer protection, and similar measures. In developing countries where financial resources are limited, such resources are more likely to be allocated toward efforts to provide basic services, build critical infrastructure, or shape and expand the national economy. Addressing these fundamental issues may leave fewer resources available for grappling specifically with safety concerns. However, the good news is that addressing basic services and infrastructure is correlated with improvements in safety.

The most influential structure in almost every society is its national government. As a provider of essential services, the originator of regulations and policies, and one of the most significant sources of economic resources, a government has a direct impact on the day-to-day lives of people it governs and can greatly influence their future.

Several organizations that rate the overall effectiveness of governments also assess the role that governments play in promoting systems of safety. Societies with higher levels of government effectiveness generally exhibit a greater ability to develop and enact policies that can positively influence safety outcomes. In countries where government effectiveness is low, this ability is often significantly diminished or impaired.

The UN SDGs encourage governments and all stakeholders to pace themselves and aspire to providing the key essentials for development. As technology and machines constitute essential tools of development, it is obvious that SDG targets will require the harnessing of technology. Such development necessitates a focus on the safety of human beings. In that sense, considering SDGs in the technological framework of the safety of the human-machine interface is a natural and essential requirement.

IEC International Standards and IEC Conformity Assessment (CA) Systems contribute actively to the fulfilment of all of the 17 SDGs. They provide a foundation allowing countries and industries to adopt or build sustainable technologies and apply best practices, and they form the basis for innovation as well as quality and risk management.

While almost all of the SDGs incorporate safety aspects and objectives, of particular relevance to the issues addressed in this white paper are SDG 8: Decent work and economic growth, and SDG 3: Good health and well-being. Among the component targets of SDG 8, the safety of machinery and tools, electrical safety, electromagnetic interference (EMI) protection and overall risk management particularly affect the security and safe operating conditions of workers in human-machine collaborative environments. As will be demonstrated later in this paper, aspects of the medical device technology addressed by IEC technical committees in the context of SDG 3, are increasingly being integrated into state-of-the-art workplace safety solutions.

Similarly, right to education is widely seen as a universal human right. This is also clearly enshrined in the UN framework as SDG 4: Quality education. However, access to education varies widely between individual societies around the world. In the system of safety, researchers have shown there is a direct correlation between levels of safety and widespread access to basic education. Basic education provides people with the means to better understand the environments in which they live and work and gives them access to vital information that they can use to influence the people and systems that affect them. Additionally, many education systems have incorporated safety education programmes, providing more in-depth information about specific hazards such as fire and drowning.

Thus, a prudent approach involves considering the safety of workplaces and environments. This goes beyond mere use of electricity. Safety and health at work can be of crucial importance to sustainable development. Investment in occupational safety and health (OSH) can help contribute to the achievement of key elements of the UN SDG agenda.

Technology is advancing at an ever-increasing rate across the world. Innovations in computing, communications, materials science and engineering are contributing to individual and collective progress. For the most part, advances in technology result in better products and systems for consumers, reduced levels of personal and environmental risk, and improvements in standards of living. Furthermore, technology can be leveraged to uncover and assess hazards, communicate

important safety information more broadly, and coordinate programmes and policies for more effective outcomes, making it an important influencing force for safety.

1.3.2 Safety frameworks

Safety frameworks are policies and practices designed to leverage both institutions and resources in achieving specific goals related to injury prevention. Some of the policy areas having a direct impact on safety outcomes include road safety, occupational health and safety, consumer protections, and legal codes and standards.

Road traffic accidents constitute the single largest contributor to injuries, with an estimated 1,2 million deaths occurring globally in 2017 alone. With rapid urbanization and a growing middle class in many developing economies, road safety has become a key area of focus for the World Health Organization (WHO) and many civil society organizations during the past decade. Instead of simply blaming individual drivers for accidents, most governments and organizations now embrace a safety system approach that recognizes the value of transportation planning, road infrastructure, vehicle safety and road use, including by pedestrians.

Most adults spend approximately one-third of their time on the job, and many occupations expose employees to significant safety and health hazards. Work-related risks vary greatly according to occupation, as do the regulations and standards intended to protect workers from those risks. The ILO has developed a series of international conventions and guidelines to provide minimum levels of occupational safety and health, but the adoption of these ILO conventions is voluntary and at the discretion of national governments. An assessment of the presence of ILO OSH guidance in each country can be used as a measure of the relative strength of basic worker safety around the world.

All members of a society are consumers of goods and services. The use of or exposure to unsafe consumer goods can result in a variety of injuries, from lacerations to burns to poisoning. Protecting people from unsafe products is a responsibility of corporations, civil society, and governments. Protective measures include requirements for safe design and manufacturing, inspection and control of imported products, removal of unsafe products from the marketplace, and many other safety measures. The relative strength of these laws, regulations and policies will have a significant influence on the overall safety system within a country.

Codes and standards are a means of providing manufacturers, installers, architects, builders and operators with concrete requirements, guidance and best practices to address safety issues related to products and infrastructure. In most countries, construction codes set the minimum requirements for the safety and security of buildings. Product safety standards help to ensure that products and systems are designed to minimize risk, are manufactured to accepted norms, and can be safely used by the intended audience. Thus, a strong system of codes and standards helps to protect people from unsafe products and environments. Standards and conformity assessment form a key part of the safety framework layer of systems of safety. They both flow from regulation (mandatory schemes) and inform regulation (voluntary schemes).

1.3.3 Safety outcomes

Measuring safety outcomes has been a key component of safety management systems for many years. Focused primarily on incident statistics, more recently such measurement has been augmented to include “leading indicators” of safety performance, with a view to adopting a more preventative approach. In order to gain a comprehensive picture of safety, each level of the safety ecosystem should be measured to

understand the various influences and externalities affecting the environment as well as the specific components of the system to be managed. The complex, multi-tiered nature of contemporary systems of safety requires a novel approach to their measurement. A composite indicator comprising a structured combination of individual measures of the system constitutes one method of creating a dynamic, nuanced and adaptable measurement method that can be applied to safety.

1.4 Behaviour-based safety – humans at the centre

According to various studies, humans continue to play a major role in causing workplace accidents, whether at the design and planning stages or during execution of the work. Overall, the major contribution of human error is estimated to be between 76% and 96% [8]. Companies usually try to influence work behaviour related to safety through a mixture of education and enforcement. However, to date no study has managed to confirm the success of these approaches in producing lasting change in safety-related behaviours or accident rates. As a result, any efforts to improve safety in human-machine collaboration must focus specifically on human behaviour, including that of both managers and workers. This is where behaviour analysis adds significant value, particularly the approach entitled "behaviour-based safety" (BBS).

Behaviour analysis dates back almost a century to attempts by scientists in the 1930s to establish a set of natural laws of behaviour based on laboratory experiments [9]. The resulting theory viewed behaviour as a mechanistic system that produced specific types of behaviour under the influence of antecedents, operant conditioning and environmental factors [10]. The theory states that antecedents set the stage for behaviour by triggering it or enabling it, with the resultant behaviour itself generating further specific consequences, i.e. all of the events ensuing from the behaviour. Such consequences create opportunities for learning, which in turn feeds back on behaviour in the future. This dynamic constitutes a powerful mechanism for reinforcing or penalizing specific forms of behaviour, all of which take place in a specific context, for example the workplace.

BBS involves the application of behaviour-analytic intervention strategies for workplace safety [11]. Initially, a BBS measurement takes place in a setting allowing for observation of safe behaviour in an active, observable, measurable and reliable manner. Where adequate steps are taken, reliable data concerning the behaviour of workers can be used as the basis for scientifically sound interventions. Factors determining the success of such interventions include:

- setting safety goals that the recipients of the feedback can achieve by changing their behaviour. Goal-setting shapes behaviour, goal attainment reinforces the behaviour change
- giving behaviour-specific feedback to workers. Behaviour can only change through feedback. Feedback is either delivered personally and specifically concerning the behaviour of an individual worker or is group-specific in the form of a behaviour-based line graph
- changing behaviour by using positive reinforcement. To reinforce behaviour, various forms of recognition may be used: praise, social approval or simply acknowledgement that the safe behaviour is appreciated

1.4.1 Safety risk management: risk analysis and assessment

BBS is an approach to managing human behaviour, but this approach cannot be considered in isolation from safety leadership and management strategies. In broad terms, safety risk management encompasses the practical, efficient, and effective implementation of business processes meant to preserve the safety of humans by preventing

accidents, minimizing the effects of those that occur, and enabling flexible, efficient recovery. Safety management encompasses a systematic application of policies, procedures and practices for promoting safety.

Traditionally, rules and procedures have been static instruments based on task and risk analysis effected by experts and enforcers. These rules are documented in manuals or databases and are made available to the workforce in the context of training, with employees being asked to sign off on their compliance. This constitutes a top-down, rational approach to rules, and is most effective in situations involving routine work conducted by low-skilled workers or trainees coping with emergencies.

However, rules may also emerge as patterns of behaviour based on experience with actions and activities by those who conduct them. In contrast to written rules, these procedures are local and applicable in a specific activity and context. This approach to rules is bottom-up and dynamic and is based on a perception of procedural directives as never being perfect and always requiring adaptation according to specific situations and contexts. It fits best with dynamic, complex, high-uncertainty/high-risk work, involving a great degree of variety and the need for flexibility imprecision, as in the case of surgeons, pilots, and seamen, who are experts armed with extensive experience and deep knowledge and who therefore may only need advisory protocols. It uses experience and expertise to deepen, update and refine action rules on the basis of feedback. Both approaches are required and complementary for defining rules and behavioural aspects needed for safety in the future [12] [13].

Risk analysis forms a key part of safety management and encompasses the following activities:

- establishing the context in which the risk activity takes place
- assessing the risk
- installing the necessary safety measures
- monitoring the risk and the measures adopted
- reviewing all aspects of the safety management system
- recording deviations and reporting to the authorities

Safety management requires that safety experts, managers and their workers collaborate to achieve a safe and efficient production system. It should be an integral part of management and decision-making and can be applied at the strategic, operational, programme or project levels.

The safety risk assessment approach aims to reduce risk to people arising from the design, production, distribution, use (including maintenance) and destruction or disposal of products or systems. The complete life cycle of a product or system (including both the intended use and the reasonably foreseeable misuse) must be considered, whether the product or system is intended to be used in industrial processes, workplaces, household environments or for leisure activities. The goal is to achieve tolerable levels of risk for people, property and the environment, and to minimize adverse effects.

The underlying principles of a safety risk assessment can be used wherever safety aspects require consideration, and as a useful reference for other stakeholders such as designers, manufacturers, service providers, policymakers and regulators. General safety-related guidance and risk assessment aspects are covered by ISO/IEC Guide 51. More specific guidance for safety-related risk assessment and risk reduction in connection with the development of low voltage equipment and related standards is covered by IEC Guide 116.

1.5 IEC role in ensuring safety

Safety of electrical systems has always constituted an important subject of concern to the IEC. Since launching its first technical committee (TC) devoted to addressing human-machine safety, (TC 16: Basic and safety principles of man machine interface, marking and identification[1]) in 1926, IEC has created more than a dozen new TCs for whom safety is a central focus of their standardization work.

However, safety concerns are not limited to these specific technical committees, as many IEC Standards cover a variety of safety aspects. The IEC Advisory Committee on safety (ACOS) provides overall guidance to IEC TC/SCs on questions of safety, as well as offering a forum for discussion of difficult issues involving several TCs or differences in opinion among them. The ongoing list of basic safety and group safety publications changes periodically, as the IEC keeps abreast of technological developments. New publications appear and older ones are updated. The lists can be obtained from the ACOS homepage under the tab Safety Functions[2].

The IEC has also issued horizontal standards fostering a consistent approach to the collation of groups of standards covering products, systems, services and certification schemes. IEC Guide 108 defines rules for dealing with horizontal functions and horizontal publications. It is to be used in conjunction with the ISO/IEC Directives and with the aspect-specific guides. IEC Guide 104 specifically defines rules for developing horizontal safety publications. The structure of the horizontal standards in IEC is shown in Figure 1-2.

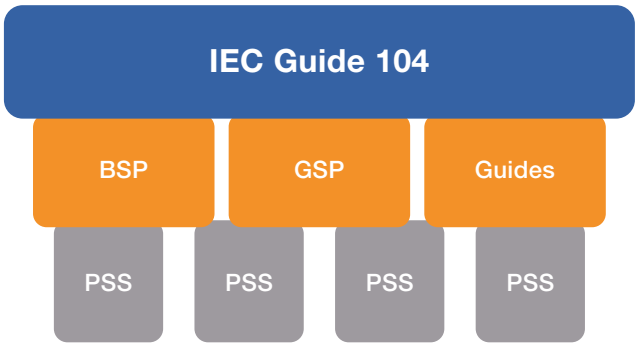


Figure 1-2 | Collating standards for safety according to IEC Guide 104

IEC Guide 104 contains procedures for developing:

- basic safety publications (BSP) covering horizontal safety principles, such as:
  - IEC 60529, *Degrees of protection provided by enclosures (IP Code)*
  - IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*
  - IEC 61140, *Protection against electric shock – Common aspects for installation and equipment*

1 SMB Decision 143/18, the SMB confirmed the disbanding of TC 16, and the transfer of ownership of TC 16 publications to TC 3

2 www.iec.ch/acos

- group safety publications (GSP) covering the generic safety of equipment types, such as:
  - IEC 60364-4-41, *Low voltage electrical installations – Part 4-41: Protection for safety – Protection against electric shock*
  - IEC 62477 (all parts), *Safety requirements for power electronic converter systems and equipment*
- specific safety guides, such as:
  - IEC Guide 110, *Home control systems – Guidelines relating to safety*
  - IEC Guide 112, *Guide on the safety of multimedia equipment*
  - IEC Guide 117, *Electrotechnical equipment – Temperatures of touchable hot surfaces*
- product safety standards (PSS) covering safety-related requirements of specific products, such as:
  - IEC 62368-1, *Audio/video, information and communication technology equipment – Part 1: Safety requirements*

1.6 Implications for standardization

Computers have changed the way entire industries function, altering the means by which workers in these industries operate. The digital revolution has created functionalities beyond the traditional reach of electrical engineering by adding a dimension that is traditionally associated only with humans: intelligence. Discussions concerning basic principles, harmonization and standardization are no longer the sole purview of electrical engineers, as the input of specialists from other domains is required. In 1987 the IEC adapted to this challenge by joining forces with ISO through the creation of Joint Technical Committee 1 on information technology (ISO/IEC JTC 1). This committee maintains more than 20 subcommittees dealing with a wide range of topics, such as artificial intelligence (SC 42), document description and processing languages (SC 34) and software and systems engineering (SC 7).

Section 2

Trends, initiatives and challenges impacting safety in the future

2.1 Introduction

Societal megatrends of various natures are creating unprecedented opportunities and perspectives for safety in the future, but their intrusive emergence also implies a daunting series of new challenges and threats. Business strategist Sarwant Singh defines megatrends as “global sustained and macro-economic forces of development that impact businesses, economy, society, cultures and personal lives, thereby defining our future world and its increasing pace of change” [14].

While the future can hardly be predicted with precision, technological and societal megatrends will clearly impact the future of work and safety. This will also be the case with regard to demographic developments, global and local economic trends, and political shifts, upheavals and evolutions. The drastic changes currently taking place imply increasing variability and complexity at the global level, leading to volatility, uncertainty and ambiguity both in society and at work. Consequently, traditional approaches to risk management, safety and standardization no longer suffice in themselves and require rethinking.

This section of the white paper identifies technological, societal and legislative trends affecting issues of safety and their resolution in the future. The purpose of this brief examination is twofold: to secure a fundamental understanding of the ongoing shifts in advanced and digital technology over the course of the coming decade, and to assess the projected effects of these advances on social developments and the resulting changes in how society functions.

2.2 Advanced technologies opening new safety perspectives

Intelligent machines constitute the primary drivers of the digital transformation affecting nearly every aspect of society. This transformation is designated by a variety of names around the world, such as “Industry 4.0” in Germany, “Smart Manufacturing” or “Made in China 2025” in China, “Industry in the Future” in France, and “Connected industries” or “Society 5.0” in Japan. This digital transformation is based on existing technologies such as the Internet of Things (IoT), big data, artificial intelligence (AI), advanced robotics and cloud/edge systems. These various systems facilitate the collection of enormous amounts of data and provide massive computing capabilities that allow powerful analytics to extract relevant information from raw data, interpret that information, detect unknown relationships between specified factors, take autonomous decisions, and predict future trends. Some of these applications mimic (or even exceed) human intelligence, as they can effect more accurate predictions and process greater amounts of data than humans are able to do.

Digital technologies and their resulting applications are not limited to selected industries or sectors of the economy, but rather are far-reaching and impact all levels of society, including financial systems, mobility, heathcare, education and general well-being. The information spaces of factories, traffic systems, personal healthcare and home servicing are but some of the aspects of daily life that increasingly will be digitized and

connected. These transformations imply a needed redefinition of social, political, cultural, and economic developments, including safety, in the 21st century.

Key technologies likely to exercise a disruptive impact on many facets of work and life include the following[3]:

- artificial intelligence
- virtual reality and digital twins
- holograms
- smart assistance and robotics
- autonomous mobility and driving
- ultrafast networks based on 6G and F6G
- 5G Wireless and Wi-Fi-6
- block chain technology
- edge and cloud computing
- quantum computing

All of these technologies are in their infancy today but are increasingly likely to shape the fabric of daily life in the coming decade. Some of the expected capabilities and potential impacts of these technologies are as follows.

- **Artificial intelligence on a chip**: Chipset AI encompasses the migration of software for AI algorithms in cloud-based operations to information communication (IC) circuits in chips, in the process making AI acceleration possible in local work environments. Such chipsets provide superior access to AI applications but also increase the availability of AI substantially. As a consequence, optimization of the entire information and communication technology (ICT) system will change. Machine-borne AI could become almost ubiquitous in every aspect of human-machine interaction.
- **Ultrafast fixed networks**: Such networks will be based on F6G (a fixed line 6G next-generation network). The future of fixed networks is entirely optical. The F6G gigabit network represents a huge advance in three key categories: bandwidth, number of connections and network experience. These three features of F6G will enhance user experience in traditional industry access scenarios and will help optical fibre networks to overcome traditional industry barriers and thus rapidly penetrate diverse sectors such as enterprise, transportation, security, and campuses. F6G will also help industries transform themselves digitally even faster than they do today.
- **Ultrafast mobile networks**: Based on 6G, such networks will deliver similar functionalities. Pilot architectures incorporating 6G are expected around 2030, with commercial 6G launches foreseen for 2030-2035. Various 6G capabilities in the areas of wireless sensing, imaging and location determination will make it possible to support multi-technology heterogeneous networks, thereby allowing smart manufacturing enterprises to deploy different access networks and integrate AI in their operational functions. The 6G networks will provide a single platform to address the required communication, computing and AI capabilities. This will allow for centralized and distributed intelligence (at the edge).
- **Quantum computers and networks**: A quantum computer is a computation system that makes direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data. Quantum computation uses qubits (quantum bits) instead of binary digits (bits), and quantum networks facilitate the transmission of qubits between physically separated quantum

3 See also https://future-summit.com/webinars/10-megatrends-and-future-technologies-2020-2030-business-new-part-1-2 [User password required for access]

processors. Quantum computers and networks both offer the promise of unprecedented speed in calculation (potentially reducing calculating times for some types of calculation from thousands of years to mere minutes) and networking (data transmission literally at the speed of light).

The latest ICT developments involving sensors, cameras, etc. are enabling organizations to gather real-time information on certain safety risks, particularly those directly or indirectly associated with human and machine movements. Based on such information and once again on ICT, it is becoming possible to develop dynamic control of such risks. An existing example of this is how a Japanese steel engineering company implements safety monitoring solutions for field engineers and workers. As shown in Figure 2-1, a platform registers the conditions and status of each field worker. In addition to worker information such as body temperature, heart rate and posture, the surrounding situation is converted into data via a wearable camera and is analyzed by AI engines in the data platform. In this way the supervisor can be informed in advance to take necessary actions to prevent accidents.

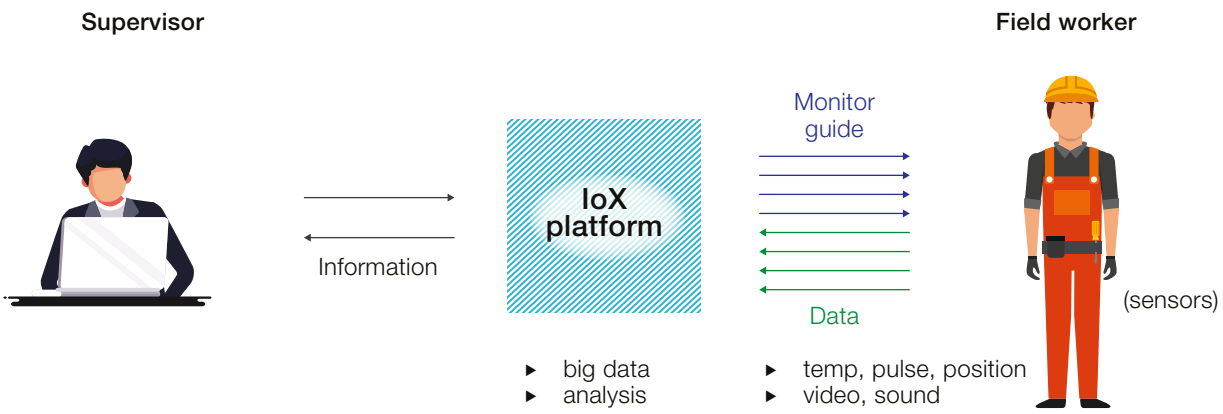


Figure 2-1 | Real-time risk assessment and control

The advent of new technologies impacts work in several ways. The European Agency for Safety and Health at Work (EU-OSHA) [15] conducted a thorough investigation in 2019 focussing on changing work relationships in a digital environment under the direct impact of such technologies. Their findings identified a number of characteristics, including:

- novel forms of human-machine cooperation
- emergence of the platform (or gig) economy
- increasing individualization of work
- expansion of teleworking
- rising screen time and increased sedentary work and behaviour

The rapid spread of new technologies also implies a heightened need for concrete measures to ensure that AI applications respect human values. The EU itself has issued a white paper stating that for AI to be acceptable as a tool, it must abide by seven principles in order to create an ecosystem of trust for its use [16]:

- human agency and oversight
- technical robustness and safety
- privacy and data governance
- transparency
- diversity, non-discrimination and fairness
- societal and environmental well-being
- accountability

Finally, the emerging age of digitalization also implies that the seamless functioning of most technological applications is becoming increasingly dependent on the quality and (cyber)security of the software, including the availability and excellence of software updates.

It should also be noted that the predominance of technological megatrends in digitalization in no way precludes the fact that megatrends in other technological domains are also likely to exercise major impacts on human life in the coming decades. Most prominent among these are developments in the life sciences, such as genome editing, immunotherapy, anti-ageing research, and cloning techniques. Other relevant technological developments either currently occurring or expected to emerge soon include applications in the fields of nanotechnology and non-fossil fuel energy technologies (solar, hydrogen fusion, new types of nuclear). Although the technological breakthroughs in these areas are clearly taking place in other domains, it is likely that in their applications they will also be influenced by digitalization.

2.3 Societal and legislative trends

In addition to megatrends in advanced technology, societal trends will have a major impact on business, work and life in the coming decade.

An example of this is the concept of the circular economy, principles of which are captured in SDG 12: Responsible consumption and production. The circular economy aims at realizing an economic order in which the unlimited ongoing reuse of products, parts and resources is effected without reducing their fundamental value. Circular supplies, resource recovery, product life extension, sharing platforms, and products as a service constitute critical pieces of the circular economy loop. This type of economy “replaces the end-of-life concept with restoration, shifts towards the use of renewable energy, eliminates the use of toxic chemicals which impair reuse, and aims for the elimination of waste through the superior design of materials, products, systems and business models”, see Figure 2-2.

Recent trends are also affecting data and privacy. Ever since the EU’s General Data Protection Regulation (GDPR) took effect in May 2018, the world of data privacy has shifted its focus from guidance to stepped-up enforcement. On the legislation side, the California Consumer Privacy Act (CCPA) went into effect on 1 January 2020. In Brazil, the General Data Protection Law (LGPD in Portuguese) is slated to start in August 2020. These two significant pieces of legislation are amplifying the momentum created by GDPR [18] (i.e. through a shift to regulation).

These legislative acts translate the growing conviction that data gathering and processing must ensure privacy, the quality and integrity of data, and data protection. Transparency concerning access to data, decision rules, and ways to ensure the prevention of unfair bias and discrimination is judged as more important than ever. The trustworthiness of new technologies that are regarded by governments and industry

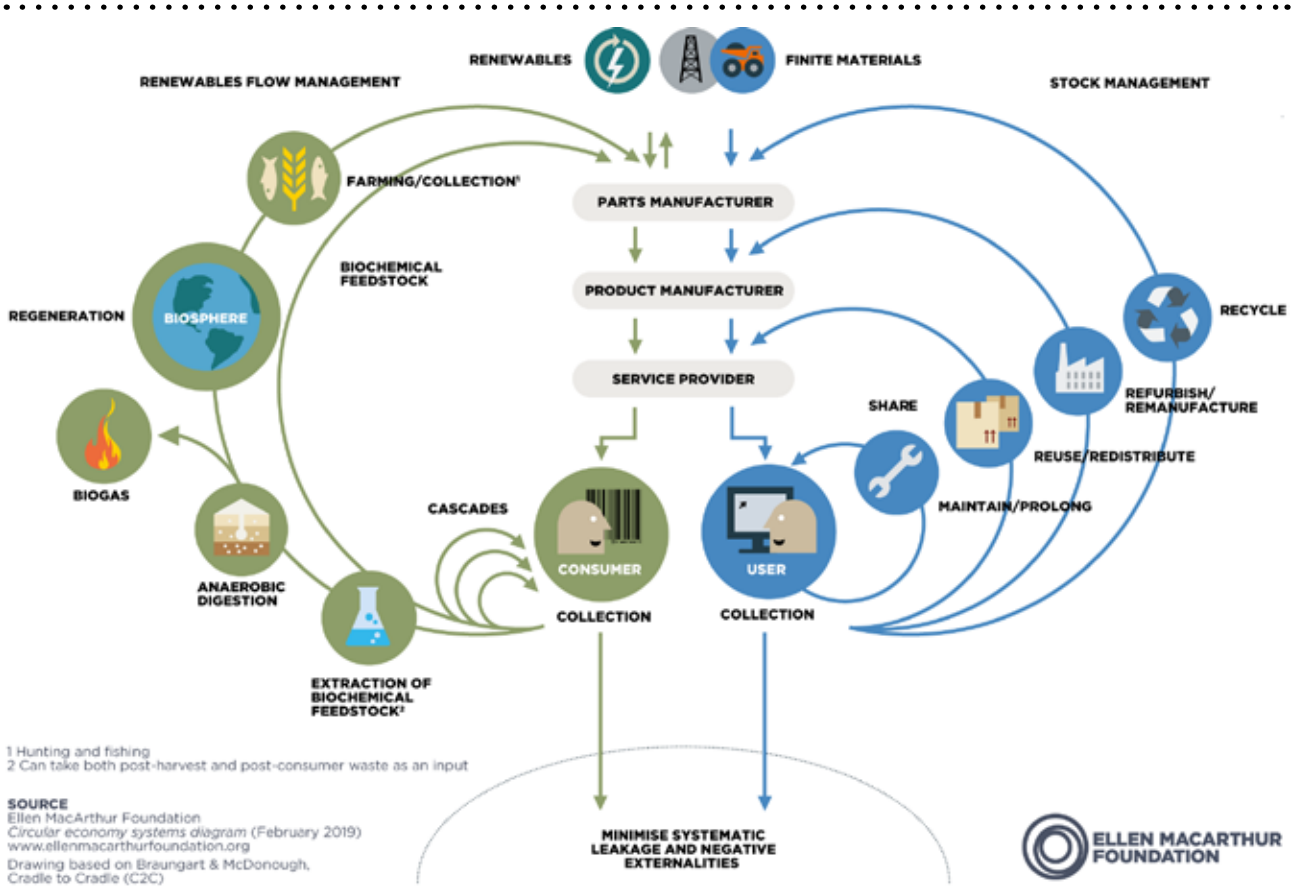


Figure 2-2 | Process in the circular economy [17]

as forming part of their "vital infrastructure" will increasingly be essential for their acceptance and adoption. Such infrastructures need to be secure and resilient to physical and cyber attacks, extreme weather conditions and natural disasters.

2.4 Additional trends, concepts and options

2.4.1 Innovating to zero

Another societal concept involves the trend toward "innovating to zero". According to Singh, "… more a concept or mind-set than a technological, economic or demographic development… it is an expression of the desire for perfection in our society: a vision to contribute to a world with zero carbon emissions, zero accidents, carbon-neutral cities, etc." [14]. As such it is also applicable to electrotechnical systems involving strategies focusing on zero defects and zero breakdowns. Innovating to zero is closely related to global long-term ambitions for a better world, e.g. zero poverty and decent work for all, as expressed in the UN SDGs.

Innovating to zero is primarily an approach to adapting operational strategies, it is not a programme. "Success in innovating to zero requires an innovation agenda that aims at breakthroughs in the face of radical goals – goals that intend to create a better world, free of unhelpful externalities and defects". This clearly implies an ethical dimension, a close link with corporate social responsibility and with the UN SDGs. It also requires long-term ambition, proactive leadership and a supporting organizational or societal culture.

For example, the Nippon Electric Control Equipment Industries Association (NECA) describes its vision for 2025 as “5-Zero Manufacturing”: the use of innovative technology to strive for zero defects, zero production loss, zero late delivery, zero accidents and zero downtime. The goal of completely eliminating accidents is also part of the “Zero-Accident Total Participation Campaign” initiated by the Japanese Industrial Safety and Health Association (JISHA)[4] in 1973. The campaign translates a vision whereby excellence in safety is regarded as a necessary element for manufacturing excellence and economic success, see Figure 2-3.

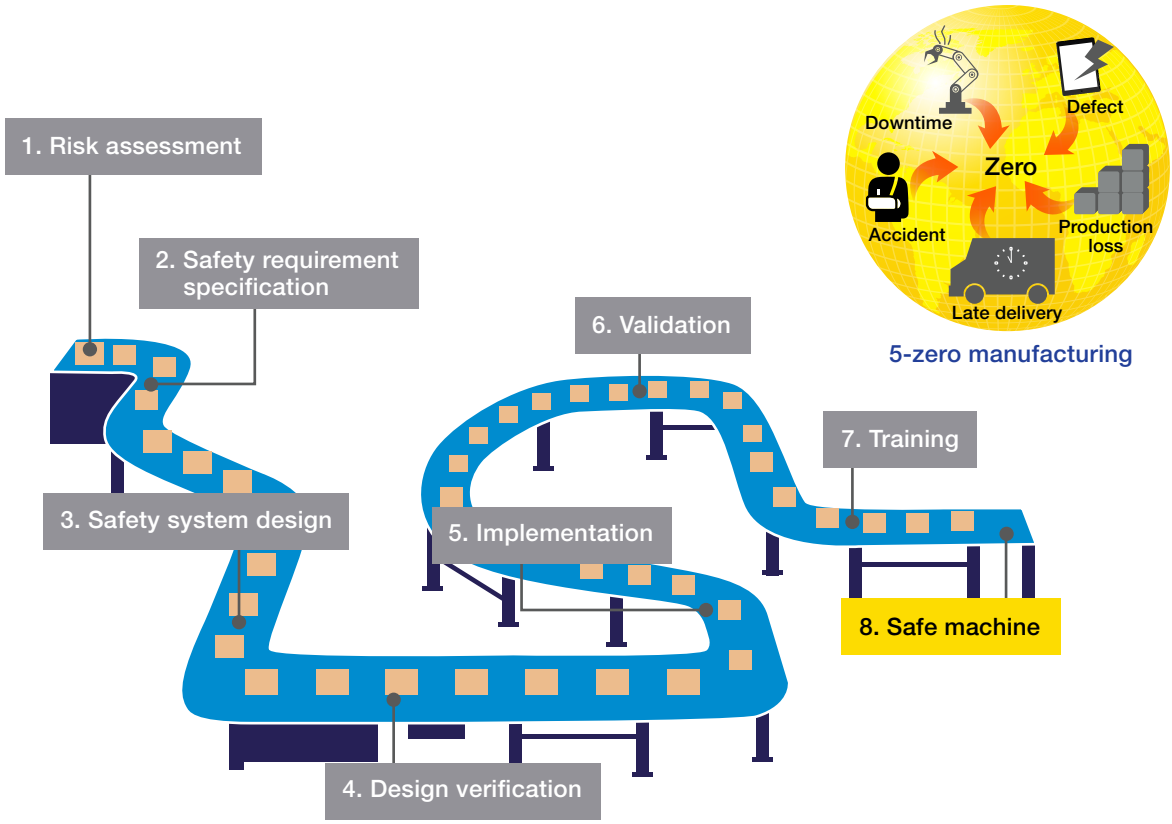


Figure 2-3 | 5-zero manufacturing [19]

A related initiative in safety promotion involves broadening the safety horizon to include health and well-being, a strategy already incorporated in the concept of occupational safety and health (OSH). Combining efforts and objectives in these fields creates synergies between the three areas, as safety, health and well-being at work are based on the same human and social values. This merger of fields is converging with the “innovating to zero” concept in a movement developed by the International Social Security Association (ISSA) called “Vision Zero”, see Figure 2-4.

4 www.jisha.or.jp/english/index.html



Figure 2-4 | Vision Zero as integrating safety, health and well-being [20]

Vision Zero is described as "the ambition and commitment to create and ensure safe and healthy work [conditions] and to prevent all accidents, harm, and work-related diseases in order to achieve excellence in safety, health and well-being" [21]. In this context it is important to place the human being at the centre of safety considerations, which should extend beyond mere prevention of unintended injury to include a sense of emotional security derived from the absence of danger and a level of psychological safety [22].

Six elements are highlighted in Vision Zero:

1) a strategic commitment to promoting safety, health and well-being
2) integration of these elements as cornerstones of what constitutes safe business
3) triggering innovations for improvement in this area,
4) development of a prevention culture
5) creation of a foundation on business ethics and contributing to broader programmes for corporate social responsibility and sustainability
6) requiring networking, co-creation and co-learning

2.4.2 Collaborative safety

Initial experiences with real-time risk assessment and control have led to elaboration of the concept of collaborative safety. This approach leverages digital technologies and human-machine interaction to support industries and economies that are themselves built around digital applications. The concept has been developed in the area of machine safety and human- machine interactions but is valuable and applicable in many other situations.

Underlying the collaborative safety concept is a model of how machine safety efforts have developed over time, see Figure 2-5. Key to this schema is identification of the specific element invested with the role of ensuring safety in situations of human/machine coexistence at each stage of the evolution. Initially (in the age termed Safety 0.0), safety depended mainly on human awareness, competence and actions. People had to pay attention to the specific dangers posed by machines.

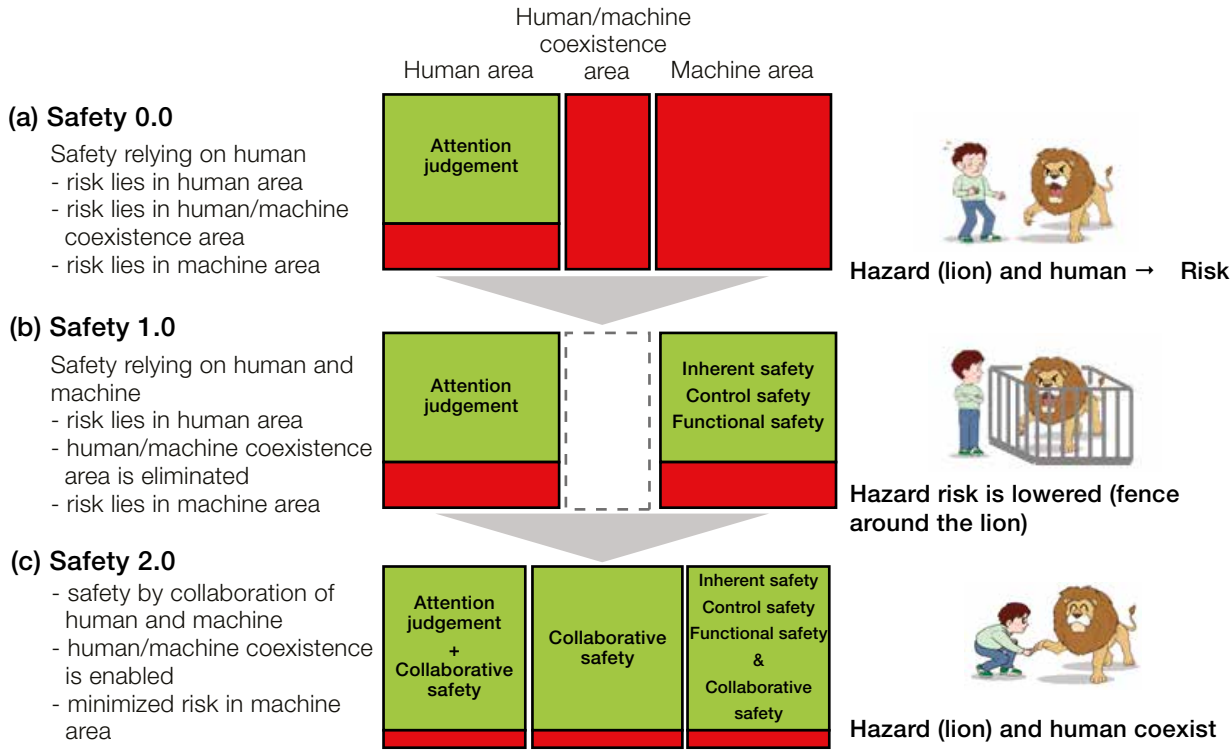


Figure 2-5 | Three ages in the development of (machine) safety

In the next phase, in which machines began performing increasingly complicated tasks, both machines and the systems in which they operated were equipped with safety measures aimed at shielding human operators from dangerous machine movements. Safety at this stage of the model (Safety 1.0) is mainly ensured by engineering solutions, i.e. via technology. Currently, the safety technology of machines is mainly focused on hardware-oriented aspects based on a three-step approach: 1) inherently safer design, 2) guards and protective devices, and 3) information on use, with reference to ISO/IEC Guide 51. The basic principle involved at this stage is to isolate the machine from human beings and to stop the machine from operating when the machine and humans coexist.

The development of IoT, AI, image processing, big data and other ICT technologies has introduced previously impossible safety functions, with machines now being invested with the intelligence to deploy flexible operations, such as slow-speed motion in the presence of inexperienced workers, or suspension of operation in cases of danger. The latter situations can be identified on the basis of data transmitted to the machines via wearable devices such as radio frequency identification (RFID) tags worn by workers, which provide the machines with relevant data concerning any workers present, e.g. physical condition, experience/career history, qualifications and capabilities. Such systems are being developed in many parts the world, giving birth to a new era of collaborative safety, termed Safety 2.0.

Collaborative safety is achieved when humans, machines and the operational environment share digital information with one another, communicate and collaborate. In this context, the environment includes physical settings, organizations, systems,

databases, standards, regulations and rules. Collaborative safety, unlike earlier approaches, places the same level of importance on human capability as on technology and organization. Skills, capacities, satisfaction, self-esteem, health, and a sense of well-being are equally valued.

The basic concept of collaborative safety consists of the following elements:

- maximum use of ICT to monitor information on a real-time basis concerning machine motions, human behaviour and the working environment
- safe control of machine motions and/or human behaviours through detection and transmission of potential risk information during normal operation or maintenance service periods
- ensuring that the adoption of safety technology using ICT does not sacrifice the operation rate of the machines or the humans' working efficiency
- ensuring that the adoption of safety technology contributes to the trustworthiness of workers/operators in pursuing the application of safety measures in a sustainable manner

The essential aim of collaborative safety is to establish a mutually supportive partnership between machines, humans and the environment they operate in, by way of multi-traffic information flows between them. The human is warned to restrict his or her behaviour by the machine, and the machine is warned to slow down or stop by human intervention. Thanks to maximum use of the latest ICT technology in collaborative safety strategies, the responsibility of workers/operators for ensuring safety in the use phase is largely taken over by the machine and the information technology. As a result, the operators require less specific training and expertise and experience reduced working pressures.

2.4.3 Prescriptive legislation and the standardization/conformity assessment option

Traditionally, legislation regulating the protection of safety and health could, at least in principle, be enforced through governmental inspections. Apart from the limited capacities of inspectorates, more fundamental reasons exist for why this model is increasingly challenged. The above-mentioned megatrends in society, technology and work imply a rapidly changing world. Technological innovations, particularly those associated with information technology, are impacting production processes, the nature and conditions of work, as well as industrial relations. In this context, prescriptive legislation is almost by definition lagging behind reality, while at the same time hindering innovation.

In many jurisdictions, four types of responses are materializing to address this problem:

1) making legislation more flexible by focusing on processes rather than products. For instance, a focus on the quality of safety management processes accords industries a high degree of freedom in how they design and implement such processes
2) reducing administrative pressures by prescribing safety and health aims instead of means. This allows industries more freedom in choosing how they wish to achieve the mandatory objectives
3) using economic incentives as a trigger for meeting safety and health obligations, thereby making use of market mechanisms inherent in the industries
4) complementing mandatory requirements with voluntary agreements (e.g. between governments and social partners, or governments and industrial sectors) at the national or regional (e.g. European) level

As a result, standardization and conformity assessment have become more than merely

private initiatives. They increasingly are viewed, and indeed are already functioning, as vital complements to legal safety regulation. This also entails a new type of pressure on industry to develop such standards.

Standardization and conformity assessment of safety management systems (e.g. ISO 45001 and national or regional systems for contractor safety management) are natural complements to legislation that focuses on management practices. Conformity assessment implies private control, which is different from enforcement, but is increasingly recognized by governments as an important factor complementary to governmental inspections or allowing for fewer such controls. In addition, standardization has a role to play in devising economic incentives, while the nature of such incentives may be based on certain specific standards. Likewise, voluntary agreements normally require a variety of monitoring activities (what is the impact?) and monitoring the implementation rates of safety standards and conformity assessment is often an important element incorporated in the agreements. Furthermore, it is important to realize that international safety standards also have a major impact on safety in countries where adequate safety legislation is not available.

2.4.4 Megatrends and their impact on work

Many of the technological and societal megatrends discussed in this section directly impact – or will impact – the world of work. As a result, the character and structure of work is changing and is increasingly associated with new challenges of relevance to safety, health and well-being in the future. A summary of the most prominent trends and their effects on work is given in Table 2-1.

Table 2-1 | Megatrends and their impact on work

Megatrends	Impacts on work
Digitalization	▪ Increase in teleworking ▪ The emerging platform (or gig) economy ▪ Increasing individualization of work ▪ New forms of man-machine cooperation ▪ Rising screen time and increased sedentary work and behaviour ▪ Increase in stress and mental health issues
Economic and political developments	▪ Increase in dependency of remote headquarters ▪ Increase in service industries ▪ Rise of self-employment ▪ Increasing flexibility of work and employment ▪ Rise of “flexicurity” ▪ Dichotomy between work and society
Globalization and new business models	▪ Increasing relevance of (global) supply chain and OSH ▪ Outsourcing and off-shoring of work ▪ Subcontractor management ▪ Frequent restructuring of organizations and reorganization of work

Demography	▪ An ageing workforce ▪ Higher pension retirement age (longer working life) ▪ Increase in chronic illnesses at work ▪ Greater diversity in the workforce (ages, cultures, languages, religions, etc.) ▪ Mismatch between required and available competences (knowledge, skills, attitudes)
Sustainability	▪ Increase of work at the end of the life cycle

2.5 Risk management, risk governance and standardization challenges

Megatrends are demonstrating the need to manage a variety of risks which can have an impact on safety. Physical workplace safety aspects can no longer be managed independently from other types of risks such as cyber security, environmental damage, ethical challenges, etc. However, the concept of "risk" is defined variously in existing ISO and IEC Standards, with two contrasting understandings emerging as the context for standardization responses:

- a widely shared definition in safety standards drawn from ISO/IEC Guide 51: "the combination of the probability of occurrence of harm and the severity of that harm"
- a management definition from the ISO 31000 series and ISO Guide 73: "the effect of uncertainty on [the achievement of] objectives", see Figure 2-6

The ISO definition implies that the effect of uncertainty may be either negative or positive (involving either down-side or up-side risk). This understanding usually refers to business risks. The positive aspect of risk is also found in the so-called "Safety-II" approach. Safety-II is defined as "a condition where the number of successful outcomes is as high as possible. It is the ability to succeed under varying conditions. Safety-II is achieved by trying to make sure that things go right, rather than by preventing them from going wrong" [23]. Within the IEC context, however, the more traditional understanding of risk addressing negative outcomes is prevalent.

The purpose of risk management has been, and remains, the creation and protection of humans and value. Risk management addresses adverse outcomes of the system of interest and controls performance by improving human-technology interaction, averting deviations and accidents, encouraging innovation and supporting the achievement of objectives (including business continuity). It should be established and maintained by the organization that has ownership over the system of interest. The rapid digitalization of data systems and the ubiquitous connectivity via sensors makes it possible to support safety aims in a much more direct manner.

However, reporting on risk management is not straightforward. Sensors, cameras and ICT systems are collating enormous amounts of data, yet the things which are the easiest to measure are not necessarily the most relevant factors for controlling risk and achieving safety. Factors such as human behaviour, cultural values, organizational culture, leadership commitment and interpersonal

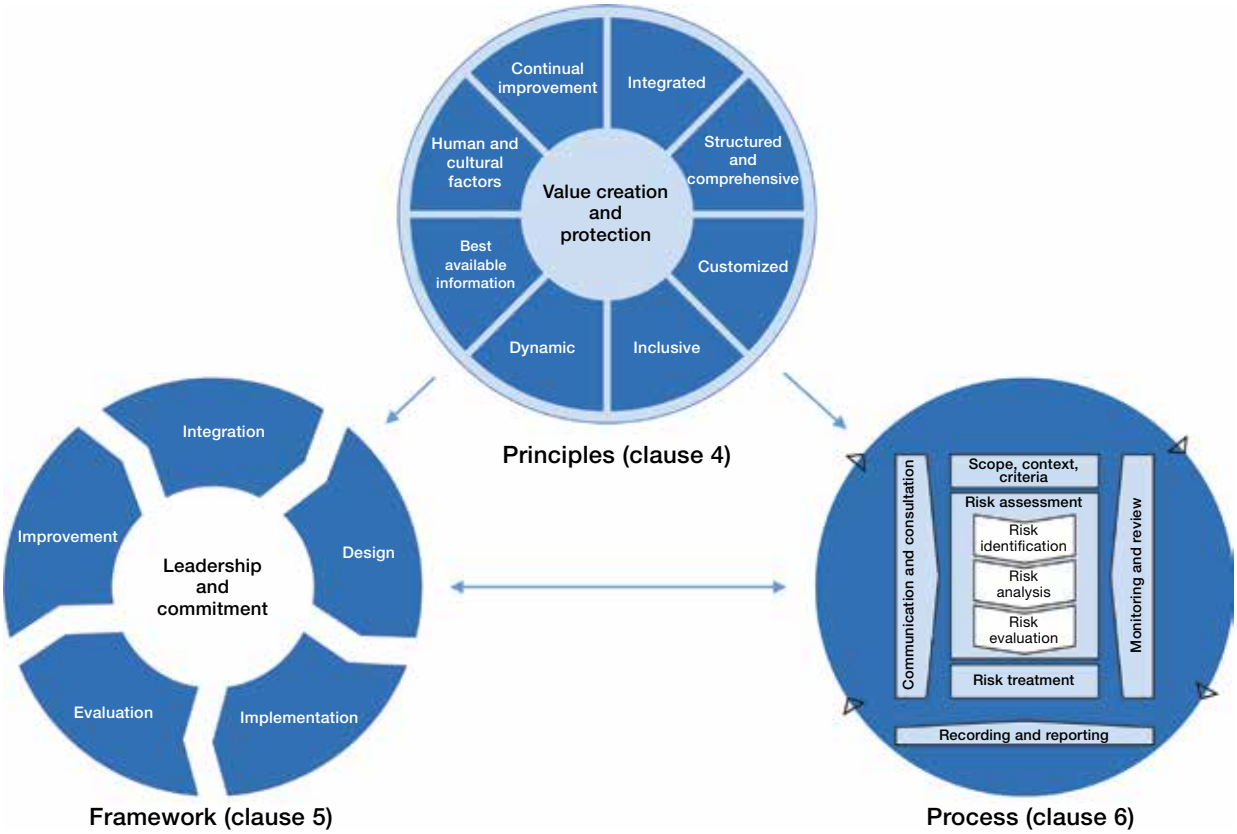


Figure 2-6 | Risk management framework (ISO 31000)

communication are not so easily captured in data systems. Research is beginning to be conducted in this area, but it is picking up slowly, and the danger exists that such factors may be neglected in a world of big data.

Consequently, both policymakers and industries must deal with new types of uncertainties and conduct discussions involving a variety of stakeholders regarding the opportunities and risks posed by new technologies and innovations. The approach involved in guiding these processes is called risk governance and is based on cooperation between public and private institutions and organizations. The cooperative approach to risk governance is built on an iterative process comprising five steps:

1) pre-assessment, recognition and framing
2) appraisal involving assessment of the technical and perceived causes and consequences of the risk
3) characterization and evaluation: making a judgement about the risk and the need to manage it
4) management: selecting and implementing risk management options
5) cross-cutting various aspects: communicating, engaging with stakeholders, considering the context [24]

This risk governance process explicitly involves stakeholders in the management of uncertain,

complex and ambiguous risks. Transparency and open communication are essential for inviting, supporting and involving all significant stakeholders, and for developing mutual trust as a basis for joint evaluations and decision-making. Collaboration with stakeholders in governing the risks of complex systems incorporating innovative technologies implies another dimension to the term “collaborative safety”.

The aim of the risk governance process is to arrive jointly at decisions on how to deal with (partly) unknown risks. The strategy involved is to control such risks by influencing the development of new technologies and innovations, not by hindering the emergence of the risks. The characteristics of risk influence strategies and stakeholder involvement are specified in Table 2-2.

Table 2-2 | Risk characteristics, strategy and stakeholder involvement[5]

Risk characterization	Characteristics	Strategies	Stakeholder involvement
Simple risks	Risks are known, scientific knowledge is available	Applying routine- based strategies	Instrumental discourse
Complex risks	Limited knowledge of cause-and-effect relationship. Many interactions in systems limit predictability and lead to emerging properties	Consensus seeking. Identifying and characterization of available evidence. Sense determination. Improving robustness	Epistemological discourse
Uncertain risks	Recognizing that knowledge about the risk is limited. Risk assessments are (partly) speculative	Using proxies for risk characterization. Improving capability to cope with surprises, strengthening resilience. Considering precautionary approaches	Reflective discourse

5 Adapted from the International Risk Governance Council (IRGC), 2017

Ambiguous risks	Different values, axioms or stakes imply different opinions and norms about what is acceptable risk and/or who is accountable	Mapping all relevant information including associated values and stakes. Apply conflict resolution methods. Build confidence and trustworthiness	Dialogues and participative discourse, often including general public
Unknown unknowns	Unprecedented and unknown types of risks	Systematic assessment of known risk information reduces the likelihood of unknown risk but cannot exclude it	

Research on risk strategies and stakeholder involvement is monitoring the rapid developments occurring in technology and society but is inevitably lagging behind. As a result, the scientific basis for control of new risks remains limited. Often a variety of stakeholders are involved in projects to assess and harness the new technologies, with each set of participants having diverse stakes in the outcome as well as perceptions of the opportunities and risks involved. As a consequence, the authority of scientists and engineers is no longer accepted uncritically or exclusively. Presently no generally accepted standards exist covering risk governance processes, a lack which is hampering widespread implementation of such processes. In the related area of cyber security, uncertainty, complexity, ambiguity and unknown risks can combine to create complex issues of safety. As a result, future safety standards will no longer be defined solely by electrotechnical engineers but will reflect the input of a wide range of stakeholders, including governments and society at large.

Now and in the future, risks associated with the advent of new technologies and disruptive innovations will increasingly be considered within the framework of wider societal discussions or even controversies.

2.6 Standards challenges

Many existing ISO and IEC safety standards covering specific types of machines or products still fail to include holistic safety aspects (relevant safety technology but also communication technology, reaction time, operational management, core personnel competences, etc.). The standardization community must reconsider its role in ensuring safety. Safety standards that focus on technical components alone have the same sort of limitations as prescriptive legislation: they may hinder innovations and may need to be updated at increasing frequencies, which poses a challenge for international standardization processes. As the principle of collaborative safety is commonly applicable to a variety of industrial sectors (e.g. manufacturing, civil engineering, construction, agriculture, healthcare and transportation), standards development may need to adopt different approaches involving a wider range of stakeholders. One option could

be to develop more “performance-based” (as distinct from “specification-based”) standards for collaborative safety, describing the intended objectives and performance targets of such a collaborative approach, and specifying the minimum requirements for the process to achieve the objectives adopted.

With governments relaxing their grip on safety via less stringent legislation, and corporations compensating for this regulatory alleviation by assuming social responsibility for safety through private initiatives, an opportunity is opening for the development of new types of industry-supported standards for safety. In this way, standards for the industrial sectors would become less restrictive, and maintenance of the standards developed would be less burdensome and more responsive to technological evolutions.

Section 3

The tripartite system for safety

This section focuses on the inevitable evolution of the concept of safety under the impact of technological advances and their effects on workplace safety. At its core, safety will undergo the impact of a fundamental shift in human-machine interaction, in which humans and machines share tasks both manually and mentally. As a consequence, it is envisaged that digital capabilities will facilitate workspaces in which humans and machines can interact seamlessly in a shared working environment, or indeed in any other space involving joint human-machine collaboration. In describing the concept of safety and its delivery in such a framework, we simplify the functioning of the new workspace paradigm in terms of a tripartite system in which humans, machines and the environment collaborate to ensure the future. The tripartite system for safety model facilitates a systematic approach to discussing key elements of safety in the future.

Following a description of the tripartite system, including a focus on information flows, systems boundaries and linkages, and the various levels of sophistication involved, this section examines key examples of current and projected technologies being deployed in this context and considers the technological necessity for cyber security, as well as implications for standardization and conformity assessment.

3.1 Humans, machines and the work environment

In 2030 the concept of safety will be delivered in an integrated system in which humans, machines and the environment collaborate. Such collaboration will be made possible by information flows going back and forth between the different components of the system: human workers, (semi-)autonomous machines and the IT-enabled environment in which they function. We call this collaborative framework the tripartite system for safety, as illustrated in Figure 3-1 [25].

In the figure, the human represents an individual or individuals performing a work task. The machine represents a machine, robot or tool equipped with electronic capacities and machine intelligence or with an elaborate control system. The environment represents the computer and support systems installed to support the ongoing work process. These can be electronic monitoring systems or edge nodes in the workplace itself, supervisory control and data acquisition (SCADA) systems in a factory setting, or even cloud-based services dedicated to supporting the given operation. Depending on the activity, and whether it involves farming, robotized manufacturing, chemical processing or logistics, the design of the human tasks and technologies involved may vary widely, yet these three core elements are always present in one form or another.

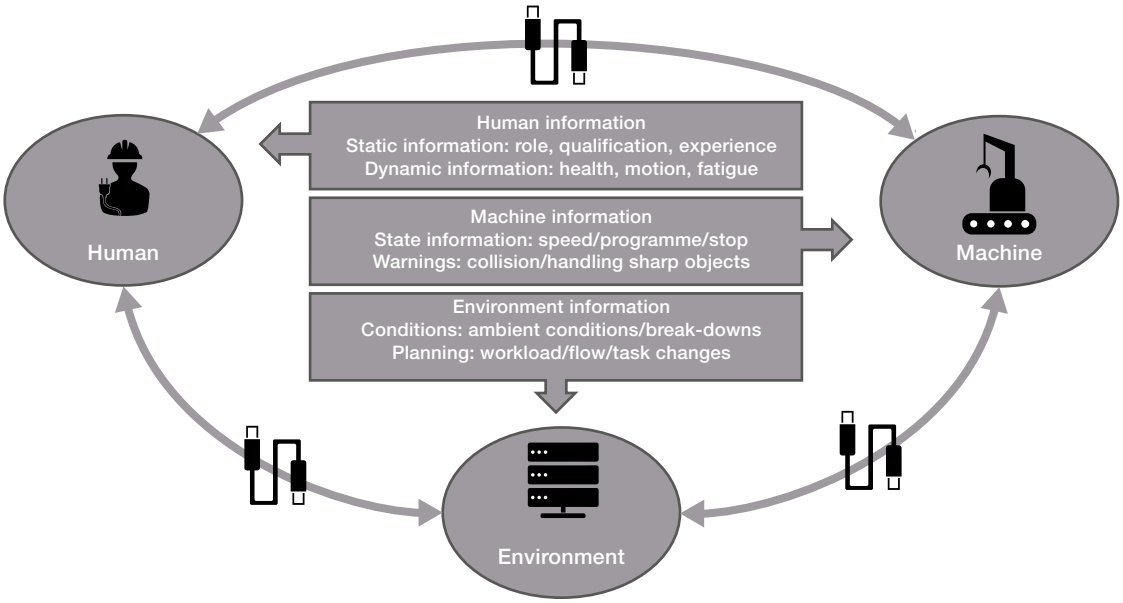


Figure 3-1 | Tripartite system for safety in the future

3.2 Information flows in the tripartite system

Three kinds of information pass between the components of the tripartite system, see Figure 3-1. **Human information** is information relevant to the machine that allows it to adapt its operation to the human or humans involved. This can be either static or dynamic information but is always focussed on human conditions. Static information is information that changes very little over time, for example, concerning a worker's qualifications, career path or employment experience. Dynamic information is information that changes daily or in real time, such as a worker's level of fatigue or specific actions undertaken, e.g. correcting small mistakes or taking an impromptu comfort break. The machine, perhaps assisted by the surrounding environment systems, needs to adapt its operations to these variances to ensure safe production. The human condition may be monitored through devices registering physiological data or bodily movements, including pulse and body temperature or information on the worker's behaviour and position.

Machine information contains the status of the working machine: whether the machine is in operation or in stand-by, whether a safety-critical part is functioning correctly, information concerning a robot's hand, operation status information such as programme operation or cooperative operation, etc. This information needs to be conveyed to the human in order to encourage safe behaviour. Machine alarms indicate immediately that the machine has failed or is on the verge of doing so. Such information is key for working in environments where people and machines coexist. As of today, machines can also communicate next steps in the work process, but equally, the machine could suggest a change of posture during the course of the work (e.g. by advising the person to stand up, or by suggesting that he or she takes a break). In collaborative environments in which several people work simultaneously, the machines could suggest switching working posts with a colleague to improve the health and safety of both individuals.

The working environment constitutes an integral part of the tripartite system, with **environment information** facilitating the contact between

humans and machines and simultaneously forming a link to the wider enterprise systems. For humans, the role of the environment is to create safe working conditions in terms of ergonomics, space, ambient conditions and social interaction. For instance, it is beneficial for the human worker to know that a particular machine has received software updates that could change its operation. Equally, the environment provides a network for technical ICT systems to support the machines by letting them know which workers are present on a given day and what specific safety requirements are associated with those individuals. At the same time, the local work environment maintains links with the wider enterprise environment of the company, which can provide information about safety procedures or changes in safety policies.

3.3 System boundaries and linkages in the tripartite system

The tripartite safety system approach requires a clear description of the process falling within the boundaries of the system and the linkage to external forces and elements such as stakeholders, objectives, contingencies and rules. As advanced human-machine collaborations are technologically complex, so are the networks to which they are linked. An example of such a system description is provided in Figure 3-2, which illustrates that the safety of the system of interest does not exist in isolation but rather depends on an ecosystem of systems inside the company that is in touch with other institutions and the global society at large. These linkages introduce options and limitations to the system of interest. These can include:

- satisfying business objectives that are intangible (e.g. production targets)
- optimizing compliance with other objectives and with the system's internal objectives according to a hierarchy of priorities that must be established
- complying with health and safety standards for workplaces (e.g. regulations)
- fulfilling standards for safe human-machine collaboration
- dealing with security risks that ICT systems and the internet pose

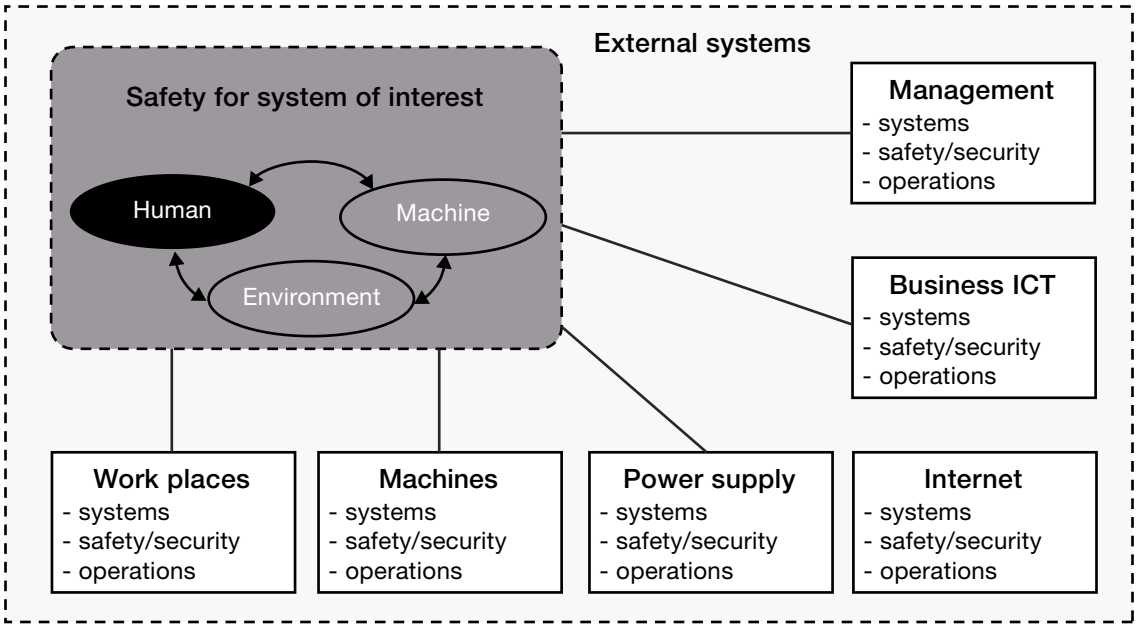


Figure 3-2 | Abstract system definition for tripartite system for safety

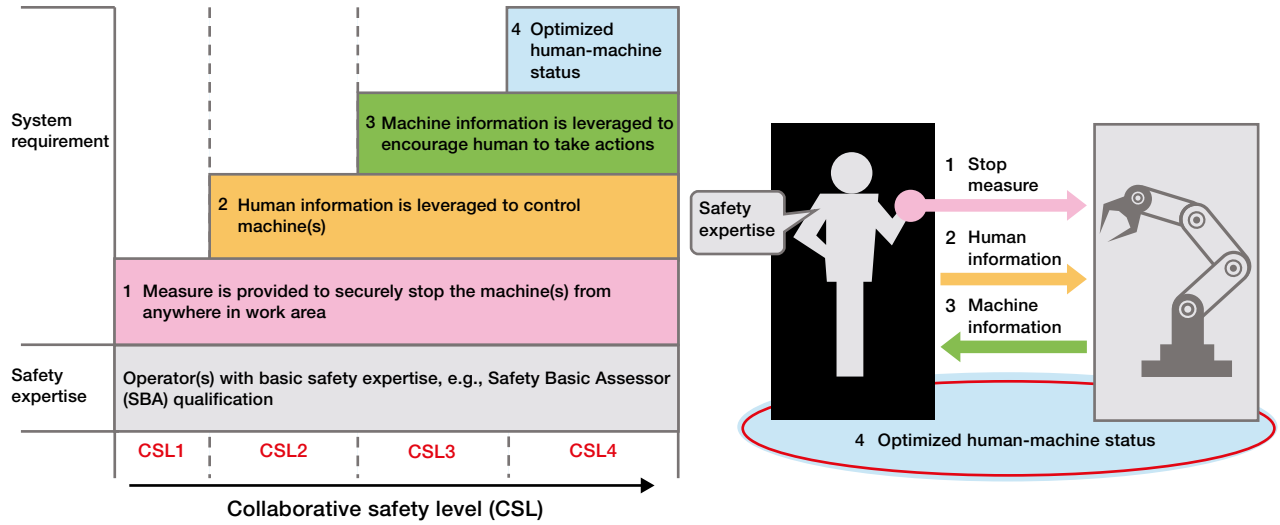


Figure 3-3 | Collaborative safety level

Safety issues usually arise due to deviation from normal operations inside or outside the system of interest. Deviations can be caused by changing the design or the objectives of the system but can also be triggered by external changes. For the purposes of this white paper, the focus here is on safeguarding systems that depend on complex interactions between humans, intelligent machines and ICT systems.

3.4 Levels of sophistication in the tripartite system

Not all work processes are constructed in the same way, and requirements for safety and reliability may differ considerably from one system to another. Therefore, differing levels of sophistication are envisaged for future safety systems. The collaborative safety level (CSL) concept illustrated in Figure 3-3 provides the basis for a transparent framework [26].

The CSL model adds four levels of sophistication to the basic safety level. These describe specific performance criteria for cooperative safety:

- SBA – The Safety Basic Assessor qualification defines a specific level of basic knowledge and skills related to safety required of all workers. This level represents legal requirements for safety at work as they exist today. The approach may be based on national or local qualification systems
- CSL-1 – Currently, most stationary workplace and manufacturing machines contain emergency stop mechanisms (though some machines, such as vehicles, do not). At this level, it is envisaged that the collaborative safety environment makes it possible to trigger stop functions from anywhere in the work area
- CSL-2 – This level introduces machine processing power enabling machines to make use of human information. At this level, information on the worker is communicated to the machine to enable performance of relevant safety controls
- CSL-3 – At this level, bi-directional communication is established. In addition to CSL-2 functionality, machines are equipped with ergonomic human interfaces to transmit safety information to workers

- CSL-4 – At the highest level, the system is optimized to improve the health and safety of the system as a whole. In this case, data networks in the environment aid the optimal safe and efficient functioning of the production process

3.5 Key enabling technologies of tripartite systems

Various currently applicable and foreseen technologies are providing the conceptual framework and basic interconnectivity needed for the sophisticated inter-functioning of tripartite systems. Subsections 3.5.1 to 3.5.3 present three key enabling technologies being harnessed to address the complex challenges involved in assuring information flows between the active components of such systems.

3.5.1 IoE

As the tripartite system depends on integrated machines and intelligent algorithms, connectivity through wireless networks and internet is a core enabler. As a concept, the Internet of Things (IoT) is central in this regard. The IoT designates a system of interrelated computing devices and mechanical and digital machines that transfer data over a network without requiring human-to-human or human-to-computer interaction. In working spaces, IoT facilitates the seamless integration of various machines equipped with sensing, identification, processing, communication, actuation and networking capabilities. When the same approach is used for safety purposes, the concept is relabelled as the Internet of Humans (IoH).

Ultimately, the system applied to monitor humans (IoH) and the system employed to monitor machines (IoT) are very similar. Both have detectors for monitoring purposes, both use extensive communication networks to send data back and forth within the system, both collate data in data centres and both rely on analytics, either in the centralized cloud or in localized edges, and sometimes even in the sensors themselves. In short, the basic infrastructure is the same, and it makes sense to combine the two into an Internet of Everything (IoE) system. With an IoE system at work, the processes illustrated in Figure 3-4 are accelerated, product demands are met immediately, and real-time optimization of production is the norm.

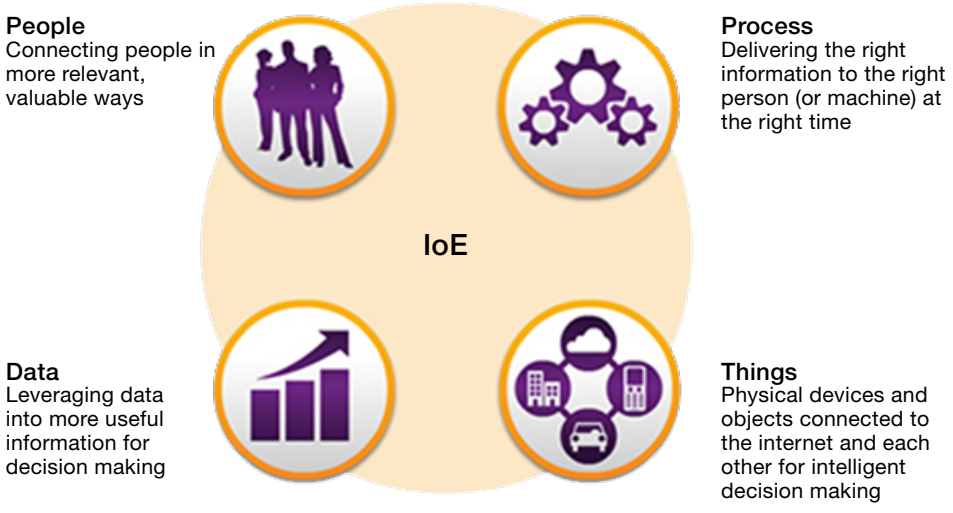


Figure 3-4 | Internet of Everything

The IoH system proposed by a Japanese ICT solutions provider equips workers with a smartphone incorporating GPS, a camera, acceleration and gyro sensors, a smartwatch capable of measuring vital data, and a temperature and humidity sensor. These are considered the basic sensing devices for monitoring humans on an individual level.

The devices are connected to a data system in the cloud or on the premises through an on-site communication system. Under normal working conditions, the information collected is used to determine a worker's physical position and status (heart rate, stress level, movement speed, altitude, dynamics, and water content) and to detect automatically whether the individual is walking or running or is subject to some form of distress. Since the information is collated on a worker's smartphone, it is possible to combine this data with the position and status of other workers and to determine whether they are in the vicinity of a dangerous object or gas cloud or are working at height. If the tasks involved are performed indoors, indoor positioning technologies such as beacons and ultra-wideband (UWB) sensors may be required. This makes it possible for a supervisor to alert someone if they are entering a dangerous area, for instance an ATEX[6] explosion zone.

The sensors in the phone can easily pick up abnormal movements such as immobility, stumbling, and falling. In such cases, an alert is immediately transmitted to the controller's display, and emergency notifications can be sent to the smartphones of the user involved and nearby workers. When colleagues are nearby, they can assess the situation directly and, whenever possible, proceed to the rescue. The camera on the phone can be used to capture images, which are then immediately transmitted to the IoH platform and stored. These static images can be checked by the supervisor and can be acted upon directly or at a later stage. In addition to images, near miss reports, status reports and any other types of operational communication can be transmitted to the system without delay. Nor should it be forgotten that the phone itself can be used to place a call.

The sensors in the smartwatch can detect signs of hypothermia, heat stroke or fatigue. On the basis of the pulse data from the smartwatch, complex calculations can be performed combining temperature and humidity data and the amount of energy exerted. As a result, the watch can notify workers of the need to take a break.

At the end of the workday, the data recorded can be collectively analyzed for indications of danger, using pattern recognition algorithms based on deep learning. The results can then be applied to improve specific working procedures or to support individual-based training requirements.

Apart from deploying their technological capabilities, it will be essential for such systems to ensure the privacy of the workers involved and to involve worker representatives in supervision of data processing, data protection and the algorithms used.

3.5.2 Ontology and semantic interoperability

Information exchange is key to the functioning of tripartite systems for safety, and to ensure success in this respect, ICT systems must be able to communicate amongst themselves and with participating humans. The complexity of the tripartite system increases significantly when it involves interfaces with multiple ICT systems providing AI capability. An example provided in the recent IEC White Paper *Semantic interoperability* illustrates this complexity [27].

6 Equipment for potentially explosive atmospheres (ATEX)

Assume a situation in which a worker needs to be informed that the motor in a collaborative robot is overheating. In order to detect the problem in the first place, the temperature of the motor needs to be measured, and then the information has to be digitized intelligibly. In addition to the numeric value of the temperature itself, the data must include the time, the unit of measurement (e.g. °F or °C), indicators identifying both the sensor and the part being measured, and perhaps additional elements of information. The data is then sent to an IoT system, where an algorithm assesses whether the temperature of this component (and presumably that of many other systems at the same time) is excessive, and whether the worker needs to be informed of the increased risk. Here the IoT application needs to "understand" the data involved and the decisions associated with it, the worker needs to understand the content and import of the message, and the surrounding ICT system in the environment needs to "understand" that the message was understood.

Thus the first prerequisite in this particular information system is that the individual parts need to have a shared understanding of overheating and know in what way this factor is relevant. The human, who can be trained individually and is endowed with reasoning and intelligence, is the easy link in the chain. But all of the machines involved need to be programmed: they must work according to rules based on knowledge abstractions, especially if they are to be infused with intelligence themselves.

This understanding must be defined in a knowledge representation schema in order to be exchanged. It is usually the task of human designers or programmers to map the relevant knowledge into a knowledge model or ontology[7]. Ontologies, established with dictionaries and semantic rules, can represent knowledge about things at any level of abstraction, from basic properties, such as mass, length and time, up to the level of defining problems via use of a machine, or even considering the ethics of using machines at all. The knowledge thus represented is based on information models which describe data stemming from the real world. To this end, the attempt is made to transfer implicit knowledge of the real world, encapsulated by humans in explicit knowledge configurations, into a form that can be used by machines. The process of digitizing real-world things contains these mentioned abstraction levels.

Ontological data models can be made for each small part of a system (the human worker, a thermometer, an algorithm) but they can also be connected by higher-level ontologies that either capture all aspects of the interaction system or combine them with a few high-abstract concepts. Table 3-1 shows a rudimentary ontological definition derived from a well-known safety model, the bowtie method.

Table 3-1 | Ontological definitions for safety [28]

Concept	Ontological definition
Hazard	OBJECT or ACTIVITY which has the potential to cause HARM. It is PART OF the TOP EVENT and is RELEASED by a THREAT.
Threat	A possible CAUSE that produces a TOP EVENT where the HAZARD is RELEASED. BARRIERS are ATTACHED to specific CAUSES.

7 Ontology in this sense is defined as "a set of concepts and categories in a subject area or domain that shows their properties and the relation between them", www.lexico.com/en/definition/ontology

Barrier	A MEANS of PREVENTING a TOP EVENT or MODIFYING the CONSEQUENCE EVENTS in order to REDUCE the DAMAGE. It PREVENTS other BARRIERS in a point of TIME and is ATTACHED to a specific THREAT.
Critical event	SCENARIO or UNDESIRED STATE which is PRODUCED in a point of TIME by a THREAT. It is PREVENTED by BARRIERS and RELEASES CONSEQUENCE EVENTS.
Consequences	A potential EVENT RELEASED by a TOP EVENT, which directly PRODUCES DAMAGE. This EVENT is MODIFIED by BARRIERS.

Semantic interoperability, or “the ability of computer systems to exchange data with unambiguous, shared meaning”[8], can be considered the key technological requirement in the tripartite system for safety, as the three components involved have to communicate with one another seamlessly. But semantic interoperability will also be determinant for the success of the overall industrial project of creating future IoT ecosystems with open, comprehensible and unified solutions, proceeding from today's still highly fragmented, heterogeneous range of technologies, interfaces, processes and data models.

For communication across different IoT systems such as the tripartite safety system, the semantic level is essential to achieving interoperability. To that end, both sides of the information exchange (i.e., the different IoT systems under consideration) must refer to a commonly agreed reference model. An elaborate system of ontology-driven interoperability solutions has been developed to deal with this challenge.

IEC is already developing ontologies within the IEC common data dictionary (IEC CDD) where product descriptions include structured safety-related properties. Because semantic interoperability is essential for tripartite safety systems, more specific safety-related concepts should be developed in standard database form and hosted in the IEC CDD.

3.5.3 Assurance algorithms

AI offers the promise of solutions to complex problems that extend beyond the reach of mere human intelligence. However, this development comes with an inherent problem: the explanation of a solution does not necessarily mean that the solution discovered is safe. The AI engine may generate hazardous events due to inappropriate data in the learning phase and generalization errors in the reasoning phase. Therefore, safety needs to be enforced and AI systems themselves need to be equipped with independently operating safety verification algorithms. The concept is illustrated in Figure 3-5 [29].

Assurance algorithms operate on the basis of deep learning (DL) networks. DL is a method of machine learning utilizing neural networks containing middle layers composed of more than two levels, see Figure 3-6.

DL is characterized by three types of learning: supervised, unsupervised and reinforcement learning.

8 en.wikipedia.org/wiki/Semantic_interoperability

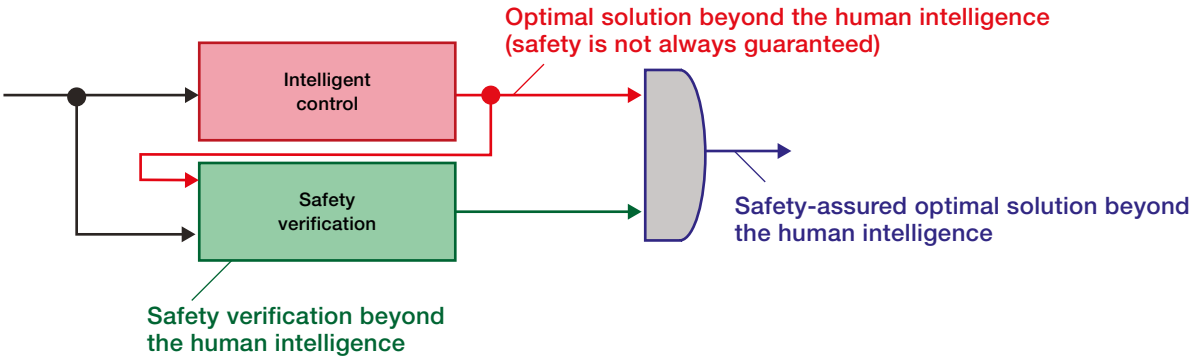


Figure 3-5 | AI equipped with a safety verification

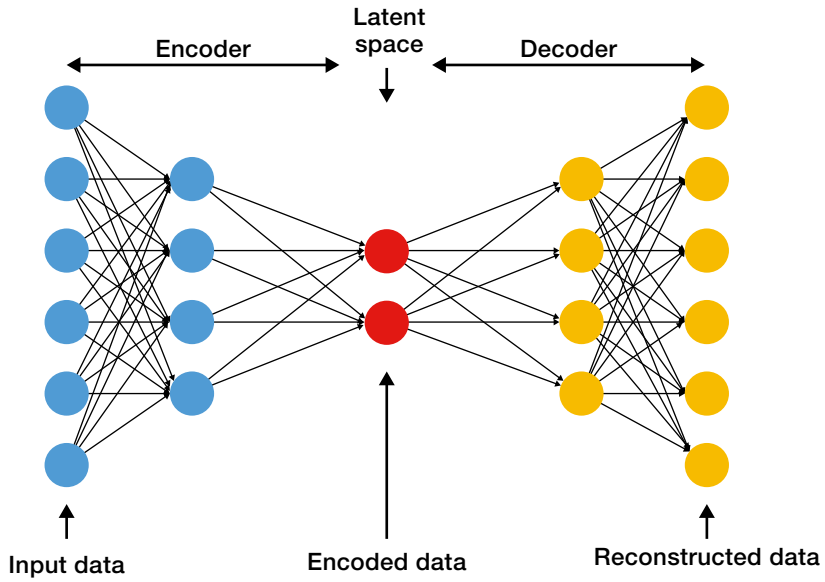


Figure 3-6 | Deep learning neural networks

In **supervised learning**, specific input data and corresponding output data are both provided. The particular merit of supervised learning lies in data compaction. Although the method is efficient, it is not designed to discover new trends. The safety of supervised learning depends on the quality of the data provided. It is especially susceptible to the effects of incomplete data or incomplete calculation (the inability to deal with data unused for learning). If this learning type were employed for safety assurance, it would be necessary to provide standardized protocols for human supervision (perhaps strengthened via algorithms) to ensure that AI engines were trained with the correct data and adequately tested in both the learning and reasoning phases of the AI process.

Reinforcement learning uses envisaged outputs as a reward function. It continues to depend on the introduction of (known) key topics but also allows for variations and new topics via a flexible reward function. The merit of reinforcement learning lies in automated optimization involving

a certain degree of control over the objectives. The safety of reinforced learning depends on the input data provided and the output-based reward function (which contains evaluation criteria), as well as the completeness of the calculation. For safety verification, a human controlled verification function needs to be added (a kind of safety-related function that monitors solution boundaries) in order to steer the AI engine away from unsafe solutions during the reasoning phase.

Unsupervised learning functions on the basis of input data only. Corresponding output data is not provided. The merit of unsupervised learning lies in its data-mining-like function. In other words, the extraction of the potentiality variable is possible with this type of learning, though the method is relatively weak in labelling outputs in the way a human would normally do. This can be a problem vis-à-vis the completion of safety objectives. In fact, unsupervised learning offers no safety guarantees whatsoever. If a safety function were added, it would need to consist of a fully automated safety verification function operating as part of a control of the unsupervised learning algorithm and, paradoxically, might actually contain unsupervised learning itself.

3.6 New technologies for tripartite systems

In addition to the key technologies described above as well as others like them currently in application, newly developed technological approaches promise to revolutionize the digital environment in which the interaction of humans, machines and ICT systems forms the basis of tripartite systems for safety.

3.6.1 Digital twins

Among the range of possible responses in its operational arsenal, the IoT industry disposes of a ready-made solution based on established available technologies, which can simulate the workspace in a digital environment: the so-called digital twins construct. In the simplest of terms, a digital twin involves the bridging of cyber and physical worlds. In a broader sense, a digital twin is the emulation, or mapping, of the physical world into a cyberspace, by which changes effected within either sphere are reflected, predicted, or looked for in the other. In a safety context, a digital twin constitutes a holistic digital model used to support a safety case.

Examples of such mappings include building information systems (BIS) in the construction industry, through which ambitious building projects are entirely modelled on computer systems [30], and in manufacturing, where computer-aided design and manufacturing (CAD/CAM) systems aid in the design of components, parts and machines [31]. In terms of safety, this technology enables enhanced worker safety and contributes to a better understanding of impending or unforeseen safety issues. Digital twins offer an optimal framework for testing specific safety practices, simulating fires and explosions virtually, and deploying tested proven materials such as water sprinkler/extinguisher systems in a simulated context.

But the potential of digital twins does not end there. When a digital twin mimics a real working environment, it brings a dynamic approach to workspace practices, an approach that in the past was strictly static and limited solely to the physical world. The example in Figure 3-7 illustrates the case of a digital twin in a manufacturing environment. When the term “digital twins” is applied within the context of worker safety, a more suitable designation might be “digital twins for collaborative safety”, or “digital twins for human-machine workspaces”.

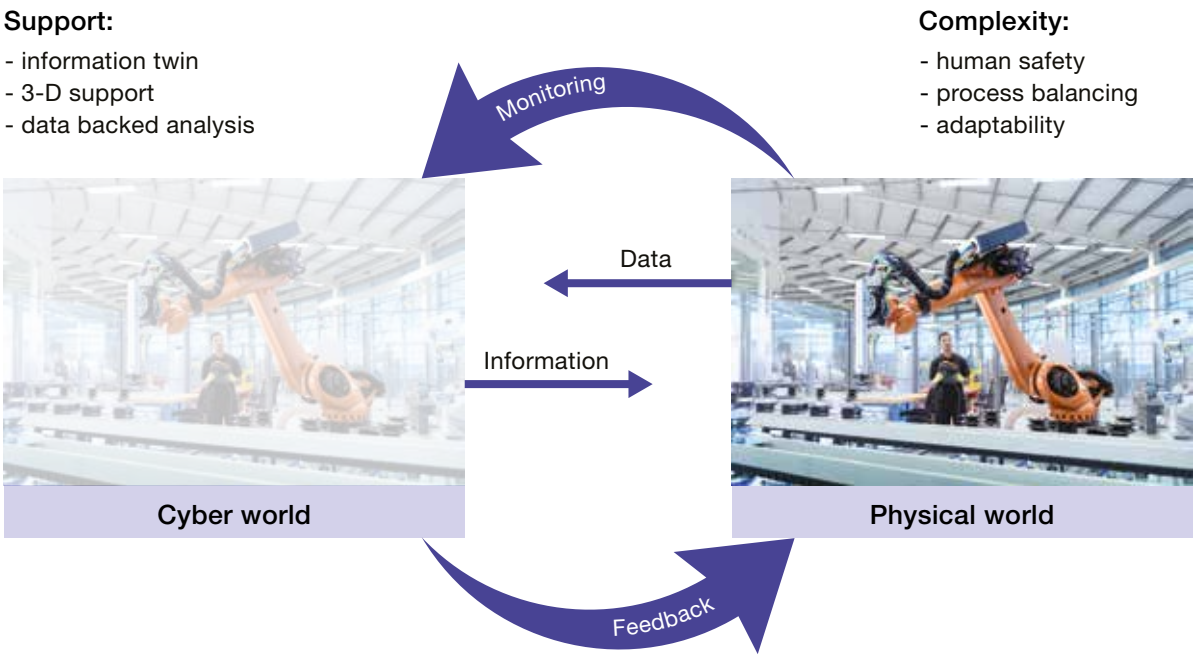


Figure 3-7 | Digital twin operating in parallel with the physical world

3.6.2 Real-time collision avoidance

Real-time processors (whose functioning is colloquially referred to as "high performance computing (HPC)", when coupled with vision, motion and other sensors, can create a working environment that includes robots in motion which are capable of preventing collision with humans and other objects, regardless of whether such objects represent static or dynamic obstacles.

Collision avoidance is a concept widely used in autonomous vehicle systems, including remotely operated vehicles, marine shipping and cars. However the concept has proliferated to include robots as well. With regard to transport operations, collision avoidance systems represent a significant and potentially paradigm-changing approach to the design of workspaces in which humans and machines collaborate operationally together without need of shielding, halting or proximity warnings.

This white paper foresees the future of human-machine interaction being based on real-time motion detection, processing and response that is rapid enough to outperform human reflexes. The speed involved requires next-generation robotics that feature real-time processors for dynamic, real-time motion planning. Such planning allows for the calculation and execution of specific robot motions from a given starting point to a projected end point (goal), while enabling for avoidance of stationary or moving obstacles that may have entered the robot's field of motion. Figure 3-8 illustrates what such real-time motion detection could look like.

When an obstacle is placed in the way of a robot, for instance while a person is in the process of putting a box on the workbench, both the obstacle and the human are sensed by the robot via visual or other detection equipment, and the system calculates a new motion roadmap. Depending on the speed with which the objects move, several responses are possible:

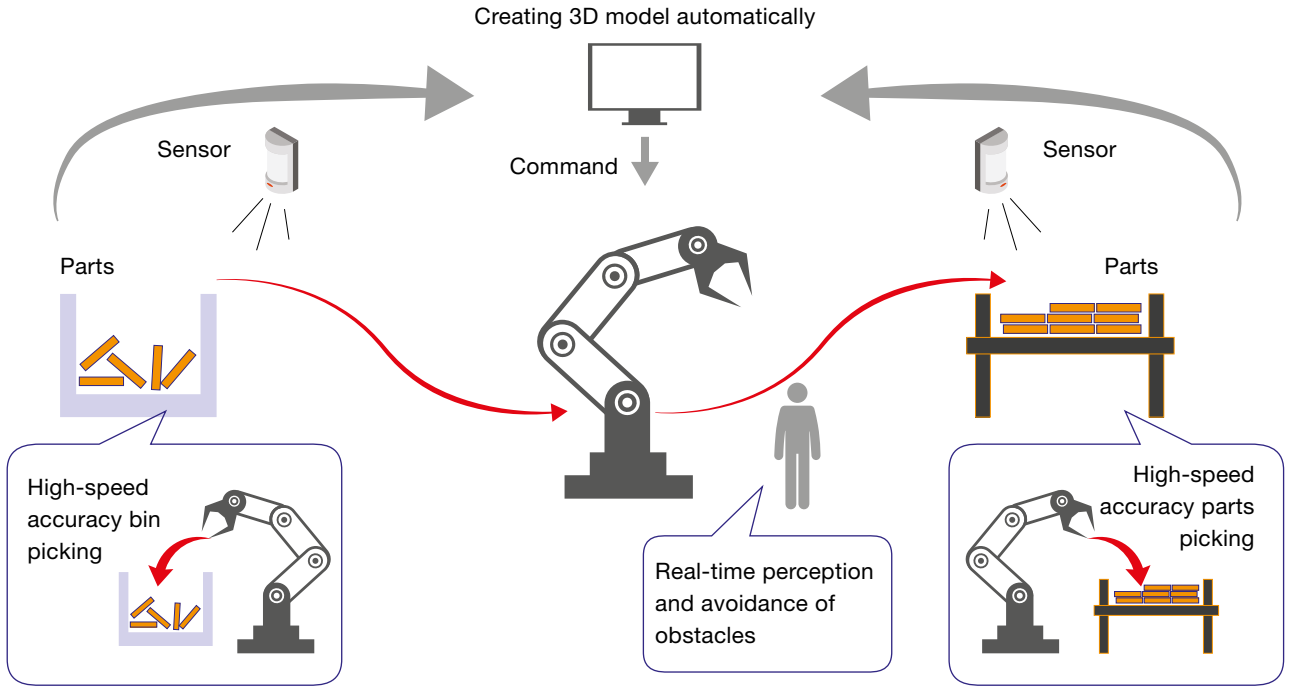


Figure 3-8 | Key elements of real-time motion: detection, recalculation and execution

- in the case of stationary or slow-moving obstacles in the way, or people performing normal work-tasks, the system prevents a machine from continuing along its original path
- in the case of fast-moving objects, the system stops the robot's motion in time to prevent it from colliding with the obstacle and re-assesses its goals in order to create a new motion path
- if the intrusion is too fast for the mechanical arm to respond, the system stops its motion in an attempt to minimize damage

3.6.3 AI-assisted behavioural analysis

Advanced edge AI will be able to detect unusual human motions without the need for prior "teaching data" from the cloud. AI will thus be capable of analyzing human motion and behaviour in the workplace. With sufficient computer power from the machine itself, or additional computing power furnished by the environment, the machine can be trained to inform the worker of unsafe motions or unhealthy postures in performing operations. Such information can then be used in a traditional Deming cycle model that supports continuous improvement of the work process and the work environment. The Deming improvement cycle (plan-do-check-act) will thus become an additional arena in which AI and humans share roles to improve the overall safety of work environments, see Figure 3-9. Indeed, with the right instructions, AI can even perform certain tasks for worker safety.

In their most basic configuration, such systems encompass sensor and signal processing technology that is capable of detecting, even without prior machine learning, slight differences in human movement that may be overlooked by the worker or by those around him.

Edge AI coupled with faster processing times can detect aberrations in motion or unneeded motions on the part of the worker, that are otherwise undetectable by typical human observation. Several techniques could be applied to detect such anomalies, including, among others:

- boundary estimation of motion elements: after repeated observation of work processes the algorithms determine the reach of the normal workspace and any exceedances of that space
- standard operation patterns: the algorithms recognize how long repetitive tasks normally take and detect any deviations from the pattern. This may help prevent fatigue, unintended injury or other health and safety-related problems
- detection of non-standard behaviour or postures: the algorithms detect non-ergonomic positioning during standing or sitting or extreme body movements that indicate fatigue or boredom (such as stretching or walking in circles)

When such anomalies are detected, the AI algorithms can suggest small alterations in human behaviour, such as lifting with a straight back or walking a bit more slowly. Equally the system can suggest breaks or adapt the work process in collaboration with individuals.

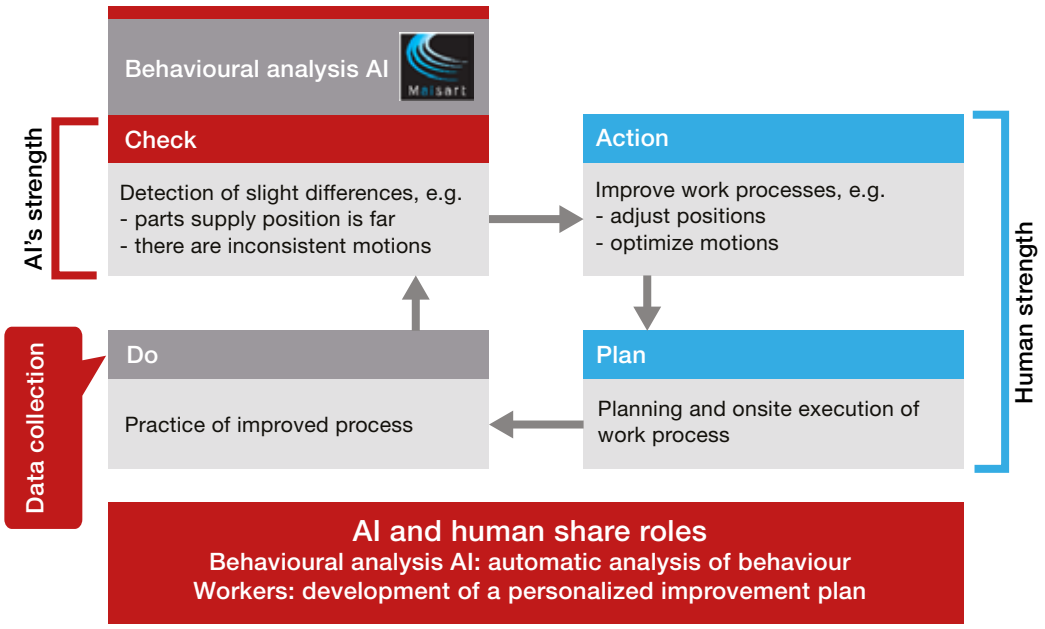


Figure 3-9 | Behavioural analysis AI

3.7 Technological necessity: cyber security

With the increased use of information technology, cyber security forms a cornerstone of efforts to manage the growing complexity of safety control systems, particularly as this pertains to smart manufacturing and collaborative safety mechanisms. But the complexity of such systems is increasing their vulnerability to threats which can lead precisely to the loss of the safety functions.

ISO/IEC 27000 provides an overview of information security management systems (ISMS). It constitutes the base security standard used as the reference for all sector-specific standards according to IEC Guide 120, *Security aspects – Guidelines for their inclusion in publications*. The ISMS framework is used to protect the confidentiality, integrity and availability of sensitive information. An information security management system provides a systematic approach to risk management, containing measures to address the three pillars of information security: people, processes and technology.

However, industrial control systems (ICS) differ substantially from general information systems. While protection from dynamic and variable threats remains important to both, safety represents the most crucial element in ICS. If an ICS is corrupted by an attack, the risk reduction offered by its safety function no longer works. The system becomes unsafe, and employees can be at risk. The objective of safety necessitates security. The goal of a new information security management system for industrial control systems is to associate integrity, availability, confidentiality and safety. Some ISMS implementation measures may include safety aspects in the availability factor. But this is insufficient for industry. Social impacts due to threats and vulnerabilities such as hacking, natural disasters, and internal problems inherent in the control system can cause great damage resulting in severe economic and social disruption.

Therefore, safety should be acknowledged as an essential value in ISMS, at a level equal with integrity, availability and confidentiality in industrial control systems. The systems approach of risk management is essential for this purpose. All system and product standards supporting safety functions and connectivity should include cyber security requirements based on ISO/IEC 27000 or other sector-specific security standards.

3.8 Implications of standardization and conformity assessment for the tripartite model

Regulators monitoring human-machine safety in the tripartite model will need to take into account a variety of factors, including:

- the conformity assessment of the individual components, such as the product
- the sum of all the products and their interaction systems type certification
- the personnel competency and certification of persons working in these environments

Whether individuals are working in a robotics assembly line or on a construction site, product safety, systems safety and personnel competency are all critical for a safe work environment.

The tripartite safety approach makes it easier to separate individual standardization activities in order to focus on different parts of systems in their entirety. Technically, the demand will be for standardizations and/or guidance for each component of the tripartite system on a relatively high abstract level: ensuring safe work environments for humans collaborating with intelligent machines; defining achievable safety goals for the machines, especially those implanted with intelligence; and providing a framework for interface with systems on the periphery of the workplace, focusing on (semantic) interoperability, computing power and ethical and security standards.

Standards for the machine will differ little from existing standards containing technical specifications. Such specifications may range from relatively straightforward standards addressing the physical systems that humans work with, to electrical, machine and robotic systems safety standards. Where machines interact in a collaborative environment, novel high-level standards may have to be developed to provide safety goals for intelligent machines, perhaps including such elements as reaction times, movement speeds and/or maximum impact on the human body.

Something similar holds for systems in the environment. The ISO/IEC JTC 1 provides a framework for discussing requirements for peripheral edge equipment or equipment in the cloud. Its subcommittee on AI (SC 42) also seems a relevant forum for discussion, but safety aspects may have to be treated separately or in conjunction with horizontal standard groups for safety.

Regarding humans in the workplace, it seems sensible to install a certification system that clarifies the level of knowledge and competence that a person needs to possess in order to work with, maintain, program or design machines intended for intelligent human-machine collaboration.

For the tripartite system, where the three components come together, certification frameworks should be developed focusing on integrated systems rather than parts. This could include an elaborate risk analysis, such as that used for railway safety cases (IEC 62278, *Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS)*), but simpler systems demonstrating conformity of individual system components could suffice.

In each of these parts, conformity assessment seems relevant. As defined in ISO/IEC 17000, conformity assessment is the demonstration that specified requirements are fulfilled. Such requirements may include regulations, standards or technical specifications. Conformity assessment can cover many different types of activities, such as testing, inspection, validation, verification and certification, applied either individually or in combination. Three functions are used to demonstrate that specified requirements are met: selection, determination and review, see Figure 3-10).

Conformity assessment activities utilize various ISO/IEC Standards developed under ISO CASCO for accreditation purposes. These include ISO/IEC 17025 which covers the general requirements for the competence of testing and calibration laboratories, ISO/IEC 17065 which is the product certification bodies accreditation standard, and ISO/IEC 17024 which specifies criteria for the operation of a personnel certification body (also known as a certification body for persons).

With regard to innovative technologies applied in the tripartite model, such as AI in the environment, human-machine interaction and functional safety for workers, conformity assessment bodies and regulators will need different skill sets, competencies and adaptation techniques in order to address requirements of the digital transformation era without slowing innovation. In the new context, a product is no longer just a mechanical and electrical device. It is embedded in a tripartite work system in which humans, machines and intelligent software in the periphery of the work environment are all interconnected via machine learning capabilities. Conformity assessment bodies, standardization organizations and regulators will have to incorporate the technological environment in which products evolve and pay explicit attention to the role of humans and of human and social values in this environment.

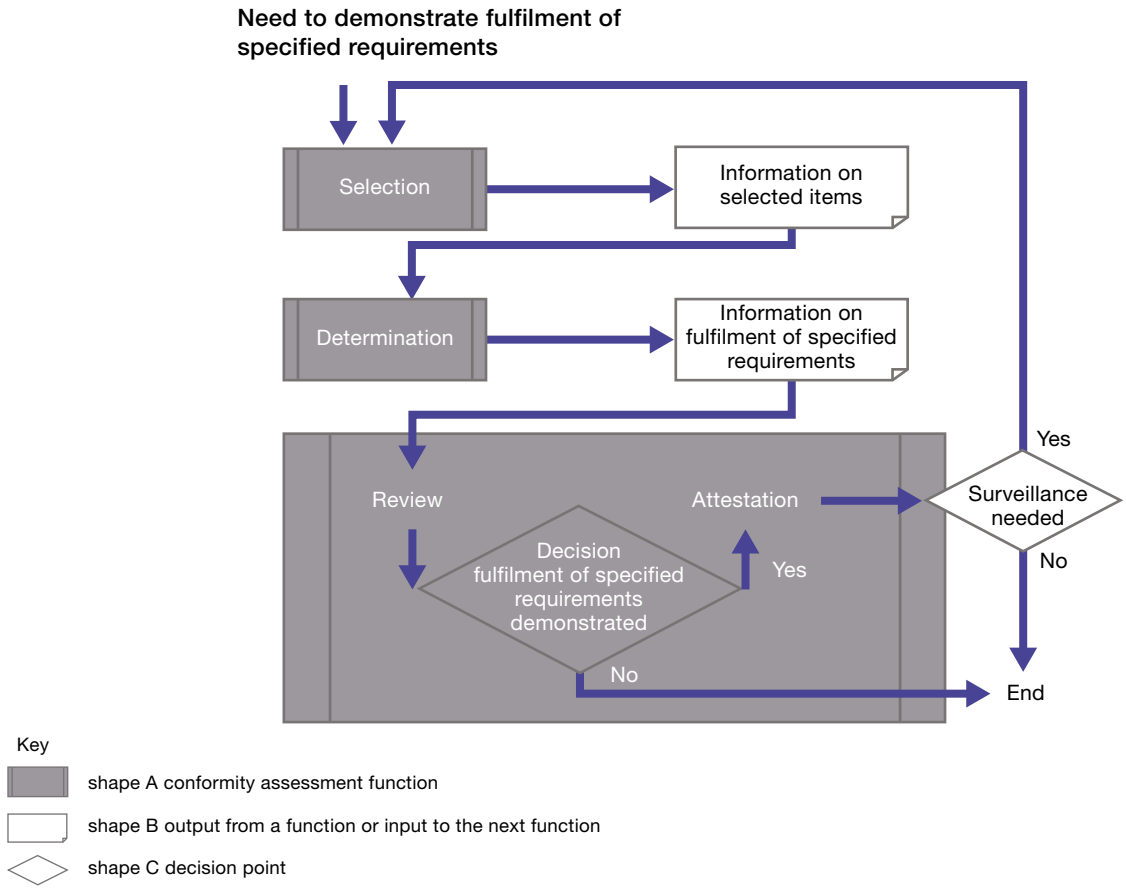


Figure 3-10 | Functional approach to conformity assessment (ISO/IEC 17000)

Section 4

Application areas of the tripartite system

This section provides various examples of projects, works and companies that are pioneering innovative safety solutions for the future involving electrotechnical equipment and intelligent machines. The applications involved are not necessarily logically connected, but patterns of use in the tripartite system for safety can be recognized. Some of the solutions developed focus on exploitation of the raw computational power offered by AI in safety-related environments such as health care or manufacturing. Others focus on networks as the backbone for safety, such as in remote sensing maintenance or industrial farming, or target safe interaction between humans and machines, which mostly takes place in manufacturing sites involving robots. All of the examples highlight the need for clear interfaces between local workspaces and their environment and can marshal the forces necessary to develop the innovative safety solutions that the future demands.

4.1 Human-machine collaboration in manufacturing

Many examples exist of the use of collaborative robots in workplaces involving human-machine interaction but without the presence of safety fences. While conventional industrial robots are generally separated from humans by barriers, collaborative robots eliminate the need for such safeguards, allowing direct interaction with humans in environments in which both human workers and machines cooperate. Under such conditions, the robot is mainly assigned responsibility for repetitive or physically taxing work (the so-called 3D tasks: dangerous, dirty, demanding), with humans thus able to concentrate on tasks requiring manual dexterity [32]. Figure 4-1 illustrates such a situation. Concrete examples of this kind of arrangement are detailed below.



Figure 4-1 | Example of a working environment where workers and robots collaborate (source: www.acro.com)

To maximize space and flexibility in a hybrid vehicle (HV) inverter production process, involving small and varying product quantities, a major Japanese automotive company[9] has adopted collaborative

9 Toyota motor corporation, https://global.toyota/en

robots to facilitate assembly and checking. For instance, a robot determines the position and orientation of HV inverters depending on the worker's height. Collaborative robots can also be used in pairs to perform the function of a jig: one for simple screw tightening and another to place the workpiece at a convenient angle for the worker's intervention. In addition to reducing burdensome work procedures for workers by up to 60%, the use of collaborative robots in manufacturing represents an effective method of lightening both physical but also psychological stresses [33].

At a leading manufacturer of robots[10], collaborative robots are used to assemble ball screws, with robots carrying the heavy actuators and workers performing tasks that require manual dexterity, such as setting the bearings.

A multinational machine tool manufacturer[11] is developing an automated guided vehicle (AGV) robot consisting of an AGV, a collaborative robot, a vision sensor, an electric hand and a laser scanner. The AGV robot can be used, for example, for installing and removing work pieces, blowing air, and deburring. It is capable of running autonomously to a given destination, while avoiding obstacles around it. This eliminates the need to place electromagnetic tapes on the workspace floor, thus facilitating changes to the factory layout. The AGV robot can also be used for distributing goods inside the factory. Unlike with a conventional automation system, this technology makes it possible to provide a free layout design and take charge of logistics in a factory. The appearance of AGV robots signifies that the robots have legs. That is, rather than constituting an automated system in a closed space or a restricted area, the AGV robot works in the same area and at the same level as a human, thereby advancing the coexistence of the robot and the human.

The above examples highlight human-machine collaboration in the tripartite system. The systems demonstrate that, given sufficient aptitude and speed in avoiding humans, they can be made to interact safely with their human counterparts [34]. Currently such systems constitute early adaptors and are custom-made responses to specific operational challenges. This makes it difficult to scale these systems up to involve a wider variety of workplaces within the same factory, let alone transpose safety lessons from one worksite to another. These work environments would benefit from tripartite systems by identifying and clarifying the interactions occurring between humans and machines and optimizing their functioning for safety, based on consideration of both the parts and the whole. Another advantage would involve taking environment systems into consideration when designing safety functions.

4.2 Intelligent machines in construction

In western Japan, construction is underway of the Takimurozaka tunnel on national route 57 in Aso, where cutting-edge sensing, lighting, and AI technologies have been experimentally introduced to improve safety [35]. An intricate network of smart safety systems is installed that leverages human information as well as machine and environment information, see Figure 4-2.

Several smart safety systems are installed in the work environment. To begin with, the tunnel is equipped with beacons and detection sensors installed in many locations, including in the construction area, on the workers' helmets and on the heavy machinery. This allows the location of the machinery and the workers to be tracked and viewed on tablet terminals. To prevent accidents, the wheel loader is equipped with AI cameras on the right, left, and back, with an alarm light and

10 FANUC Corporation, www.fanuc.com

11 DMG MORI. CO. LTD., www.dmgmori.co.jp/en

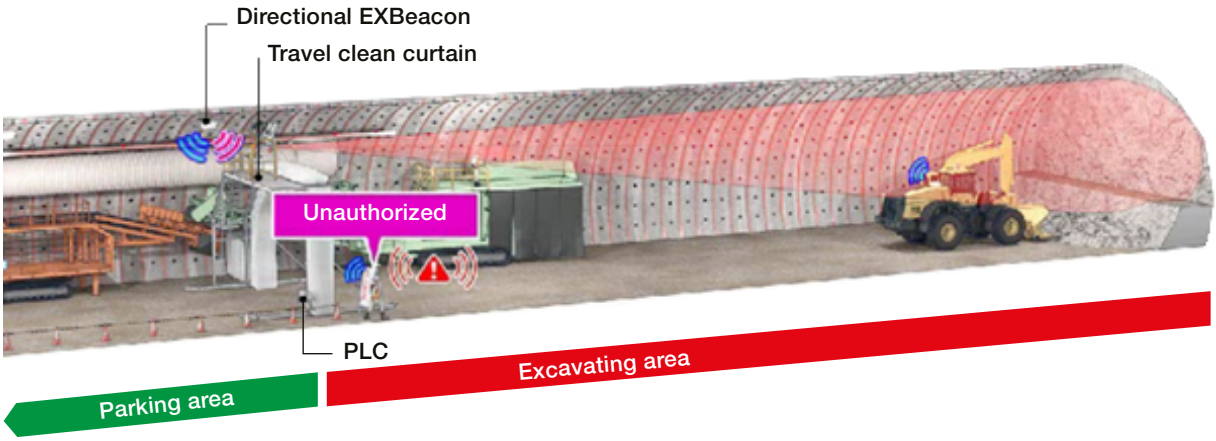


Figure 4-2 | Tunnel protection system connecting workers, machinery and the environment via ICT

buzzer connected to each AI camera. The AI cameras detect workers near the wheel loader and warn them about any wheel loader manoeuvres. Even the lighting system supports safety. First, because the site works at higher light intensities than is normal in these situations: 200 lux is the standard for this tunnel protection system rather than the usual 100 lux standard. That alone increases safety compared with average tunnel construction sites, as good visibility makes working conditions easier and facilitates the detection of abnormalities. Second, when a worker enters a restricted area, creating a potentially dangerous situation, the lighting colour changes from white to red, and a warning alarm is triggered. Given that excavation sites are particularly noisy, changing the colour of the lighting is quite effective. This rigorous approach to safety won the project a Safety 2.0 conformity marking from the Institute of Global Safety Promotion (IGSAP) in March 2020. The conformity marking attests to the fact that a system satisfies the requirements of collaborative safety.

In terms of the tripartite system, this workspace constitutes a strong showcase for intelligent machines: roll loaders are equipped with cameras and AI to detect humans and inform them at the appropriate time. The collection of systems, the intelligent cameras on vehicles, the lighting and worker tracking systems all make this worksite a front-runner in terms of a dedicated AI system for safety. It integrates the worker, machines equipped with AI functionality and environmental systems (the lighting system). Because location information on workers and machines is shared to support safe control of machines and safe actions by workers, the collaborative safety level rating of this system may be considered to be close to CSL-3, with clear guidelines in standards. The CSL level could be determined more specifically and formally and points for improvement could be prescribed. The tripartite approach could contribute to making it easier for systems that are constructed like this to design a safe work environment by standardizing requirements for the individual systems involved, as well as safety certification of the system as a whole.

4.3 Intelligent networks in the environment facilitating farming safety

Digital farming is emerging as a major trend in the agricultural industry. In digital farming, workers, machines and the environment are connected by

ICT to promote safety as well as boost production activities. For instance, the resulting network facilitates better management of chemicals used in agriculture, in part via sensors supported by the GPS system, see Figure 4-3. In addition to fixed sensors, mobile sensors placed on machines and unmanned aerial vehicles (UAVs) help collate maps concerning moisture, soil compaction, fertility, leaf temperature, micro-climates, and insect, disease and weed infestations, which are all analyzed by the data management system using AI technology. Thus, ICT systems support farmers in knowing exactly which and how many chemicals need to be put in the field, and where. This precision helps to minimize the use of chemicals for crops production, thereby reducing the risk of chemical exposure and related diseases for people living near the farm.

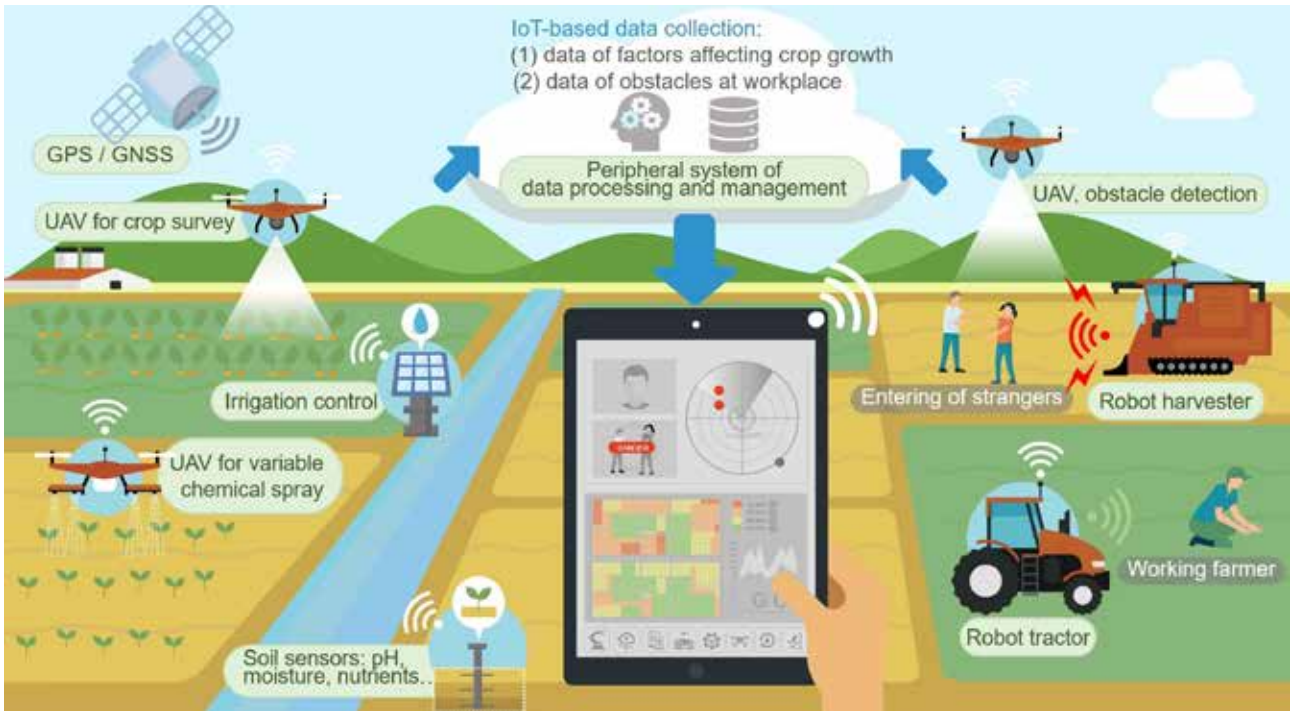


Figure 4-3 | Networked throughout for farm health and safety (Source: The National Agriculture and Food Research Organization (NARO))

But the network is also a showcase of how humans and machines and digitally enabled environments can work together to maximize total performance. Machines are good at performing repetitive and heavy tasks, and humans are good at rearranging objects, decision-making and creativity. Thus, the concept of human-machine collaboration is an appropriate strategy in terms of both production improvement and safety control in agriculture.

As in the example of the tunnelling project in Aso, the addition of sensors, safety devices and drones can map out risks associated with production. Safety information is then conveyed to peripheral systems, where data processing is conducted. If a hazardous situation is likely to occur, the system can generate an alert to the supervisor and to the machines involved to take appropriate actions. Such systems will provide farm managers with the possibility of removing obstacles to accident prevention in the future.

The above example highlights how a well-developed digital network that coordinates the

work between humans and machines can facilitate safety. Extensive peripheral ICT networks and systems help workers to stay safe and share health information with the farm manager. The system can issue alerts if weather conditions change, and if the worker is equipped with wearable detectors, his health can be monitored. If computing power in the periphery is sufficiently strong, AI can support analysis, prediction and prevention of accidents.

4.4 Electrical power distribution systems with automated safety features

The safety of electrical power distribution systems has been in the forefront of concerns since their inception: transporting abundant amounts of energy is inherently unsafe. However, the energy landscape is facing a variety of dramatic changes, in particular due to the introduction of distributed and/or renewable energies, the progressive shutdown of major power plants which were guaranteeing the stability of the grid, and the implementation of advanced energy efficiency programmes at user levels, including the possibility for any grid user to become a "prosumer" rather than a consumer of energy. Related local production and auto-consumption trends include running off-grid as a microgrid, when needed, implementing aggregated forms of consuming electricity or providing services directly to the grid.

This new metamorphosed energy landscape clearly poses challenges concerning the way the safety of electrical infrastructures needs to be addressed. However, once again, many innovative strategies are being deployed to ensure the same level of resilience of electrical infrastructures in the face of new risks. The first of these strategies is the intensification of digital means to allow:

- an increased monitoring and control functionality of the infrastructure itself, as well as on the part of end users (through smart meters); this technology adds an ever-increasing ICT functionality to power distribution control centres
- detection and reduction of common mode faults, e.g. those caused by the multiplication of (small) unmanaged distributed energy sources
- predicting and responding to outages
- increased energy forecast capabilities based on smart-grid meters
- a progressive shift toward conditioned-based maintenance of assets, again through the use of end-users' smart grids, but also drawing data from the network itself

In a drawback to the intensified use of digital means, the industry has been plagued with cyber security threats. In many ways, cyber security has become a major concern and source of safety risks, as a result possibly impacting the resilience of the grid. Even if grid management systems do not normally interact directly with workers, many workers depend on them in order to function. The problems faced by this industry highlight the need for cyber security in any digitally-enabled safety system. They also demonstrate the fact that local tripartite safety systems must clearly describe system interfaces in terms of grid codes, smart monitoring and reliability.

4.5 Smart monitoring maintenance of power distribution networks

High-voltage power transmission lines span a variety of geological environments. This often poses significant safety risks for inspection personnel, in addition to those generated by natural disasters such as floods, earthquakes and landslides. Intelligent inspection approaches based on AI enable more efficient and timely line inspections, thus greatly reducing the security risks faced by personnel. The intelligent inspection material involved is equipped with local AI model reasoning capabilities to autonomously identify

relevant parts of the system being investigated and link them with major risk scenarios.

Transmission line inspections need to identify various types of risk scenarios, including body defects (such as insulator defects, loose bolts, metal deformations, etc.), passageway risks (posed by dangerous constructions, ultra-high buildings, etc.) or external foreign objects (bird nests and other natural intrusions.). This requires intelligent inspection equipment that can process high-definition images and video rapidly. The identified risk alarms are transmitted to the on-site inspectors in real time and sent to the central monitoring master station via the wireless network for timely processing. At the same time, labelled images identifying the risks are also summarized in the cloud for model training and optimization.

Since the environments involved and the faults vary widely, the model itself needs to be optimized and updated continuously. It is thus very important that the intelligent inspection system be able to perform cloud-edge collaboration. In the cloud, the powerful AI acceleration capability is used to generate and optimize the model, and the information is transferred to the intelligent inspection equipment through the network to synchronize the update.

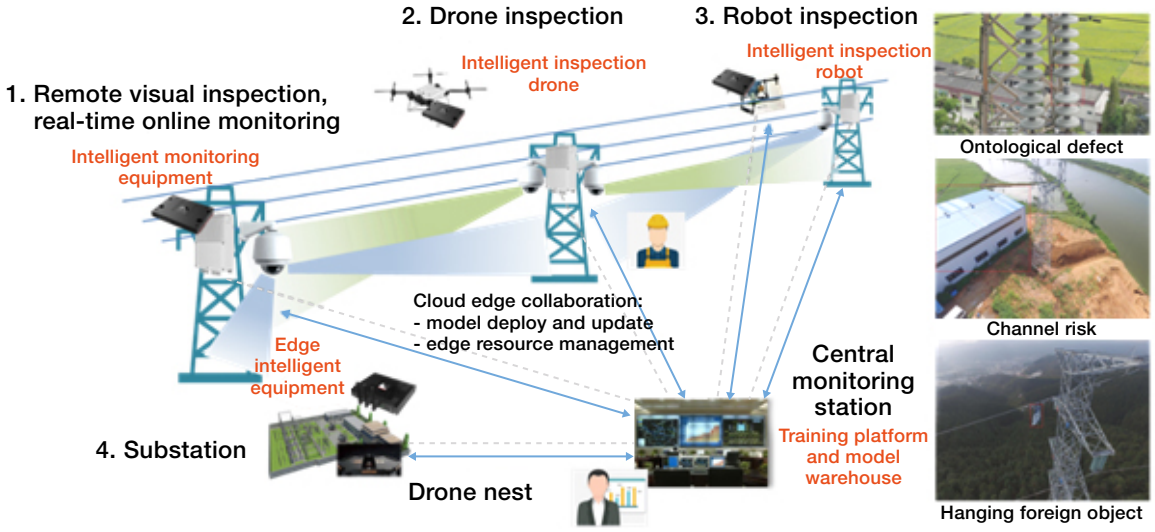


Figure 4-4 | Smart monitoring systems for power lines

The example in Figure 4-4 demonstrates how maintenance work can be rendered much safer when sensing systems support humans. Inspectors do not have to scale dangerous heights, can identify hazardous situations more quickly and, when such systems are used in conjunction with power networks, can solve problems remotely.

4.6 Public safety in cities

While many cities, particularly those who have invested substantially in safe city technologies, may experience a reduction in crime rates in the future, traditional crimes (e.g. burglary, extortion, kidnapping, assault, public order infractions, serious traffic crimes) will nevertheless persist, especially in cities marked by high unemployment

rates and sharp wealth distribution inequalities. It is expected that criminals will modify their behaviour to counter the effects of safe city technologies, for example by avoiding surveillance cameras, not carrying electronic devices on the body, or travelling to cities with fewer safe city technological mechanisms in order to commit their crimes. Organized crime groups, especially those involved in transnational crimes, will widen their reach through the use of digital platforms, and links may emerge between terrorists and organized crime groups, whose illicit gains are generated mainly through smuggling, drug trafficking, production of synthetic drugs and illicit trade of natural resources.

Beyond the sphere of crime, globalized health threats will continue to impact public safety. With bodies as diverse as the World Health Organization and the World Economic Forum opining that public health outbreaks are likely to become ever more complex and challenging, it is evident that the current COVID-19 crisis will not be the last serious pandemic the world faces. Furthermore, under the effects of ecological degradation and global warming, cities will become increasingly dense, and shanty towns – marked by inadequate housing and a lack of basic services such as water, sewerage, electricity and waste management – will swell. Under such conditions, epidemics are likely to contribute to public disorder in the same way crime does.

In response to such evolving threats to public safety, authorities in most countries are elaborating digital safety systems. Most of these systems are operated independently, but where privacy regulation permits, databases may be connected with one another to increase the chances of detecting crime, terrorism, epidemics and even natural disasters. This kind of cooperation constitutes collaborative public safety and will be increasingly adopted in the future. Many public safety agencies will have implemented some form of collaborative C4ISR or C-C4ISR[12] solutions, which contain the following main components:

- collaborative Command & Control (C2): Enabling a converged and visualized command centre, allowing multiple agencies to work together through a single emergency number with automatic call analysis, filtering and distribution, and with visualization beyond mapping, such as real-time video surveillance and social media integration
- collaborative Communication (C): An enterprise LTE-based broadband critical communication trunking system that allows voice, video and mobile apps to operate on a single device and has the ability to interoperate with other similar as well as legacy systems. The system must provide a rapid version for fast deployment in areas with no coverage
- collaborative Cloud (C): An OpenStack-based scalable and elastic platform that maximizes computing resources, supports information exchange, allows user-centric apps, provides dynamic resource allocation when demand surges, and facilitates agile deployment of new services
- collaborative Intelligence (I): Using big data technologies including massively parallel processing database and analytical algorithms, to discover unknowns and to connect the dots
- collaborative Surveillance (S): A two-tiered intelligent video surveillance cloud for effective analysis and efficient archiving, with virtualized processing at the edge nodes, and super-fast transfer of high-resolution video between edge nodes and the central node
- collaborative Reconnaissance (R): A secured IoT cloud platform, with unified API interface for sensors from various suppliers, that supports massive concurrent processing

12 C4ISR and C-C4ISR are collaborative public safety solution frameworks developed by Huawei, www.huawei.com/en/news/2017/4/C-C4ISR-Public-Safety-Solutions

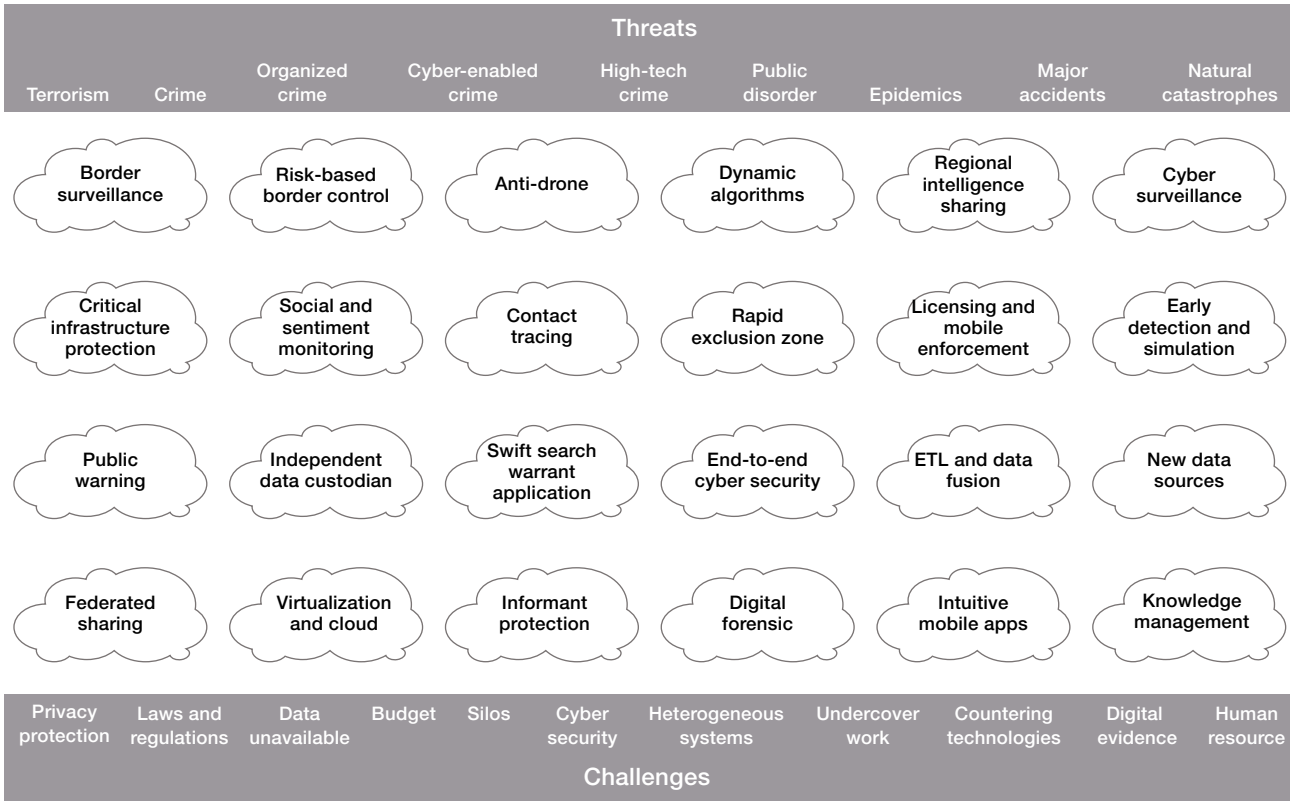


Figure 4-5 | Threats and challenges for collaborative public safety

With regard to the tripartite system, the collaborative public safety strategy demonstrates that city- or nationwide ICT systems are being developed that will eventually become the backbone of various enterprise systems, see Figure 4-5. Furthermore, it shows that the "environment" of the workplace may be connected to a massive enterprise architecture system, in which various forms of information converge to generate smart decisions based on data integration and AI. Even if international corporations have diverse objectives, their enterprise systems may be expected to be of a similar scale and complexity to enable collaboration with a wide range of entities (e.g. an oil company monitoring thousands of well-heads, refineries and pipelines of different makes and brands). In the case of both public safety frameworks and corporations, the need exists for laws and regulations governing data exchange between different entities. Such sharing can occur either on a case-by-case, batch, or real-time basis. As the data comes from different sources, the challenge posed by the lack of an encompassing data standard also needs to be resolved.

4.7 Access to electricity

Today, around 1,1 billion people worldwide have no regular access to electricity. SDG 7: Affordable and clean energy, focuses on ensuring access to affordable, safe, reliable, and clean energy for all by 2030. But providing electrical power is easier said than done. Connecting every dwelling and home worldwide to a stable electric grid is expensive, time-consuming, mired in regulations and fraught with the challenges posed by rough, remote terrain. As a result, the conventional grid model involving far-flung power plants connected to remote sites

through a complex network of transmission lines and substations is under pressure to evolve and to adapt to the new possibilities offered by technological developments.

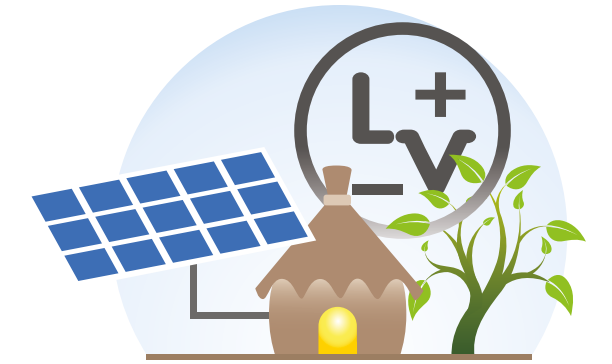


Figure 4-6 | LVDC, electricity as the essential resource of modern life

One solution lies in adapting existing local power technologies, such as solar panels, limited power converters and batteries, to provide power for basic appliances such as lights, radios and possibly even medical kits. Yet safety remains a challenge even in these seemingly simple networks. To ensure protection against electric shock, the voltage of electrical installations is limited to safety extra-low voltage (SELV) using DC power. This enables rural communities to establish low voltage direct current (LVDC) electricity access, which is inherently safe and also remains affordable. This has had a positive impact on securing energy access and reducing inequalities, see Figure 4-6. IEC dedicated systems committee SyC LVDC[13] provides guidance on the standardization of LVDC to achieve this aim. Furthermore, to ensure protection against thermal effects and fire hazards, the total value of loads or appliances (calculated in watts) is also limited, so that the battery capacity and the electric supply passing through the distribution cables are both restricted, and the distance between the appliance and the battery is also specified.

Paradoxically, such rudimentary power systems may be used to charge smartphones. When social media is installed on the phone, the novel electricity users are invariably exposed to AI that may or may not be of service to them. However, the network may also be equipped with tools and apps that instruct users on how to make their LVDC systems safer and which perhaps even monitor such systems via other apps. On the face of it, this technology would not seem to benefit from the tripartite system, which tends to focus on high-tech work environments, but nothing could be farther from the truth. Through the use of networked systems, the novel electricity user will have interface with previously unfamiliar vendors or clients and possibly with the gig economy. This example highlights the importance of interfaces in the tripartite system and, to some extent, the needs of humans and the machines that serve them.

4.8 Implications for standardization

This section has shown that the human being is central to safety protection efforts. Machines, whether intelligent or not, facilitate manufacturing, food production, power distribution and information exchange, but they must do so in a safe manner. The works described here demonstrate that it is feasible to install AI-supported safety functions in almost any environment where electricity is available. This re-enforces the IEC view that it would be worthwhile, in collaboration with JTC 1, to establish a dedicated workgroup on guidance and/or standardization activities related to the role of AI in digital safety systems.

Another feature highlighted in this section is the fact that many variations of the tripartite

13 go.iec.ch/syclvdc

system exist in every industry that depends on electricity. Technical standards most likely must be developed to facilitate progress in all of these industries. For example, and as indicated above, given that the standardization of LVDC technologies requires a holistic approach, the IEC has established a dedicated systems committee on the subject. SyC LVDC provides guidance on the standardization of low voltage direct current and includes input from various IEC technical committees, including those related to solar photovoltaic (PV) energy systems (TC 82), the safety of electrical installations (TC 64) and electric accessories (TC 23). For utilities and electrical systems, many standards are already available which potentially provide a basis for designing new standards to guide the introduction of AI systems for safety. The same may hold true for networked (especially wireless) systems. The farming industry, on the other hand, may need to think about developing standards specifically relevant for its needs.

Section 5
Conclusions

5.1 Working with machines that are smarter than humans

This white paper demonstrates that megatrends in society, technological innovations and developments in industry are changing our understanding of safety. Of particular relevance in this regard, ICT systems are infusing machines and workplaces with AI. With further improvement of such technologies projected over the next decade (via quantum computers, superfast networks and chip-based AI), it may be necessary to assume that the human is no longer the smartest component in a system. It is against this background that this white paper addresses safety in the future.

5.2 Putting humans first

It is recommended that standards in the future progress beyond mere prevention of unintentional injury (up to and including death) to design technical systems that work seamlessly with people and in which the definition of safety encompasses a psychological sense of freedom from danger. This means that the IEC and other standardization bodies may have to widen and deepen horizontal coordination efforts on safety, demanding more explicit interactions between experts in different technical committees, and/or enlisting the expertise of safety psychologists or sociologists to represent and address social responsibility issues.

At the same time, standardization bodies need to fulfill their primary mandate – to focus on technical standards for machine developers, suppliers and system integrators to ensure safety in the future. In this context it should be understood that if humans are paramount in collaborative systems, safety by design constitutes the most sensible approach. Worker representatives should be involved in the development of standards for safety, and the standards should consider all stages of the life cycle of electrotechnical products or systems.

5.3 What are the challenges for ensuring safety in the future?

5.3.1 A pillar of trust for social responsibility

IEC origins lie clearly in the development of technical standards covering manufactured electrotechnical systems and their safety, But with the advent of intelligence-infused machines, it cannot ignore the social responsibility dimensions involved. Meanwhile governments are relaxing their grip on safety protection regulations (and regulatory strategies in some other social areas) by replacing restrictive technical laws with goal-oriented legislation. Under this less stringent framework, corporations are expected to compensate the loosening of regulatory requirements by assuming social responsibility for safety. But standardization bodies also have an important role to play in facilitating social responsibility through practical standards and conformity assessment processes. Standardization bodies are already engaging with social stakeholders to contribute to achieving social objectives such as safety and security and are uniquely well positioned to bridge the gap between industry drivers and governmental regulators. It is not outside the IEC mandate to move beyond exclusive focus on standardization efforts in order to contribute to achieving aspirational societal

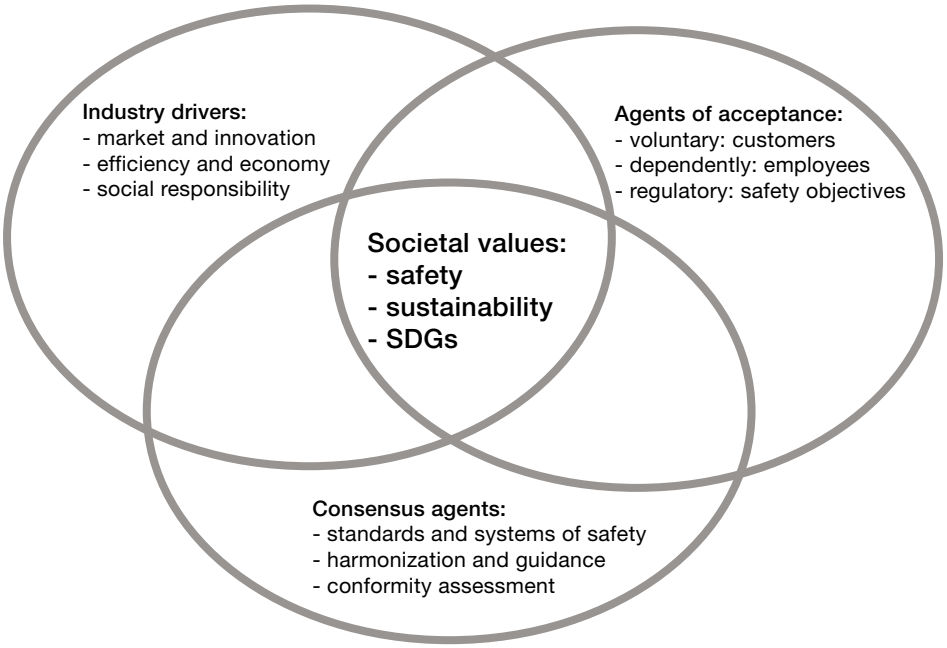


Figure 5-1 | Standards organizations as enablers for societal progress

objectives such as the SDGs. Figure 5-1 proposes a schema in which IEC takes up its position as a third pillar to create trust between drivers of change and regulators. Under this framework, the IEC and other standardization agencies consolidate their position as international consensus brokers to achieve societal goals without diminishing the importance of the work they are already performing. Safety could be a springboard, but as the dimension of safety is deeply entrenched in the SDGs, the opportunity exists to take on a wider role as an enabler of societal progress.

5.3.2 Standardization toward an ecosystem of intelligent systems

The tripartite model for safety offers a systematic approach to safety in the future, a concept illustrated in this white paper with various examples. The tripartite approach makes it possible to distinguish key interests in the collaboration between humans, machines and intelligent ICT systems in the workplace and elsewhere. The flow of information between the various components of the system constitutes the key to safe and efficient production. Whether in farming, robotized manufacturing plants, chemical processing or logistics, the specific design of the human tasks and technologies involved may vary, but the key elements of the tripartite framework are nearly always present in one form or another.

The tripartite system puts humans and their working environment first, but individual frameworks exists in a highly connected world. The tripartite ecosystem not only provides connectivity to adjacent workspaces or the business environment but also extends to financial and banking systems, government entities and legal frameworks, social networks and unions. This intricate web of interconnectivity creates an ecosystem of systems. Whereas the legal frameworks for those ecosystems are better placed within governments and global institutions (the EU white paper on AI refers in this respect to an “ecosystem of trust”),

the technical and operational details of such collaboration more suitably fall within the purview of the IEC and other standardization bodies and their efforts to standardize safety methods, collaboration systems, technical details, innovation frameworks and confidentiality. The tripartite system provides an excellent starting point for such standardization, but eventually individual standards will have to address the ecosystem of systems as well.

But despite the impressive and sometimes overwhelming impact of ICT systems, it should not be forgotten that human qualities of relevance to ensuring safety now and in the future (e.g. values, organizational culture, leadership, commitment and interpersonal communication) are not easily captured in data systems. The danger exists that such factors may become neglected. It is therefore recommended that in the development of future standards for safety, explicit attention be paid to non-technical factors in the social and organizational environment. Here again, performance-based (as opposed to specification-based) standards could be very helpful, especially in addressing minimum safety requirements as the starting point for standardization processes.

5.4 Conformity assessment with intelligent agents

Governments, corporations, employees and consumers rely on the various aspects of conformity assessment to ensure the component safety of the product, process, system, installation, data, design or personnel under review. The introduction of intelligent ICT systems has necessitated the development of new types of standards, which in turn calls for innovative developments in conformity assessment.

First, with the introduction of standards for intelligent systems and ICT, conformity assessment documents (such as rules of procedure and operational documents) need to address the more agile operations involved in a fast-moving technological environment. Second, the institutions covered in tripartite systems are evolving into organizations that support this agility with faster and more efficient decision-making processes and deal with much more information than is currently the case. Moreover, humans may no longer be the only intelligent agents able to perform conformity assessment. Machine readable documents may enable CA to support a more agile assessment society, so that changes can be effected in real time, as products and systems evolve. Similarly, test methods will need to evolve along with CA documentation, perhaps in the form of downloadable machine-readable procedures that control digitally-enabled test environments.

Digital twinning constitutes a versatile solution in support of conformity assessment. It offers a realistic approach for the assessment of existing and/or future products or systems. Subsequently it can also serve as a vehicle for monitoring the system as it is built, operated, changed and decommissioned. As a digital twin can simulate systems before they are constructed, it is recommended that they adhere to safety-by-design principles. This allows conformity assessment for safety and other aspects to be discussed and verified in advance with stakeholders.

With the introduction of independently operating safety verification algorithms based on AI, humans are no longer the only intelligent agents in the system charged with assuring safety. Even if such systems are currently in their infancy, it is worthwhile contemplating their eventual impact on conformity assessment. Developments in this direction are introducing a fundamental shift in conformity assessment objectives and new forms of trust. Machine-readable documents for CA are paving the way, but the IEC and its stakeholders need to investigate the feasibility, appetite for and implementation of such systems for preparing safety in the future.

5.5 Achieving global safety excellence

A further important factor remains with regard to the installing of mechanisms for continuous improvement of systems, standards and practices. Measuring safety outcomes has formed a key part of safety management systems for many years, with a focus on incident statistics. However, a more forward-looking, proactive approach could be adopted by introducing “leading” indicators into the calculation. To gain a more complete view of safety, each level of the safety ecosystem should be measured to understand influences exercised by externalities on the environment, as well as on the specific system being managed. The complex, multi-tiered nature of the system of safety requires a new approach to its measurement. Inclusion of a composite indicator, a structured combination of individual measures of the system, constitutes one method of creating a dynamic, nuanced and adaptable measurement method that can be applied to safety.

To achieve global safety excellence, global diversity must be acknowledged. While most societies aspire to provide a safe and secure environment for their people, available resources are always a limiting factor in that effort. A country’s gross domestic product (GDP) per person is one measure of available resources in that society. In developed economies, more “discretionary” resources are potentially available for allocation to specific safety programmes, including safer infrastructures, consumer protection and similar measures. In developing countries, where financial resources are less abundant, government spending is more likely to be allocated toward efforts to provide basic services, build critical infrastructure or shape the economy. Addressing these issues may leave fewer resources available for specifically tackling safety concerns, but strengthening basic services and infrastructure is usually correlated with improvements in safety.

While steering the world toward global safety excellence is a massive, complex, multifaceted challenge, the IEC, with its long-established history of coordinating experts on safety, engineering, systems integration and ICT, is particularly well-placed for bringing stakeholders together to broker consensus. Ultimately, it will be partnerships established between policymakers, regulators, industrial enterprises, insurers, academics and private research organizations that will enable success in efforts to secure safety in the future.

Section 6
Recommendations

6.1 Recommendations to governmental regulators, industry drivers and standards bodies

- **Regulators**
  - Governments and regulators should invigorate the debate concerning the needed shift from restrictive to goal-oriented safety laws.
  - Social goals should be established that aim to achieve both safety and efficiency, by shifting from a safety model based on separation of man and machine to one in which safety is achieved through man-machine cooperation.
- **Industry drivers**
  - Industry promoters should recognize that human-system communication is an essential ingredient of all future systems and should promote the development of technologies to ensure safety and security.
  - Consideration should be given to the possibility that humans may not be the smartest component in a new human-machine collaborative system. A new concept of safety should be elaborated through the development of technology and the reconfiguration of man's place in the system.
- **Standards bodies**
  - Standards bodies need to expand and deepen their holistic approach to safety. This will require incorporating not only traditional technical expertise but also insights gathered in the fields of safety psychology, sociology and human behaviour. In other words, it is recommended that in the development of future safety standards, clear attention be paid to non-technical factors.
  - At the same time, it is the duty of standards bodies to focus on the elaboration of technical standards for machine developers, suppliers and system integrators to ensure that they underpin security efforts in the future. A prerequisite for this effort is understanding that safety by design constitutes the most sensible approach if humans are considered paramount in a cooperative system. The standard should consider all stages of the life cycle of the product or system.
  - Standards bodies have an important role to play in promoting social responsibility in practical standards and conformity assessment processes. Standards bodies are already engaged with social stakeholders in contributing to the realization of social objectives such as safety and security and are uniquely positioned to bridge the gap between industry promoters and receptors.

6.2 Recommendations to the IEC community

- **Standard Management Board (SMB)**
  - In the IEC, one of the functions of a standardization evaluation group (SEG) is to anticipate emerging markets/ technologies that require a systems approach as well as define and implement enhancements to the TC/SC structure for improved functionality. It is recommended that the SMB should establish a SEG for "safety in the future" to begin discussing the review of guidelines, the establishment of a new body of standards, and the modification and maintenance of previous standards necessary for achieving cooperative human-machine safety. It would be desirable for this discussion to be led by the Advisory Committee on safety (ACOS) since membership in a SEG is drawn from within and beyond the IEC community. It is recommended that liaisons from other standards bodies be invited to serve on this standards evaluation committee as a first step towards efficient standards development.
  - The ACOS (in collaboration with ISO) should accelerate the review of the guidelines on safety (ISO/IEC Guide 51) currently underway, as the development of peripheral technologies to achieve cooperative safety may be accelerating more quickly than expected.
  - The development of standards for safety in the future referred to in this white paper may require the establishment of a new technical committee, rather than relying on a traditional one. Without eschewing the option of establishing a new technical committee, the SMB should nevertheless conduct a full and prompt discussion on the division of roles with the existing technical committees.
- **Conformity Assessment Board (CAB)**
  - It is recommended that the CAB and its CA systems (IECEE, IECEx, IECQ, IECRE) develop a new conformity assessment service concerning the tripartite safety system based on the standards developed according to a holistic approach under the SMB. Conformity of the tripartite safety system includes, but is not limited to:
    - product/machine safety according to existing safety standards
    - collaborative safety as an integrated system level, including interactive performance of ICT
    - personnel competence of safety assessors, supervisors and their management staff
  - It is recommended that CAB establish a communication channel with ILO/ISSA to encourage national authorities and regulators to realize the global acceptance of IEC conformity assessment results pursued by IEC registered bodies.
- **Market Strategy Board (MSB)**
  - The MSB should continue to investigate social, market and technological trends and provide input to the SMB and the CAB on any notable changes that appear to be directly related to safety. If necessary, this white paper on safety should be reviewed.
  - The MSB should also establish a permanent scheme of direct collaboration with the SMB and the CAB, so that they can systematically share their knowledge with each other on safety issues.

Bibliography

[1] United Nations, *About the Sustainable Development Goals* [Online]. Available: www.un.org/sustainabledevelopment/sustainable-development-goals. [Accessed: 22 October 2020].

[2] International Labour Organization, *Safety and health at work* [Online]. Available: www.ilo.org/global/topics/safety-and-health-at-work/lang--en/index.htm. [Accessed: 22 October 2020].

[3] Japan Industrial Safety and Health Association, *OSH Statistics in Japan* [Online]. Available: www.jisha.or.jp/english/statistics/index.html. [Accessed: 22 October 2020].

[4] Worksafe / New Zealand Government, *Dataset: Fatalities* [Online]. Available: https://data.worksafe.govt.nz/graph/detail/fatalities. [Accessed: 22 October 2020].

[5] Safe Work Australia, *Work-related traumatic injury fatalities* [Online]. Available: www.safeworkaustralia.gov.au/collection/work-related-traumatic-injury-fatalities. [Accessed: 22 October 2020].

[6] Health and Safety Executive (HSE), *Workplace fatal injuries in Great Britain, 2019* [Online]. Available: www.hse.gov.uk/statistics/pdf/fatalinjuries.pdf#page5. [Accessed: 22 October 2020].

[7] U.S. Bureau of Labour Statistics, *Fatal occupational injuries by event* [Online]. Available: www.bls.gov/charts/census-of-fatal-occupational-injuries/fatal-occupational-injuries-by-event-drilldown.htm. [Accessed: 22 October 2020].

[8] LOAFMAN, B. Rescue from the safety plateau. *Performance Management Magazine*, 14(3), pp.3-10, 1996.

[9] SKINNER, B. F. *The Behavior of Organisms*. Appleton-Century-Crofts, New York:1938.

[10] BAER, D. M., WOLF, M. M. and RISLEY, T. R. Some current dimensions of applied behavior analysis. *Journal of Applied Behavior Analysis*, 1(1), pp. 91-97, 1968.

[11] WIRTH, O. & SIGURDSSON, S. O. When workplace safety depends on behavior change. *Journal of Safety Research*, 39(6), pp. 589-598, 2008.

[12] HALE, A. and BORYS, D. Working to rule, or working safely? Part 1: A state of the art review. *Safety Science 55*, pp. 207–221, 2013.

[13] HALE, A. and BORYS, D. Working to rule, or working safely? Part 2: The management of safety rules and procedures. *Safety Science 55*, pp 222-231, 2013.

[14] SINGH, S. *New Mega Trends – Implications for our future lives*. Palgrave Macmillan, Hamshire (UK), New York (US): 2012.

[15] European Agency for Safety and Health at Work, *Foresight on new and emerging occupational safety and health risks associated with digitalisation by 2025* [Online]. Available: osha.europa.eu/en/publications/foresight-new-and-emerging-occupational-safety-and-health-risks-associated/view. [Accessed: 22 October 2020].

[16] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust* [Online]. Available: ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. [Accessed: 22 October 2020].

[17] Ellen McArthur Foundation, 2014. *Towards the circular economy* [Online]. Available: https://www.ellenmacarthurfoundation.org/publications. [Accessed: 22 October 2020].

[18] ELIEZEROV, R. / The Future of Commerce. *3 consumer privacy & data protection trends for 2020* [Online]. Available: https://www.the-future-of-commerce.com/2020/01/09/data-protection-trends-2020. [Accessed: 22 October 2020].

[19] Nippon Electric Control Equipment Industries Association, "Towards Vision 2025." In: *Profile of NECA* [Online]. Available: https://www.neca.or.jp/en/neca_outline/brochure. [Accessed: 22 October 2020].

[20] International Social Security Association, *Vision zero: Safety. Health. Wellbeing* [Online]. Available: visionzero.global. [Accessed: 22 October 2020].

[21] ZWETSLOOT, G., KINES, P., LEKA, S., JAIN, A., *Vision Zero – Proactive Leading indicators, a Guide to measure and manage safety, health and wellbeing at work*. Geneva: International Social Security Association, 2020.

[22] DOHI, M., SHIMIZU, T., NOBUHIRO, M., YAMADA, H., YAMADA, M., FUJITA, T. An Approach toward Safety by a Japanese Company – Vision Zero Activity, ISO 45001 Certification, and Effort toward Ensuring the Safety of Machineries and Developing Human Resources with Safety Expertise. *Vision Zero Summit 2019*, Helsinki, pp. 85-88, 2019.

[23] HOLLNAGEL, E. *Safety-I and Safety-II*. Ashgate Publishing, Farnham, UK, 2014.

[24] International Risk Governance Council (IRGC), *Introduction of the IRGC Risk Governance Framework*, revised version, Geneva, 2017 [Online]. Available: https://irgc.org/publications/core-concepts-of-risk-governance. [Accessed: 22 October 2020].

[25] MUKAIDONO, M., TAKAOKA, H., OGIHARA, H., ARIYAMA, M., FUJITA, T., Japan's Approach for the Realization of Future Safety Concept by Implementing Collaborative Safety Technologies. *9th International Conference on Safety of Industrial Automated Systems (SIAS)*, France, pp.77-87, 2018.

[26] DOHI, M., OKADA, K., MAEDA, I., FUJITANI, S., FUJITA, T. Proposal of Collaboration Safety in a Coexistence Environment of Human and Robots. *2018 IEEE International Conference on Robotics and Automation* (ICRA), Australia, pp. 1924-1930, 2018.

[27] IEC White Paper, *Semantic interoperability: challenges in the digital transformation age* [Online]. Available: go.iec.ch/wpsemantic. [Accessed: 22 October 2020].

[28] FIGUERES-ESTEBAN, M., HUGHES, P., EL-RASHIDY, R. and VAN GULIJK, C. Manifestation of ontologies in graph databases for big data risk analysis. In: ESREL 2018, Haugen, Barros, Van Gulijk, Tongsvik, Vinnem (Eds.) *Safe societies in a changing world*, pp. 3189-3193, Taylor & Francis, New York, 2018.

[29] KANEKAWA, N. Implementation of Security Function utilizing Safety Verification Function for Collaboration of Security and Safety. Invited Talk 3, *ITC-Asia 2019: The 3rd International Test Conference in Asia*.

[30] EASTMAN, C., TEICHOLZ, P.R., SACKS, K. L. *BIM Handbook: A Guide to Building Information Modeling for Owners, Managers, Designers, Engineers, and Contractors*. John Wiley & Sons, 2008.

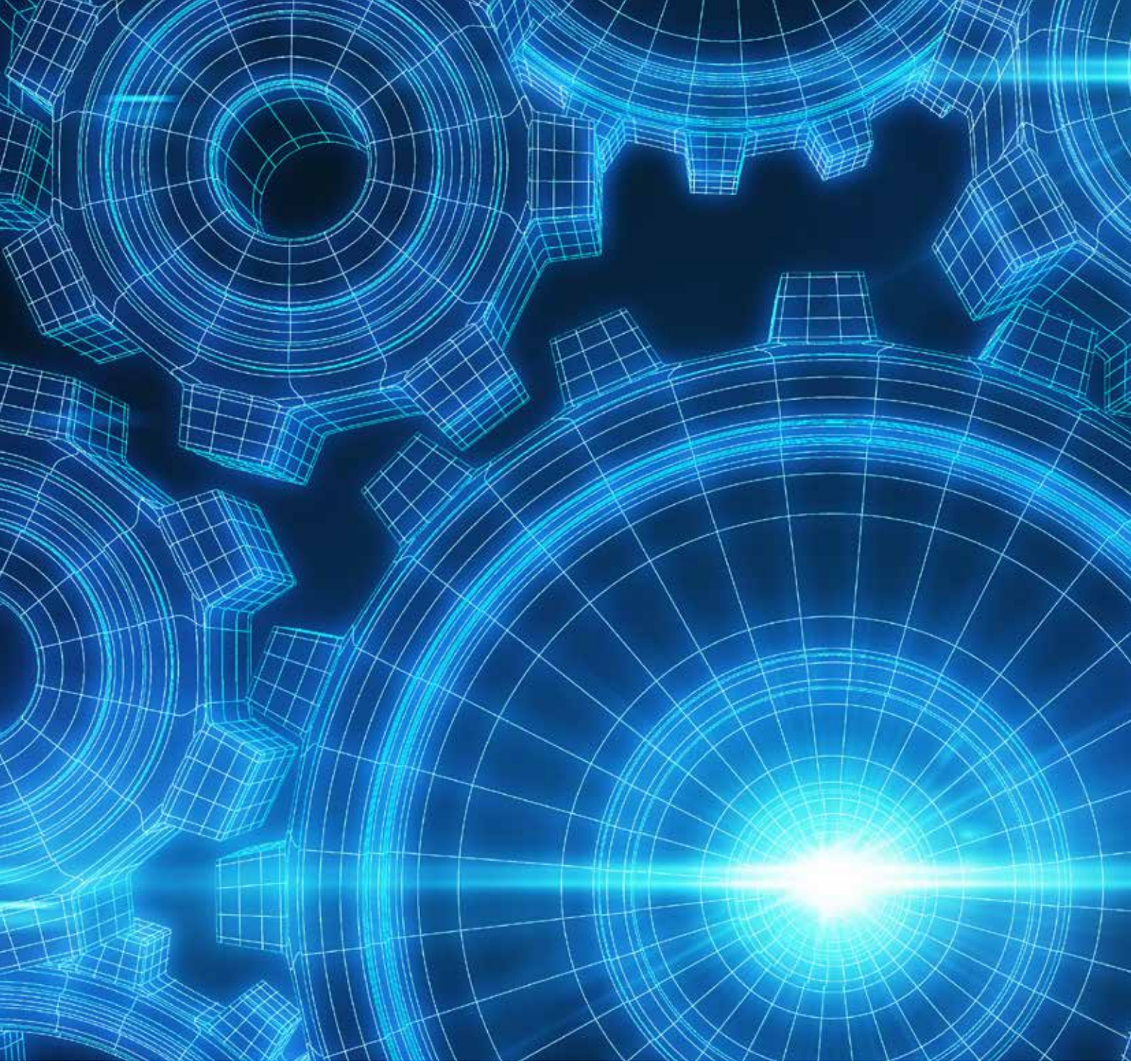
[31] MACHOVER, Carl. *The CAD/CAM Handbook, McGraw-Hill*, 1996.

[32] MAEDA, I., NOBUHIRO, M., SHIMIZU, T., OKADA, K., DOHI, M., FUJITANI, S., INADA, K., FUJITA, T. New concept of safety to realize improvement of higher productivity and safety in an environment of human-robot collaboration, and proposal of the concept of Collaboration Safety Level. ISR 2018 - *50th International Symposium on Robotics Munich, Germany*, pp. 468-473, 2018.

[33] SUITA, K. Jidousha seizo ni okeru kyoudouka no torikumi to kongo no kadai [Approach to collaboration in automotive production and challenges in future]. *ROBOT No. 252*, pp. 28-32, Japan Robot Association (JARA), January 2020.

[34] SHIMIZU, T., FUJITANI, S., MAEDA, I., OKADA, K., DOHI, M., FUJITA, T. New Collaborative Safety Concept in Various Coexistence Areas for Human and Machinery. *9th International Conference on Safety of Industrial Automated Systems (SIAS)*, France, pp.88-94, 2018.

[35] KAWATA, T. Introduction of Safety 2.0 and Shimizu Smart Tunnel System to Improve Productivity and Safety. In *Proceedings of Vision Zero Summit 2019*, pp. 131-134, November 2019.



ISBN 978-2-8322-8870-2

CHF 50.-

International Electrotechnical Commission

3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
info@iec.ch
www.iec.ch

® Registered trademark of the International Electrotechnical Commission. Copyright © IEC, Geneva, Switzerland 2020

IEC WP Safety in the future:2020-10(en)