# A Framework for Ensuring Safe Plant Design and Operation in the Process Industries

*Naoto Arai* [*1]

***The safety of industrial plants is a prerequisite for reassuring local communities and achieving a sustainable society. The process industries operate large, complex man-machine systems and even a single accident in a plant could cause immense damage to facilities, local communities, and the environment, and, in an extreme case, could destabilize the whole of society. To prevent such serious accidents, laws and regulations concerning process safety were discussed globally and the concept of risk reduction with multiple protection layers and a management system through the design and operation of safety instrumented systems was established as a framework for the safety of the process industries. This paper reviews this framework with reference to the trend of related standardization activities and introduces how AI is used to support safety in the process industries.***

## INTRODUCTION

Occupational accidents occur somewhere in the world every day. According to the International Labour Organization, 2.78 million workers die each year from occupational accidents and work-related illnesses, and 374 million workers are injured. This loss is equivalent to almost 4% of the world's GDP, and it exceeds 6% in some countries[(1)]. Although mental distress and stress cannot be quantified, they should not be ignored.

*1 Technology Marketing Department 1,
External Affairs and Technology Marketing Center,
Marketing Headquarters

Past research and practice show that many occupational accidents could have been prevented or alleviated. To continue growing while pursuing a sustainable society, industry has a duty to minimize the damage.

The prevention of accidents is particularly important in the process industries such as oil, gas, and petrochemical. Many of the raw materials, intermediate products, and finished products handled in process plants are flammable or toxic. In addition, these factories use huge amounts of energy. An accident such as an explosion or leakage may cause tremendous damage not only in the plant but also in the neighboring community. Furthermore, the economic and environmental damage may extend globally, causing an enormous impact on society.

Conventionally, information about safety in plants

was insufficient. Therefore, alarm systems and emergency shutdown systems were installed at each facility based on conventions or experience. In process plants, however, safety should be evaluated comprehensively and systematically, since many devices connected by pipes are controlled by computers in a sophisticated manner. This information should be shared and coordinated with the disaster prevention plans of local communities.

This paper describes how laws and regulations on process safety were established in the wake of major accidents, and explains risk assessment, which is recognized as an international framework, and the concept of risk reduction by multiple protection. In addition, the paper outlines safety instrumented systems (SIS), which are becoming popular as an effective risk reduction tool, and the functional safety standards that specify its requirements, along with Yokogawa's solutions. The use of AI to support safety and the trend of related standardization activities are also introduced.

## SERIOUS ACCIDENTS AND THE SAFETY REGULATORY FRAMEWORK

In 1976, pressure accidentally increased in a reactor at a pesticide plant in Seveso, Italy, which activated a rupture disc to release the pressure. Although the reactor was not damaged, a large quantity of substances including highly poisonous dioxin was released, contaminating approximately 1,800 ha of soil and affecting more than 220,000 people. This accident led the European Community to issue the Seveso Directive in 1982 as a safety regulation for chemical plants.

Two years later, huge amounts of highly poisonous methyl isocyanate spilled from a pesticide plant in Bhopal, India (a subsidiary of a US chemical company). According to the local state government, about 3,800 people were killed and more than 500,000 people suffered health problems, making it the worst accident in the history of the chemical industry. In response, the US Occupational Safety and Health Administration (OSHA) enacted the Process Safety Management (PSM) regulation in 1992. PSM is a comprehensive framework that requires business entities that possess chemical substances to implement their own risk management practices. Table 1 shows the 14 main elements of the regulation.

**Table 1** 14 elements of OSHA/PSM

| | |
|---|---|
| (1) Process safety information | (8) Mechanical integrity |
| (2) Process hazard analysis | (9) Hot work permit |
| (3) Operating procedures | (10) Management of change |
| (4) Employee participation | (11) Incident investigation |
| (5) Training | (12) Emergency planning and response |
| (6) Contractors | (13) Compliance audits |
| (7) Pre-startup safety review | (14) Trade secrets |

In response to the investigation report on the Bhopal accident, the Seveso Directive was greatly revised twice (Seveso II Directive in 1996 and Seveso III Directive in 2012). The basic objectives are to prevent serious accidents caused by hazardous substances and minimize the harm to humans and the environment. Each member country of the European Union is obliged to prepare a safety report including a safety management plan, an emergency plan, provision of information to neighborhood residents, and a land use plan around a target facility. Following the issuance of the Seveso II Directive, the U.K. abolished the Control of Industrial Major Accident Hazards Regulations (CIMAH) and enacted the Control of Major Accident Hazards Regulations (COMAH).

Figure 1 shows how laws, regulations, and international standards such as IEC 61508 and IEC 61511 were developed in response to serious accidents. Yokogawa's European affiliates have been participating in developing standards since the 1980s when the concept of functional safety emerged. After entering the safety business in 1997, Yokogawa's Headquarters sent experts and has been continuously participating in the development and revision of the standards.

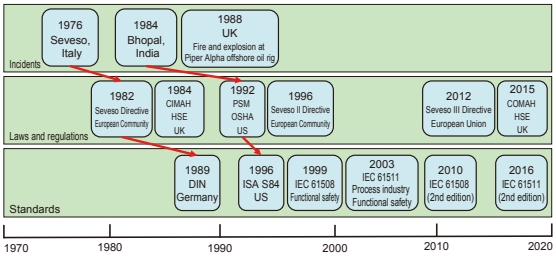



**Figure 1** Timeline of laws, regulations, and standards developed after serious accidents

The key elements in PSM, Seveso III Directive, and COMAH are also included in the Safety Performance Indicators for Chemical Accident Prevention released by the Organization for Economic Cooperation and Development in 2008. As guidance for industry, public authorities, and communities, it shows examples of indicators to be used for internal communication, safety reports, cooperation with other organizations, and reporting of accidents, near-misses, and other "learning experiences"[2][3].

In recent years, Safety Case has been attracting attention. This comprehensive and systematic document aims to provide sufficient evidence that a particular system is safe. It is prepared by a business operator and submitted as an explanation of the system to the regulatory authority[4]. Safety Case has a long history. The discussion started just after the explosion on the Piper Alpha oil platform in the North Sea in 1988. The UK mandates its preparation and submission in various industrial sectors. In Singapore, the preparation and submission of Safety Cases became mandatory for oil, gas, and petrochemical process plants in 2017[5]. Yokogawa provides consulting services on risk assessment and SIS and other solutions for risk reduction, helping customers prepare their own Safety Case document.

## RISK ASSESSMENT

ISO/IEC Guide 51 is the standard for developing safety standards. It defines safety using the word 'risk' as "freedom from risk which is not tolerable." Risk is defined as the "combination of the probability of occurrence of harm and the severity of that harm," and tolerable risk as the "level of risk that is accepted in a given context based on the current values of society"[6].

Risk assessment is the most crucial step in constructing a safe plant and is carried out mainly by the plant owner. In this process, hazards are identified using analysis methods such as the hazard and operability study (HAZOP) to clarify how things result in accidents. The probability of occurrence and impact are combined to determine the magnitude of the risk. If it exceeds an acceptable level, the risk is avoided, reduced, transferred, or retained based on the considered risk response policy. Figure 2 shows the procedure of risk assessment[7].

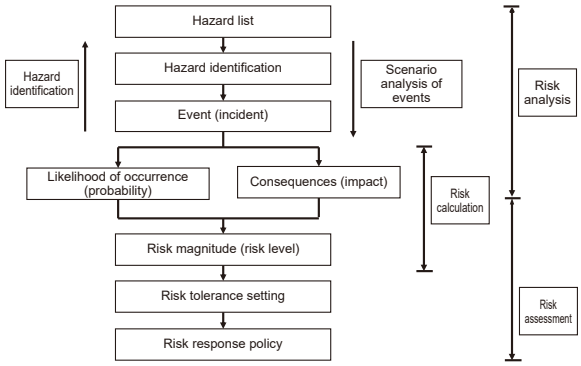
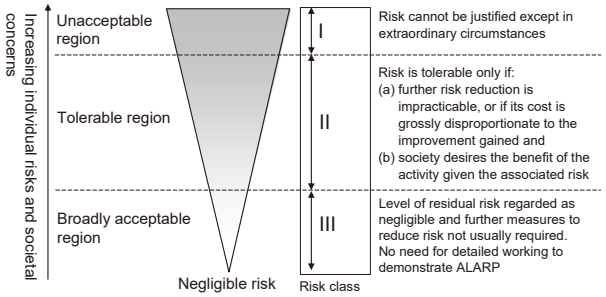



**Figure 2** Risk assessment procedure[7]

In principle, the concept of "as low as reasonably practicable (ALARP)" is used to determine acceptable risk[8]. As shown in Figure 3, three regions are defined for the tolerance of an incident. Stakeholders (e.g., safety regulators, risk generators, and those exposed to the risk) hold discussions based on this definition and determine the frequency, consequences, and risk class of an incident (Table 2). In determining acceptable risk, it is necessary to refer not only to the global regulations of the company and the guidelines of the industry sector but also to the standards of communities (national and local). For example, regarding the individual risk per annum (IRPA), the UK Health and Safety Executive (HSE) has set the upper limit of the "tolerable" region (boundary between I and II) to $10^{-3}$/year and that of the "broadly acceptable" region (boundary between II and III) to $10^{-6}$/year[9].




* Compiled from IEC 61511-3 ed. 2.0. Copyright © 2016 IEC, Geneva, Switzerland. www.iec.ch

**Figure 3** Tolerable risk based on the ALARP concept[8]

**Table 2** Example of risk classification of incidents

| Frequency | Risk class | | | |
|---|---|---|---|---|
| | Catastrophic consequence | Critical consequence | Marginal consequence | Negligible consequence |
| Likely | I | I | I | II |
| Probable | I | I | II | II |
| Possible | I | II | II | II |
| Remote | II | II | II | III |
| Improbable | II | III | III | III |
| Incredible | III | III | III | III |

## REDUCING RISK WITH MULTIPLE PROTECTION MEASURES

The Center of Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE) proposed the independent protection layer (IPL), which stimulated discussions on safety design that considers the entire plant as a large-scale system[10]. Figure 4 shows the protection layers from IPL1 to IPL8, which are independent of each other. Even if an inner protection layer becomes invalid, the outer protection layer can prevent an accident or contain the spread of damage. The following are descriptions of each IPL.

- IPL1 is related to inherent safety. In process design, hazards are minimized by reducing the amount of hazardous materials that are retained, reducing catalysts to slow down the reaction rate, and using normal temperature and pressure conditions for operation. In equipment design, measures are taken, for example considering the maximum load in the intended operating range and making the walls of the reactor thick enough. Since facilities and equipment degrade over time, maintenance activities are indispensable to keep their integrity.
- IPL2 is a basic process control system (BPCS). A typical example is a distributed control system (DCS). It keeps the operation stable and prevents abnormalities.
- When a process abnormality occurs, IPL3 issues an alarm, notifies it to the operators, and encourages them to intervene and manually restore normal operation.
- When operators cannot intervene in time, SIS in IPL4 automatically shuts down the plant and ensures safety.

- IPL5 and IPL6 mitigate the damage with physical protection. Pressure relief valves and rupture discs that prevent excessive pressure from damaging equipment fall under IPL5, while liquid dikes to limit the expansion of the leakage area of hazardous materials fall under IPL6.
- IPL7 and IPL8 are emergency response plans; IPL7 contains the damage within the plant, while IPL8 minimizes the damage outside the plant to prevent it from spreading to the neighboring community.

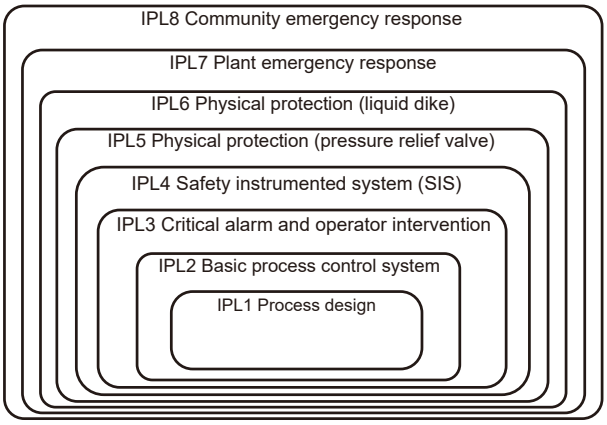



**Figure 4** Concept of independent protection layers

The layer of protection analysis (LOPA) is used to evaluate how much IPL can reduce the frequency of occurrence of initiating events. In the Swiss cheese model in the upper part of Figure 5, the thickness of the arrows shows that the frequency of accidents decreases as the initiating event passes through IPLs. The event tree analysis in the lower part shows that the frequency of accidents reduced by IPLs (residual risk) can be estimated by multiplying the frequency of occurrence of initiating events by the probability of each IPL failure.

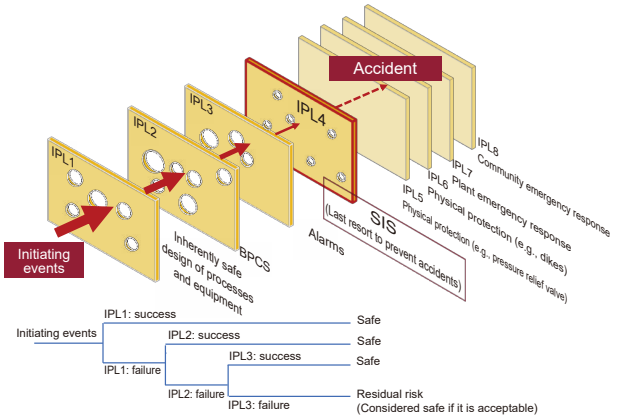



**Figure 5** Concept of LOPA

If the residual risk is acceptable, safety is ensured. If it exceeds the upper limit, the need for SIS and then the safety integrity level (SIL) required for SIS are determined.

## SIS AND FUNCTIONAL SAFETY STANDARDS

SIS is the last resort of proactive safety measures; it consists of sensors, logic solvers, and final elements (e.g., actuators). SIS is different from BPCS, another instrumentation system, in that SIS has one or more safety instrumented functions (SIF), and that each SIF has a risk reduction capability depending on the SIL to be achieved. LOPA is an SIL assignment method.

Table 3 shows the relation between SIL and the average probability of dangerous failure on demand (PFDavg)[11]. The reciprocal of PFDavg means how much risk can be reduced by the corresponding SIL. A higher SIL requires a smaller PFDavg. Note that Table 3 assumes a low demand mode (safety function demand rate is less than or equal to once a year).

**Table 3** SIL and PFDavg

| SIL | Low demand mode | |
|---|---|---|
| | PFDavg | Risk reduction target |
| 4 | $\geq 10^{-5}$ to $< 10^{-4}$ | > 10,000 to ≤ 100,000 |
| 3 | $\geq 10^{-4}$ to $< 10^{-3}$ | > 1,000 to ≤ 10,000 |
| 2 | $\geq 10^{-3}$ to $< 10^{-2}$ | > 100 to ≤ 1,000 |
| 1 | $\geq 10^{-2}$ to $< 10^{-1}$ | > 10 to ≤ 100 |

To achieve SIL, the design and operation of SIS must comply with two functional safety standards: IEC 61508 for generic standard and IEC 61511 for the process industry sector specific standard. Figures 6 and 7 show the relation between IEC 61508 and IEC 61511. IEC 61508 is applied to the manufacturers and suppliers of SIS components while IEC 61511 is applied to users and system integrators who use these components to build SIS.

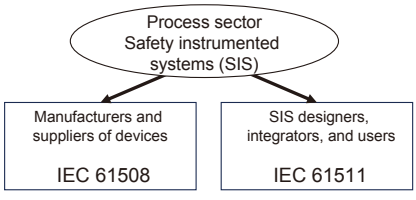
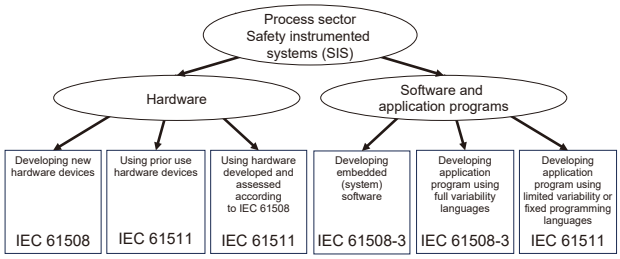





**Figure 6** Relation between IEC 61508 and IEC 61511[11]




* Compiled from IEC 61511-1 ed. 2.0 Copyright © 2016 IEC, Geneva, Switzerland. www.iec.ch

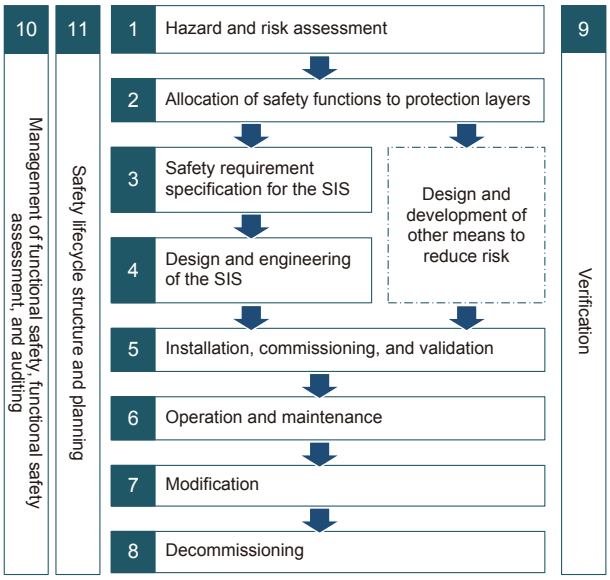
**Figure 7** Detailed relation between IEC 61508 and IEC 61511[11]

Yokogawa released ProSafe-RS, a SIL 3-certified PLC, in 2005. Regarding field devices, the EJX/EJA series differential pressure/pressure transmitters, the ADMAG AXR two-wire magnetic flow meter, the YTA temperature transmitter, and the TDLS8000 tunable diode laser gas analyzer have obtained SIL 2 certification (SIL 3 certification in a dual configuration) for their standard specifications. This means that their conformance to IEC 61508 has been verified by a third-party certification body. To obtain the certification, products must satisfy various requirements (for example, the PFDavg derived from the hardware failure rate of the components must fall in the range of the target SIL in Table 3). In addition, the software development process and the management system of the development organization must conform to the standard.

As an integrator of SIS, Yokogawa also combines SIL-certified devices and other devices based on operational experience in similar environments (prior use), develops application programs, and achieves SIL in each SIF unit.

As in IEC 61508, IEC 61511 requires that the PFDavg derived from the hardware failure rate of the devices be within the range of the target SIL in Table 3 and that the organizations involved in SIS have a functional safety management system. Yokogawa has incorporated the management of functional safety into the Group Management Standards, has established appropriate operational procedures, and has been providing training to the staff involved in SIS projects.

The requirements of IEC 61511 for functional safety management span the entire SIS safety lifecycle[11] shown in Figure 8. The SIS safety lifecycle stretches from Phase 1 "Hazard and risk assessment" to Phase 8 "Decommissioning." Requirements applicable to the eight phases are compiled in Phases 9, 10 and 11. In Phase 4 "Design and engineering of the SIS," Yokogawa takes the initiative in preparing the management system for functional safety. In other phases, users and other organizations are expected to take the initiative. Yokogawa has been offering the Sustainable SIS solution since 2017. This solution proposes a comprehensive set of services, systems, and software packages that support risk assessment, post-implementation operation, and maintenance (e.g., proof testing to maintain the integrity of the SIS).




* Compiled from IEC 61511-1 ed. 2.0 Copyright © 2016 IEC, Geneva, Switzerland. www.iec.ch

**Figure 8** Phases in the SIS safety lifecycle

## SAFETY SUPPORT BY AI

The fourth industrial revolution[12] made us aware of the possibility of utilizing the vast amount of data in plants. Data acquired by high-precision sensors and cameras are accumulated in cyberspace in real time through the Internet of Things (IoT). The development of AI technologies such as image recognition, process data processing, and natural language processing makes it easier to analyze big data. In countries where it is increasingly difficult to secure skilled workers due to the declining birthrate and population aging, AI is expected to reduce the dependence on human workers by replacing and supporting some of their roles and tasks.

Yokogawa has been developing various solutions and conducting demonstration tests for plant operation support AI and maintenance support AI. For example, for operation support, we combine AI and Sushi Sensor, Yokogawa's unique wireless sensor for the Industrial IoT (IIoT). AI detects signs of abnormalities from the large amount of data sent from this sensor which is installed across a plant[13]. We are also developing AI that optimizes plant operation instead of PID control[14].

Figure 9 shows a typical example of maintenance support AI, which predicts the thinning of pipe walls. In the upper piping of an atmospheric distillation column for oil refining, corrosion is inevitable and thus time-based maintenance (TBM) is performed periodically. However, this method cannot detect rapidly progressing corrosion, and unnecessary inspection and replacement of piping reduces profits. Therefore, we obtained two-year process data and wall thickness data at 20 locations as training data, modeled the relation between process data and wall thinning, formulated a regression equation, and predicted the progress of wall thinning. We built a system that displays the estimated values in real time on the screen. This enables operators to

carry out repair or replacement at the right time, shifting to condition-based maintenance (CBM). We also analyzed the data, identified main causes (e.g., temperature drop), and successfully suppressed the progress of wall thinning by changing the operating conditions.

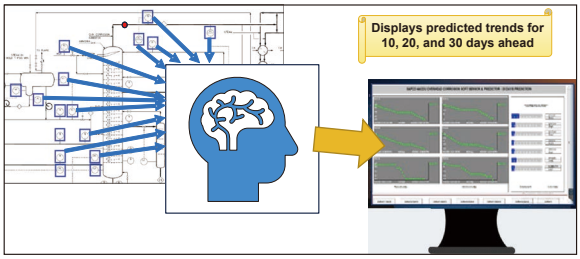



**Figure 9** AI prediction of pipe wall thinning[15]

To incorporate AI into the protection layer of a plant to replace or support human workers and existing systems, it is necessary to properly evaluate the quality (especially safety) of AI and hold it accountable to stakeholders both in and outside the plant. In Japan, the Ministry of Economy, Trade and Industry (METI) took the lead in formulating the "Guidelines on Assessment of AI Reliability in the Field of Plant Safety" in 2020 through discussions between the public and private sectors. In addition to the prediction of pipe wall thinning, the guideline provides methods for using pipe image diagnosis, equipment deterioration diagnosis, prediction and diagnosis of early signs of abnormality, and optimization of operation[15].

Figure 10 shows the relation between development scenarios of accidents in process plants and the use of AI. Currently, AI applications are concentrated in operation support and maintenance support. In most cases, final decisions rest with humans, and SIS or other means to ensure safety are added to the AI system. AI systems are not intended to replace SIS. In other words, SIL is not set for AI systems as the subject of functional safety standards.

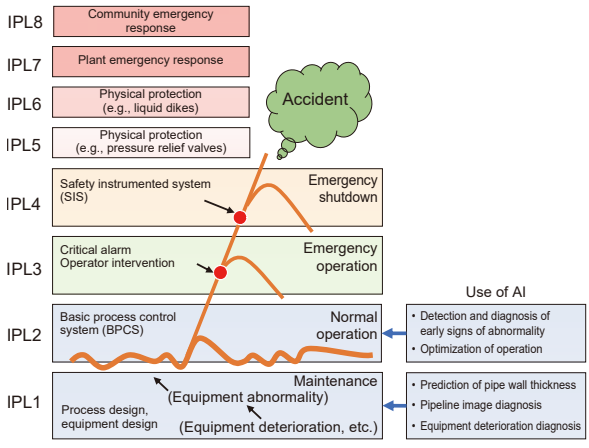



**Figure 10** Development scenarios of accidents in process plants and the use of AI

IEC 61511 is in the process of being revised from the viewpoint of plant owners, who ultimately take responsibility for the safety of a plant. There were tragic accidents in the past; our predecessors have learned lessons from them and built a framework for plant safety. On the other hand, plants are being transformed by incorporating AI and other new technologies. While respecting the existing framework and expecting further development of technology, we need to have careful discussions on how to ensure safety in plants in the future.

## CONCLUSION

This paper outlined risk assessment, which is recognized as an international framework for the design and operation of safe process plants, and risk reduction by multiple protection. It is important to reduce the risk of the entire plant and ensure safety by designing and operating safety measures at each level, such as inherent safety design, BPCS, alarm and operator intervention, and SIS, in accordance with international standards.

Improving the safety of the plant, its workers, and the neighboring community is the key to achieving a sustainable society. For more than half a century, Yokogawa has been developing products and solutions to contribute to the safe operation of process industries. Yokogawa will continue to work hard to prevent tragedies caused by plant accidents and to achieve a society in which all people can lead safe, secure, and affluent lives.

## ACKNOWLEDGMENTS

We would like to express our gratitude to the International Electrotechnical Commission (IEC, headquartered in Geneva) for their kind permission to extract and reproduce information on their international standards. For further information on the IEC, please refer to its website (https://www.iec.ch). All copyrights to the information contained in the extracts and reprints belong to IEC, which reserves all rights. All responsibility for extracts and reprints rests with the authors of the paper, and IEC assumes no responsibility for the form in which IEC information appears in this paper or for the accuracy of any other content in the paper.

## REFERENCES

(1) International Labour Organization, Safety and Health at the heart of the Future of Work: Building on 100 years of experience, 2019
(2) OECD, Guidance on Developing Safety Performance Indicators for Industry, 2008
(3) OECD, Guidance on Developing Safety Performance Indicators for Public Authorities and Communities/Public, 2008
(4) Tim Patrick Kelly, "A Systematic Approach to Safety Case Management," SAE International, 2003
(5) Ministry of Manpower, Singapore, Workplace Safety and Health (Major Hazard Installations) Regulations 2017, 2017
(6) ISO/IEC Guide 51:2014 Safety aspects - Guidelines for their inclusion in standards, 2014
(7) The High Pressure Gas Safety Institute of Japan, Risk Assessment Guideline (Ver. 2), 2016 (in Japanese)
(8) IEC 61511-3:2016, Functional safety - Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination

of the required safety integrity levels, 2016
(9) Health and Safety Executive, Guidance on ALARP Decisions in COMAH, https://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_37/ (accessed on July 1, 2021)
(10) AIChE/CCPS, Guidelines for Safe Automation of Chemical Processes, 1993
(11) IEC 61511-1:2016, Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements, 2016
(12) Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond," World Economic Forum, 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ (accessed on July 1, 2021)
(13) Masahiko Sato, "Application of Machine Learning Technology to Trend Monitoring with Sushi Sensor," Yokogawa Technical Report English Edition, Vol. 63, No. 1, 2020, pp. 23-26
(14) Go Takami, "AI-based Plant Control," Yokogawa Technical Report English Edition, Vol. 63, No. 1, 2020, pp. 33-36
(15) The Liaison Council of Three Ministries on Disaster Prevention of Petroleum Complexes (Ministry of Economy, Trade and Industry, Fire and Disaster Management Agency, and Ministry of Health, Labour and Welfare), Guidelines on Assessment of AI Reliability in the Field of Plant Safety, second edition, 2021