Smart manufacturing

Technology focus
A greener future for manufacturing

Conformity assessment
The connected mine

In store
Can you trust used medical devices?
Today, manufacturers face the challenge of ensuring global supply chains and delivering global orders on time. Disruptions due to bad weather, strikes or other unforeseen issues, could result in delays or cancellations of component parts. Additionally, machines break down.

The fourth industrial revolution has brought artificial intelligence (AI) technologies, such as machine learning and data analytics. These enable smart manufacturing and the ability to check machines, orders, processes and external factors in real time. The information gathered arms manufacturers with insights they can use to plan for diverse contingencies. For example, knowing the exact status of machines, allows for the deployment of predictive maintenance and can reduce equipment failure, increase reliability and improve asset performance.

Automotive manufacturers benefit greatly from the digital twin car. Diverse scenarios can be tested on this virtual model using real-world data, from design to production, to find issues, failures and solutions before a new model is built.

On a broader scale, more industries are incorporating AI into their products and services. These include advances in transport, such as airline autopilot and safety systems, and data analytics for healthcare, which help doctors choose the best treatments for patients. Increasingly, humans are putting their trust in machines.

Despite all the benefits, there are concerns around innovative technologies, which need to be addressed. In production plants, programmed robotic arms and humans work side by side, so AI systems must be trustworthy for the safety of workers. Additionally, ethical and societal issues have been raised around the ability of AI systems to learn and make decisions and the potential for inadvertent bias. Thus, there is a growing need to understand how algorithms work, so that if something goes wrong, a solution can be found, in order to avoid the problem occurring again.

IEC carries out diverse work for the development of AI standards. It is a founder member of the Open Community for Ethics in Autonomous and Intelligent Systems (OCEANIS), which brings together standardization organizations from around the world with the aim of enhancing awareness about the role of standards in facilitating innovation and addressing issues related to ethics and values.

Additionally, IEC works with ISO to develop international standards for information technologies, including AI. In this issue, we look at how these standards, aim to achieve AI systems which are more transparent.

We also hear from an expert on digital twins, who explains why we will need standards, which will cover the terminology, reference architecture and semantic interoperability of digital twins, in order to provide a foundational understanding for different stakeholders in diverse application areas.
The focus on intelligence is fundamental to smart manufacturing

Environmentally friendly machines minimize energy and paper consumption
Contents

Editorial
The artificial intelligence technologies behind smart manufacturing ...................................................... 3

Technical committees
AI standards help accelerate digitalization of smart manufacturing ...................................................... 6
Innovative technologies broaden use of digital twins .......................................................... 9
The future of the printer ........................................................................................................ 11

Technology focus!
Protecting manufacturing from cyber attacks ................................................................. 13
A greener future for manufacturing .................................................................................. 15
Disruptive technologies and positive change ................................................................. 17

In store
Can you trust used medical devices? ................................................................................. 18
New standard to boost nuclear power installations’ cyber resilience .............................................. 20
Long and winding wires ................................................................................................... 22

Conformity assessment
MET-CERTIFIED to run first marine energy certification workshop in Latin America ............... 24
The connected mine ......................................................................................................... 26
Winning trust .................................................................................................................... 28

In the next issue ................................................................................................................. 30

IEC Standards help companies introduce greener manufacturing processes
Nuclear power plants using digital systems must ensure robust cyber security measures
Connected mines use sensors and cloud technology to improve worker safety and increase production
Various analysts put the market estimate at several hundreds of billions US dollars with double digit CAGR growth. Much of this growth is being fuelled by the digitalization of the sector as emerging IT technologies such as AI, big data and analytics are improving efficiencies and unlocking insights that would otherwise be unattainable.

Together, IEC and ISO develop international standards for information and communication technologies through a joint technical committee (ISO/IEC JTC 1). One of the committees (SC 42) covers the entire ecosystem for artificial intelligence (AI).

Earlier this year, IEC and ISO endorsed a joint definition of smart manufacturing:

“Manufacturing that improves its performance aspects with integrated and intelligent use of processes and resources in cyber, physical and human spheres to create and deliver products and services, which also collaborates with other domains within enterprises’ value chains.”

In the definition, performance aspects include agility, efficiency, safety, security, sustainability or any other performance indicators identified by the enterprise, while other enterprise domains can include engineering, logistics, marketing, procurement, sales or any other domains named by the enterprise.

The definition also provides a few insights into smart manufacturing. These include:

- An encompassing approach that combines cyber, physical and human aspects
- A focus on improving both performance as well as the creation of both products and services through intelligence

**The link to AI and enabling IT technologies**

The focus on intelligence is fundamental to smart manufacturing. The key component is insights, whether providing them on improving operational efficiencies in manufacturing or for making intelligent decisions on what or where to manufacture. To provide those insights, IT systems are used to look at the large amounts of data that are coming from the manufacturing domain. This focus on data is the link to emerging IT applications such as AI.

Through applying big data and AI techniques, IT systems can take data analytics to the next level. For example, in machine learning based AI systems, the algorithms at the heart of AI can be used to predict when maintenance is needed dynamically, monitor and provide recommendations to improve quality, provide guidance on root cause analysis, improve yields and much more. AI not only enables these analytics, but by looking and learning from the data, the insights delivered can be tailored to the application and context it is being used in.

Ultimately these efficiencies can lead to cost reductions in the manufacturing process and improved production times.

**The need for AI standards**

Standards are essential to removing barriers to deployment, addressing concerns and ultimately accelerating adoption.

Horizontal AI standards, such as those being developed by SC 42, enable smart manufacturing in a number of ways:

- Terminology and foundational frameworks: As smart manufacturing brings together a diverse set of interests that include information technology experts and operational technology experts, a common
AI standards help ensure AI systems in smart manufacturing are trustworthy.
language and a framework for the use of AI machine learning are important to the successful architecture and deployment of next generation smart manufacturing systems. SC 42 is working in two standards in this area namely ISO/IEC 22989 and ISO/IEC 23053.

- Trustworthy AI: Key to the successful deployment of AI systems in smart manufacturing is to ensure that the system is trustworthy. To that effect, SC 42 is developing projects in this area that are applicable:
  - AI domain overview of trustworthiness, bias and robustness of neural networks: These projects aim to introduce the topic and some of the AI context specific concepts about trustworthiness, bias and robustness. In the area of bias, the project also addresses AI-aided decision making.
  - Risk management: This project builds on the generic ISO 31000 standard for risk management in the AI domain. The document provides guidelines on the management of risk during the development and deployment of the AI system. The purpose is to establish trust in the system by addressing issues such as this, by design and during the operation of the system in accordance with the goals of the deployment.
  - Ethics and societal concerns: The ability of AI systems to learn and make decisions brings about a host of ethical considerations. For instance, ensuring that AI enabled systems in smart manufacturing are safe. Moreover, when dealing with data and developing insights, the systems should only consider data within the application provenance and not look at data that would otherwise be unavailable to a human (commonly referred to as eavesdropping). To address these issues SC 42 is developing a project that maps such high-level concerns and looks at these across its technical programme of work. For example, ethical concerns are being collected for the various AI use cases.
  - Application guidance and use cases: One of the primary goals of SC 42 is to provide guidance to application committees within IEC, ISO and JTC 1. To-date, SC 42 has collected over 85 use cases, which include smart manufacturing and is actively working with committees and organizations looking at this domain.
  - Governance implications of AI: When an AI system is deployed in an organization, questions may arise by non-technical executives managing and deciding on the deployment of such systems. By collaborating with the committee covering IT service management and IT governance (SC 40), through a joint working group, SC 42 is developing a standard that would aid in answering some of these questions.

Additional standards work in the area of big data and analytics are of relevance to smart manufacturing deployments. As large data sets are collected over the life of a smart facility and across different facilities, big data techniques for processing the information and deriving analytics may also be applied. SC 42 has published and is developing some standards which include foundational projects on a big data reference architecture, use cases and a framework for business management of big data analytics.

Finally, as the world of AI and data science is rapidly changing, SC 42 is looking at several study areas. An example is the implications and challenges of developing and integrating AI into different applications, such as smart manufacturing through an advisory group on AI Systems Engineering. Concepts such as integration, maintenance, adaptation of best practices to AI systems and redeployment are being discussed. Another area of study is looking at a management systems standard that would provide AI-specific process requirements which would in turn allow for conformity assessment.

Building out the industry ecosystem

The opportunity of AI enabling smart manufacturing and AI applications more generally, is not only large, it’s transformative. Consequently, no single organization or standards body can go it alone. While SC 42 is taking a broad look at the entire AI ecosystem, it works collaboratively with other IEC and ISO committees, which cover biometrics, blockchain, coding of audio, picture, multimedia and hypermedia information, digital twins, health informatics and risk management and IT, as well as with external organizations through liaisons.

For smart manufacturing, SC 42 is working with a number of IEC and ISO committees such as IEC TC 65 for industrial-process measurement, control and automation, IEC Systems Committee for Smart Manufacturing, ISO Smart Manufacturing Coordinating Committee (SMCC) and other JTC 1 committees which cover cloud computing, data management and interchange and IoT.
Digital twins are virtual replicas of physical objects or systems. They use real-world data to run simulations of situations before actual devices are built and deployed, and predict different outcomes. Manufacturers then use this information to reduce maintenance issues, improve efficiency and production output.

This is all possible because of IoT sensors, which gather masses of data and artificial intelligence technologies, including machine learning and data analytics. These provide the insights and predictions based on this data.

From the production line to investor funds

Automobile manufacturers have created the digital twin car, which comprises the car’s exterior, mechanics, electrics and software. Diverse scenarios can be tested from design to production to find issues, failures and solutions before the new model is built.

However, as the technology evolves, these data-rich virtual models are being used in many other situations. For instance, urban planners can get a bird’s eye overview of the city or drill down to the most accurate detail at street or building level, to improve infrastructure, plan new constructions or run disaster scenarios and take measures to prevent floods and train first responders.

Banks and investment services use digital twins to run simulated cyber attacks in order to improve the security of customer funds, while surgeons enhance patient safety and care by practicing on digital twin patients or body parts before operating.

The need for standards

e-tech caught up with Dr Sha Wei, Convenor of the IEC and ISO Advisory Group carrying out standardization work for digital twins. This group is part of the joint technical committee which develops standards for information technology (ISO/IEC JTC 1). Wei works for the China Electronics Standardization Institute, which is a mirror committee for JTC 1, as well as in standardization of smart manufacturing and artificial intelligence.

How will standards contribute to this technology?

Digital twins are an important enabling technology and driving force of digitization, which is reshaping the world in multiple scales, such as for buildings, factories, automobiles or entire cities.
As digital twins are implemented, there are several standardization requirements for aspects of terminology, reference architecture and semantic interoperability. To start with, in the literature and reports on digital twins, stakeholders, such as developers, engineers and users, refer to the technology as digital representation, digital mapping, CPS and administration shell. Digital world, as one of the essential components of digital twins, is also called virtual world, virtual space and cyber space. This is why terminology and definitions are always the first standard to be developed for new technologies, so that everyone is on the same page.

In order to describe the current application of digital twins in smart manufacturing, smart cities, smart energy, smart farming, smart healthcare, etc. Smart manufacturing is one of the most active areas for these applications. As summarized in the paper Digital twin-driven smart manufacturing: Connotation, reference model, applications and research issues, by authors Lu, Yuqian & Liu, Chao & Wang, Kevin & Huang, Huiyue & Xu, Xun, GE has developed a digital twin platform PREDIX that can better understand and predict asset performance. SIEMENS uses a digital twin to cover smart operations during the complete process of product design, production and operation. ABB emphasizes the digital twin’s effects on enabling data-driven decision makings. Microsoft has geared up its digital twin product portfolio, providing a ubiquitous IoT platform for modelling and analyzing the interactions between people, spaces and devices. Initiatives from these tech leaders have significantly pushed the boundaries of digital twins for engineering applications.

“We need to develop a general reference architecture, which would cover components, such as data connected from the physical world, models stored in the digital world, a communication interface between the digital and physical worlds, services, as well as their reciprocal processes. Also, data is the most important element for realizing system optimization using digital twins. In practice, because data is normally collected from different sources and unstructured, the consistency of the digital and physical worlds is not easy to guarantee. Therefore, a standard defining semantic interoperability between the digital and physical worlds, is vital for the implementation of digital twins.”

What is the main area of focus?

Digital twins are being applied in many areas, including smart manufacturing, smart cities, smart energy, smart farming, smart transport, smart buildings, smart healthcare, etc. Smart manufacturing is one of the most active areas for these applications. As summarized in the paper Digital twin-driven smart manufacturing: Connotation, reference model, applications and research issues, by authors Lu, Yuqian & Liu, Chao & Wang, Kevin & Huang, Huiyue & Xu, Xun, GE has developed a digital twin platform PREDIX that can better understand and predict asset performance. SIEMENS uses a digital twin to cover smart operations during the complete process of product design, production and operation. ABB emphasizes the digital twin’s effects on enabling data-driven decision makings. Microsoft has geared up its digital twin product portfolio, providing a ubiquitous IoT platform for modelling and analyzing the interactions between people, spaces and devices. Initiatives from these tech leaders have significantly pushed the boundaries of digital twins for engineering applications.

“We are focusing on a general IT framework standard for digital twins, which can be applied to different areas, but a series of new horizontal standards, such as terminology, reference architecture and semantic interoperability needs to be formulated to provide general understandings for different stakeholders and different application areas. I’d like to cooperate with experts from relevant standards development organizations to generate harmonized digital twins.”

More about IEC standardization activities

IEC works together with ISO on the development of international standards for information and communication technologies. The Joint Technical Committee (ISO/IEC JTC 1) covers many areas including AI, automatic identification and data capture techniques, biometrics, cloud computing, data usage, IoT, IT for learning, education and training, virtual reality and quantum computing.

Digital twins is also a focus area of IEC Technical Committee 65, which develops international standards for industrial process measurement, control and automation. For example, TC 65 Working Group 16 is working on a framework that specifies model elements and rules for creating and managing digital representations of production systems.
Nearly all industries are impacted by the move to an all-digital environment. The reality is no different for the printing machine industry as the total sale of printers decreases worldwide and fewer documents are kept in print format. Yet, the printing machine industry is not consigned to obsolescence. Interest is emerging in new areas such as 3D printing and scanning and companies, seeking cost savings, are looking for new business models to meet their printing needs. New technologies, such as Internet of Things, cloud computing and artificial intelligence, are also enabling services and opportunities.
To develop standards for copying machines, printers and scanners, the ISO and IEC joint technical committee on information technology established its subcommittee on office equipment, ISO/IEC JTC 1/SC 28. At the recent JTC 1 Plenary in New Delhi, e-tech spoke with the Chair of SC 28, Takashi Ito who provided an update on the work of the subcommittee as well as its plans for the future.

Explaining the scope

SC 28 is one of the few JTC 1 subcommittees that produces standards for products and hardware. Standards focus on product specification descriptors, methods for measuring the productivity of the devices, the quality of the output and the yield of the consumables such as ink and toner cartridges.

According to Ito, “SC 28 has created a lot of standards for office equipment such as copying machines and printers. These standards address specifications for office equipment, the colour of the printing, measurement methods for printed image quality and toner ink cartridge”.

Increasingly, data collected by printers and scanners can be useful for manufacturers to better understand the needs of their customers. Ito notes, “the data also helps us to improve our machines”.

Since its establishment in 1989, SC 28 has published 33 standards for office equipment. As Ito explains, “at this point, we want to undertake a thorough review of our standards. This means that we will get rid of obsolete standards and revise other standards as needed. We are undertaking a lot of maintenance work”.

Making printers and copiers easily accessible to the disabled is one area where standards are in the process of being updated. Features such as simplified displays to help those with weak eyesight, reduced height of multifunctional printers and easy sliding trays are a few examples. “ISO/IEC 10779 accessibility guidelines from 2008 have been updated and a new version will be published in early 2020”, Ito remarks.

Overcoming challenges

One of the biggest challenges facing SC 28 remains: the office equipment industry is quite small. Only 32 members participate in the work of SC 28 given that few countries have office equipment industries.

Ito admits, “we are worried about the number of participants and the number of national bodies. Printers are primarily made in Japan and the United States so it is a very small group. But we continue to reach out to potential members and are always happy to welcome new members”.

Looking to the future

New technologies are enabling new opportunities for the printing machine industry.

According to Statista, global spending on 3D printers is projected to reach USD 7.8 billion by 2022. Interest in these applications has surged in recent years as affordable desktop 3D devices are increasingly found in office environments where they are particularly relevant for architectural, industrial and art design firms.

In 2015, SC 28 expanded its scope to include 3D printing and scanning. Ito notes that “SC 28 is looking at productivity in 3D printing. For example, with conventional printers, we provide measurements of how many copies are produced per minute. For 3D printing and scanning, we will look at how many hours are needed for production”. SC 28 has also established liaisons with the JTC 1 working group on 3D printing, ISO/IEC JTC 1/WG 12.

Other technologies such as IoT and cloud computing are providing opportunities to offer new print services. For example, companies may outsource their printing needs or use networks to centralize their printing needs. Data collected from the printing network can be used to identify underperforming machines or automate the delivery of printing supplies. And remote printing from off-site locations and from any devices is possible. To leverage some of these new opportunities, SC 28 has set up a liaison with the JTC 1 subcommittee on the Internet of Things, ISO/IEC JTC 1/SC 41.

The introduction of networked services can bring security risks. “As you know, SC 27 handles security”, remarks Ito. “They developed general concepts and principles for IT products with their standard ISO/IEC 15408 which describes how to evaluate security”.

“However, the criteria in ISO/IEC 15408 have an associated cost and time burden for certification which means that it is only practical for higher class machines. But we want to keep the smaller machines, such as support machines, secure so we want to develop such security standards for them”, explains Ito. Based upon the results of its study group to assess new opportunities for office equipment, SC 28 will address security for mid- to low-end office equipment in a new preliminary work item.

Another area of interest includes environmentally friendly machines. According to Ito, “the environment is becoming a big market. We need to support this market by offering standards or guidelines to minimize energy and paper consumption. Another issue is refurbishment and maintaining the quality of products when using used parts”.

3D printing, ISO/IEC JTC 1/WG 12.
Protecting manufacturing from cyber attacks

Adopting a risk-based approach and erecting defence-in-depth architecture to ensure business continuity is the best way to protect the manufacturing sector and other critical infrastructure.

By Michael A. Mullane

Half of the manufacturing companies that took part in a recent survey in the US admitted they had suffered a data breach or cyber attack in the previous 12 months. Unfortunately, such attacks are part of a growing global trend as the Industrial Internet of Things (IIoT) accelerates the convergence of the once separate domains of IT and operational technology (OT). This has made cyber security intrusions and threats not only more difficult to detect but also to prevent.
According to cyber security specialists F-Secure the chief motivations for hackers targeting the manufacturing industry are financial gain and industrial espionage. The “Duuzer attacks” of a few years ago is one of the best known examples of cyber criminals launching malware attacks to steal sensitive data and intellectual property. Physical damage remains another significant threat. In 2014, for instance, a steel mill in Germany suffered heavy damage after hackers gained access to the mill’s control systems via a spear phishing campaign – targeted e-mails that appear to come from a trusted source and trick recipients into opening a malicious attachment or clicking on a malicious link. The hackers stole the login names and passwords they needed to gain access to the mill’s office network, and from there crossed over to its production system.

**IT vs. OT**

A US government report published last year suggests that understanding the differences between IT and OT is key to achieving cyber resilience. For IT environments the priority is confidentiality of data. While this is also important for operational environments, the priority for the OT technologies is availability of data to ensure that systems can continue to produce. The problem is that when engineers designed many of today’s industrial environments cyber security was not a concern. OT teams were used to working within closed systems that relied heavily on physical security mechanisms to ensure integrity.

With the emergence of IIoT and the integration of physical machines with networked sensors and software, the lines between the two are blurring. As more and more objects connect, communicate and interact with each other, there has been a surge in the number of endpoints, and the increased possibility of computer failures, human mistakes, malicious attacks and natural disasters to affect physical systems. A variety of threat actors, ranging from lone hackers to organized cyber criminals and nation states, are continually finding ways to exploit vulnerabilities to move from the digital sphere of IT to the physical sphere of OT.

**Understanding differences between IT and OT is key to achieving cyber resilience.**

The growing interconnectedness of technology has exposed manufacturing, as well as other industries such as power and utilities, that also rely on industrial control systems (ICS) that use OT and IT. Generally speaking, an ICS integrates hardware and software for the purpose of automating and operating industrial processes. The issue, in terms of cyber security, is that an ICS must allow access to a wide range of different operators and even third-party vendors. For example, operators need to be able to manually override automated systems in case production is in danger of stopping, or if there are threats to health and safety, for example, or the environment. A number of international studies and reports have highlighted an alarming increase in cyber attacks targeting the supply chain. One such survey, conducted in the Americas, Asia and Europe, suggests that two thirds of companies have experienced a cyber attack on their supply chain.

**A risk-based approach**

Companies must be able to identify which of their assets are critical to achieving their stated mission in order to ensure that appropriate resources are allocated to protecting them. This is known as a risk-based approach to cyber security. The aim is to balance the cost of security threat mitigation against the potential impact of a successful cyber attack. Any solutions implemented must be monitored over time to ensure their continued effectiveness and to ascertain whether possible attacks could potentially overcome the control solutions. IT and OT security experts can then work together to erect a defence-in-depth architecture.

IEC Technical Committee (TC) 65, Industrial-process measurement, control and automation, has developed the IEC 62443 series of standards on Industrial Communication Networks – Network and System Security. Designed to keep OT systems running, it can be applied to any industrial environment or critical infrastructure facility. Because standards provide even more value when they are combined with conformity assessment the industrial cyber security programme of the IECEE – the IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components – tests and certifies cyber security in the industrial automation sector. The IECEE Conformity Assessment Scheme includes a programme that provides certification to standards within the IEC 62443 series.
Industry is becoming increasingly aware that it contributes to global warming by emitting greenhouse gases (GHG). It also produces waste that can be polluting for the environment and difficult to dispose of. IEC Standards help companies introduce greener manufacturing processes.

A growing number of companies are looking to produce goods in ways that are more energy efficient, less wasteful and less polluting. Green manufacturing, which refers to the renewal of production processes and the establishment of environmentally friendly operations within the manufacturing field, is making headway. Greener production processes are not only better for the planet, they can also help industry to save costs by drastically reducing their energy bills and use of raw materials.

Lowering GHG emissions

Benchmarks need to be established in order to help enterprises reduce their carbon footprint. The Science Based Targets initiative (SBTi) started back in 2015, in the run-up to the Paris climate change conference. Its aim is to help companies set targets to reduce their GHG emissions according to scientific information on how to avert climate change. The initiative is a collaboration between the non-profit Carbon Disclosure Project (CDP), the United Nations Global Compact (UNGC), the World Resources Institute (WRI), the Worldwide Fund for Nature (WWF) and the non-profit We Mean Business Coalition.

Currently, 684 companies worldwide have joined the initiative. They have agreed to
meet different targets to reduce their GHG emissions. For instance, a Danish energy provider aims to reduce its GHG emissions by 96% by 2023. “Faced with a situation where our fossil fuel business started to decline and present a real risk to our future profitability, we made the decision to completely transform our business model to become a renewable energy company”, explains Filip Engel, Senior Director of Group Sustainability, Public Affairs and Branding at the company and quoted on SBTi.

IEC expertise crucial for greener processes

IEC helps companies planning to make a transition to cleaner sources of energy by developing standards for renewable energy systems. Several IEC Technical Committees enable small and big renewable energy systems to operate safely and efficiently, on-grid or off-grid. They include:

- IEC TC 4: Hydraulic turbines
- IEC TC 5: Steam turbines
- IEC TC 82: Solar photovoltaic energy systems
- IEC TC 88: Wind energy generation systems
- IEC TC 114: Marine energy – Wave, tidal and other water current converters
- IEC TC 117: Solar thermal electric plants

The standards they publish help to fulfil several UN Sustainable Development Goals (SDGs), including SDG 13, which is to take urgent action to combat climate change and its impacts.

Boosting energy efficiency

Promoting energy efficiency by introducing new procedures and technologies, such as energy harvesting, is no longer exceptional for enterprises across a wide range of industries. Energy efficiency is not only better for the environment, it also enables companies to make substantial cost savings.

IEC has developed many standards which enable manufacturers to measure energy efficiency gains and set performance requirements. For example, IEC TC 2 prepares performance and safety standards for rotating machinery which is used in multiple manufacturing plants across the globe. It publishes the IEC 60034 series of standards, ranking electric motors according to their energy efficiency. These standards have been widely adopted throughout industry and regulators have often taken this classification system on board.

LEDs used in factories, warehouses and plants enable companies to widely reduce energy consumption for lighting on manufacturing sites. IEC TC-34 produces safety and performance standards for lighting, including IEC 62031 which establishes safety specifications for LED modules for general lighting. According to the International Energy Agency (IEA), 2016 and 2017 were critical turning points to the International Energy Agency (IEA), for energy efficient lighting, with LEDs reaching one third of market sales.

IEC Standards also help offshore oil platforms become more energy efficient. IEC TC 18 has published a major revision of the IEC 61892 series of standards which are key documents for the safety and performance efficiency of offshore platforms recognized by industry and regulators worldwide.

The series has been thoroughly brought up to date in line with fast technology changes in offshore platform electrical and electrotechnical technology. Improving energy efficiency is a key driver: the standard specifies the efficient use of generated power, as well as of high efficiency motors and variable speed drives to optimize power consumption. It also recommends the use of low-loss transformers and other high-power equipment as well as the re-use of lighting fixtures with high efficiency long-life lamps. In addition, it specifies energy optimization by using waste heat recovery as well as the establishment of an energy management system.

Managing e-waste

A growing number of companies are looking at ways of recycling electronic waste rather than disposing of it in landfills or by burning it in incinerators. Circular economy models are starting to be implemented by the more environmentally conscious enterprises. These models reassess how resources are managed and how waste is perceived throughout the entire lifecycle of a product from its initial design to its use, repair, reuse, remanufacture and, finally, its transformation into parts for new products.

The Advisory Committee on Environmental Aspects (ACEA), which provides guidance to the IEC Standardization Management Board (SMB) on issues related to the environment, and IEC TC 111, which develops several standards relating to environmental issues, are examining requirements for the circular economy. For instance, IEC 62430 specifies procedures to integrate environmental aspects into the design and development of products as well as the materials and components from which they are composed.

While there is still much work to do before the different industries around the world can claim to use green manufacturing processes, IEC International Standards are already supporting companies and manufacturers that are pioneering these new production methods.
Disruptive technologies and positive change

Artificial intelligence, ethics, digital transformation and international standards

By Michael A. Mullane

This is an edited excerpt from a new OCEANIS (open community for ethics in autonomous and intelligent systems) think piece about the role of standards in developing the dependability and trustworthiness of AI-related technologies. IEC is a founder member of OCEANIS and contributed to the publication entitled Role of standards in facilitating innovation while addressing ethics and value in autonomous and intelligent systems.

Artificial Intelligence Systems (AIS) are the key to enabling digital transformation and are already changing many aspects of daily life. Related technologies are being applied to boost efficiency, solve problems and create scalable individualized experiences. Finding answers to the many ethical dilemmas raised – that take into account issues such as privacy, security and integrity for the widest possible benefit – is vital to the development of innovative AIS technologies.

Digital transformation is not only about re-imagining business in the digital age to deliver greater value to customers. It is essential that ethical considerations shape the design process in order to maximize public good while limiting the risk of inadvertent harms or unintended consequences. International standards developed by multiple stakeholders should ensure the right balance is struck between the desire to deploy AIS rapidly and the need to study their ethical implications.

Above all, digital transformation can be most successfully implemented where trust is achieved through transparency and the process is driven by ethical principles. AI relies on data sets, including personal information. How this data is collected, managed and used is also an ethical issue. All stakeholders must have a clear understanding of what organizations hope to achieve and how they will use the data. Full permission must be granted to use personal information with adequate understanding of the likely consequences.

A key issue is bias and fairness of Algorithmic Decision Making Systems (ADMS). While it may be relatively easy to detect and mitigate bias, it is often difficult to get to the bottom of how ADMS are making decisions in order to solve the problems, as more often than not algorithms operate within a ‘black box’. It is one of the most important challenges we face, as algorithms are increasingly at the centre of our daily lives, from search engines and online shopping to facial recognition systems and booking flights. There are ethical concerns, for example, about the use of data collected by facial recognition applications, including development bias.

Wider adoption of such technologies and systems will depend to a large extent on effective risk management and the joint technical committee set up by IEC and ISO (JTC1/SC 42) is carrying out important standardization work in this area. A new ISO/IEC standard will provide guidelines on managing risk faced by organizations during the development and application of AI techniques and systems. It will assist organizations in integrating risk management for AI into significant activities and functions, as well as describe processes for the effective implementation and integration of AI risk management.

Disruptive technologies like artificial intelligence pose both challenges and opportunities across all sectors. For this reason, the joint ISO and IEC technical committee is liaising with a number of committees, in both organizations, that focus on different technologies and industries, as well as external organizations and consortia.
A new standard has been published, IEC 63077, that specifies the process for ensuring the performance and safety of refurbished medical imaging equipment.

Healthcare costs are rising across the world. As populations age and healthcare services become available to a greater number of people, the demand for services is increasing. Maximizing the value of medical equipment by reusing it can be one way of reducing costs. Refurbishment provides a process for ensuring that used medical equipment complies with the manufacturer’s specifications.

The IEC has recently published a new standard IEC 63077, *Good Refurbishment Practices for Medical Imaging Equipment*, that defines a systematic process for refurbishing used medical imaging equipment. The safety and performance of the medical equipment can be guaranteed without compromising the equipment’s performance, safety specification or intended use. IEC Subcommittee 62B: *Diagnostic imaging equipment*, developed this standard based upon an industry specification.

Markus Braun, the Convenor for Working Group 53, which was responsible for the preparation of the standard, has participated in standardization work related to refurbished medical equipment for many years. He notes that “safety and performance are the most important aspects to be considered with medical equipment and this is no different when reutilizing used medical equipment. Refurbishment is a method to ensure the continued safety and performance of used equipment as it moves from one medical facility to another”.

Medical imaging equipment, which includes X-ray, computed tomography (CT), magnetic resonance imaging (MRI) and ultrasonic equipment, requires a significant financial investment. According to Braun, “for complex and expensive equipment, it makes sense not to waste all of the inherent work and value. Generally, such equipment can be used for as long as service support is provided”.

**Circular economy**

Interest is emerging for a circular economic model that calls for a change in current production and consumption. It reassesses how resources are managed throughout the entire lifecycle of a product from its initial design to its use, repair, refurbishment and, eventually, to the recycling of its materials.
The European Union has encouraged a shift towards the circular economy as it seeks to generate economic benefit for the region while also remaining mindful of wasting resources. In a recent report, it has noted that refurbished medical equipment is applicable to the circular economy as it “contributes to creating access to quality healthcare and growing the economy while conserving resources”.

Several initiatives have been taken in Europe that address the requirements of the circular economy by maintaining products in the economic cycle for as long as possible. However, existing medical device regulations place stringent rules on the safety of the equipment. The processes defined in IEC 63077 prepare medical imaging equipment for future medical use. This allows the equipment to remain within the economic cycle while also ensuring its safety and performance as required in the medical device regulatory framework.

History of the standard

IEC 63077 is the final milestone in a process that started more than 10 years ago. Braun notes, “it began with an agreement by international industry associations to develop a document setting out the basic requirements for refurbishment. The aim was to ensure that the refurbished medical imaging equipment is safe and performs as when it was new”.

Without such requirements in place, many national regulatory authorities have placed bans on the import of refurbished medical equipment given the questions regarding their quality and safety. According to Braun, “these bans usually fail to distinguish between high-quality refurbishment based on the original manufacturer’s specifications and used equipment of undefined quality, with the effect that patients could be denied access to safe and economical medical equipment”.

COCIR, the European trade association representing electromedical industries, recognized the need to address the regulatory vacuum on refurbishment. It issued a Green Paper in 2007 followed by a so-called COCIR Industry Standard entitled Good Refurbishment Practices in 2010. The industry standard was also adopted by the US-based medical imaging association Medical Imaging & Technology Alliance (MITA), a division of the National Electrical Manufacturers Association (NEMA), and submitted to the IEC where it became a Publicly Available Specification (PAS) in 2016.

In October 2017, the US National Committee proposed a new work item to promote IEC PAS 63077 to become a normative standard. Using their knowledge of quality assurance for refurbishment, the experts in WG 53 successfully completed the process of standardizing IEC 63077 in less than two years’ time. WG 53 benefitted from the support of the Japan Medical Imaging and Radiological Systems Industries Association (JIRA).

In addition, ISO standards have also been considered in IEC 63077, such as those linked to quality management (ISO 13485) and risk management (ISO 14971).

A growing market

The refurbishment of medical imaging devices has been an established practice for nearly two decades. According to analysts, the market for refurbished medical equipment is growing and will exceed USD 16 billion by 2024. The North American market, comprised of the United States and Canada, represents the largest market for refurbished medical devices and is projected to have high growth rate in the coming years.

According to Braun, “refurbishment addresses the high demand for affordable and reliable products. Customers of refurbished medical imaging equipment are not only small hospitals with limited budgets but also leading medical institutions. Refurbishment is a well-established element of the global healthcare economy”.

As an international standard, IEC 63077 allows companies to get certified through an auditing process to check the integrity of the refurbishment process. “This standard is intended to give regulators confidence on the well-established processes in the refurbishment”, concludes Braun.
New standard to boost nuclear power installations’ cyber resilience

The scope and cost of cyber-malicious activities are increasing worldwide

By Morand Fachot

According to Cybersecurity Ventures’ Cyber Crime Annual Report 2019, the annual cost of cyber crime for the global economy will double between 2015 and 2021 to reach USD six trillion by 2021. In addition to financial losses, attacks on critical infrastructure are of growing concern.

The concept of critical infrastructure differs from country to country. The US government lists 16 critical infrastructure sectors. Three of these, dams, energy and “nuclear reactors, materials and waste” are directly related to power systems. Lists from other countries may be different, but most would include the nuclear sector and nuclear power plants (NPPs), some with more than one nuclear reactor.

Any incident or accident at a nuclear installation can have potentially catastrophic human and environmental consequences. There is increased concern also as NPPs become prime targets for cyber attacks from a number of actors (criminal, state or parastatal).

Taking into account that 444 nuclear reactors were in operation in the world as of June 2016, with 66 more under construction and an additional 172 planned, ensuring robust cyber security and resilience of these installations to cyber threats is not to be taken lightly.

NPPs built for physical protection and safety, not cyber threats

The main systems within a nuclear power plant fall broadly into two categories.

Primary systems control the reactor itself and, when needed, shut it down and maintain it in a safe condition to protect it. Secondary systems control the power generation equipment. Many of these systems, built years ago, are still based on analogue equipment that is not connected to the network and so is less susceptible to cyber attacks.

However, both systems in older NPPs are being gradually retrofitted with digital equipment, while new NPPs are designed with fully digital primary and secondary systems.

A 2015 nuclear safety report by the London-based Royal Institute of International Affairs notes that the nuclear sector has adopted digital systems later than other types of critical infrastructure. The report says that “the cyber security risk is growing as nuclear facilities become become more reliant on digital systems later than other types of critical infrastructure. The report says that “the cyber security risk is growing as nuclear facilities become become more reliant on digital systems later than other types of critical infrastructure.

In October 2016, the International Atomic Energy Agency (IAEA) Director General, Yukiya Amano, told Reuters news agency that “this issue of cyber attacks on nuclear-related facilities or activities should be taken very seriously.”

Long IEC involvement in cyber security

The IEC has been closely involved in the development of standards relevant to cyber security for years through its work in ISO/IEC JTC 1/SC 27: IT security techniques. This Subcommittee was set up by the IEC and ISO Joint Technical Committee for information technology.

IEC/ISO JTC 1/SC 27 has prepared dozens of documents covering various aspects of IT security techniques, including the ISO/IEC 27000 family of standards on information security management systems.

Other series of IEC Standards are relevant to the protection of communication networks, control systems and power installations against cyber threats. They include:

- IEC 62443: Industrial communication networks – Network and system security
- IEC 61850: Communication networks and systems for power utility automation
IEC 60870: Telecontrol equipment and systems
IEC 62351: Power systems management and associated information exchange

But most, except IEC 62443, which is relevant also to NPPs, fail to address certain special needs of the nuclear industry.

To fill this gap, IEC SC 45A: Instrumentation, control and electrical systems of nuclear facilities, set out to develop specific standards for cyber security. The scope of this SC, a subcommittee of IEC TC 45: Nuclear instrumentation, includes the preparation of “Standards applicable to the electronic and electrical functions and associated systems and equipment used in nuclear energy generation facilities (...) to improve the efficiency and safety of nuclear energy generation”. It implements principles and terminology of the IAEA safety and security guides.

Greater focus on NPPs

IEC SC 45A focused on safety, including some software aspects, but didn’t tackle the generic issue of NPP cyber security. In recent years it started developing specific standards to prevent, detect and react to cyberattacks, which it defined as “malicious acts by digital means on Instrumentation and Control (I&C) programmable digital systems. This includes any unsafe situation, equipment damage or plant performance degradation that could result from such an act”.

IEC SC 45A published its first standard addressing cyber security issues in August 2014. The second, comprehensively overhauled, edition of this standard, IEC 62645:2019, Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements, has just been published. It excludes site physical security and non-malevolent actions and events.

The standard notes that “ISO/IEC 27001 and ISO/IEC 27002 are not directly applicable to the cyber protection of nuclear I&C programmable digital systems. This is mainly due to the specificities of these systems, including the regulatory and safety requirements inherent to nuclear facilities”.

However, it also states that “this standard builds upon their valid high-level principles and main concepts of the generic security standards (...) adapts and completes them to fit the nuclear context and coordinates with the IEC 62443 series.”

IEC 62645 includes coverage of the following issues:

- managing a nuclear I&C programmable digital system security programme. This includes overall concepts for the preparation of programme, policies and procedures, roles and responsibilities, establishment, implementation and operation of the programme
- Life-cycle implementation for I&C programmable digital system security, which embraces requirements, planning, design, installation, operation and maintenance activities and more
- All aspects (technical, physical and administrative) of cyber security controls, such as policy, organizing security, asset management, access control, etc.

IEC 62645, was developed “to prevent and/or minimize the impact of attacks against I&C programmable digital systems on nuclear safety and plant performance. It covers programme level, architectural level and system level requirements.”

Nogent-sur-Seine nuclear power plant, which houses two reactors (Photo: EdF)

“IT is intended to be used by designers and operators of NPPs (utilities), licensees, systems evaluators, vendors, subcontractors and licensors.”

Unlike the first edition of the standard this one gives a table of high-level correspondence between the IEC 62443 series and IEC 62645, listing dozens of subclauses related to context of the organization, lifecycle implementation for I&C programmable digital system security and security controls.

Together with other relevant IEC Standards it should contribute significantly to the protection and resilience of NPPs against cyber attacks.
Long and winding wires

A new standard improves and clarifies the continuity tests for winding wires, making them more reliable and reproducible for on and offline measurement

By Catherine Bischofberger

Millions of kilometres of winding wires are produced every day – enough to go around the earth at least ten times! IEC Standards make sure they are used safely in millions of devices. They also pave the way for future developments involving the use of nano materials and electric vehicles (EVs).

Winding wires are far from being on everybody’s radar and yet perhaps they should be. They are in millions of electric and electronic devices we use every day and are a key component which enables these items to perform properly, safely and in an energy-efficient manner.

“Winding wires are in anything that needs an electric motor, a generator or a transformer, basically. There are many different applications in the white goods industry: winding wires are in most of the consumer electronic devices which make our lives easier at home. Whether utilized as conductors or primary insulators, they are also essential parts of the different motors used in cars, for instance. They are employed in the windscreen wiper motors as well as in the valves and ventilation devices used around the combustion engines, to name but a few. They are also widely deployed in industrial applications for automation or in wind turbines”, confirms Andreas Levermann, one of the

Winding wires can be densely packed in small areas (Photo: Shutterstock)

In electric motors, these key components transform electrical energy into mechanical energy by creating electromagnetic fields. Most of the wires are made of very pure copper, a highly conductive material, which can be densely packed into small areas. “If the requirements are for lighter wires, aluminium can sometimes be used but it is less conductive than copper and is therefore not suitable for high efficiency applications”, Levermann points out.

New standard for continuity specifications

Winding wires are so ubiquitous that manufacturers produce millions of kms of wire a day. “I would say that each day, enough winding wire is produced to go around the earth at least ten times”, Levermann remarks. Yet, the technology to produce these wires is very complex. “So many different properties are required: thermal, electrical, dimensional, chemical, insulating... The IEC 60317 and IEC 60851 series, which together comprise more than one hundred standards, deal with those aspects”, Levermann explains.

Levermann heads the working group which developed the new edition of IEC 60851-5, that now exists in a consolidated version, including the amendments made in 2008 and the very recent ones added in 2019. “The important aspect we wanted to specify in the new edition is continuity measurement. When you produce millions of kms of winding wire, it is impossible to avoid insulation weaknesses. IEC 60851-5 specifies reliable test methods and a low number of defects for a given length of wire. We worked hard to make this standard as international as possible – it is a compromise that makes it suitable for a wide number of countries”, he says. IEC TC 55 members reflect this striving for compromise: all continents are represented, with participating National Committees from China, France, Germany, India, Iran, Italy, Japan, Russia and the US as well as many observing countries, including Australia, Brazil and South Africa.

What’s in the future for wires?

Demand from electric and hybrid car manufacturers is growing rapidly, leading to new levels of quality requirements for winding wires such a resistance to pulse endurance testing. The TC is studying a project which may lead to new standards in that area.

New insulating materials are also being developed which might have an impact on IEC TC 55 Standards. “We liaise with a number of technical committees and one of them is IEC TC 113: Nanotechnology for electrotechnical products and systems. New nano materials can be included in the enamels, which are used as insulating layers in the wires. This can lead to enhanced or even new properties, such as lower coefficients of friction or higher corona resistance”, Levermann informs.

Cutting-edge, energy efficient, safe... Winding wires will continue to be essential in years to come and will remain as unobtrusive as they have always been – thanks to IEC Standards.
MET-CERTIFIED to run first marine energy certification workshop in Latin America

The Pan-American Marine Energy Conference (PAMEC) Energy Association is organizing PAMEC 2020, in San Jose, Costa Rica from 26-28 January

By Antoinette Price

The Conference will examine areas including resource assessment, environmental impacts, wave, tidal, offshore wind, floating offshore wind, ocean thermal energy conversion (OTEC) and salinity gradient technologies, as well as storage and integration, policies to enable remote coastal community solutions and technologies to enable micro-electricity demand solutions.

The MET-CERTIFIED project has been invited to hold a workshop on IEC standardization and certification of marine energy convertors, which will explain the marine technologies sector of IECRE, the IEC System for Certification to Standards Relating to Equipment for Use in Renewable Energy Applications.

Boosting Innovation through standards and certification

“We are grateful to have this opportunity to raise awareness with technology developers, test facilities and investors, about the role of IECRE certification, and how it builds investor confidence, reduces technology risks, helps raise project finances and facilitates global market access”, says Peter Scheijgrond who manages the EU MET-CERTIFIED project.

Scheijgrond works with the Dutch Marine Energy Centre which manages the MET-CERTIFIED project. He is Convenor of the IECRE Marine Energy Working Group on Scope of certification, and chairs the Dutch mirror committee to IEC Technical Committee 114, which develops international standards for marine energy, including wave, tidal and other water current converters.

Building relationships

The workshop is part of a strategy to build relationships with end-users of certification products and better understand their needs for certification.

One of the aims is to increase the participation of Latin American service providers, such as test facilities and certification bodies in IEC and IECRE related activities, through membership or active application of the certification system.

A range of stakeholders are expected to participate, including banks, project developers, insurers and maritime regulators, test laboratories, classification bodies and technology developers.
On the agenda

The workshop will cover the following topics:

- Updates in the development of standards for marine energy convertors under IEC TC 114
- How certification works under the IECRE marine energy (ME) sector
- Discussions of participant roles in certification, their propositions and/or needs
- Interactive session enabling participants to understand the value and relevance of certification
- Overview of how to get involved in IEC TC 114 as experts, or with the IECRE ME sector

About IECRE

An ever-increasing demand for electricity, and the need to reduce fossil fuels power generation, have led to rapid development and growth of the RE sector. IECRE was established in 2014 because of the need to address the specific requirements within this sector, which are not covered by the existing IEC Conformity Assessment Systems.

IECRE aims to facilitate international trade in equipment and services for use in RE in the marine, solar photovoltaic (PV) and wind energy sectors, while maintaining the required level of safety.

About MET-CERTIFIED

MET-CERTIFIED is funded by the European Interreg 2 Seas programme for low carbon technologies, and is co-financed by the European Fund for Regional Development (ERFD) for the period September 2016–December 2019. Additionally, the Ministry of Economic Affairs in the Netherlands, Province of South-Holland and North-Holland and the Belgian Province of West Flanders are offering financial support.

More about PAMEC

PAMEC has global membership and supports research and development of renewable energy from the ocean’s tidal currents, waves, ocean thermal current (OTC) salinity gradient (SG), and offshore wind, particularly floating offshore wind in the Americas.
The connected mine

IECEx helps mining embrace the digital age safely and efficiently

By Claire Marchand

Mining is one of the most ancient trades performed by humans. It is also one of the trades whose evolution has been fairly slow, considering that the first mining efforts were to search for stones suitable for making tools approximately 2.6 million years ago. Today, mining is a far cry from the traditional depiction of pack mules, pickaxes, canaries and rugged prospectors.

Mining in the digital age

Modern mining is high-tech, efficient and safer than ever, even though there are still many places around the world where mines operate more or less as they did last century. However, in developed economies, where worker safety is heavily regulated and efficiency is valued, things are changing rapidly and the mine of the future is not far from becoming the norm.

Through the latest in sensor and cloud technology, connected mines are modernizing the extraction process, improving workers’ safety and increasing productivity.
Modern mining companies that embrace the digital age can rely on a wide array of recent technological advances for their operations. Here are a few examples:

**Automation:** autonomous vehicles and automated technologies can be used in ultra-deep and remote mines.

**Ventilation on demand:** the airflow system is only turned on to direct fresh air where and when required, thus reducing ventilation costs.

**Sensors:** smart mining can track and optimize mining operations, capture a multitude of data that can be analyzed in real-time and provide vital information. The data collected allows engineers to create simulations to plan and schedule operations and prevent failure and downtime.

**GPS:** high-accuracy GPS technology can assist in precision drilling and in directing autonomous haul trucks.

**Drones:** can provide real-time aerial footage of mining sites for maintenance, monitoring and mapping.

**EVs:** Electrical and hydrogen-powered vehicles reduce carbon emissions and provide better air quality for workers in underground mine shafts.

**Wearables:** portable communication and monitoring devices provide real-time access to critical information on air quality, equipment maintenance operations in general.

**3D printing:** the technology can help increase productivity and efficiency, including the on-demand production of repair and replacement parts.

**3D imaging:** the 3D imaging can help understand the geology of ore deposit, thus reducing waste.

In the connected mine, all operations are optimized: productivity, efficiency and safety increase dramatically. Supervisors and engineers on site can receive alerts via text messages, email or in-app notifications and can, in turn, react to critical issues in real time and maximize productivity. In addition, advanced data analytics can be applied to the raw data to create insights, visualizations, and recommendations. This information is delivered to mine managers and employees in real time on their mobile devices.

**Designed and built for Ex areas**

As is the case with larger pieces of equipment used in explosive (Ex) atmospheres, any device – such as sensors – has to be designed and built in compliance with the very strict requirements set out in standards and specifications, most notably in IEC International Standards developed by IEC Technical Committee 31: Equipment for explosive atmospheres.

Designing and building equipment and devices in compliance with IEC International Standards is not enough on its own. To ensure that any piece of equipment meets the required criteria, it has also to be tested and certified. Products associated with a certificate of conformity satisfy the criteria for safe usage in hazardous environments.

**Tested and certified by IECEx**

IECEx, the IEC System for Certification to Standards Relating to Equipment for Use in Explosive Atmospheres, is the only truly international conformity assessment system that provides testing and certification for all items of Ex equipment – electrical and non-electrical – and installations as well as certifying the skills and competence of individuals working in hazardous areas.

The System addresses the inspection (location and other), installation, maintenance and repair of equipment and systems and assesses the competence of personnel working in this highly specialized area.

IECEx has been endorsed by the United Nations (UN) through the UN Economic Commission for Europe (UNECE) as the certification system for the assessment of conformity in Ex areas.

IECEx operates the following schemes:

- IECEx certified equipment scheme
- IECEx certified service facilities scheme
- IECEx scheme for certification of personnel competence (for explosive atmospheres)

It also runs the IECEx conformity mark licensing system which provides on-the-spot evidence that products bearing the conformity mark are covered by an IECEx certificate of conformity.

**Easy access to all IECEx certificates**

All master certificates are available on the IECEx website, allowing for instant checking on computers or mobile devices. Most importantly, the IECEx certificate database has been recently revamped for easier, more user-friendly access to any certificate. Certificates can be searched by date range, certification body, applicant (manufacturer, service facility, person), status (current, cancelled, suspended), scope, country or keywords.
In today’s world of ultra-smart technology, being smart doesn’t only mean being well connected, but also well protected against security breaches. While that is an aspect that individuals must consider, it has become a vital and non-negotiable factor for industry at large.

Huge multinationals and small or medium enterprises face security breaches on a daily basis and thus have to ensure they can thwart attacks on their operations and eliminate – or at least reduce – the impact of such breaches.

Evolving technology equals evolving risks

A corollary of the ever faster pace at which technology advances is the rapidly evolving nature of security risks. Keeping up with new technologies, trends and threat intelligence is a challenge that businesses must tackle if they want to prevent information security breaches that cost vast amounts every year in stolen intellectual property and confidential data.

For years, “the traditional approach,” as explained by the TechTarget website, “has been to focus resources on crucial system components and protect against the biggest known threats, which meant leaving some of the components undefended and not protecting systems against less dangerous risks.”

The positive outcome of the numerous security breaches affecting all kinds of companies throughout the world in recent years may be the way they have changed their approach to security and implemented information security management systems (ISMSs) to address their needs and vulnerabilities.

An information security management system (ISMS) is a set of policies, procedures and controls that protect the integrity, confidentiality and accessibility of a company’s sensitive data. It encompasses processes, data, technology as well as employee behaviour. When enforced comprehensively, it is bound to become part of the company’s culture.

Enhancing information security

To help organizations enhance their information security, the joint technical committee on information established by IEC and ISO, ISO/IEC JTC 1, through one of its subcommittees, SC 27, published ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.

The international standard specifies requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organization, as well as the assessment and treatment of information security risks tailored to the organization’s needs. The requirements are generic and intended to be applicable to all organizations, regardless of type, size or nature. It makes recommendations regarding leadership, commitment and policies, as well as actions to address risks and opportunities. It also covers support matters such as resources, competence, awareness, communication, operational planning and control, information security risk assessment and issues including treatment and performance.

Multiple aspects of ISO/IEC 27001

ISO/IEC 27001 goes further than cyber security and covers how an organization manages the security of information it holds, both for its own operations and from external sources, such as suppliers, customers, etc.

A management system that meets ISO/IEC 27001 will look at overall security such as:

→ Are there locks on the front doors?
→ Who can have keys and how is the
allocation of keys/passwords to enter the building managed?

- Under what conditions can external organizations have access into the building, e.g. cleaners, service organizations, essential services, etc.?
- Is there a policy to lock up files overnight to prevent security staff and cleaners from seeing sensitive information on desks?
- How are old records – paper and electronic – disposed of?
- What happens with the hard drives of computers that are discarded and replaced?

ISO/IEC 27001 also addresses threats that come from deliberate cyber attacks.

There are many benefits in using the holistic approach of ISO/IEC 27001: compliance with national and/or regional regulations; resilience and better response to cyber threats; reduced costs through a centrally-managed system that gets rid of multiple and ineffective procedures; well-informed employees aware of their security responsibilities.

By achieving certification to ISO/IEC 27001, an organization demonstrates to its stakeholders and customers that it is committed to managing information and securely. In short, the company can be trusted.

While certification to ISO/IEC 27001 has existed since the standard was published in 2013, it is only recently that IECQ, the IEC Quality Assessment System for Electronic Components, has set up a scheme for the certification of ISMS.

IECQ is part of the solution

The ever-growing need for organizations to provide independent proof of compliance with ISO/IEC 27001 for their information security management system (ISMS) has led industry to request that IECQ certification bodies (CBs) be able to cover the assessment and certification to ISO/IEC 27001 under the approved process scheme (AP scheme) while conducting other IECQ assessments, for example avionics or hazardous substance process management.

What drove industry to approach IECQ recently was the lack of harmonization among the many certification bodies that offer their own individual certificates and apply their own individual interpretations of ISO/IEC 27001. Over time, this has resulted, in different approaches and differences in what is accepted by the various certification bodies. Thus, industry felt that IECQ was able to offer a single approach to the application of ISO/IEC 27001. All certificates can be found on the IECQ website.

About IECQ

IECQ provides industry with a supply chain verification tool for seeking assurance that electronic components, assemblies, processes and related materials conform to declared technical standards and specifications. IECQ certificates are used worldwide as a tool to monitor and control the manufacturing supply chain, thus helping to reduce costs and time to market, and eliminating the need for multiple re-assessments of suppliers.

IECQ is an essential player and a key partner of industry that helps companies manage their all-encompassing and complex information security systems.

An ISMS that meets ISO/IEC 27001 will look at who can access the facilities including cleaning teams.
New year, new tech! In issue 01 of e-tech we will be taking a look at some of the technologies that are likely to be big in the new year, including brain-computer interfaces, the latest in electric vehicles and mobile driver’s licences. New, as well as established technologies, need to take sustainability into account from their inception, now more than ever. ACEA, the IEC Advisory Committee on Environmental Aspects aims to ensure standards developers take environmental protection concerns into consideration in their standardization work. e-tech spoke to several industry insiders to find out what companies are doing to move towards a more circular economy.