Issue 01/2019

e-tech

news & views from the IEC

Technology trends

IEC world

Looking to the future

Technology focus

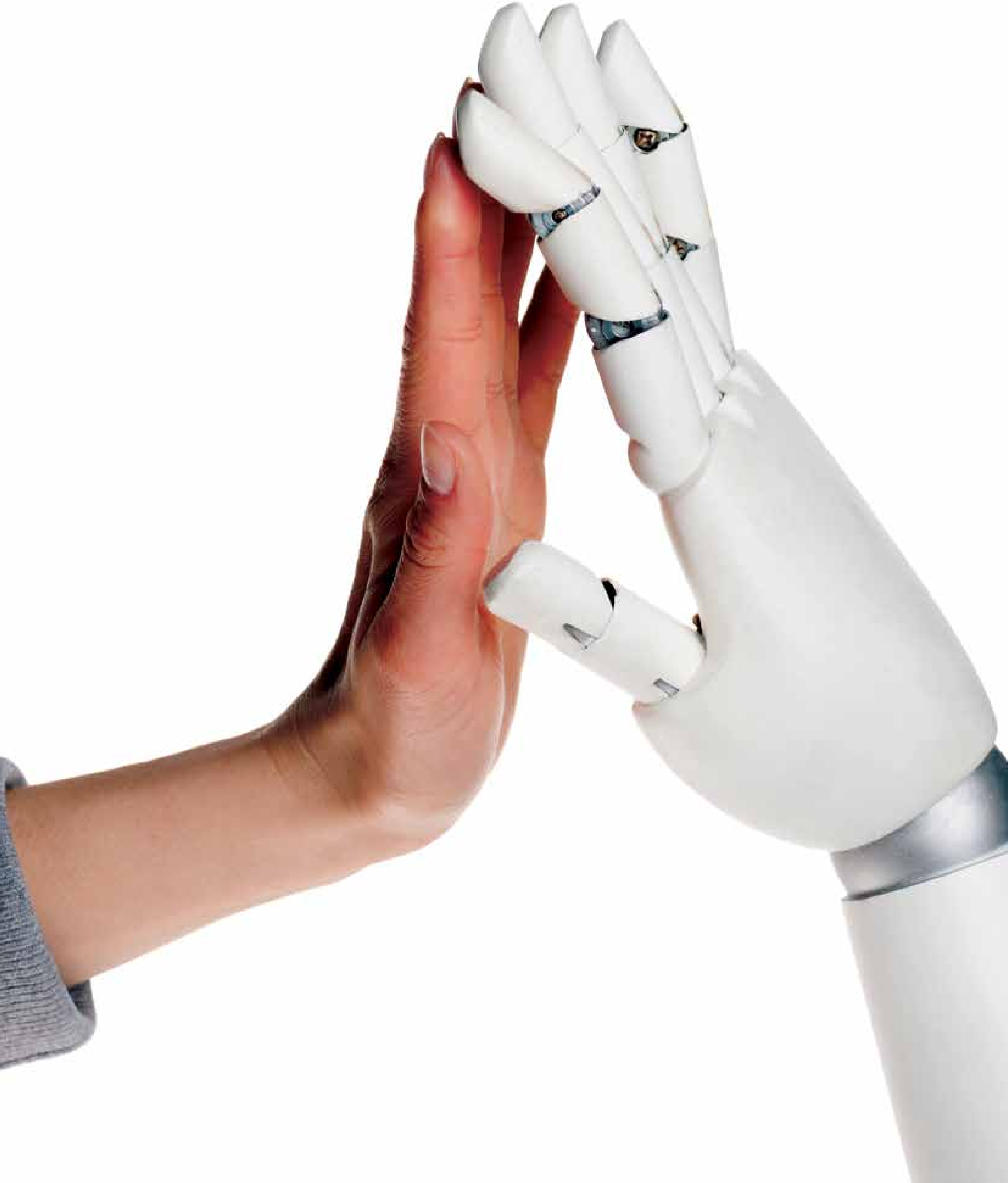
Automatizing the power grid

Robot cars

Who needs AI

In store

Form and substance



Bringing the ethics into innovation

Innovative technology is not created in a vacuum but by, and for, society as a whole

Zoë Smart
Managing Editor e-tech

At this time of the year many eyes are turned towards the new technologies coming out of big trade shows, such as the Consumer Electronics Show (CES) in Las Vegas and the Mobile World Congress in Barcelona. And while new technologies still have their detractors, it would be very difficult to dismiss the benefits many of them are bringing to areas such as medicine, manufacturing and ICT, to name but a few.

There is absolutely no doubt that technological innovation is revolutionizing the way we lead our lives. From smart technology that will help us live longer, healthier lives to blockchain that could be used to optimize humanitarian relief, technology has the potential to "make the world a better place". And yet, innovative uses of technology have also demonstrated how it can be problematic. These aren't the imagined scenarios where machines leave most of the world's population jobless or AI takes over the universe but real situations with real repercussions; two examples are the PredPol and COMPAS cases, where programmes used by the US police force and judicial system respectively, were shown to carry racial bias.

There is a widespread belief that technological innovation shapes society as if it were somehow disassociated from it, and yet it is a product of that very society it helps to shape and define. As such, it is imperative that the ethical implications of the technologies are taken into account right from the onset of development. This means considering the needs of civil society, working in open and transparent ways and within partnerships.

Some universities are beginning to introduce courses on ethics for their engineering students and the Council of Europe recently adopted the first European Ethical Charter on the use of artificial intelligence in judicial systems. A number of IEC standardization activities are already addressing ethical issues around AI in technologies.

In our article *Looking to the future*, Peter Lanctot, Secretary of the IEC Market Strategy Board (MSB), talks about the growing importance of digital transformation and the possibility of the IEC looking into the development of standards that can mitigate the impact of potential biases resulting from algorithms.

More concretely, in July 2018, IEC together with eight other founding organizations, launched OCEANIS, a global platform whose aim is to openly discuss and collaborate on how best to support the ethical application of autonomous and intelligent systems, taking end users' concerns into account.

With all the excitement of new tech comes the responsibility to ensure that it best serves the interests of those for whom it has been created. Ethical frameworks can help ensure this is the case.

IEC *e-tech* is a magazine published by the International Electrotechnical Commission in English.

Impressum

Editor in Chief
Gabriela Ehrlich

Managing Editors
Zoë Smart – Antoinette Price

Contributors
Catherine Bischofberger, Morand Fachot, Claire Marchand, Natalie Mouyal, Michael A. Mullane

Read us online
www.iecetech.org

Subscription
If you would like to receive a publication alert, please click the "subscribe" button on www.iecetech.org

Disclaimer
The content of this issue of *e-tech* is for information purposes only.

The IEC assumes no liability or responsibility for any inaccurate, delayed or incomplete information.

Articles may be reproduced in whole or in part but must mention
Source: IEC *e-tech* (issue number, year, author name), www.iecetech.org

Available for download
Download on the App Store
GET IT ON Google Play

18

Moving to quantum cryptography now could help safeguard data

25

New technologies are increasing healthcare access and improving lives

35

IECQ provides global certification solutions for global markets

Editorial

IEC world

Technology focus

Industry spotlight

Technical committees

Conformity assessment

In store

IEC MSB has been set up to identify key technology trends and market needs in the areas of IEC work

Looking to the future

An overview of the Market Strategy Board's hot topics for 2019

By Natalie Mouyal

It is a generally accepted notion that we are living in times of rapid change. If, to paraphrase Heraclitus, change is the only constant, then organizations must anticipate areas of possible change and prepare themselves accordingly.

Within the IEC, the Market Strategy Board (MSB) has been set up to identify key technology trends and market needs in the areas of IEC work. Comprised of high-level industry leaders and IEC officers, the MSB offers strategies to help guide long-term IEC activities. It provides recommendations to the IEC on the areas that could trigger possible disruptions but also offer opportunities to the IEC in the future.

To better understand some of the key topics this year, *e-tech* spoke with Peter Lanctot who serves as Secretary to the Board.

A new type of resilience

Hurricanes, heat waves and flooding are some of the extreme weather events occurring with increased frequency. The impact on the delivery of electricity can be devastating with blackouts affecting millions of people. As a result, Lanctot notes that "a new type of resiliency for utilities is needed to cope with the resulting effects of climate change".

Peter Lanctot speaking at the 2018 IEC General Meeting in Busan

Resiliency refers to the characteristics of an electrical system to recover its operations. It is the ability to avoid or minimize disruptions to the grid after an extreme weather happening. This can be achieved by, for example, splitting networks into smaller circuits or deploying intelligent switches that can detect a short circuit, block power flows to that area and reroute the electricity so users do not lose access.

According to Lanctot, MSB members will tackle the issue of resiliency for utilities. "Legacy grid equipment is at risk as we face more extreme storms and temperatures. It is necessary to make the electricity distribution systems more climate-resilient and this could include an overhaul of standards".

Digital transformation

Digital transformation is the integration of digital technologies into organizational processes and competencies. It encompasses artificial intelligence, data management and smart systems. Given its importance, the MSB will be publishing a White Paper in October 2019 on the topic of ontologies and the semantic web in the digital transformation age.

According to Lanctot, "MSB members agree that artificial intelligence is the next phase of innovation and will cause long term disruption to market and technology". For the IEC, areas of future work could include the development of standards that can mitigate the impact of potential biases resulting from algorithms.

> "More systems are becoming data driven and therefore more vulnerable. Standards can provide solutions."

Data is an important feature of the digital transformation, especially as it becomes increasingly easy and cheap to collect and store. However, this raises questions regarding data access, management, ownership and protection. Lanctot notes that “data allows for ‘smartness’ - such as smart energy, smart cities, AAL, smart manufacturing – but how do we use the data that come out of these systems? The IEC is well positioned to find a common ground on these questions. With the digitalization of the economy, the IEC can help to define a standard for the usage of data”.

Within smart systems, the MSB will examine the integration of people, smart devices and machines. This can also include digital twinning which, according to Lanctot, “will become a business imperative and serve as the foundation for connecting products and services between the physical and virtual worlds”.

Maintaining safety

Safety is one of the core remits of the IEC beginning with standards which have enabled the safe transmission and delivery of electricity. As new technologies are introduced, the IEC develops standards to ensure that users are safe.

The MSB has identified two technologies where safety is an area for further study: artificial intelligence and the Internet of Things (IoT). Questions raised within the MSB include how to maintain current levels of safety with IoT devices and how to guarantee the safety of home appliances as these increasingly rely on autonomous decision-making. “Specifically, the MSB would like to examine the impact of machine learning on functional safety”.

Related to safety, cyber security is an increasing threat to organizations and individuals. This is another area of focus especially since, as Lanctot notes, “more systems are becoming data driven and therefore more vulnerable. Standards can provide solutions”. With the massive proliferation of IoT devices, security questions regarding hacking, data management and privacy are emerging. The MSB has also raised the issue of upgrading firmware on IoT devices and how to ensure that it is implemented securely.

Lanctot also remarks that while the IEC is well-positioned to bring together the various stakeholders to discuss solutions for safety and security, not all participants may have benign intentions. “How do we control who joins the discussions on topics such as security? And, if some of the participants are not responsible, they will nonetheless retain the keys to the functioning of the security system”. Guiding stakeholder participation and responsibility could be an area that the IEC will need to address.

A new type of resiliency is required for utilities to cope with extreme weather conditions

Risk management has also been raised as a potential topic of further study. According to Lanctot, regulators are keen to implement risk management solutions for basic safety features. However, the question remains how it can be best used and integrated. Working with regulators will also become an area of increased focus. “Every country has its own rules and regulations but there are some commonalities. I think that in 2019, regulations will become one of the topics that the MSB looks at more deeply”.

Future trends to follow

Robotics in the service industry and battery-propelled jet airplanes are two topics that will be on the MSB agenda for discussion and likely to become areas of interest in the next few years.

“A recurring topic is robotics and how it will affect the service industry. We already have robots making drinks for us at the bar, but what about in places with lots of people, like on cruise ships, where there is more of a social atmosphere?” Questions remain on whether robot assistants will be deemed sufficiently useful and an acceptable alternative to human personnel.

While the electrification of cars and buses has begun, many issues constrain the development of electronic airplanes such as the weight and space requirements of batteries that will be used for propulsion. However, as Lanctot notes, “it’s an area where the IEC has a lot of knowledge. It is something to look at a little further as a new opportunity for the IEC”. He has been tracking industry activities and has observed that “companies and universities are starting to look into this issue even though it is a little outside of the box”.

Standards for key information technologies

For many today, smart technologies facilitate carrying out daily activities, business operations, the management of critical infrastructures and more

By Antoinette Price

The Internet of Things (IoT), increased connectivity and advances in artificial intelligence (AI) technologies, such as algorithms and machine learning, are enabling industries to streamline processes, improve efficiency and reduce costs as they become more digitized.

Advancing innovation through standardization

IEC and ISO develop international standards for information and communication technologies (ICT) for business and consumer applications, through their joint technical committee (ISO/IEC JTC 1).

Some examples include automatic identification and data capture (AIDC) techniques for RFID tags used in retail and

IoT technologies, smartphones, apps and agribots make farming smarter and more efficient supply chain management; biometrics, cards and personal identification, for accessing buildings and smart devices. The scope also covers AI, cloud computing, coding of audio, picture, multimedia and hypermedia information, data management and exchange, IoT, IT security techniques, programming languages and system software interfaces, virtual reality and more.

Staying ahead of the game

Technologies are changing how we live, do business, monitor our health and communicate. In just over two decades, smart devices, email, Internet and social media have largely replaced former communications channels.

Factories are more automated, car manufacturers are developing self-driving vehicles, while algorithms can already predict health problems before they develop, so what about the future? How will life be in another 10 years?

> “As long as the adoption of ICT technologies continues to spread rapidly into all industries, the role and responsibilities of ICT standards will become more important.”

Keeping an eye on the horizon

Against this backdrop, the Joint Advisory Group (JAG) Group on Emerging Technology and Innovation (JETI) was established in 2016, in order to find and recommend opportunities to JTC 1 to facilitate standards development for future emerging and innovation technologies.

e-tech caught up with Seungyun Lee, JETI Convenor, to hear about the latest work and activities.

What are the top technologies you are currently working on?

We established a list of 15 top technologies following a JETI group survey in 2018. Right now the top five include:

- Quantum computing and autonomous and data rich vehicles, for which JTC 1 has created new study groups following JETI recommendations.
- Autonomous systems, which is being worked on in JTC 1 technical committees for IoT and AI.
- Digital twin and brain-computer interface for which we are developing technology trend reports as an initial investigation and analysis process.

Seungyun Lee, Convenor, JETI

Technology doesn’t stand still. Are there new topics in addition to the top 15?

During the 2018 survey, 32 technologies were identified. These were gathered from many other professional technology forecasting organizations, such as Gartner, IDC and Forest Research.

The list is broad, so we will have to decide which areas need urgent attention and see how we can streamline overlapping topics where possible. Some examples include:

- augmented data discovery
- virtual assistance
- blockchain
- smart farm/agriculture
- machine learning
- smart dust
- edge computing

Are there any challenges?

As long as the adoption of ICT technologies continues to spread rapidly into all industries, the role and responsibilities of ICT standards will become more important.

As the ICT-based convergence of industry expands, the approach to standardization needs to be differentiated from existing approaches to make sure we consider the various converged industries and eco-systems as well.

At the moment, ISO, IEC and JTC 1 are using a systems approach to standards to support this. We expect the systems approach could become more complex and critical and in this sense, we (JETI) will need to consider how we could improve planning for future emerging technology and what the best methodology to support future ICT standards would be.

The challenges of cyber security in a connected world

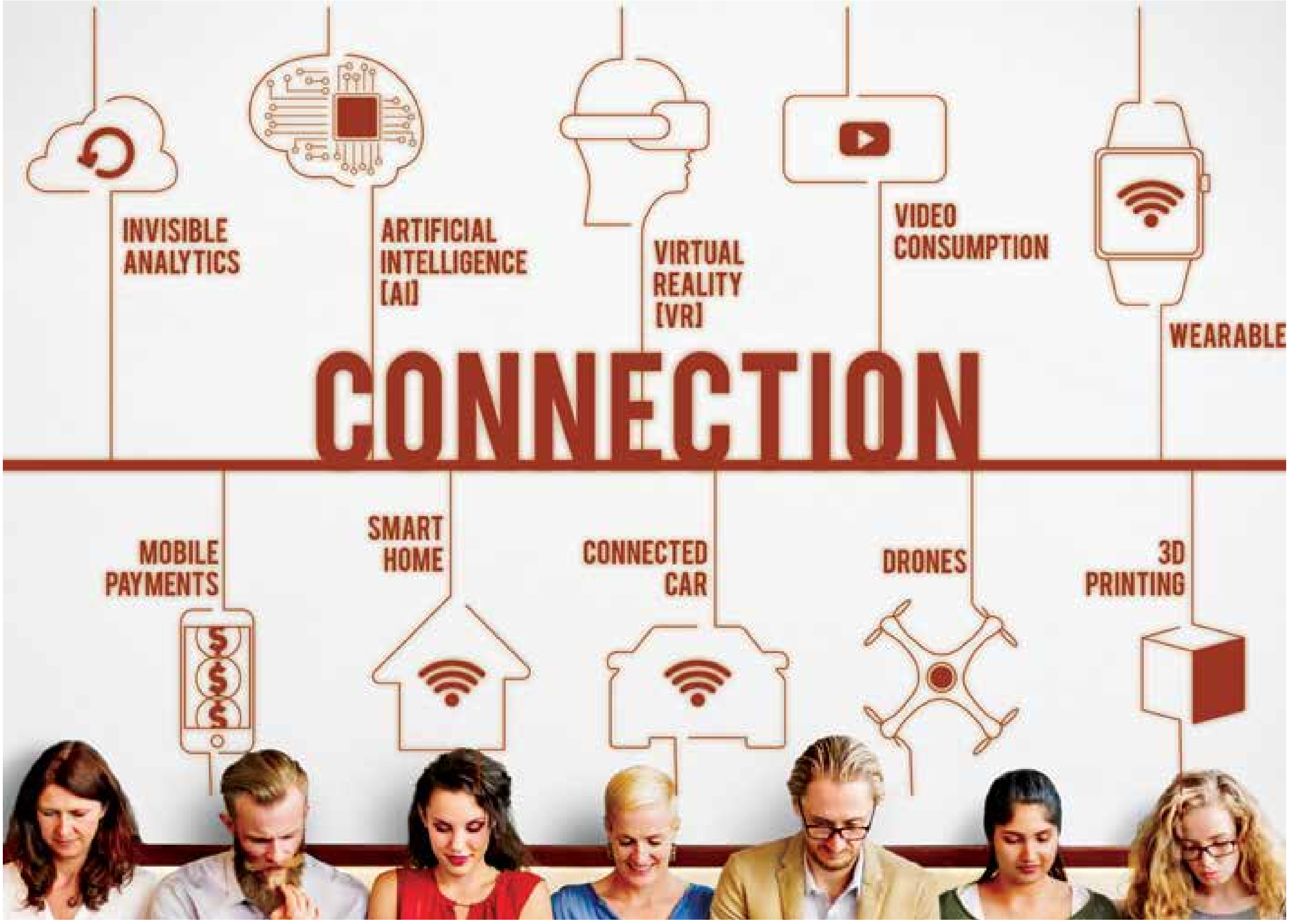
Why cyber security measures must address personnel, processes and technologies

By Michael A. Mullane

The growth of connected devices has accelerated the convergence of the once separate domains of information technology (IT) and operational technology (OT), resulting in Industrial IOT (IIOT).

IT and OT are increasingly complementary, but also very different. IT exists in the virtual world, where data is stored, retrieved, transmitted and manipulated. OT, in contrast, belongs to the physical world and deals with real time processes.

While IT has to safeguard every layer of the system, OT is about maintaining control of systems: on-off, closed-open, and so forth. IT is about confidentiality; OT is about availability.



More connected objects means more risk

All this has made cyber security intrusions and threats more difficult to detect and prevent. At the same time, tools like the IoT search engine Shodan have made it easier for hackers to pinpoint vulnerable devices in a network, whether they are refrigerators, heating systems, or IoT-enabled garage-doors. The fact is that when connected to a network, any device with weak security poses a risk to the whole organization.

Only as strong as the weakest link

Malware gives hackers an even quicker route into a network if their targets can be tricked into opening infected documents. Secret papers leaked in 2017 revealed that CIA agents regularly use malware to turn connected televisions into bugging devices. Malware currently threatening businesses and consumers includes VPN filter malware, banking Trojans and ransomware. It is also evolving. Spear phishing, for example, targets specific individuals or companies, in contrast to the random, untargeted approach of traditional phishing.

The aim of any cyber security strategy is to protect as many assets as possible; certainly the most important assets. Since it is not feasible, sensible or even efficient to try to protect everything in equal measure, it is important to identify what is valuable and needs greatest protection. The next step is to identify vulnerabilities in order to prioritize and to erect a defence-in-depth architecture that ensures business continuity.

Resilience is not achieved simply by installing secure technology. It is mostly about understanding and mitigating risks in order to apply the right protection at the appropriate points in the system. It is vital that this process is very closely aligned with organizational goals because mitigation decisions may have a serious impact on operations. Ideally, it should be based on a systems-approach that involves stakeholders from throughout the organization.

Defence-in-depth

A key concept of defence-in-depth is that security requires a set of coordinated measures. There are four steps that are essential in dealing with the risks and consequences of a cyber attack:

1. Understanding the system, what is valuable and what needs most protection
2. Understanding the known threats through threat modelling and risk assessment
3. Addressing the risks and implementing protection with the help of international standards, which are based on global best practices
4. Applying the appropriate level of conformity assessment — testing and certification — against the requirements.

ABC of cyber security

This is the ABC of cyber security:

A. for assessment
B. for best practices to address the risk
C. for conformity assessment for monitoring and maintenance

A risk-based systems-approach increases the confidence of all stakeholders by demonstrating not only the use of security measures based on best practices, but also that an organization has implemented the measures efficiently and effectively. This means combining the right standards with the right level of conformity assessment, rather than treating them as distinct areas.

The aim of the conformity assessment is to assess the components of the system, the competencies of the people designing, operating and maintaining it, and the processes and procedures used to run it. This may mean using different kinds of conformity assessment – ranging from corporate self-assessment to relying on suppliers' declarations or independent, third-party assessment and testing – whichever seems most appropriate according to the different levels of risk.

In a world where cyber threats are becoming increasingly common, being able to apply a specific set of international standards combined with a dedicated and worldwide certification programme is a proven and highly effective approach to ensuring long-term cyber resilience.

Horizontal and vertical standards

The most robust defences rely on both "horizontal" and "vertical" standards. Horizontal standards are generic and flexible, applicable over a broad area and covering fundamental principles, concepts, definitions, terminology and similar general information. In contrast, vertical standards address application-specific areas.

Two examples of horizontal standards stand out. The ISO/IEC 27000 family helps to protect purely information systems (IT) and ensures the free flow of data in the virtual world. It provides a powerful, horizontal framework for benchmarking against best practices in the implementation, maintenance and continual improvement of controls. IEC 62443, the other horizontal standards series, is designed to keep OT systems running in the real world. It can be applied to any industrial environment, including critical infrastructure facilities, such as power utilities or nuclear plants, as well as in the health and transport sectors.

Complementing the horizontal standards are custom solutions designed to meet the needs of specific sectors. There are vertical standards covering the specific security needs of the nuclear sector, industrial communications networks, industrial automation and the maritime industry, for example.

Testing and certification

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.

Cyber security is a key strategic focus of both the IEC Standardization Management Board (SMB) and the IEC Conformity Assessment Board (CAB). They take a systems-approach to their coordination activities by involving all IEC stakeholders. The SMB has set up an Advisory Committee on Security (ACSEC) with a scope that includes:

- Dealing with information security and data privacy matters which are not specific to a single IEC Technical Committee
- Coordinating activities related to information security and data privacy
- Providing guidance to technical committees/subcommittees (TCs/SCs) for the implementation of information security and data privacy in a general perspective and for specific sectors

The IEC CAB is working with the United Nations Economic Commission for Europe (UNECE) to create United Nations Common Regulatory Objectives Guidelines for Cybersecurity that describe a generic process integrating the four essential steps given above. It also focuses on the often-overlooked aspect of appropriate conformity assessment.

A holistic approach to cyber security

The best way to prepare for all these challenges is by implementing a holistic strategy that combines best practices with testing and certification. Holistic means addressing everything from systems and processes to people.

Spear phishing is increasingly used to target individuals and companies

Robot cars

The latest advances in self-driving technology at CES

By Catherine Bischofberger

Artificial intelligence (AI) is transforming cars into friendly robots. The Las Vegas Consumer Electronics Show (CES), which took place in January, offered tantalizing glimpses into the future for automotive vehicles.

Highly complex algorithms are required for self-driving technology to work

Some say it is overhyped but self-driving technology has become one of the main draws of CES in just a few years. Organizers of the event claim it is the largest auto show out there and this year around 170 different exhibitors came together to demonstrate their self-driving know-how, which ranged from connected cars right down to futuristic concept vehicles. Even if fully autonomous cars are far from hitting the roads, self-driving technology has progressed in leaps and bounds over the last year, partly thanks to more complex analytics algorithms.

Getting better all the time

Most cars on the roads today have some form of driving assistance, helping drivers to park, for instance. At CES, advanced driving assistance made the headlines, including passenger and road edge detection and automatic emergency braking. Pre-collision systems, including passenger detection, are meant to help drivers and notify them that an obstacle is in the way. These systems combine software with sensors, cameras and, in some cases, radars to detect objects near or in front of the car.

Even more sophisticated algorithms are required to move to fully autonomous vehicles. Researchers from MIT's Computer Science and Artificial Intelligence Laboratory have been working on a new change lane algorithm which allows automated cars to behave like humans and make split-second decisions on whether to stay in a lane or not. The researchers tested their algorithm in a simulation with up to 16 autonomous cars driving in an environment with several hundred other vehicles, without collision. The rise in edge computing has made cars more capable of processing and finding patterns in the data provided by sensors. The data is stored in the car itself instead of a central cloud, making it faster and easier to process. It is also more difficult to hack. (For more information about edge computing, read the IEC White Paper Edge Intelligence.)

Brains and brawn

There is still some way to go, however, before autonomous cars can compete with the human brain. According to Tigran

Shaverdyan, one of the inventors of a self-driving van that launched at CES 2019, “it is still very difficult to create an algorithm that would enable an autonomous car to choose the right option in an unlikely scenario. It is the ‘chicken crossing the road” quandary.’ Their van, a sort of grocery shop robot, is piloted remotely for now, essentially for safety reasons. “We will be testing increased autonomy next year. But the technology will still involve some form of monitoring from afar. A number of safety issues have to be addressed before we can launch a fully autonomous vehicle but we are confident we can solve these problems in the longer run.”

IEC is preparing the ground for the increasing use of AI technology in our daily life. The joint technical committee of IEC and ISO on information technology (ISO/IEC JTC 1) and several of its subcommittees (SCs) prepare international standards that contribute towards artificial intelligence. For instance, SC 42 was set up to provide standardization in the area of AI as well as guidance to other committees developing AI applications. IEC is also a founding member of the Open Community for Ethics in Autonomous and Intelligent Systems (OCEANIS).This global forum brings together organizations interested in the development and use of standards as a means to address ethical matters in autonomous and intelligent systems.

A series of standards published by IEC TC 47, IEC 62969, specifies the general requirements of power interfaces for automotive vehicle sensors. IEC TC 100 issues several standards relating to multimedia systems in cars. One of its most recent publications is IEC technical specification (TS) 63033. It specifies the model for generating the surrounding visual image of the drive monitoring system, which creates a composite 360° image from external cameras. This enables the correct positioning of a vehicle in relation to its surroundings, using input from a rear-view monitor for parking assistance as well as blind corner and bird’s eye monitors.

Connecting the dots

Connected cars were one of the big trends at CES 2019. Improved features and technology were touted on the back of the arrival of 5G networks. The connection speed of this latest generation mobile communication system is much higher and delivers signals more reliably than previous networks. This is very useful for high quality virtual reality (VR) applications, for instance. One of the novelties at the show was content producers teaming up with car manufacturers, chip makers and smartphone companies to offer passengers in-car VR immersive experiences. ISO/IEC JTC 1/SC 24 is preparing standards in the area of augmented and virtual reality.

5G will also help with the implementation of vehicle to everything (V2X) communication between self-driving vehicles and other cars, appliances or obstacles, such as traffic lights and pedestrians, etc. IEC 62232, issued by IEC TC 106, provides methods for determining radio-frequency field strength near the radio base station. This standard takes into account frequencies to be used for 5G for the purpose of evaluating human exposure. IEC TC 106 has established a new joint working group with the Institute of Electrical and Electronics Engineers (IEEE) to develop international standards’ for 5G device testing by 2020.

In the mood for a drive

Several concept cars at CES demonstrated voice and image recognition systems, used to guess drivers’ moods. A well-known voice recognition tool has been integrated into many cars, where it performs a wide variety of tasks which include acting as a safety assistant and warning of potential dangers on the road. A Korean manufacturer’s concept car featured facial recognition technology that uses artificial intelligence to assess the emotional state of the person holding the steering wheel. The software can change the vehicle’s interior lighting, for instance or warn drivers when it detects that they are tired.

Before becoming fully autonomous, cars are developing into friendly robots, happy to help and serve, while drivers still retain a modicum of control. This could be the best of both worlds – reducing the risk of human error while preserving the enjoyment of driving.

Robomart is controlled remotely for safety reasons. (Photo: Robomart)

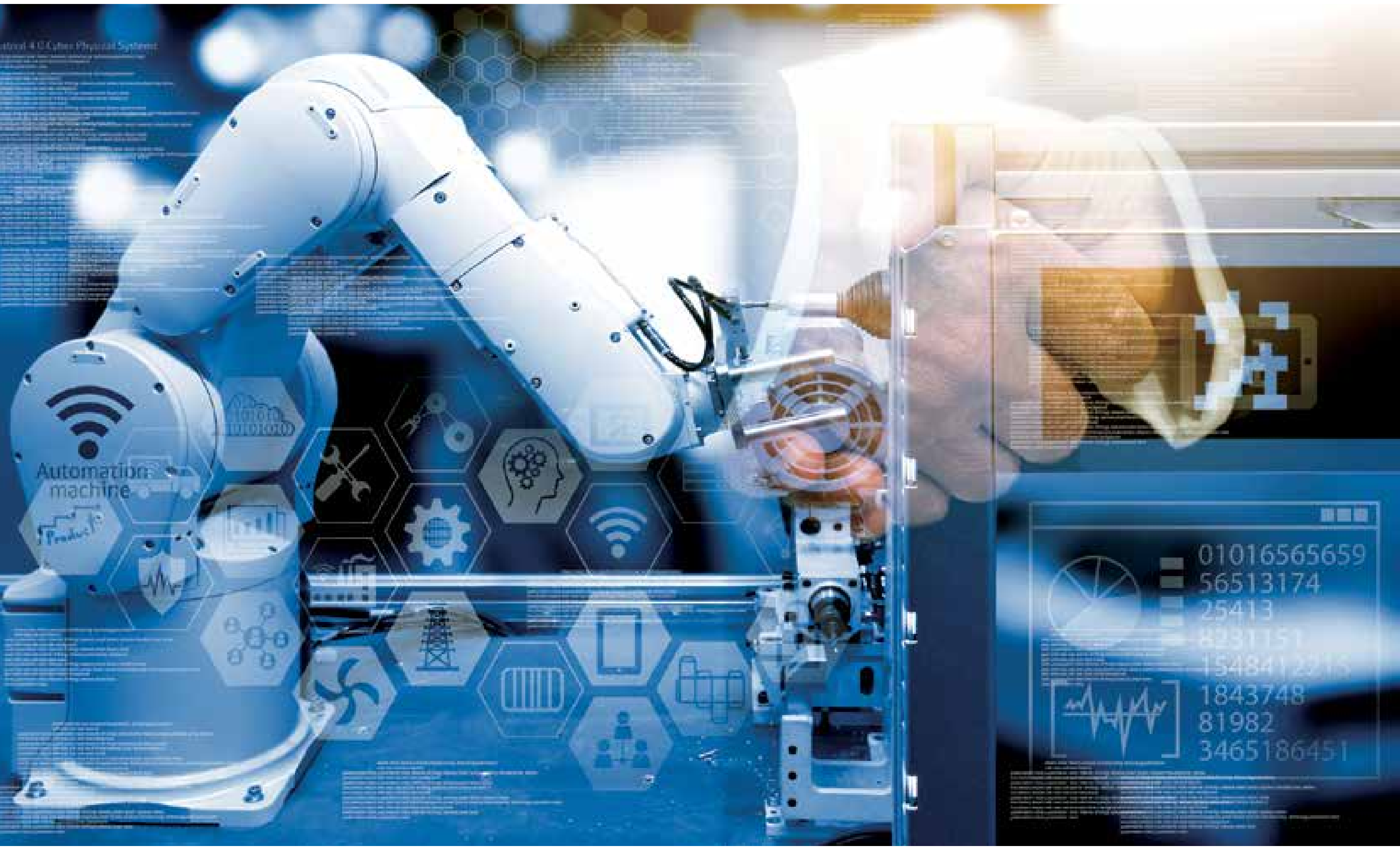
Who needs AI

AI is transforming industries and society, but we're still working out how to use AI-enabled devices in our everyday lives

By Michael A. Mullane

There have been a lot of media reports recently about the failings of AI devices, from disappointing gadgets on show at the CES to malfunctioning hotel bots. Some of the stories are very funny, but all they tell us is that the technology is still in development and that some products are better designed than others.

The Wall Street Journal writes about a guest in a robot-staffed hotel in Japan who was woken every few hours by the in-room assistant asking him to repeat his command. The hotel manager finally realized that heavy snoring by the guest had triggered the robot's voice recognition system. For every clanger, though, there is also a success story. For example, a chess-playing programme called AlphaZero, developed by the Alphabet-owned (Google's parent) AI research company DeepMind, has been making significant advances.



Automation controls everything from manufacturing processes to home systems and appliances (Photo: www.businesscomputingworld.co.uk)

AlphaZero has developed a new style of playing chess which is much closer to human improvisation than traditional computer chess. That is because AlphaZero learns from its past successes and mistakes, rather than calculating millions of possible permutations as it plays. According to Wikipedia, AlphaZero searches 80,000 positions per second in chess, compared to 70 million for the Stockfish chess engine. AlphaZero uses (deep) neural network technology – sometimes called deep learning – which has resulted over the past decade from notable improvements in machine learning. As computing power has increased, deep neural networks have produced machines capable of performing tasks in a way that would not have been possible using traditional programming techniques.

This has transformed technologies such as computer vision and natural language processing (NLP), which are nowadays being deployed on a massive scale in many different products and services. Manufacturing, healthcare and finance are just some of the sectors that use deep learning to uncover new patterns, make predictions and guide decision making.

"In the area of smart manufacturing, AI can help to streamline efficiency," says Wael Diab, who is leading international standardization work in this field. "It can help to provide insights in terms of where improvements can happen and more importantly it can provide insights into where a particular organization may want to go in terms of its production planning."

> We're looking at the different components that go into AI, from the computational side to the ethical side.

Sales of industrial robots have doubled in the past five years, according to the International Federation of Robotics. The IFR predicts that in 2021 the annual number of robots supplied to factories around the world will reach about 630,000 units. Industrial robots are satisfying a real need. In contrast, much of the focus on consumer electronics is still on the novelty value of gadgets. To a large extent this is because we have not quite worked out how we intend to use AI-enabled devices in our everyday lives or what we expect of them.

The Korea Joongang Daily reported in October that Koreans not only use their smart speakers for changing the TV channel, but also to discuss their feelings. In people's homes, a staggering 15% of the things said to smart assistants appeared to be attempts at conversation, including "I'm bored" and "I'm sad". The newspaper noted a similar pattern in hotel rooms, where more than 18% of the commands were attempts at conversation. The Joongang Daily acquired the data from KT Corporation, the country's largest telephone company.

In 2017, IEC and ISO became the first international standards development organizations (SDOs) to set up an expert group to carry out standardization activities for artificial intelligence. Subcommittee (SC) 42 is part of the joint technical committee ISO/IEC JTC 1. SC 42 is working with other JTC 1 subcommittees, such as those addressing the Internet of Things, IT security, and IT governance, as well as the IEC Systems Committee (SyC) for Smart Cities. SC 42 has set up a working group on foundational standards to provide a framework and a common vocabulary. Several study groups have been set up to examine the computational approaches to and characteristics of AI systems, trustworthiness, use cases and applications and big data.

IEC Standards are playing a key role in the transition to the Fourth Industrial Revolution. IEC TC 65, for instance, carries out important work related to industrial-process measurement, control and automation.

"We're looking at the different components that go into AI, from the computational side to the ethical side. Having standards allows for a common language and way for the different stakeholders to interact," explains Diab.

"What that leads to is the ability to innovate on top of widely adopted standards in the market place."

People use smart speakers to facilitate their lives but also to discuss their feelings

Being prepared for quantum computing

Quantum computers threaten to break encryption, but moving to quantum cryptography now could safeguard data

By Michael A. Mullane

One of the MIT's best-known physicists, Seth Lloyd, uses a musical analogy to explain quantum computers. Classical computation, he says, is like a solo voice that produces a series of pure tones which form a single melody. Quantum computing is more like an orchestra, where many different instruments form individual melodies that compete and complement each other to form a symphony. Quantum computers are certainly music to the ears of scientists who predict that they will eventually be able to solve incredibly complex computational problems much faster than any technology we have today.

"The reality of quantum computing is probably 10 to 15 years away, yet it merits our attention now," says Dr Seungyun Lee of the joint committee on information technology (JTC1) set up by IEC and ISO.

"The excitement in the industry for this new paradigm of computer hardware is understandable, given the promise of far greater computational power with whole new multidimensional capabilities."

The technology looks set to bring massive benefits, such as accelerating medical research, making advances in artificial intelligence and perhaps even finding answers to climate change. But it also poses a huge risk for some of our most sensitive data. Quantum computers will be powerful enough to crack the encryption codes that currently protect all our sensitive data, from mobile banking to medical records. That is because the science of cryptography is at the heart of cyber security.

Mobile phone calls, messaging and online banking all rely on complex mathematical algorithms to scramble information in order to protect it from malicious hackers, spies and cyber criminals. It is no exaggeration to say that there would be no confidentiality or security online without encryption and that many of the operations we take for granted today would no longer be feasible. Faced with increasing cyber attacks against critical infrastructure – including but not limited to power utilities, transport networks, factories and the health care industry – encryption is evolving to meet the threat.

> "The reality of quantum computing is probably 10 to 15 years away, yet it merits our attention now."

The most prevalent system nowadays is public key encryption. It works by giving users two keys: a public key, shared with everyone, as well as a private key. The keys are large numbers that form part of an intricate mathematical algorithm that scrambles a user's messages. The sender encrypts a message by using the receiver's public key in order that only the intended recipient can unlock it with her or his private key. Even though the public key is freely available, the numbers involved are sufficiently large to make it very difficult to reverse the encryption process with only the public key.

As computers become more powerful, however, and in the face of rogue states with the technology resources to pose a more serious threat, cryptographers are turning away from mathematics and looking to physics – specifically the laws of quantum mechanics – to achieve greater security. Wikipedia defines quantum cryptography as "the science of exploiting quantum mechanical properties to perform cryptographic tasks."

That is because quantum cryptography is based on the behaviour of quantum particles, which are smaller units than molecules. For example, an encryption system called quantum key distribution (QKD) encodes messages using the properties of light particles.

The only way for hackers to unlock the key is to measure the particles, but the very

Quantum computers may not be available for another decade, but quantum cryptography has already been available for a few years

act of measuring changes the behaviour of the particles, causing errors that trigger security alerts. In this way, the system makes it impossible for hackers to hide the fact that they have seen the data.

The threat is so great that scientists are urging organizations to start looking at and adopting quantum encryption systems. Quantum computers may not be available for another decade, but quantum cryptography has already been available for a few years.

Quantum cryptography is an area of interest for two key expert groups at the IEC:

- IEC Technical Committee (TC) 65 on industrial-process measurement, control and automation, which is responsible for the IEC 62443 series of standards on industrial communication networks system security.
- ISO/IEC JTC 1/Subcommittee 27 is best known for the ISO/IEC 27000 series of IT cyber security standards.

The joint technical committee set up by IEC and ISO is currently preparing a report on quantum computing. The study will provide context and analyze trends, including the latest developments in technology and activities in the open source community. It is expected that the report will recommend creating an International Standard on quantum computing as soon as possible. Such a standard would cover concepts and terminology in order to facilitate better communication and understanding in industry, academia, governments and standards committees.

Automatizing the power grid

The electric grid is modernizing, helped along by IEC standards

By Catherine Bischofberger

Human machine interfaces (HMIs) play a key role in grid automation. A new IEC standard is in the works to make these systems vendor-agnostic.

Human machine interfaces are widespread across transmission and distribution networks (Photo: CSIRO Wikimedia Commons)

In this day and age, relations between humans and machines have become rather fraught. A growing number of anxieties crystallize around the use of robots and automation in various industries, not to mention our homes. Things were quite different in the late 19th Century, when the introduction of the first machines were expected to relieve people from toiling away for long hours in exhausting circumstances. Families, in particular, reaped the benefits from time-saving appliances. Washing machines, dishwashers and microwaves gradually became mass market consumer goods throughout the 20th Century.

Nowadays, we worry about robots taking our jobs and becoming smarter than us. But whether we like it or not, the future spells an increasing interaction with machines in one form or another. As this trend intensifies, human machine interfaces (HMIs) will become an ever more important technology for us to master as they will enable us to control and interact with machines. While these three letters, HMI, might seem like just another acronym, they are one of the keys to our future world. And one of the areas where HMIs are already ubiquitous is in electricity generation and transmission. They are a key feature of grid modernization.

HMIs and the electricity grid

You can find HMIs in power plants and substations as well as in wind and solar farms. According to the IEC glossary, it is a "display screen, either as part of an intelligent electronic device (IED) or as a stand-alone device, presenting relevant data in a logical format, with which the user interacts. An HMI typically presents windows, icons, menus and pointers, and may also include a keypad to enable user access and interaction."

Power grids are getting smarter which allows them to operate in a more energy efficient and effective manner; HMIs are typically "the face" of this process. The HMI application plays a key role in the visualization and control of substation automation systems or the monitoring of the real time status of a solar or wind farm, for example. Engineers, technicians and operators depend on the information collected and relayed by IEDs to get a clear picture of the state of the substation and the distributed energy resources (DER).

These DERs could be wind turbines, a solar farm or a microgrid, for example. As the power grid continues to modernize, the dependency on HMI applications will therefore increase and operators will require help to monitor and control multi-vendor systems.

HMI applications are built upon graphical building blocks including basic shapes, colours, text, forms or pages to communicate and exchange information. Utilities increasingly want HMIs to work with any vendor IED, requiring minimal manual configurations. A vendor-agnostic solution would simplify installation, reduce maintenance costs and diminish the complexity of power automation systems. It would facilitate the interoperability with multi-vendor IEDs and support data-driven configurations that place the work burden on tools instead of human beings.

Unfortunately, all the graphical components and building blocks that go into an HMI are assembled in a proprietary fashion by HMI software manufacturers. To date, there aren't any standardized means of specifying, designing and commissioning HMI applications.

New international standard in the works

But this is about to change. The IEC is working on a new document which aims to define the configuration languages required to achieve digital substations, including the HMI application. The planned standard, which is currently being drafted, will be part of the IEC 61850 series of publications, which includes some of the core international standards used for integrating digital communication processes into the existing electrical grid.

One of the objectives of the new publication is to automatically generate the HMI application, including all the associated data mappings and graphical renderings. This effectively dispenses operators, engineers or technicians from carrying out a manual configuration of the substation system and therefore saves time and cost for utilities by using resources more efficiently.

It also removes the risk of human error. "You could call it 'magical engineering': instead of taking weeks, sometimes even months, to configure the HMI applications, it literally will take minutes and even seconds for smaller substations," says Dustin Tessier, who leads the task force responsible for the new standard project at the IEC.

California dreamin'

The HMI document is based on a proof of concept technology developed by Southern California Edison (SCE), the primary electricity supply company for most of Southern California. For many in the electricity transmission industry, SCE is viewed as a compass: other utilities follow the company's technology roadmaps and its data-driven HMI application is just another example of its technological savviness. The HMI is part of a 3rd generation substation automation architecture developed by the company and based on IEC 61850 standards.

Mehrdad Vahabi is one of the engineers who worked on the HMI prototype. "Southern California Edison has always been a forward-thinking utility. In 2010-11, the company decided to modernize the grid. While HMIs were already used, they were proprietary which created a number of problems, including cost, the amount of manual work and the time required to make changes to the systems and so on. These legacy problems with HMI were one of the major reasons for moving to 3rd generation substation automation," Vahabi explains.

The power grid is modernizing

During their research, SCE engineers came into contact with the IEC 61850 standards and their applications for substation automation. "They are a very useful tool set but the HMI part was not yet standardized. We got involved with the IEC experts working on these aspects. We proceeded to implement our prototype in the field and give them information which was fed into the drafting of the new IEC document," Vahabi adds. SCE has already started implementing the new HMI in its substations. "The plan is to automate 400 substations with this SA-3 technology by 2028," Vahabi indicates. Further down the line, the company plans to prototype a totally virtualized substation automation system in the lab.

It may be a brave new and increasingly complex world out there but it would seem that, with HMIs, we have some of the tools to overcome many of these complexities. And the power grid is a great place to start.

Cyber security – a priority for broadcasters and media companies

Comprehensive protection of assets and content relies on a number of international standards and on standards and recommendations developed by all industry players

By Morand Fachot

Protecting physical and digital assets, for production, storage and distribution, ensuring continuity of service, safeguarding valuable content from being stolen or misused, are some of the challenges facing broadcasters and media content producers and distributors.

Broadcasting, a central part of critical infrastructure

The communications sector, which includes broadcasting, is part of critical infrastructure. Broadcasting, for instance, provides essential services at times of national emergency or natural disasters. Over the decades, broadcasting installations have often been the first targets in international conflicts or in attempts to change a regime. The threats have evolved from physical – bombing or taking over stations – to disabling or paralysing broadcasting installations which rely increasingly on digital tools and processes.

The US administration "identifies the Communications Sector as critical because it provides an 'enabling function' across all critical infrastructure sectors." Broadcasting is listed as one of the sector's five components (together with wired, wireless, cable and satellite networks). This concept is also being adopted in a growing number of countries. Broadcasters are content creators and providers as well as distributors.

Merging IT and OT

The broadcasting industry (and media content providers) rely increasingly on IT, the Internet, internal and web-connected networks for content production, storage and delivery.

As a result, protecting content production, storage and delivery of broadcast and multimedia services from cyber threats relies on both IT and operational technology (OT). This requires a multi-layered, multi-sector approach, for which IEC and ISO/IEC joint standards, as well as industry-specific standards and recommendations from other organizations, provide solutions.

Sector-specific issues

Cyber attacks on broadcasting and multimedia companies may take many forms, have multiple objectives and be instigated by multiple actors, such as criminal gangs or individuals, state or state-sponsored wrongdoers, some maintaining informal links with each other. This makes such attacks extremely difficult to prevent, identify or mitigate in real time, which is essential in the broadcasting sector where latency can be a major issue. The motives may include taking down a network, extortion or disruption of services.

Examples of attacks on broadcasters include:

- An April 2015 sustained cyber attack on French international TV broadcaster TV5Monde. The network, which is available in 200 countries, came under attack from a group claiming to be the "Cyber Caliphate". The attack took the broadcaster's 12 channels off the air and according to its director-general Yves Bigot, nearly led to the total destruction of its systems.
- A July 2015 cyber attack on the UK-based Islam channel, lasted for around five months before cyber specialists from British intelligence cleared hackers from its systems.

One size doesn't fit all

Media companies, broadcasters and content producers, rely increasingly on IT and connected networks, and have Internet offers for production and other services (websites, blogs, audio and video streaming, etc.) The multiplicity of services (and threats) means that many tools are needed to address them. They include international standards developed by IEC and the joint work it carries out with ISO and International Telecommunication Union (ITU). For the broadcasting sector industry-specific standards and recommendations are also essential to protect networks and content. These are developed by the World Broadcasting Union (WBU) and its member bodies. Additionally, the Association for International Broadcasting (AIB), set up a Cyber Security Working Group to share information and expertise about existing cyber threats to media companies.

Multiple threats

As media services, including those of content providers, have become more connected, spanning different technologies, they face multiple kinds of attacks, including Distributed Denial of Service (DDoS) and the use of ransomware and malware. Other incidents are state-sponsored, such as the November 2014 release of confidential data from Sony Pictures aimed at hurting the entertainment company or the large (and still ongoing) piracy operation launched against the Qatari pay-TV service beIN in October 2017, aimed at damaging the country's economic interests.

Vulnerabilities

The multiplicity of systems potentially at risk from cyber attacks and of vectors used to carry these out, mean that broadcasters and media content providers must protect against a wide range of threats and mitigate their impact, should they succeed in penetrating and compromising systems. Vulnerabilities include:

- Equipment: many media companies rely on connected media devices that have a low security threshold. Off-the-shelf components and devices used may not meet the latest adequate cyber security measures or include available software updates or security patches protecting them, to a certain extent, against cyber threats.

Broadcasters can face multiple types of attacks

- Processes and procedures: implemented by media companies to protect against cyber threats to operations and systems, such as Industrial Automation and Control Systems (IACS).
- Personnel: the human factor, should be a priority for all media companies, yet often proves to be the weakest link in the cyber security chain. The most effective attacks use social media engineering to manipulate people and lure them into divulging confidential information, using, for instance, phishing. Personnel may include suppliers, vendors, maintenance staff and operators.

Protecting against vulnerabilities

Broadcast industry companies started using cloud services for their workflow, editing and storage, and to ensure resilience and continuity of services in case of cyber attacks.

A number of standards and recommendations address vulnerabilities and provide solutions for protection. Some span across different kinds of vulnerabilities. As regards IT aspects the ISO/IEC 27000 family of Standards for IT service management, developed by ISO/IEC JTC 1/SC 27: IT security techniques, is the absolute reference. The IEC 62443 series of standards, developed by IEC TC 65: Industrial-process measurement, control and automation, addresses OT vulnerabilities linked to IACS. Both are referenced as essential for the broadcasting sector in publications such as the US National Association of Broadcasters (NAB) guide to broadcast cyber security.

Other relevant IEC standards include the IEC 62351 series for telecontrol equipment and systems, which addresses the issue of role based access control (RBAC), in other words, restricting access to authorized users. When properly implemented, these standards may prevent unauthorized personnel accessing systems.

Protecting content (a valuable asset), from production to delivery, requires among other things, the implementation of digital rights management (DRM)

Protecting content production, storage and delivery of broadcast and multimedia services from cyber threats relies on both IT and operational technology (OT)

measures. IEC TC 100 has developed standards to protect content. These cover interoperability solutions that allow the distribution of content according to digital living network alliance (DLNA) guidelines for home networked devices, as well as IEC 62698, which provides a standardized framework to ensure that multimedia content, under copyright, can be shared legally across different systems, including Internet protocol TV (IPTV).

Blockchain can be used to protect content

Blockchain technology can be used to validate and protect multimedia content from piracy and tampering.

EBU Senior Project Manager Adi Kouadio told *e-tech*: "Blockchain technology makes it possible to improve the traceability of content by recording a signature for each content resulting from a process (editing, compression, etc...). Better traceability means faster detection of content that is either tampered with or labelled with the wrong source. Each operation on the content can be considered a transaction and registered on the blockchain (which cannot be altered)."

Much more at stake and even more to come in the future

Other technologies such as artificial intelligence (AI) and machine learning (ML) can both be used to disseminate and thwart cyber attacks. IEC and ISO recently established the first international standards committee, ISO/IEC JTC 1/ SC 42, that is looking at the entire AI ecosystem, addressing among others, issues concerning trustworthiness, privacy and security, bias in algorithms, as well as societal concerns and ethics.

Rethinking the healthcare ecosystem

New technologies are increasing healthcare access, improving lives and saving costs

By Antoinette Price

Today, for many, technology is an inextricable part of life and healthcare. Friendly robots administer daily medications; algorithms diagnose diseases more accurately than top specialists, and a doctor's appointment can happen over skype.

Doctors can livestream and virtually train students anywhere

The algorithm doctor

As the medical and technology worlds converge, the entire healthcare ecosystem is evolving and being given new perspectives and solutions for how best to deliver healthcare, by advances in artificial intelligence (AI) technologies, such as algorithms and machine learning, together with connected smart medical devices and apps.

This couldn't be more evident than at the Consumer Electronics Show (CES), Vegas. During the *Disruptive Innovations in Healthcare* conference, topics included digital therapeutics, latest remote patient monitoring, expanding telehealth services, new insurance reimbursement models for virtual care and the power of AI, as predictive analytics increase evidence-based discoveries and provide new treatment options. The conference offered insights from a variety of participants, including top physicians, health insurers, medical device companies, legal advisors, health service providers and technology experts.

> It's vital that new smart technologies in healthcare are safe and secure for everyone from the get go.

Such is the impact of technology on health, that in 2018, CES nominated Rene Quashie as its first vice president of policy and regulatory affairs for digital health. Quashie led a panel which looked at technical and regulatory issues relating to consumer digital health and wellness technology products, services, software and apps, and which need to keep pace with developments.

New tech, new concerns

When it comes to health, people need to trust their doctors and take for granted that their personal records remain private. They also need to know that any devices they may have to use are safe and secure. A number of concerns around AI technologies and smart medical devices need to be addressed rapidly.

Advances in AI mean the entire healthcare ecosystem is evolving

Can we trust AI with our health?

Accenture research expects the AI health market to reach USD 6,6 billion by 2021, growing 40 percent annually, and potentially generating USD 150 billion in health care savings by 2026.

Whether crunching through masses of big data and improving patient diagnostics, detecting health insurance fraud, providing care to people in their homes or managing patient data, AI could impact most aspects of healthcare in the not too distant future.

But can algorithms based on data-sets inputted by imperfect humans really be bias free? What if the algorithm ends up harming a patient? Will patients want to be managed by algorithms and health bots instead of their human doctors and caregivers?

What about data privacy and security?

According to IBM Watson Health the average person will generate one million gigabytes of health-related data in their lifetime.

This is not so hard to imagine as many already track health and fitness using medical wearables, or treat conditions using smart devices, for example for diabetes. There are a number of important issues around these devices, such as how safe and secure is this data? What if algorithms end up replacing nurses and running all the devices in a critical care unit? What if they miss something only a nurse in the room could have seen, because a particular symptom or situation was not foreseen in the data set that trained it?

The role of standards

International standards developed by IEC for safety and performance of electrical equipment used in medical practice cover a broad spectrum of devices, systems and domains. They are developed by medical and IT experts, industry and regulatory bodies.

"It's vital that new smart technologies in healthcare are safe and secure for everyone from the get go. We're already working on standards for new architectures and applications in the field of digital health, artificial intelligence and data analytics, together with ISO," says Michael Appel, certified anaesthesiologist and Chief Patient Safety Officer for Northeast Georgia Health System, who leads IEC work in this area.

IEC and ISO work together to develop international standards for information technologies through their Joint Technical Committee (ISO/IEC JTC 1). Subcommittee 42 was established to look at the entire AI ecosystem. IT and domains experts from different sectors are taking a broad approach in order to cover the different AI technologies and consider synergies with analytics, big data, cyber security, IoT and more.

Needs must

The healthcare sector is using innovative technologies to address a number of key issues, for instance, climbing costs as populations grow and age, and many more people require health-related services.

Around the world, surgeries, hospitals and care homes are becoming overstretched and understaffed. Connected medical devices enable patients to monitor, and in some cases be treated for, different conditions, wherever they are. The result is reduced doctor visits and costs, improved quality of life through tailored medicine, while doctors have more time for more patients.

Growing use of VR

This year at CES, the benefits of telemedicine were showcased. Broadening the point of care, doctors are able to treat patients with limited mobility, living far away, or who don't have access to healthcare, remotely.

There is nothing worse than needing to see a doctor and not being able to get an appointment. Some US service providers offer doctors on demand without long waits or appointments. Patients get help when required, can have prescriptions delivered rapidly to the door, and by avoiding emergency care or doctor visit charges, it is more affordable.

Virtual and augmented reality programmes are also being used to train healthcare professionals to respond effectively in emergency situations, such as the outbreak of the Ebola or a disaster situation in a city.

Surgeons can livestream and virtually "train" students watching from anywhere, or consult with other surgeons around the world, in real-time, during complicated surgical procedures.

Virtual reality technologies fall within the remit of JTC 1. Subcommittee 24, produces standards which cover the interfaces for information technology-based applications relating to computer graphics and VR, image processing, environmental data representation, support for mixed and augmented reality (MAR), and interaction with, and visual presentation of information.

Looking ahead

Innovations in all areas of health tech will continue to be developed, but in order for them to be adopted on a large scale, many safety, security, societal and ethical concerns will need to be resolved as traditional healthcare models and doctor - patient relationships move with the times.

Keeping track of things with RFID

Agriculture, healthcare and retail are some of the industries that already benefit from radio frequency identification (RFID) tags.

By Antoinette Price

RFID plays a key role in streamlining supply chain management applications, as the digitization of industries advances.

This simple, effective and low-cost technology is being deployed by automotive manufacturers, dairy farmers, warehouse inventory managers and retailers, to name a few. It is also being used to fight counterfeit products, such as aerospace and motor vehicle parts, apparel, electronics, handbags, pharmaceuticals and watches.

Technology based on internationally agreed standards

IEC and ISO work together to produce international standards for barcode and RFID technologies. They cover data formats, syntax, structures, encoding, and technologies for the process of automatic identification and data capture (AIDC). The scope also includes associated devices for inter-industry applications and international business interchanges.

Barcodes are ubiquitous with some six billion scanned daily at retail checkouts alone. While both barcodes and RFID read and collect data, and track assets and inventory, there are differences – the main one being that optical scanners only work with an unobstructed view of the barcode, known as a clear line of sight. For example, products are scanned one at a time at the checkout. However, when RFID tags come within a certain distance of their reader, they are activated by radio signals, which means that potentially hundreds of tags could be read per second.

The use of RFID-based inventory management systems is growing, because they offer features which allow businesses to track items in real time, improve stock management and cut down checkout times.

Interview with Henri Barthel

e-tech caught up with Henri Barthel, who leads the development of IEC and ISO international standards for AIDC techniques, to learn more about the benefits of RFID and latest developments.

Henri Barthel oversees standards development for AIDC technologies

What type of applications use RFID?

Increasingly, RFID applications are used for inventory management, for warehouses, factories and retail outlets.

For example, in the car manufacturing industry, tagging component parts makes it easier to check that everything has been assembled correctly, as well as enabling the quick location of parts when required.

In the case of apparel, research shows the number of tags used in 2018 was in the range of eight billion worldwide, which represents only 10% of potential market capacity for that specific sector.

RFID tags can be embedded into the clothing or on a label and are disposable. They identify items uniquely in inventory management systems and cost between four and six cents, which is very affordable for large-scale deployment.

"This is a great example of the broad use of technology based on internationally agreed standards. RFID is well suited to the clothing industry where there are many variants of each product, such as size, shape or colour. In addition to the checkout process, it can be used for

RFID tags enable inventory management systems to locate and track items in real time

inventory management, to know in real time, what is in stock and what needs reordering. Stores can also control loss or theft of items as well as purchases, because when the RFID tag is scanned at the exit point, the stock system is made aware that the item has left the store. So if an item makes it through without being scanned, an anti-theft detection gate linked to the inventory system can trigger an alert."

In the healthcare sector it is vital to be able to quickly identify, locate, authenticate and engage with different items particularly in hospitals. RFID applications enable staff and doctors to locate the exact equipment required for surgery and other treatments and ensure it has been properly sterilized. They can also secure the medicine supply chain, track tissue and specimen samples, improve patient flow, and more.

What are some of the main projects for 2019?

While the barcode is a relatively old technology it is very much alive and continues to evolve.

Rectangular DataMatrix and QR code

Currently, work is being done to develop a DataMatrix rectangular barcode (ISO/IEC DIS 21471) and a similar project is coming up for a rectangular QR code. The rectangular shape is easier to put on certain items, such as very small medical devices and equipment used in hospital theatre rooms. Current technologies enable to print or to engrave very small barcodes onto the products and to read them successfully.

A standard is being worked on, which will cover the quality of the printing or engraving of tiny codes, also known as the direct part marking of barcodes.

"We need conformance and performance standards to measure the quality of RFID for consumer and other goods. It is good to have a technology standard, but then how do you assess that the given product conforms to the standard? How can you say 'my system is better than yours', in other words how can you objectively measure the conformance and performance of RFID systems?"

User guides for applying RFID standards

The basic technologies of barcodes and RFID are relatively mature and being deployed, with 120 standards developed by IEC and ISO already in use. Now, there is a need for more application standards that explain how to use the technology, and give some sort of framework around what needs to be thought of and what the options are for end users who are going to adopt these AIDC technologies.

"We are working on a standard for electronic labelling (ISO/IEC WD 22603) using a barcode with a number, which would enable access to product data. This could include regulations which affect the product in different regions. In the electronics industry each country or region has different regulations and the requirements for explanations (books) of how to conform to these different regulations. This is a challenge. The idea is to scan the product barcode which takes you to a website and gives you the regulatory information on the specific item. This use of websites could be expanded to product indications for pharmaceuticals, a full list of ingredients in a food product, or a user manual for your washing machine, there are countless examples. This is already being done today in a proprietary manner, so our ambition is to have a standard which gives the framework for how to implement this kind of approach."

> "We need conformance and performance standards to measure the quality of RFID for consumer and other goods."

Looking ahead

Smart fitting rooms, targeted advertising, marathon messaging, hand washing in hospitals, tracking casino chips and your drinks tab are some of the innovative ways RFID technology is being used.

IEC and ISO continue to follow industry progress, in order to deliver the standards required in a timely manner, to ensure RFID technology is interoperable, secure and works efficiently.

ROVs, AUVs and AIVs

Underwater vehicles play major role in Ex environments

By Claire Marchand

Remotely operated vehicles (ROV), often described as "robot submarines", have been used by the oil and gas industry for many years, mainly for underwater drilling, construction and installation, inspection, maintenance and repair jobs in the wells of offshore oil platforms. Equipped with very sophisticated electronic devices, they are the eyes, ears and hands of those who operate them from ships or offshore platforms.

ROVs can reach depths to which no human diver could descend. They look like giant steel boxes, about the size of a small car. Their manipulator arms can pick up tools and some are capable of lifting weights of up to a tonne. They are deployed in a protective cage which carries them to their subsea location, from where they operate, sometimes in harsh conditions and very low visibility, to complete numerous subsea missions, from turning bolts to closing valves.

As an example, during the 2010 oil spill in the Gulf of Mexico, robotic submersibles were sent underwater to contain and ultimately cap the spill on the sea floor, where direct human intervention was impossible.

Going back in time

Attempts to develop a ROV were made as far back as the mid-1860s when Luppis-Whitehead Automobile developed a kind of torpedo, the Programmed Underwater Vehicle (PUV) in Austria. Almost a century later, in 1952, Dimitri Rebikoff, a French engineer, oceanographer and underwater photographer, built the first underwater scooter which evolved into the world's first tethered ROV, named the Poodle.

In the 1960s, technological advances came from the US Navy. Their Cable-Controlled Underwater Vehicle (CURV) was destined to perform deep-sea rescue operations. A CURV was used to recover a nuclear bomb lost in the Mediterranean Sea after the 1966 Palomares crash of a B-52. Another CURV helped save the pilots of a sunken submersible off the Irish Coast in 1973.

Essential to the oil and gas sector…

The oil and gas industry quickly saw a future for ROVs: they could assist in the development and deployment of offshore oil rigs. From the 1980s onwards, ROVs have been used for an ever increasing number of tasks that could never have been undertaken by human divers, from the simple inspection of subsea structures, platforms and pipelines to connecting pipelines and placing manifolds.

…but not only

While the oil and gas industry has most certainly benefitted from the introduction of ROVs in its operations, other sectors have taken advantage of the technological advances that have allowed the development of a wide range of ROVs, from small inspection vehicles to deep ocean research systems. Those are used mainly for scientific applications. In 1995, an ultra-deep ROV, Kaiko, made by JAMSTEC, a Japanese firm, reached the deepest part of the ocean, the Challenger Deep in the Mariana Trench, at 10 909 metres.

Technological advances

Over the years, there has been a growing need for more powerful and more reliable ROVs that could go deeper and accomplish increasingly complex tasks. One major improvement, in the early 1980s, was the use of control data and video over fibre optic in the offshore oil and gas sector. This meant that ROVs, which previously used data over copper, could operate in greater depths.

Depending on their category, ROVs may be equipped with video cameras and variable lighting; acoustic and tracking sensors (tracking and measurement devices, scanning sonars, profiling sonars, bathymetric systems and pipe trackers); non-destructive testing sensors used to check structural integrity; cleaning devices (rotating wire, nylon brushes, water-jetting, etc.) to clean offshore infrastructure; and multiple single-purpose or multi-mode work tools; simple bars, hooks and knives.

The lighter category of vehicles, fitted with camera, lights and sonar, are used mainly for observation, although some can perform basic manipulative tasks as well.

The much larger work-class ROVs are deployed in the drilling and construction support sector; they also perform subsea pipeline inspection and monitoring. Heavy work-class ROVs are the most sophisticated: they can operate in deep water, have manipulators and grabbers that can lift huge loads and can perform tie-ins and subsea installations.

Today's most technologically advanced ROVs, equipped with machine vision and motion sensors, can maneuver to a precision of 5-10 mm and attain high levels of safety and efficiency in subsea operations.

AUVs and AIVs

The emergence of autonomous robotic vehicles – self-driving cars, unmanned aerial vehicles (UAVs), industrial and domestic robots – and the groundbreaking technologies they're associated with has also had an impact on underwater exploration. The development of vision-based robotic navigation has led to the development of autonomous underwater vehicles (AUVs) and autonomous inspection vehicles (AIVs).

AUVs and AIVs can be used for critical infrastructure protection, rapid environment assessment, search and rescue operations, intelligence, surveillance and reconnaissance, harbour and costal surveillance, offshore rigs, subsea work, mining, data gathering and deep water survey and inspection.

Docking stations placed on the sea bed allow AUVs to charge their batteries and AIVs also have their own station underwater, meaning that all power resources are dedicated to the missions they undertake and not wasted on dive and recovery processes.

Autonomous inspection vehicle (AIV) – Subsea 7 (Photo: Heriot-Watt University)

Battlespace Preparation Autonomous Underwater Vehicle (BPAUV) during a US Navy exercise (Photo: Bluefin Robotics Corporation)

Ex-proof equipment

Sensors, connectors, switches or cameras are just a few items that equip ROVs, AUVs and AIVs. When these vehicles are intended for the oil and gas industry, they have to meet very specific and strict requirements to be explosion-proof, as any equipment or material used in explosive atmospheres. The fact that they operate underwater doesn't make any difference.

The IEC solution for Ex equipment

The IEC has been at the forefront in this field for many years, preparing International Standards and establishing a Conformity Assessment System that provides testing and certification for Ex equipment.

International standards

IEC Technical Committee (TC) 31: Equipment for explosive atmospheres, has a complete series of international standards that cover all specific requirements for Ex equipment and systems, from general requirements to protection levels for apparatus used by all sectors that operate in hazardous environments, such as oil refineries, offshore oil rigs, gas plants, mines, sugar refineries, flour mills, grain silos and the paper and textile sectors.

Safe access to global markets

Producing devices and equipment based on Ex standards is not enough. Most manufacturers and suppliers trade on the global scene and have to meet the very strict requirements put in place by national regulations and legislation. Proving their adherence to those requirements can be costly and time-intensive.

The IEC, through IECEx, the IEC System for Certification to Standards Relating to Equipment for Use in Explosive Atmospheres, has the mechanisms in place to help industry, authorities and regulators ensure that equipment (electrical and non-electrical) as well as the people working in Ex locations benefit from the highest level of safety.

The System is truly international and has been endorsed by the United Nations Economic Commission for Europe (UNECE) as the world's best practice model for the verification of conformity to international standards for explosive atmospheres.

Accordingly, UNECE issued a UN Publication, *A Common Regulatory Framework for Equipment Used in Environments with an Explosive Atmosphere*, identifying the use of IEC TC 31 International Standards supported by IECEx Certification.

Testing and assessment under the IECEx certified equipment scheme are accepted in all its member countries and beyond. The System provides access to global markets and drastically reduces costs by eliminating multiple re-testing and certification.

Protecting renewable energy equipment from extreme weather

International standards help ensure wind turbines withstand external conditions

By Antoinette Price

2018 was a year of extreme weather. Some of the lowest and highest temperatures were recorded in both hemispheres, while gale-force winds fuelled wildfires in a number of regions and hurricane-strength typhoons caused severe flooding in others.

Different factors contribute towards global climate change, caused by the build-up of greenhouse gases. One way to address this issue is to use clean, renewable energies.

Growth of renewables continues

According to statistics from the International Renewable Energy Agency (IRENA), global renewable generation

Certification requirements for wind turbines cover aspects such as design and external environmental conditions capacity increased by 167 GW and reached 2,179 GW around the world by the end of 2017, representing a yearly growth of around 8.3%.

Following solar photovoltaics (PV), wind grew by 10% with three-quarters of new capacity installed in five countries: China (15 GW), US (6 GW), Germany (6 GW), UK (4 GW), and India (4 GW).

How do wind turbines weather the storms?

As extreme weather events are likely to occur more frequently, manufacturers must ensure from the outset, that their equipment will endure all weather conditions throughout its lifecycle.

Sandy Butterfield, Chair of IECRE, the IEC System for Certification to Standards Relating to Equipment for Use in Renewable Energy Applications, for the wind, solar PV and marine energy sectors, explains how IEC standards reinforce wind turbines.

Sandy Butterfield, Chair, IECRE

In practice, all commercial wind turbines are designed to meet international standards, specifically IEC 61400 series of standards, which have been developed by IEC Technical Committee (TC) 88. IECRE is the only transparent and international certification system for assessing whether a turbine design meets the requirements defined in the standards.

The turbine design conditions are defined in IEC 61400-1 and include external environmental conditions together with a wide variety of turbine operating conditions, which onshore wind turbines must satisfy in order to meet certification requirements. IEC 61400-3 covers external conditions for offshore turbine designs.

“Hurricane conditions are not specifically defined within the standard, instead they are treated as extreme conditions on a spectrum of combined weather and sea-state conditions that may be heavily affected by local geographic conditions.

Most offshore and many onshore wind turbines are designed to withstand 70 m/s (155 mph, nearly 250 km/h) winds (IEC Class I), which is greater than most hurricanes.

The latest revision of IEC 61400-1, which is in its final approval steps, contains a special design class for areas with very high extreme winds, which may result from tropical cyclones, also called hurricanes in the Atlantic ocean. The new design class raises the extreme wind speed that wind turbines are designed for to about 80 m/s (almost 180 mph, around 290 km/h) and allow design for more severe external conditions when needed.”

How to address unique hurricane characteristics in the design process

The standard contains informative annexes which includes the unique characteristics of hurricanes and guidance on how to address them in the design process. Magnitude of winds, waves and other important design conditions are determined by specific site data.

“Every offshore (and onshore) installation must specifically define all the external conditions that may occur at that site over the expected life of the project, which is usually 30 years but no less than 20 years. This requires the project developer to gather historical data for their site and use it to forecast a set of design conditions which projects the extreme winds, waves, currents, and any other events that the turbines could experience, including hurricanes.”

More design challenges may result from combinations of wind (less than the extreme wind) and waves together with certain wind turbine operating conditions. Designers simulate many thousands of these combinations with very sophisticated computer models to assure themselves, certification bodies, regulators, and customers that they have indeed addressed all the conditions that could damage the turbines.

Trust in your electronics

IECQ provides global certification solution for global markets

By Claire Marchand

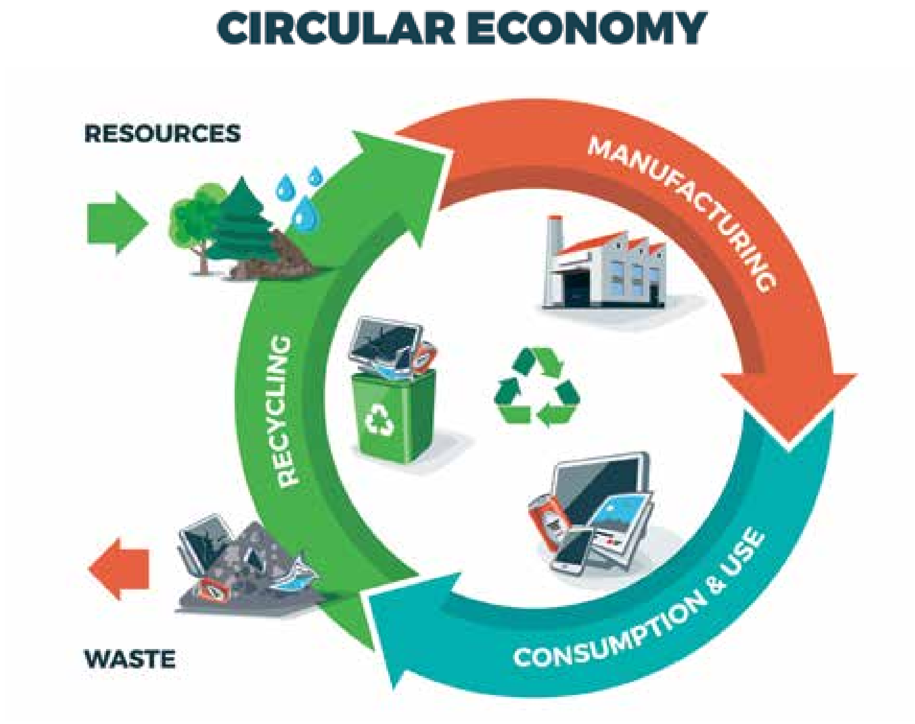
Technological development in the electronics industry has evolved not just at a rapid pace but has been accelerating steadily over the past 20 to 30 years. There have been many success stories and many failures. Competition is fierce. Companies that were start-ups a decade ago are now leaders in the electronics sector while many that were at the top have now ceased to exist. The advent of smart technology and the ever growing demand for smart devices and connectivity are bound to speed up the process even more.

Many challenges

Short life cycle and sustainability

While thriving, the electronics sector is facing many challenges. Product life cycle is one of them. With quickly changing consumer tastes, companies have to innovate, produce and market new products at increasingly shorter intervals to satisfy demand. Consumer loyalty is another factor to take into consideration in this extremely competitive market.

The emergence of strict regulations and standards to limit or eliminate the use of hazardous substances in the product components also have to be taken into account. This has an impact on the complete life cycle, from environmentally conscious design to manufacture to retail and disposal. E-waste has become a major issue and companies may in future have to meet even stricter regulations concerning eco-design.



Product life cycle from ecodesign to manufacturing and disposal has to be taken into account

A global solution for global supply chains

Products today are "made in the world". This is true for all industry sectors. Rare are those that can affirm that their output is manufactured locally. There are multiple supply chains whose components and subcomponents may travel through more than one continent before they're assembled and the end product is rolled out, hits store shelves and reaches consumers. Issues such as traceability and compliance have to be factored in.

A myriad of electronic components

Technological advances in the electronics sector would be non-existent without electronic components. Those are often classified into three main categories: active, passive and electromechanical.

Active components rely on a source of energy (DC) and inject power into a circuit. In recent years, technological advances have greatly enhanced their use in an ever growing number of applications. They include, among others, semiconductor and display devices. Semiconductors comprise diodes, transistors, integrated circuits and optoelectronic components.

Passive components are electrical components that do not generate power, but instead dissipate, store, and/or release it. Among them are capacitors, resistors and inductors. In most circuits, they are connected to active elements, typically semiconductor devices.

Electromechanical components, such as connectors, relays, fuses, switches, microphones, or wires and cables, use an electrical current to create a magnetic field which causes a physical movement.

Ubiquitous sensors

One type of electronic component in particular plays a major role today: sensors. These can be active or passive. Active sensors require an external source of power to operate while passive sensors simply detect and respond to some type of input from the physical environment. They come in many shapes and forms: vision, flow, fibre optic, gas, motion, image, colour, light, pressure, infrared, photoelectric and so on.

Sensors and sensor systems are a key underpinning technology for a wide range of applications. They can be used to improve quality control and productivity in manufacturing processes by monitoring variables such as temperature, pressure, flow and composition. They help ensure the environment is clean and healthy by monitoring the levels of toxic chemicals and gases emitted in the air, both locally and – via satellites – globally. They monitor area and regional compliance with environmental standards. They enhance health, safety and security in the home and workplace through their use in air-conditioning systems, fire and smoke detection and surveillance equipment. They play a major role in medical devices, transportation, entertainment equipment and everyday consumer products.

Smart and safe

Electronic components may come in many shapes and sizes but they have commonalities. They need to be accurate, reliable and high quality. Defective components can have serious consequences for humans and their environment. They also have to meet the requirements of national or regional regulations concerning hazardous substances.

IECQ certification: a global solution

Manufacturers and suppliers of all types of electronic components throughout the world have a powerful tool at their disposal, enabling their products to meet the strictest requirements: IECQ testing and certification. IECQ is the IEC Quality Assessment System for Electronic Components.

As the worldwide approval and certification system covering the supply of electronic components, assemblies and associated materials and processes, IECQ tests and certifies components using quality assessment specifications based on IEC International Standards.

In addition, there are a multitude of related materials and processes that are covered by the IECQ schemes. 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 provides manufacturers with independent verification that IEC International Standards and other specifications were met by suppliers who hold an IECQ certification.

The conformity assessment system provides the following core certification schemes and programmes which serve as an effective supply chain management tool for industry in verifying compliance with component specifications and standards:

- → IECQ AP (Approved Process)
  - – IECQ AP-CAP (Counterfeit Avoidance Programme)
- → IECQ AC (Approved Component)– IECQ AC-AQP (Automotive Qualification Programme)
  - – IECQ Scheme for LED Lighting (LED components, assemblies and systems)
  - – IECQ AC-TC (Technology Certification)
- → IECQ Avionics – IECQ ADHP (Aerospace, Defense, and High Performance)
- → IECQ HSPM (Hazardous Substances Process Management)
- → IECQ ITL (Independent Testing Laboratory)

IECQ contribution to a safer and more reliable world can only increase with the development of new technologies and state-of-the-art electronic devices.

More information on IECQ: www.iecq.org

Form and substance

Increased flexibility and wider reach for key standard on substance reporting

By Catherine Bischofberger

A new edition of IEC 62474 makes chemical substance reporting easier for suppliers and manufacturers in the supply chain, helping them meet regulatory requirements.

Levels of hazardous substances in electrotechnical products need to be measured and reported (Photo: jble.af.mil)

Hazardous substances can be found in many products, including electrical and electronic devices and systems. As countries become more conscious of the negative impact of these substances on the environment, regulations have been adopted to enforce their reporting. Rulings also restrict the most polluting and dangerous chemicals. IEC publishes an international standard on substance reporting which improves transparency up and down the electronics supply chain. The publication also helps suppliers and manufacturers to comply with existing regulations. IEC Technical Committee (TC) 111, which specifies environmental standards for electrical and electronic products and systems, issued the first edition of IEC 62474 in 2012. (For more information on the TC, read *Protecting the planet*, in *e-tech* issue 05 2018.)

"The standard had a huge impact when it was published because it levelled the playing field. Before IEC 62474, the biggest suppliers could dictate their terms when it came to substance reporting. It also replaced existing national or regional standards, such as the *Joint Industry Guide* (JIG-101) and the *Japanese Green Procurement Survey Standardization Initiative* (JGPSSI)," explains Robert Friedman, Co-convenor of the IEC 62474 validation team.

New edition to meet user requests

IEC has issued a new edition of the standard which includes a number of improved features, in response to points raised by industry stakeholders. They wanted greater flexibility and ease of use when it came to substance reporting. Requests to widen the reach of the standard to sectors outside the electronics industry were also voiced. "One of the most important selling points of Edition 2 is that it is a one-stop shop, a very complete standard which provides information on what to report and how to report it, including a separate mechanism for the exchange of data down the supply chain," describes Friedman. The standard is also available in a red line version, highlighting the changes with the previous edition.

A common format is used to ease the transfer and processing of data. The standard also comes with a validated open database which includes a declarable substance list (DSL), which is updated in line with regulatory requirements. The new edition enables users to employ two different methods for declaring substances.

"The standard defines a declaration for compliance and a composition declaration. The first one enables suppliers to check their products against the existing DSL, whereas the second allows them to make a broader substance declaration, which includes, at a minimum, any declarable substances in the product. The composition declaration can optionally include other substances as well, and can even become a complete substance declaration. In the previous edition, the two different types of declaration were merged into one, with no clearly defined rules for substance reporting. This new approach makes things easier for both manufacturers and suppliers," explains Walter Jager, Co-convenor of the IEC 62474 validation team with Robert Friedman.

By providing both declaration methods, the new edition equally paves the way for likely regulatory changes. "Some companies are already willing to go beyond the declarable substance list and wish to report all the substances in their products. The composition declaration is, for the time being, mostly used for simpler products which do not include many substances to report. But looking towards to the future, companies will probably have to declare an increasing number of chemical substances in more complex products to meet new regulations concerning the environmentally-conscious design of products," Jager says.

All sorts of electrotechnical products contain chemical substances

Room for exemptions

The IEC 62474 DSL is regularly updated, as new or revised regulations are released. "It is brought up to date by three different groups dealing with separate geographical areas: Americas, Asia and Europe, Middle East and Africa (EMEA). These groups keep track of the various regulatory changes around the world," says Christophe Garnier, chair of IEC TC 111. A typical example of such regulations is the EU *Restriction of Hazardous Substances* (RoHS) Directive, which restricts the use of specific hazardous materials found in electrical and electronic products and which was most recently amended in 2015.

In the new edition of IEC 62474, exemption lists are included in the database. Restricted substances can be used in specific instances, when there is no other scientific alternative. "The use of exempted substances needs to be declared through the supply chain in a consistent manner. Downstream manufacturers want to be able to assess the compliance of their products and report exemptions when required. The new edition of IEC 62474 has harmonized a number of exemption lists that can be found in existing regulations, but as other exemption lists are identified, they can be added to the IEC 62474 database," explains Mark Frimann, Co-convenor of the Maintenance Team for IEC 62474, which developed the new edition of the standard.

"This means that countries wishing to replicate RoHS-type regulations could refer to the new edition of IEC 62474 in their legislation to specify exemptions instead of creating their own exemptions list. We do the work for them by always ensuring the list is up to date," Jager adds.

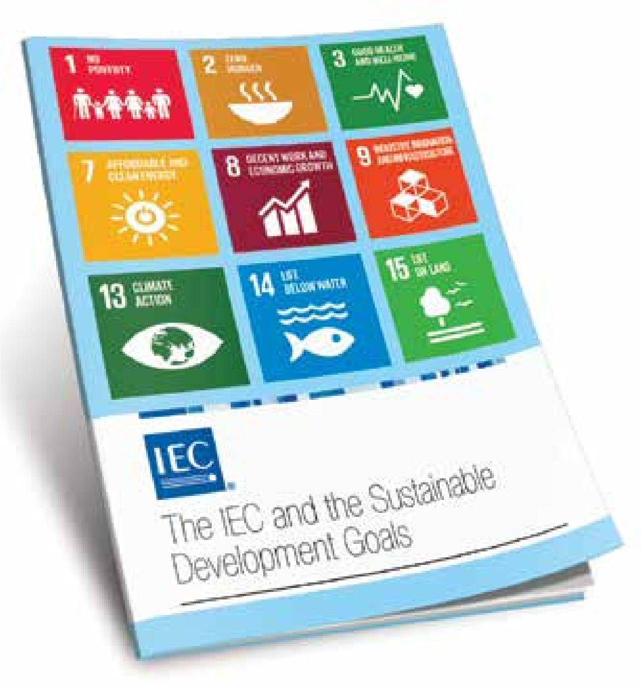
Reaching out to other industries

Another important selling point is that the standard can be used by any supply sector wishing to report chemical substances in their products. "The toy or the textile industry, to mention just a couple, could use the standard to meet their own requirements. It is easy to adapt it, all you need to do is establish the relevant list of substances in your product, using the IEC 62474 declaration methods and employ the exchange format for the transfer of data down the supply chain. The list of exemptions can also be customized," Garnier indicates.

According to Koshi Kamikagi, Co-convenor of the Maintenance Team for IEC 62474 with Mark Frimann, the new edition is a big step forward as "it can be used as a substance declaration in forward logistics, which involve all the processes required to get products to market, but also, just as importantly, as an information declaration standard linking forward logistics to reverse logistics, which relates to the reuse and recycling of products and materials."

Much further down the line, Jager envisages possibly working on a joint standard with ISO. "It makes a lot of sense to me. But there are quite a few issues to solve before we get there. One of them is making sure we keep the flexibility provided by the IEC 62474 database which is updated and validated on a regular basis," he concludes.

Form and substance


1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
IEC
The IEC and the Sustainable Development Goals

Ensuring affordable and clean energy for all, improving health and striving to provide inclusive and equitable quality education for all, are some of the 17 UN Sustainable Development Goals to be reached by 2030. In the next issue we will look at how international standards developed by IEC contribute towards achieving more than half of the UN SDGs.

Share your work

IEC work in standardization is carried out by some 20 000 technical experts, while testing and certification, is done by the many certification bodies and testing laboratories within the IEC Conformity Assessment Systems. *e-tech* covers this broad scope of work, which spans many industries and technologies.

We'd like to hear your story and report on your work or any related events you are organizing or participating in, on behalf of IEC.

Below are the *e-tech* themes for the next few months:

Issue 02/2019
SDGs
Health & well-being, energy, decent work and economic growth, industry, innovation, infrastructure, cities & communities

Issue 03/2019
Home DIY
Safety, smart apps for connected tools

Issue 04/2019
Year in review distributed at GM, Shanghai

Issue 05/2019
Medical
Digital health, data security, data analytics, AI, connected biometric sensors, nanotech

Issue 06/2019
Smart manufacturing
Industry 4.0, cyber security, robots, IoT

We'd love to hear from you!
Contact us at zsm@iec.ch or apr@iec.ch with your ideas and stories.

e-tech
news & views from the IEC

International
Electrotechnical
Commission

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

T +41 22 919 0211

Contact: communication@iec.ch

For more information visit: www.iec.ch