Issue 02/2019

e-tech

news & views from the IEC

Advancing the SDGs

Technology focus

Recovering from disasters

Women still gotta fight!

Technical committees

Digital learning is redefining education

Making IT more sustainable

In store

Super cool cables

Advancing the Sustainable Development Goals through standardization

The 2030 Agenda for Sustainable Development is a call to action to make the world a safer, more peaceful and prosperous place, for all

Antoinette Price
Managing Editor e-tech

To achieve this, in 2015, United Nations Member States adopted 17 Sustainable Development Goals (SDGs).

Building on the former Millennium Development Goals (MDGs), they will guide high-level decisions as they endeavour to eradicate poverty and hunger, improve healthcare and create a cleaner, greener planet. They will also strive to build sustainable cities and communities, ensure quality education, gender equality, decent work and economic growth, as well as resilient infrastructure and sustainable industrialization.

The UN recognizes its vision is as ambitious as it is transformational, and emphasizes the need for all stakeholders – governments (national and local), authorities, international organizations, industry, businesses and civil society – to participate in this process.

The activities of standards development organizations already play a significant role. Energy, and especially electricity, is the common thread of the SDGs, and beyond that, the development of every nation and economy. IEC work provides the technical foundation for the entire energy chain and all equipment that is driven by electricity. It improves the safety of devices, workers and populations, as well as enabling energy efficiency gains and increasing the resilience and long-term viability of infrastructure.

IEC also operates four conformity assessment schemes, which test and certify that products and services meet IEC standards. The schemes cover electrical equipment and components (IECEE), equipment for use in explosive atmospheres (IECEx), quality assessment for electronic components (IECQ) and equipment for renewable energies (IECRE).

In this issue, we will examine how IEC standardization already contributes towards achieving many of the SDGs.

For example, virtual and augmented reality (AR/VR) are used increasingly in education (science, maths and languages) and workplace training (surgery, disaster response and maintenance of power plants). In our article *Digital learning is redefining education*, we discover how standards enable interoperability of soft- and hardware systems, allowing educators and trainers to tailor teaching to the learner's needs and preferences, as well as broadening access to education (SDG 4 Quality education).

As growing populations require more electricity, energy providers are increasing the percentage of cleaner, more affordable renewables into the mix. We also look at some of the challenges faced and how IECRE certification of solar PV systems limits risks, encourages investment and instils confidence across the industry (SDG 7 Affordable and clean energy).

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, Moreno Carullo, Alan Hodgson, Claire Marchand, Natalie Mouyal, Michael A. Mullane, Thomas Sauer

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

Available for download

23

Mobile phone applications may eventually be used to replace ID documents such as passports and driver licenses

26

IECRE certification covers the entire lifecycle of a solar PV plant

34

Superconducting cables can transmit large quantities of electrical power in a highly energy-efficient way

Recovering from disasters

IEC Standards provide the tools to enable countries to recover from disasters

By Natalie Mouyal

From severe droughts to hurricanes and flooding, disasters appear more frequently and with a greater intensity than in the past. Recognizing the human and economic toll of these disasters caused by climate change, the United Nations has included climate action as one of its Sustainable Development Goals (SDG). Specifically, the UN calls for strengthening the resilience of infrastructure in the face of disasters. This is an area where the IEC already makes a significant contribution.

The IEC takes a multi-pronged approach to climate action and how countries can recover following a disaster. It calls for the appropriate measures to be put in place that can increase infrastructure resilience against disasters, but also the tools for planning and recovery should a disaster strike. This is made possible by adopting IEC Standards and undertaking testing and certification.

Ready, set, resilience

Extreme weather events and disasters have had a detrimental impact on the delivery of electricity. Blackouts can affect millions of homes and last for hours or days, if not longer. Problems are further aggravated by blackouts affecting essential services that depend on electricity, such as medical care, sanitation and water management.

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 incident including a disaster situation. This can be achieved by, for example, splitting networks into smaller circuits, so-called mini or microgrids or adding intelligence to the grid that can detect a short circuit, block power flows to that area and reroute the electricity so users do not lose access.

IEC work helps strengthen disaster resilience of infrastructure through built-in safety mechanisms, processes and minimum requirements. IEC Standards include external environmental conditions in their design requirements. For example, the IEC 61400 series of standards developed by IEC Technical Committee (TC) 88, addresses external conditions for offshore wind turbine designs which include the ability to withstand 70 m/s (155 mph, nearly 250 km/h) winds (IEC Class I), which is greater than most hurricanes.

The IEC ensures safety is an integral aspect of devices and systems, thereby protecting people, critical infrastructure, economies and the environment. These standards can address aspects of safety that apply horizontally to many products or specifically address the needs of a single product type or industry. The IEC 61508 series of standards ensures functional safety throughout the life cycle of electrical and electronic systems and devices.

However, as extreme weather events are likely to occur more frequently, a new type of resiliency for utilities may be necessary. The IEC Market Strategy Board (MSB) which identifies key technology trends and market needs, has indicated that it will tackle the issue of resiliency and ensure that electricity distribution systems are more climate-resilient.

Planning for disruption

Continuity planning for potential disasters can help mitigate the adverse effects of disasters. Planning is a key factor to minimize cost and damage should critical infrastructure become inoperable. It ensures that potential disasters have been considered and local plans developed for the restoration of services.

> “IEC work helps strengthen disaster resilience of infrastructure through built-in safety mechanisms.”

IEC TC 56 prepares standards in the area of dependability, a technical discipline that addresses the risk assessment and management of services and systems throughout their life cycle, including cyber

security threats. It has developed standards that include dependability assessment and technical risk assessment. The IEC White Paper, Microgrids for disaster preparedness and recovery, addresses the actions necessary in anticipation of major electricity outages and after a disaster has occurred.

As part of their preparation, first-responders are trained to handle emergency situations. While checklists for possible scenarios can be useful, preparation can be further enhanced through training programmes that incorporate virtual reality and thus provide users with a full immersion into a seemingly real disaster scenario. Virtual reality applications rely on standards related to image processing and computer graphics developed by ISO/IEC JTC 1/SC 24, a subcommittee of the Joint Technical Committee of IEC and ISO.

Early warning systems can be put in place to provide authorities with the time necessary to evacuate vulnerable areas before a disaster strikes. For example, warnings of an impending earthquake can be discerned with laser beams that detect tectonic plate movements or seismometers that can identify and measure the earth's vibrations. Imminent volcanic eruptions can be predicted using seismometers, gas detectors or infrared thermography cameras. All of these technologies rely on IEC Standards developed by IEC TC 76 (laser equipment), IEC TC 47 (semiconductor devices and sensors) and IEC TC 31 (equipment for explosive environments).

After the disaster…recovery

Once a disaster strikes, the recovery process begins. As a first step, drones can be sent into areas deemed too dangerous for humans in order to guide rescuers, gather data and deliver supplies.

Drones were used by the California Air National Guard in August 2018 to track the spread of the wildfires in the northern part of the state. Equipped with laser range-finders, cameras and infrared sensors, the drones were able to send images to firefighters who could use the information to determine where spot fires were located, develop containment strategies and implement evacuations.

Robots were first used to explore the wreckage following the collapse of the World Trade Center in New York after the September 2001 terrorist attacks. They have since been used to survey damage after the Fukushima Daiichi nuclear power plant accident in Japan in 2011 as well as the earthquakes in Haiti (2010) and Nepal (2015). These robots and drones rely on standards developed by IEC TC 47 and its subcommittee SC 47F (micro electromechanical systems), IEC TC 2 (motors) and SC 21A (secondary cells and batteries).

Exoskeletons can also be used in order to help rescuers clear through rubble. Following the 2011 earthquake in Japan, a hybrid assistive limb (HAL) exoskeleton suit was used as part of the clean-up effort at the nuclear reactor. Exoskeletons can be used to protect workers from dangerous radiation as well as lift weights of up to 100 kg.

Quickly restoring access to electricity after a disaster is a primary objective. Microgrids, a collection of controllable and physically close electricity production units managed locally, can help ensure the continuity of services should the traditional electricity grid fail.

No country in the world is immune from disasters and the dramatic effects of climate change. While collective action may be necessary to limit the rise in global temperature, each country must adopt disaster mitigation measures, such as infrastructure resilience and continuity planning, to ensure maximum preparation for when a disaster strikes.

Storms leave a path of destruction in their wake cutting off vital services (Photo: Wikilmages from Pixabay)

Women still gotta fight!

Still a long way to go for women in tech fields

By Claire Marchand

Women are still underrepresented in science, technology, engineering and mathematics (STEM). According to UNESCO, the United Nations Educational, Scientific and Cultural Organization, 29% of those in science research and development are women, with a low of 19% in South and West Asia and a high of 48% in Central Asia. Europe and North America are at 32%.

It may take some time before we see gender equality in STEM, but things are moving in the right direction. Actions are undertaken throughout the world. United Nations Sustainable Development Goal (SDG) 5 aims to achieve gender equality and empower women and girls. Many countries now have programmes that encourage young girls to embrace studies in these fields. The youngest inventor featured in this article, who participated in such a programme, is nine years old!

Gladys West (1930-) – The lady behind the GPS

Gladys Mae West (née Brown), born in 1930 in a rural county of Virginia, US, was determined from an early age to eschew farm or factory work, knowing that education was the key to her future. Thanks to her good grades, she won a scholarship to Virginia State College where she was one of the few women studying mathematics. "You felt a bit different," she later said. "You didn't quite fit in as you did in home economics." After graduation, she worked as a teacher for a couple of years. In 1956, she joined the Naval Surface Warfare Center (NSWC) in Dahlgren, Virginia – the second black woman ever to be employed by the Center.

Gladys West at the Pentagon (Photo: Air Force Space Command/Adrian Cadiz)

Firstly, West participated in an astronomical study that showed the regularity of Pluto's motions relative to Neptune. Subsequently her supervisor recommended her as project manager for the Seasat radar altimetry project, the first satellite that could remotely sense oceans. Over the following decades, this allowed her to develop and hone in further satellite modelling of the globe, with increasingly refined algorithms. She ended up creating an extremely accurate geodetic earth model, factoring in details such as gravitational and tidal forces responsible for slightly modifying the earth's shape. The model later became the foundation of the GPS satellite system as we know it today. Sadly, after West retired in 1986, her contributions to the GPS were largely forgotten. But she didn't remain idle in retirement, enrolling in a remote studies programme at Virginia Tech and obtaining her PhD in 2018.

Dr West's achievements were rediscovered when she wrote a short biography for one of her Alpha Kappa Alpha sorority events. A fellow member read it and spread the word. In 2017, Capt. Godfrey Weekes, then-commanding officer at the NSWC Dahlgren Division, wrote about West: "She rose through the ranks, worked on the satellite geodesy and contributed to the accuracy of GPS and the measurement of satellite data. As Gladys West started her career as a mathematician at Dahlgren in 1956, she likely had no idea that her work would impact the world for decades to come."

On 6 December 2018, in a ceremony at the Pentagon, West was inducted into the US Air Force Space and Missile Pioneers Hall of Fame. Hoping that her work will inspire a new generation of female pioneers, West said: The world is opening up a little bit and making it easier for women. But they still gotta fight."

The work of Technical Committee (TC) 47: Semiconductor devices, and its Subcommittee (SC) 47F: Micro-electromechanical systems, is essential to technological advances in the modern GPS. Several other IEC TCs also develop standards related to various aspects of the GPS technology. Notably TC 49: Piezoelectric, dielectric and electrostatic devices and associated materials for frequency control, selection and detection; TC 80: Maritime navigation and radiocommunication equipment and systems, and CISPR Subcommittee CIS/D: Electromagnetic disturbances related to electric/electronic equipment on vehicles and internal combustion engine powered devices.

Ruzena Bajcsy (1933-) – A woman in robotics

Born in Bratislava, Czechoslovakia, Ruzena Bajcsy was orphaned during World War II and placed in a Red Cross orphanage with her sister. Despite the hardships, her academic achievements were outstanding and she went on to study electrical engineering at Slovak Technical University, obtaining her MS in 1957 and PhD in 1967. That same year, she was offered the opportunity to go to Stanford University to study computer science. There she earned her second PhD.

Ruzena Bajcsy (centre), with members of the GRASP Lab, circa 1984. Bajcsy founded the GRASP Lab in 1979 (Photo: GRASP)

At the University of Pennsylvania, where she worked for the next 30 years as professor and chair of computer science and engineering, she did research in many areas, including medical imaging. In 1979, she founded the General Robotics and Active Sensory Perception (GRASP) Lab, which, under her leadership, became a world-renowned research centre. In the early 2000s, she joined the University of California, Berkeley, as professor of electrical engineering and computer sciences.

Bajcsy is the recipient of numerous awards including the 2009 Benjamin Franklin Medal in Computer and Cognitive Science and the 2013 IEEE Robotics and Automation Award. Her current research focuses on artificial intelligence; biosystems and computational biology; control, intelligent systems and robotics; graphics and computer-human interaction, computer vision and security.

IEC International Standards prepared by IEC TC 47 and SC 47F are key to robotics. Several other TCs prepare standards that contribute to the safety and performance of modern robots. As for artificial intelligence, the IEC and ISO Joint Technical Committee, ISO/IEC JTC 1: Information technology, has set up ISO/IEC JTC 1/SC 42, which carries out standardization activities in that field.

The human computers (1943-1958) – African-American women in the space race

At the onset of World War II, the National Advisory Committee for Aeronautics (NACA) – NASA's predecessor – started hiring women as "human computers", whose job was to do complex calculations. Those were done by hand, and often took a long time and many notebooks to complete. By the end of the war in in the 1950s there were hundreds of women working in aeronautical research.

In 1943, NACA's Langley Research Center in Virginia began recruiting African-American women with college degrees to work as human computers. Segregation laws of the time forced them to form their own subgroup, totally isolated from the others. They were known as the West Area Computers because they were located in the west wing of the research centre.

Their main responsibility was to process data, and on a number of occasions, they joined other teams to work on specific assignments. They were originally supervised by white women, but in 1949, Dorothy Vaughan became NACA's first African-American supervisor in charge of the group.

Dorothy Vaughan (Photo: NASA)

Vaughan (1910–2008) was a mathematician who worked at Langley from 1943 through her retirement in 1971. She prepared for the transition to machine computers in the early 1960s, teaching herself and her staff the FORTRAN programming language and in later years, she headed the programming section of the Analysis and Computation Division (ACD).

Mary Jackson (Photo: NASA)

NACA recruited Mary Jackson (1921–2005) in 1951 as a research mathematician – human computer – at Langley where she worked under Vaughan. In 1953 she worked for engineer Kazimierz Czarnecki in the Supersonic Pressure Tunnel. He encouraged her to pursue her studies. Jackson was allowed to attend mathematics and physics night classes offered by the University of Virginia and originally reserved to white students. In 1958, she was promoted to aerospace engineer, NASA's first black female engineer. Over the years she worked in several NASA divisions, obtaining the most senior position within the engineer division and as of 1979, she decided to take a demotion to be able to work on gender equality and affirmative action programmes to influence the career paths of women in science, engineering, and mathematics positions at NASA.

> "UN SDG 5 aims to achieve gender equality and empower women and girls."

Mathematician Katherine Johnson (1918-) joined the West Area Computing group in 1953. She was subsequently reassigned to Langley's Flight Research Division, where she performed notable work including providing the trajectory analysis for astronaut John Glenn's MA-6 Project Mercury orbital spaceflight. She received the Presidential Medal of Freedom in 2015 from President Obama.

Katherine Johnson (Photo: NASA)

The work of all three women (Vaughan, Johnson, and Jackson) is featured in the book and film Hidden Figures.

In 1958, when the NACA became NASA, segregated facilities, including the West Computing office, were abolished.

Ursula Keller (1959-) – Pioneer of ultrafast laser tech

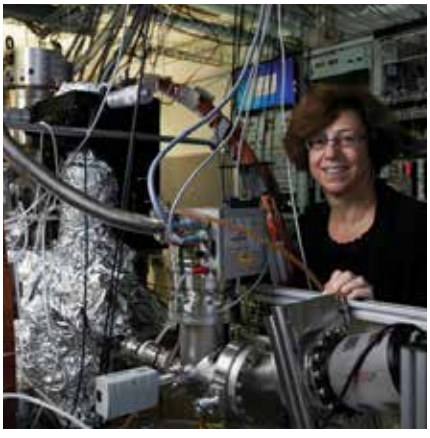
Swiss scientist and inventor Ursula Keller discovered how to turn continuous laser light into ultrafast laser pulses, a technological breakthrough that was recognized twice in 2018: she received the European Inventor Award for "Lifetime achievement" from the European Patent Office, and the IEEE Photonics Award.

Keller invented the semiconductor saturable absorber mirror (SESAM) in 1992 while working at AT&T Bell Laboratories, which, at the time, had the leading and best-equipped lab in Keller's field. Her invention gave science, industry and the medical sector an instrument of unprecedented precision – laser bursts that last from picoseconds (10^{-12} seconds) to femtoseconds (10^{-15} seconds) and can be repeated up to several billion times a second.

In the medical field, Femto-LASIK for eye surgery, based on Keller's technology, is able to make the tiniest of incisions with no risk of damaging nearby tissue. The ultrafast laser can cut away cancerous tissue without searing neighbouring healthy cells.

The technology is used in other sectors and has opened up numerous production and material-processing applications essential to, among others, the automotive and electronics industries. Most ultrashort lasers today utilize her SESAM mode-locking technology for optical communication, precision measurements, microscopy, ophthalmology, and micromachining applications. Her invention has had an impact on our everyday communications: smartphones wouldn't exist without short-pulsed lasers.

Keller also works in the field of quantum physics and has developed a clock, the attoclock, that can measure attoseconds (10^{-18} seconds or one quintillionth of a second).



Ursula Keller and the ultra accurate attoclock (Photo: EPO)

Another significant breakthrough in her career happened in 1993 when Keller became the first woman offered a university professorship in the natural sciences faculty at the Federal Institute of Technology (ETH) in Zürich, Switzerland. In 2018, she said to Swiss newspaper Le Temps: "ETH had a few women professors in architecture and pharmacy but I was the first in hard sciences. I had totally underestimated what it was like to be in a man-only environment. It proved to be very difficult in the sense that, for example, important information was only discussed in insiders' clubs, from which women were excluded."

Keller is Director of NCCR MUST, an interdisciplinary research programme launched by the Swiss National Science Foundation in 2010. The programme brings together 16 Swiss research groups working in molecular ultrafast science and technology (MUST) across the fields of physics and chemistry.

Established in 1972, IEC TC 76: Optical radiation safety and laser equipment, is recognized as the leading body on laser standardization in this technical area. It also provides guidance to other TCs preparing standards for products containing optical radiation sources.

Xóchitl Guadalupe Cruz López (2009-) – Mexican girl wins prestigious award

In February 2018, Xóchitl Guadalupe Cruz López, then aged eight, received the prestigious Women's Recognition Award from the Institute of Nuclear Science at the National Autonomous University of Mexico (UNAM). This was the first time the prize, which recognizes women's contributions to science, was awarded to a child. Her achievement: a solar water heater made entirely from discarded objects such as hoses, logs, and glass panels retrieved from a former construction site. With her father's help, she installed the heater on the roof of her house in the Mexican state of Chiapas.

Xóchitl Guadalupe Cruz López (Photo: eslocotidiano.com)

For more than half her life – i.e. since she was four – Cruz López has participated in scientific workshops through PAUTA, the "Adopt a Talent" programme, an initiative promoted by UNAM to bring science education to Mexican children and teenagers where educators, psychologists and scientists mentor students from school to university. Cruz López has benefited greatly from this initiative and several of her projects, all with high social impact, have won prizes.

In August last year, Cruz López was a special guest and speaker at an educational forum in Chiapas, attended by then President Elect Andrés Manuel López Obrador. She pled with him to save PAUTA, which faced possible closure due to lack of funding.

With her invention, Cruz López wanted to create a solution that was good for the environment and for low-income families in her community of Chiapas. She hopes to get support, in training and material, to help her neighbors in the near future.

The IEC has set up two TCs that deal with solar energy: TC 82: Solar photovoltaic energy systems, and TC 117: Solar thermal electric plants.

The women and girl featured above have set the bar very high – they have all overcome many obstacles to succeed in their field. Their stories are uplifting and inspiring and should encourage a new generation of women to follow their example.

Part of the solar water heater invented by Xóchitl Guadalupe Cruz López (Photo: mexicinewsdaily.com)

Cyber attacks targeting critical infrastructure

Such is our reliance on electricity that a prolonged blackout would jeopardize transport systems, the supply of fresh water, communications and banking

By Michael A. Mullane

Malicious hackers are threatening public safety all over the world. In the United States, for example, the January edition of the *National Intelligence Strategy Report* warns, "Cyber threats will pose an increasing risk to public health, safety and prosperity as information technologies are integrated into critical infrastructure, vital national networks and consumer devices". Addressing Congress, the US National Intelligence Director, Daniel Coats, put it even more succinctly: "The warning lights are blinking red".

Critical infrastructure facilities, whether they are power plants, national railway and local underground systems or other forms of public transport, are increasingly being targeted. Cyber attacks could cut off the supply of electricity to hospitals, homes, schools and factories. We rely so heavily on the efficient supply of electricity that its loss would also carry heavy implications for other vital services. A number of incidents in recent years demonstrate not only that the threat is tangible, but also that on more than one occasion we have escaped incurring nightmare consequences by the skin of our teeth.

The following three examples illustrate the evolution of cyber weapons, including malware designed to disrupt the operation of critical infrastructure. While the growing use of networked sensors and other connected devices in the industrial environment has brought benefits in terms of efficiency, it has also increased the attack surface.

Critical infrastructure facilities, whether power plants or different forms of public transport, are increasingly being targeted (Photo: cegoh, Pixabay)

Three times the world has held its breath

The 2010 attack on Iran's nuclear plant at Natanz has a special place in the history books. The so-called Stuxnetmalware made its first public appearance then, managing to bring the nuclear plant to a halt. The Stuxnet worm was engineered to damage motors commonly used in uranium-enrichment centrifuges by sending them spinning out of control. It succeeded in temporarily disabling 1 000 centrifuges.

Five years later, in December 2015, Ukraine experienced an unprecedented assault on its electricity grid. The attack led to widespread power outages. Hackers infiltrated three energy companies and shut down power generation temporarily in three regions of Ukraine. It left nearly a quarter of a million people without electricity for up to six hours in the middle of winter. Attackers used the BlackEnergy 3 malware to shut down the three substations. It is believed the malware was delivered in spear phishing emails, where it was hidden in fake Microsoft Office attachments.

The third and most alarming attack that we know about took place in 2017. Cyber terrorists assumed remote control of a workstation widely reported to be in Saudi Arabia. They used a new kind of malware, dubbed Triton, to take over the plant's safety instrumented system (SIS). Again, the malware was configured specifically for industrial control systems, also known as operational technology (OT).

> "IEC believes a holistic, risk-based approach is the best way to build cyber resilience."

Investigators believe it was an act of sabotage meant to trigger an explosion by disabling the safety systems designed to prevent catastrophic industrial accidents. Previous attacks have focused on destroying data or shutting down energy plants. According to some reports, only a coding error prevented this from happening. Evidence points to another phishing or spear phishing attack.

Lessons learned

What these incidents show us is that for at least the past decade hackers have been creating malicious code that targets operational technology. The fact that all three were triggered by malware also illustrates the need for adopting a holistic approach to cyber security that incorporates processes, technology and people.

The chief executive of cyber specialists Security in Depth, Michael Connory, recently told the Australian Broadcasting Corporation (ABC) that, "Ninety per cent of cyber attacks worldwide begin with an email". It is axiomatic that security can only be as strong as the weakest link in the chain.

The other key issue is the importance of understanding the difference between

IT and OT. Operational technology is becoming increasingly accessible, with threat vectors now extending to base-level assets such as smart thermostats. The challenge is that cyber security programmes are too often led by an IT approach. In reality, the operational constraints in industry sectors such as energy, but also in a variety of others including manufacturing, healthcare and transport, mean that an approach to cyber security is needed that also safeguards OT.

The primary focus of IT is data and its ability to flow freely and securely. It exists in the virtual world, where data is stored, retrieved, transmitted and manipulated. IT is fluid and has many moving parts and gateways, making it highly vulnerable and offering a large surface for a wide variety of constantly evolving attacks. Defending against attacks is about safeguarding every layer, continuously identifying and correcting weaknesses to keep data flowing.

OT, in contrast, belongs to the physical world, where it ensures the correct execution of all actions. While IT has to safeguard every layer of the system, OT is about maintaining control of systems which may be on or off, closed or open. OT systems are designed for specific actions such as ensuring that a generator is switched on or off, or that an overflow valve is open when a chemical tank is full. OT belongs in the physical world and is about ensuring the security and control of what in the past were usually closed systems. Everything in OT is geared to physically moving and controlling devices and processes to keep systems working as intended, with a primary focus on security and increased efficiency.

With the emergence of the Industrial Internet of Things (IIoT) and the integration of physical machines with networked sensors and software, the lines between IT and OT are blurring. As more and more objects are connected, communicate and interact with each other, there has been a surge in the number of endpoints and potential ways for cyber criminals to gain access to networks and infrastructure systems.

Firefighting puts out the blaze but does not deal with the underlying causes. It is essential to start considering security threats during the initial design and development phase. In many instances, organizations only look at security after implementation, rather than building cyber resilience from the beginning of the development lifecycle. The work of IEC Technical Committee (TC) 57 provides a good example of the standardization of best practices.

Security by design

IEC TC 57 has created a working group (WG 15) to make power grids secure-by-design. The group, which evaluates requirements from a technology perspective and defines a standard way to implement them, has identified the components needed for a secure-by-design power system. These include the end-to-end encryption principle, the definition of roles for all users and identity management, as well as pervasive monitoring of the system itself.

Cyber attacks could cut off the supply of electricity to hospitals, homes, schools and factories (Photo: Nicole Köhler, Pixabay)

"Everything we do today will remain tomorrow, but we need to change our focus," says WG 15-member Moreno Carullo. "We need to shift from just looking for the bad guys to security-by-design."

Currently, the IEC 62351 family of standards (see IEC 62351-1: *Introduction for an in-depth overview*) depicts the architecture of a secure power system and standardizes its protocols and components. An interesting read for a better overview of it is IEC 62351-10: *Security Architecture Guidelines for TC 57 Systems*.

Standards and conformity assessment

The IEC believes that a holistic, risk-based approach is the best way to build cyber resilience. A risk-based approach can be highly effective, especially when based on an assessment of existing, or potential, internal vulnerabilities and identified, or possible, external threats. This works best as part of a holistic approach that combines standards with testing and certification, also known as conformity assessment, as opposed to treating them as distinct areas.

Such an approach increases the confidence of 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. A systems approach works by prioritizing and mitigating risks to an acceptable level, which requires a neutral approach that accommodates different kinds of conformity assessment — ranging from

self-assessment to independent, third-party testing — according to the different levels of risk.

Many organizations base their cyber security strategies on compliance with mandatory rules and regulations. This may lead to improved security, but cannot address the needs of individual organizations in a comprehensive manner. The most robust defences rely on both 'horizontal' and 'vertical' standards. Horizontal standards are generic and flexible, while vertical standards cater to very specific needs. Two examples of horizontal standards in particular stand out.

Horizontal and vertical standards

The ISO/IEC 27000 family of standards 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 in any industrial environment, including critical infrastructure facilities such as power utilities or nuclear plants, as well as in the health and transport sectors. IECEE, the IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components, has created global certification services based on the IEC 62443 series.

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, among others.

Building resilience

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

Achieving resilience is largely 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.

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

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

Another way to think of it is as the ABC of cyber security:

A is for assessment
B is for best practices to address the risk
C is 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 or relying on a supplier's declarations all the way through to independent, third-party assessment and testing — and selecting whichever is 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 building long-term cyber resilience. Standards and conformity assessment, however, can only have maximum impact as part of a risk-based approach based on a holistic assessment of threats and vulnerabilities. Such an approach incorporates not only technology, and processes, but also people, recognizing the essential role of training.

Digital learning is redefining education

Imagine experiencing an historic moment as it happens, or discovering cellular biology in 3D from inside the body. This is now possible using virtual reality

By Antoinette Price

In parts of Asia, North and South America, Europe and Africa, digital technologies are enabling students to learn more effectively and from entirely new perspectives.

Connectivity and the Internet of Things (IoT), artificial intelligence (AI) machine learning and algorithms, virtual and augmented reality (VR/AR) are some of the innovative, disruptive technologies, which continue to change how we live, communicate, commute, deliver healthcare, enjoy entertainment, farm, work and more.

The same goes for learning. Around the world, as students of all ages prepare for their future, the education industry is rethinking its teaching systems.

But it goes beyond primary and secondary education. Aging populations working longer in environments that are being reshaped by technologies will require regular retraining or life-long learning.

Additionally, some of these technologies are providing people in developing countries, remote locations or with limited mobility, access to education, which enhances overall quality of life.

A quality education for all

Through education, it is possible to improve the quality of life and create the basis for sustainable development. The United Nations Sustainable Development Goal (SDG) 4 Quality education, aims to ensure that all girls and boys have access to and finish their free, equitable and quality primary and secondary education.

A growing number of schools are using VR programmes to teach history, maths, science and more

It also looks to ensure equal access for all women and men to affordable and quality technical, vocational and tertiary education, including university regardless of gender, disability or indigenous people.

Innovative technologies, such as virtual reality, the Internet of Things (IoT) and artificial intelligence (AI) are helping to increase and diversify learning opportunities for people in different situations worldwide.

e-tech caught up with Erlend Øverby, who leads IEC and ISO standardization work in the area of IT for learning, education and training (ITLET), to talk about latest developments and how standards can contribute not only towards the evolution of this industry, but to achieving SDG 4.

How is technology affecting the education industry as a whole?

AI and connectivity already bring many benefits to learning. For example, the more data we have, the better we can learn from it through analysis. Algorithms can mine and compare data sets from a variety of learning contexts, in order to find which activities give the best learning outcome. These include learning management systems, interactive learning environments, intelligent tutoring systems, educational games, and data-rich learning activities. This kind of tailored learning is possible because the data matches the competence level of the students with their learning activities. This can also be applied to teaching processes.

"Technology in itself does not provide learning, education or training. When things are put in context and managed by a 'teacher', then we have education. The use of technology must be put in a context that fulfils the goals of learning, education and training. Technology is nothing alone; it is how we choose to implement it that matters."

Learning institutions and the workplace require regular training for computer literacy, for teachers, educators, students and employees alike.

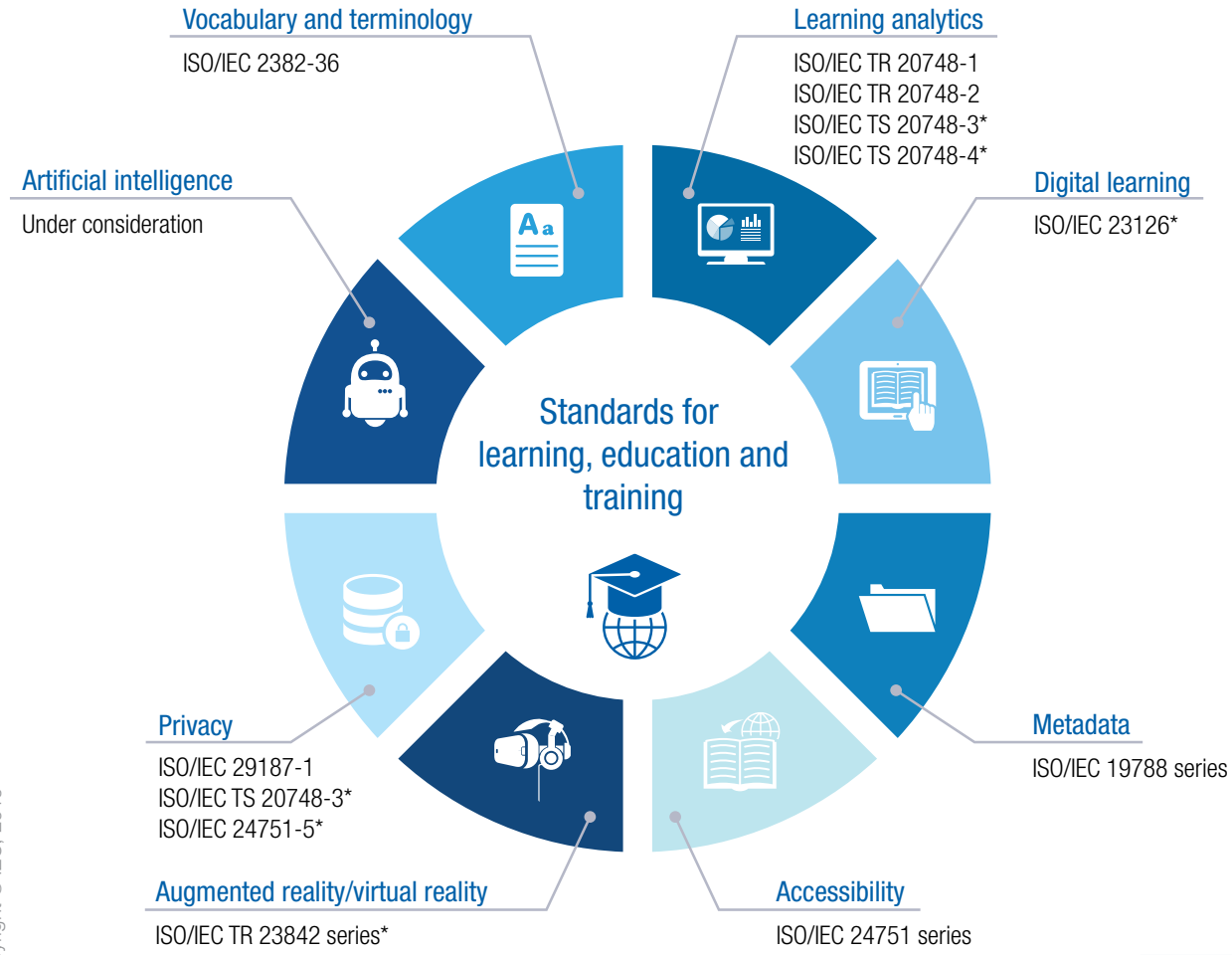
"There needs to be a shift in attitude towards seeing the computer as a tool for solving problems, and not only as a computing machine. This is what needs to be taught in schools, so that if there's something we don't understand or if we need more insights, we should know how to find the answers using technology."

Another issue is the development of proprietary technology packages, which may ultimately limit the choice of learning materials.

"Regulators need standards that will contain requirements to put forward to providers of IT programmes for schools, which must ensure the technology is independent of devices and ecosystems and is fully interoperable. This will avoid locking schools into a specific system and allow teachers to choose the best learning experience for its students."

Additionally, data security and privacy must be ensured for digital learning. For example, data created during the learning process may be stored and shared. If students role play, using online personas, which are hacked and misused, they could end up being wrongfully profiled as someone else.

JTC 1/ SC 36 standards being developed for learning, education and training



What are the challenges?

While many countries have a strategy for the use of digital resources in education, much needs to be done to incorporate IT into modern education systems around the world. Countries see the benefits that digital updated, relevant learning resources have over outdated paper school books. More standards are needed to ensure that all IT used for learning, education and training becomes seamless and free of hindrances and closed ecosystems. The ultimate goal should be for everyone to be able to participate, regardless of devices used, and have the best learning experience available.

"Our main challenge is to get more countries, developed and developing, as well as experts, to participate in our work. All countries with a digital education strategy should take an active role and give their perspectives. Equally, EdTech companies and startups, who plan to have a global presence, should see how their solutions could be easily adopted if IT-specific details are interoperable with other IT systems, for example, to better share data."

> "Through education, it is possible to improve the quality of life and create the basis for sustainable development."

The future of learning

Digital education is growing. Doctors can live stream complex surgeries to students worldwide, while disaster relief responders train for deadly diseases or urban emergencies using VR gaming programmes.

In the workplace, whether a factory, hospital or office, employees experience ongoing training, to be able to work with increasingly automated processes and understand new IT programmes.

IEC and ISO international standards for learning, education and training, will help advance the digitization of education, by ensuring soft- and hardware developers provide interoperability and data security, thereby broadening accessibility and enhancing the overall quality of global education.

In the beginning there was...terminology

Plans are afoot to make the Electropedia more accessible

By Catherine Bischofberger

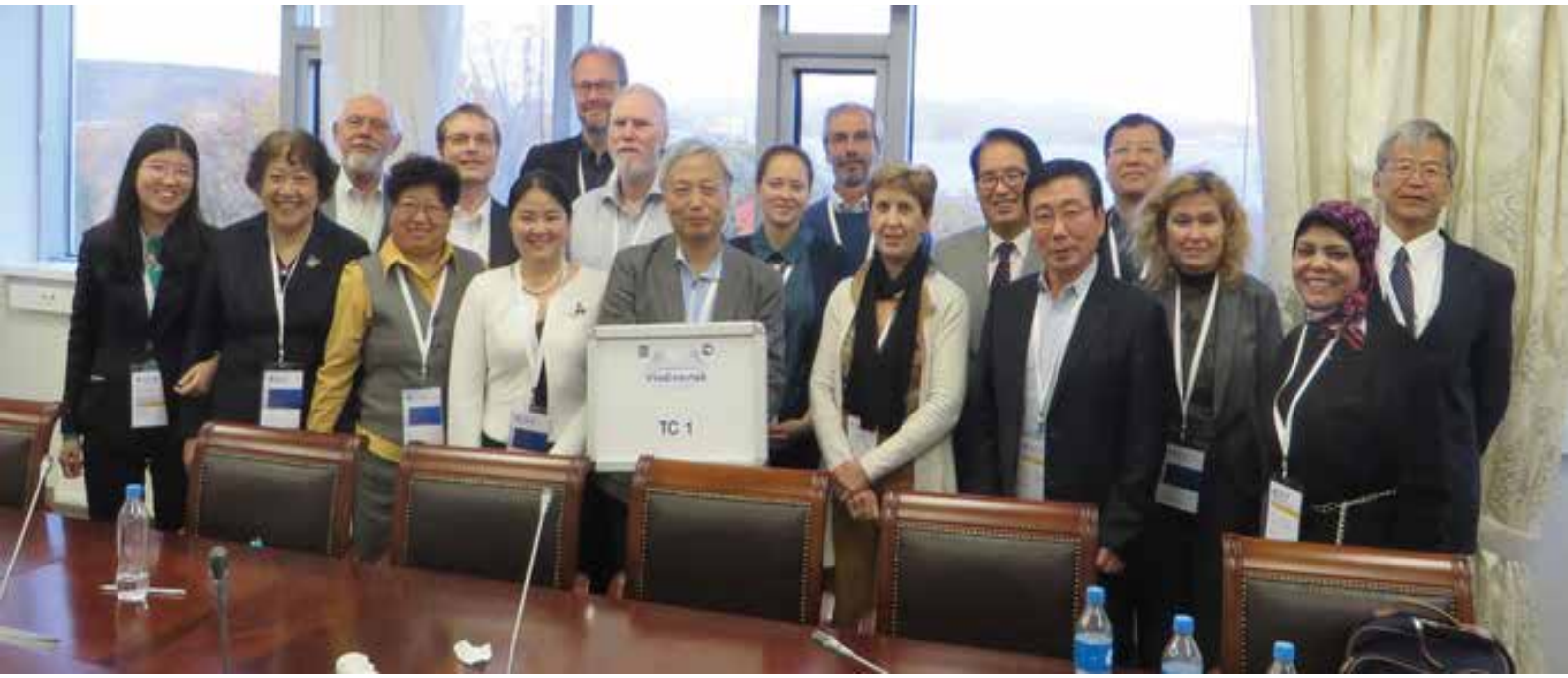
IEC Technical Committee (TC 1) is the earliest IEC TC and plays an essential role maintaining the International Electrotechnical Vocabulary (IEV) otherwise known as the Electropedia.

To quote the American astronomist Janna Levin, "ambiguity is very interesting in writing; it's not very interesting in science." In other words, what can be done to prevent or minimize the ambiguities of natural language from corrupting the precision of mathematics and science? This is where terminology can help: by providing a set of agreed definitions, concepts and terms in specific fields, it can reduce the level of ambiguity associated with words and sentences.

Electrotechnology is one of these fields. Experts in different countries around the world need to avoid ambiguity as much as possible when devising new electrotechnical devices and systems and especially when developing international standards.

e-tech caught up with Luca Mari, Chair of IEC TC 1, to find out the latest developments. "In our increasingly complex world, having a single, homogenous, well-established, harmonized body of knowledge related to terminology for the whole electrotechnical community is very important. IEC TC 1 is a horizontal TC which provides harmonization for all the terminology used by the various other TCs inside the IEC."

The reach of terminology, in his view, is often misunderstood. "Terminology



IEC works with ISO and other international organizations on the International Vocabulary of Metrology (VIM) (Photo: Wikicommons)

conveys the implicit message that it only deals with terms. But it is way more than that: it is about definitions as well as terms, and to agree on definitions we need to agree on concepts and meaning in order to understand each other."

It is important to agree on definitions, concepts and meanings in order to advance the development of electrotechnology

Available for free and constantly updated

This harmonized body of knowledge maintained by IEC TC 1 is the IEV or Electropedia. "Years ago, the IEC took the decision to make it freely available on the web so that anybody can consult it. Anyone at any moment can make a request for updating any single entry in the Electropedia and we validate it, technically, semantically and make sure it is harmonized with all the other entries. This allows the whole IEC community to keep the IEV as up-to-date as possible."

This crucial body of work is of great use to the whole IEC community but plans are afoot to make it more easily accessible to a wider audience. "We have sent a questionnaire to our members to ask them whether they agree that we should work towards expanding the intended users of the Electropedia to include people who are not directly involved in standardization work, teachers, students and translators, for instance."

> "Terminology helps reduce ambiguity by providing agreed definitions, concepts and terms in specific fields."

Prior to sending the questionnaire, a survey was conducted to find out what users think of the online tool. "500 people took part in the survey and they suggested a number of incremental changes. One of them was to make it more accessible to new types of users. Other suggestions comprised adding more examples and more references to external sources. This survey is part of a global push we made together with Technical Officer Joanna Goodwin to revive the strategy of TC 1."

An ongoing project is to provide a new generation Electropedia based on more recent technology. "We are looking at systems which are less vocabulary and more concept-oriented. One would still be able to find terms and definitions but the structure of the concepts behind these words and definitions would be more explicit. This would enable users to browse the Electropedia content in a more conceptual and efficient way. For instance, they could ask for all the examples of a given concept."

Working with metrology experts

Inside the Joint Committee for Guides and Metrology (JCGM), IEC cooperates with ISO, le Bureau International des Poids et Mesures (BIPM), the International Organization of Legal Metrology (OIML) and other international organizations on the International Vocabulary of Metrology (VIM). "The JCGM was created around 20 years ago based on the idea that something in common should be and could be exploited in metrology and lead to producing guidance documents about fundamental concepts of measurement. Everybody needs good reliable measurement results whether talking about electrotechnology, astronomy, quality management, for instance." Mari is one of the experts appointed by IEC in the international working group (WG) which produces the VIM since one of his other areas of expertise alongside terminology is the science of measurement. "I have two different roles but one feeds the other, so to speak."

The WG is currently working on the first draft of the fourth edition of the VIM which needs to be constantly updated. The recent decision of the BIPM member states to revise the International System of Units (SI) which changes the world's definitions of the kilogram, the ampere, the kelvin and the mole, is impacting the work on the VIM, as well as the Electropedia. "The statements by which the units are defined need to be carefully reviewed before being included in the Electropedia", Goodwin agrees.

The world is changing at a more rapid pace than ever and metrology and terminology are keeping up with the times, especially where electrotechnology is concerned.

Making IT sustainable

IEC and ISO join hands to develop energy efficiency benchmarks for ICT

By Catherine Bischofberger

ISO and IEC produce many joint standards which specify how to improve the energy efficiency of information and communication technology (ICT). A number of these publications deal specifically with the excessive energy consumption of data centres. Several UN sustainable development goals (SDGs) can rely on the benchmarks provided by these standards to measure progress.

Data centres use up a lot of energy (Photo: Wikimedia commons author: baltic servers.com)

We are increasingly reliant on different forms of ICT. Some of us are so addicted to our smartphones and tablets that we have withdrawal symptoms when we have to make do without them. On a macro level, ICT provides a number of tools which help industry and governments to adopt strategies aimed at improving the environment. Powerful algorithms can be used to optimize building resource consumption, for instance. Data generating sensors can enable cities to control the level of lighting they use. Somewhat paradoxically, these power-saving initiatives depend on the computing power generated by large data centres. These aggregated computer networks provide important services such as data storage, backup and recovery, data management and networking. ISO and IEC are working together to solve this paradox. Their joint technical committee (JTC 1) includes subcommittee (SC) 39, set up to prepare standards on sustainability for and by IT.

Power-hungry data centres

Large server networks are big consumers of electricity and generate a large amount of low-level heat. Not only do they require a lot of energy to function, they also need power to run the cooling and air-conditioning devices which enable them to perform at their best. While the heat generated by computing power can be repurposed and used for domestic heating for instance, routine energy management processes are implemented in the data centres themselves to reduce their overall energy and heat consumption.

While some forecasts predict a decline in the number of server factories, as edge and distributed computing solutions become more widespread in the next five years, most estimates expect total electricity demand for ICT to accelerate in the 2020s, partly as a result of the increased power usage of data centres. Jay Taylor, who heads JTC 1/SC 39, agrees. “Despite the recent and significant efforts to consolidate server factories, the fact of the matter is

that we have more data centres than seven years ago and this number is expected to continue to grow in coming years. And many data centres already consume as much energy as small cities."

Helping to meet UN SDGs

SDG 11 aims to make cities and human settlements more sustainable, SDG 12, to ensure sustainable consumption and SDG 13, to take urgent action to combat climate change. All require standardized benchmarks for improving sustainability. That's where the work of JTC 1/SC 39 can help.

Founded in 2012, the SC initially worked on a global effectiveness measurement tool for data centres, called power usage effectiveness (PUE). "There were a number of organizations, such as The Green Grid or the Standard Performance Evaluation Corporation (SPEC), which were developing specifications for data centres, but they were all going down different routes. That's how we identified a need for an international standard that could be applied across Asia, Europe and the US," Taylor explains.

The work on the PUE led to the publication of ISO/IEC 19395 which facilitates the resource monitoring and control of smart data centres. The standard paves the way for the joint or group monitoring and management of the three different resources used in data centres – IT, electrical power and cooling fluids – which are most often managed separately. Thanks to the publication, each server in the data centre can be assessed according to its computing, energy consumption or dissipation aspects, a more comprehensive and energy-efficient way of managing resources than what was previously available.

"I consider it my job to provide practical and usable tools to be able to assess large energy consumers such as data centres. These tools can be then be used to help reduce our impact on the environment," Taylor says.

Never duplicate!

SC 39 had a hectic year in 2018. It issued nine publications, most of which were technical specifications, part of the ISO/IEC 22237 series. "We developed these specifications based on the EN 50600 standard, published by the European Committee for Electrotechnical Standardization (CENELEC). EN 50600 gives comprehensive guidelines for the construction and operations of data centres in Europe. My view was that we should work within the framework of the ISO 14000 family of standards on environmental management, produced by ISO/TC 207. For instance, we wanted to include specifications relating to the operation of data centres in areas prone to earthquakes. We received a lot of input from our Japanese colleagues on that aspect. I would describe the ISO/IEC 22237 series as a set of guidelines which provides data centre operators and owners with a practical methodology they can use when they set up in different countries across the globe."

According to Taylor, collaboration underpins the whole work ethos of the SC. "The first thing I do before we start working on a project is to check whether there are any experts already working in the field and if there are, I make sure I get in touch with them. They might want to get involved with us or they might think that a standard is inappropriate for a number of reasons. We can't work in a vacuum. I don't own standards, we collectively do and we all benefit from them."

Taylor cites several examples: "We collaborate with JTC1/SC 38, which prepares standards on cloud computing, we consult with JTC1/SC 27 on cyber security, you name it…The idea is to not duplicate standards. We were asked to consider developing standards for IT-related electronic product environmental assessment but I turned the suggestion down because colleagues in IEC TC 111: Environmental standardization for electrical and electronic products and systems, are already doing that, and have a broader scope than ours. But I certainly would not mind helping TC 111 experts with their work."

> "Many data centres already consume as much energy as small cities."

A future without zombie servers

The SC is working on specifications relating to the energy efficiency of server storage systems. Zombie servers, which suck up power without doing any useful work, can be an aspect of some of the less efficient data centres. Although these energy wasters are more difficult to find in the more recent data factories that use a uniform computing architecture and can scale up to thousands of servers, energy efficiency adjustments can be still made. "The idea is to look at which servers are idle and to switch them off at certain periods of the day in order to save energy. Algorithms can be used to predict peak usage, when maximum server power is required. They can shut servers down remotely in off peak periods. One of the problems we have, however, is that unlike your average PC or laptop, servers are never totally idle, even when they are not actively processing information," Taylor explains.

SC 39 is working to bridge the gap between the increasing use of computing power and the growing requirements for decarbonization. As Jay Taylor puts it, "We are trying to get equipment to consume less energy while producing useful work which could lead to our overall energy reduction."

Balancing privacy, security and convenience in mobile devices

Industry, governments, regulatory bodies, and consumers need international standards for biometric authentication technology

By Alan Hodgson, Chair IEC TC 119: Printed electronics

Mobile devices have changed society and the way in which we interact and exchange information. For example, the mobile phone has rapidly evolved from being purely a telephone to the complex smartphone systems of today. This evolution looks unlikely to stop in the foreseeable future with a new generation of mobile, wearable devices for the future.

Having a mobile device with significant sensor, processing and communications capabilities has proved to be attractive to a wide variety of applications, particularly in combination with the capability to link information and identity. However, the challenge is for users and industry to find the balance between ensuring the privacy and security of personal data, required to use these different applications, while maintaining user convenience. The role for international standards is to make a significant contribution to addressing these issues and facilitating the wider implementation of applications with all of the above capabilities.

Authentication – from PIN codes to biometrics

One of the early challenges with mobile devices was the need to verify that the user is entitled to access the device. Early generation smartphones required the input of a personal identification number (PIN) code, to deter theft or unauthorized access to services. However, the capabilities now built into smartphones allow identity verification by the acquisition of biometric data.

A good example of the use of biometric authentication is the fingerprint reader, an embedded device forming part of a trusted system to guard against software attacks. From the consumer perspective it provides a convenient and secure method of verification and has a user convenience advantage over PIN keying systems.

However, smartphone systems have the capability of going much further, using embedded subsystems to transition from fingerprint recognition to vision-based biometrics such as iris patterns and facial features. There is a technology trend towards further form designs of wearable smart devices where biometric authentication will be the norm. Innovations in IoT, Smart Cities and

Mobile phone applications may eventually be used to replace ID documents such as passports and driver licenses (Photo: Reconnaissance)

electronic retail suggest a growing need for standardization on the "security vs user convenience" question and to provide guidance to the value chain.

The need for technology standardization

Increasing numbers of applications are being developed for the wearable smart device platform, starting with the smartphone. However, as increasing numbers of these use mobile identity authentication through biometrics on a single platform, thus, if one application is perceived to be compromised it could affect the public perception of all the applications using the wearable smart device platform. International standards for biometric authentication could play a key role in protecting public confidence in this technology. This need for technology standardization comes from three directions:

Consumer needs

From a consumer perspective, the transition from PIN numbers to biometrics was motivated by increased convenience, with the belief that the balance with data security had not markedly changed. However, stories in the press around large-scale data theft and cyber security issues are starting to diminish this belief. For the user, the issue is one of trust; which can be impacted by both real and reported issues. International standards can help reassure customers that their privacy and security is being protected.

Government and regulatory body needs

National programmes are being introduced that use biometric identification as a gateway to government services and to facilitate mobile ID for driver's licenses and passport programmes. Governments are also responding to the need for security of critical infrastructures, with initiatives like the Directive on security of network and information systems (NIS Directive) Europe. The International Air Transport Association (IATA) aims to use biometrics to provide a seamless travel experience through airports using only mobile devices.

In the absence of truly international standards, the rules of engagement look likely to be set by a series of country- and industry-driven initiatives. Various industry consortia are already active in this area, but it would be logical for all concerned if this technology were the subject of international standardization.

Industrial needs

Industry sees both a consumer and government need for mobile identity authentication solutions that it is keen to fulfil, but there is currently no holistic framework from international standards. It has noted the consumer frustration with multiple passwords and seeks to provide

A good example of the use of biometric authentication is the fingerprint reader

solutions. Consortium reports contain a call to action for consolidation around the use of standards for mobile ID authentication and note that standardization is still in an early stage.

The common thread emerging here is the need for international standards to support industrialization.

Achieving mobile data security and privacy with standards

Effective standardization for mobile data security and privacy will require a systems approach due to the overlap with emerging systems such as IoT, Smart Cities and Active Assisted Living. Security and authentication look likely to be key to the smart automotive sector too.

This complexity can be seen as a benefit in that some of the necessary standardization work is already in progress and a challenge because the work is underway in disparate international and industry standards bodies with their own issues and communities.

Failure to protect the privacy and security of consumers will impact on their standard of living and their future interaction with the electrotechnical environment. The smartphone, as the first in a disruptive series of mass market mobile and wearable devices, has made a step change in society's ability to exchange information and in turn develop and prosper. For example, smartphones have led to widespread and convenient access to data, information and services, facilitating new business models and commercial transactions. International standards for these innovative technologies have the capability to make a substantive economic and social contribution while maintaining the balance between human and technological development.

The relevant structure

A large number of industries are involved in mobile biometric authentication, including hardware, software and application. From an international standards perspective, though a substantial amount of detailed work exists or is under way at industry and national level, standardization will require more liaisons between relevant IEC and ISO standards committees.

For example, some of the issues around data security and privacy are within the scope of the IEC and ISO joint technical committee for information technology (ISO/IEC JTC 1) whose subcommittees (SCs) are working on key technology areas, such as biometrics (SC 37), artificial intelligence (SC 42) and personal identification in (SC 17).

> "Industry and users must balance privacy and security of personal data while maintaining user convenience."

Additionally, IoT issues are likely to become very important as is the imaging testing structure, which has been developed in ISO TC 42: Photography. Some of the future design factors around wearable devices are being charted by IEC TC 110: Electronic displays. One early task will be a gap analysis to define what is missing.

A logical option for bringing these together in a central forum would be under IEC TC 124: Wearable electronic devices and technologies, which has most of the relevant liaison structure in place, or alternatively some of the ISO/IEC JTC 1 groups highlighted above.

Constructing a roadmap for future work

This article outlines the need for international standardization to protect the privacy and security of the highly personal biometric data of individual consumers, with sound commercial and governance arguments.

From a commercial perspective, research published in 2017 by a leading payment solutions company on biometric-based payment solutions, showed that the absence of a single standardized form of biometric authentication is an impediment for implementing these solutions. From a governance standpoint, during the days of hard copy documents, governments dictated how identity was verified, using driver's licences and passports, however now they are losing control to smartphone manufacturers and apps.

It also highlights areas where work is already in progress, how this could be coordinated, and notes that other emerging areas could benefit, for instance, autonomous and connected vehicles. International standards could make a significant contribution to the social and technical environment of the emerging connected society.

Significant challenges arise due to the scope and complexity of the issues involved. There is a need to assess the gaps in standardization, which are relevant to our requirements, and to work with industry to construct a roadmap for future work.

A plan to do this will be proposed during an industry meeting of a new event called Digital Document Security Conference to be held in May in Berlin. The Conference aims to bring together some key industry and government players to examine the role that international standards may play in this debate.

Safety and performance assurances are key to solar PV investments

Certification to IEC international standards instills confidence

By Thomas Sauer, Convenor WG 004 and WG 404, IECRE

A significant number of solar photovoltaic (PV) power plants underperform for various reasons, including deterioration, or to the point that the financial viability of the PV power plant is at stake.

Performance risks are everywhere. Prevalent causes for defects are related to production of components and installation, while operations and maintenance play a significant role when it comes to performance losses. Hence, issues involving performance and/or safety can occur anytime from inception through to decommissioning.

As part of overall PV power plant project due diligence, the financial sector currently

PV load testing simulates heavy snow which can accumulate on a sloping roof (Photo: TÜV Rheinland)

bases its investment decisions and lending commitments etc., on technical assessment reports.

Answering the need for a global certification system

Until a few years ago, no encompassing international standards existed for quality assurance or assessment reports. Depending on the assessor, these reports could vary significantly in terms of thoroughness, accurateness, completeness, reliability, validity and, transparency. This led to two possibilities:

- Quality assurance measures were not necessarily sufficient to ensure that the planned performance would actually materialize over the typical planning timeframe of 20 or more years.
- The diversity of technical assessment reports (lacking any standards) resulted in a high workload for investors, such as banks, and more importantly, in uncertainties around evaluating the true risk exposure of a PV power plant project.

IECRE is established

This status quo motivated IEC member bodies to establish IECRE, the IEC System for Certification to Standards Relating to Equipment for use in Renewable Energy applications. It covers the marine, solar PV and wind energy sectors, and uses IEC International Standards developed by the technical committees for these.

IECRE certification, offers a common platform on a systems level for quality assurance, which enables fair and efficient competition. Under the System, the entire lifecycle of a PV power plant can be certified, from initial design aspects to annual inspections and ultimately asset transfer.

The potential for a rating system

Currently, IECRE is considering the development of a technical rating system for PV power plants. This follows the analysis of several thousand insurance claim cases, which revealed that internally caused damage represents approximately 20% of all claim cases and equally importantly, the amount of internally induced damages significantly increases with the service life of a PV power plant.

LCOE is the measure of a power source that allows comparison of different methods of electricity generation on a consistent basis. The continued reduction of LCOE seems to be ongoing and may be a cause of a growing number of quality issues in the field. The only viable way to ensure successful business for all stakeholders at such levels of LCOE, is to continue reducing actual costs, while simultaneously implementing effective quality assurance practices.

A key point in the race to drive cost down at acceptable quality levels is to establish standards that are valid across the industry, including quality assurance and conformity assessment standards. IECRE tests and certifies renewable energy equipment against IEC International Standards. The addition of a rating system could help assess the risk exposure, which goes along with PV power plant investments, in a more effective and uniform way.

Find out more: www.iecre.org

Fostering sustainable consumption and production

Relevance of IEC and IECQ work in SDG 12

By Claire Marchand

In the last 50 years, the global population has consumed more goods and services than the combined total of all previous generations. This has fostered economic growth and improved the quality of life for many while having a negative impact on the environment. However, consumption patterns differ significantly between developed and developing nations.

History in brief

The unsustainable consumption patterns that were the norm for many years were an important factor in destroying the environment, drastically depleting stocks of natural resources, contributing to social problems such as poverty, and hampering sustainable development efforts.

In 1992, the United Nations Conference on Environment and Development, held in Rio de Janeiro, Brazil, recognized sustainable consumption and production (SCP) as an "overarching theme to link environmental and development challenges".

In 1994, the Oslo Symposium on Sustainable Consumption came up with a definition of SCP: "The use of services and related products, which respond to basic needs and bring a better quality of life while minimizing the use of natural resources and toxic materials as well as the emissions of waste and pollutants over the life cycle of the service or product so as not to jeopardize the needs of future generations".

In 2015, the United Nations General Assembly adopted 17 Sustainable Development Goals (SDGs), covering a wide array of social, economic and environmental development issues, to be achieved by 2030. IEC has identified 12 out of the 17 SDGs where its standardization and conformity assessment work can make an impact. One of these goals is SDG 12: Sustainable consumption and production.

IEC work for SDG 12

The IEC can contribute to several of the targets set by the UN for SDG 12, including:

- → By 2030, achieve sustainable management and efficient use of natural resources and substantially reduce waste generation through prevention, reduction, recycling and reuse.
- → By 2020, achieve the environmentally sound management of chemicals and all wastes throughout their life cycle, in accordance with agreed international frameworks, and significantly reduce their release to air, water and soil in order to minimize their adverse impacts on human health and the environment.
- → Encourage companies to adopt sustainable practices and integrate sustainability information into their reporting cycle.
- → Support developing countries to strengthen their scientific and technological capacity to move towards more sustainable patterns of consumption and production.

Many IEC technical committees (TCs) develop international standards in a wide range of technological fields linked to sustainable production, for example, TC 21: Secondary cells and batteries, TC 35: Primary cells and batteries, TC 59: Performance of household and similar electrical appliances, TC 100: Audio, video and multimedia systems and equipment, TC 105: Fuel cells technologies, TC 108: Safety of electronic equipment within the field of audio/video, information technology and communication technology and TC 113: Nanotechnology for electrotechnical products and systems.

Controlling the use of hazardous substances

IEC International Standards together with the IEC Conformity Assessment Systems can help control the use of hazardous substances in the life cycle of electrical and electronic devices.

IEC TC 111, deals with environmental standardization for electrical and electronic products and systems and has published a number of crucial international standards. For instance IEC 62474 establishes the requirements for reporting the substances and materials included in electronic and electrical products. It also facilitates the transfer and processing of this data by defining a common data format which applies to exchanges in the supply chain. The standard comes with a validated open database, which includes a list of substances, substance groups and common material classes.

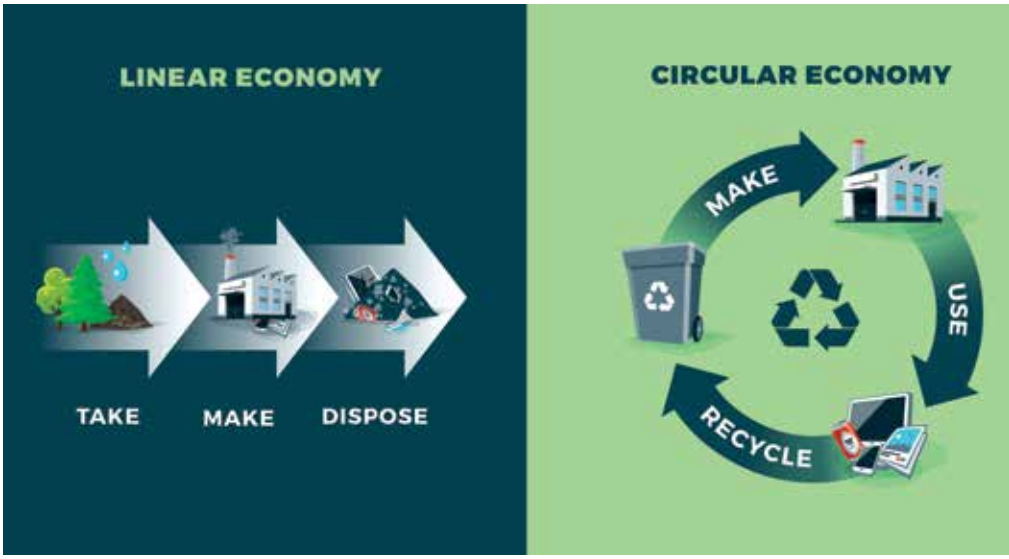
Another is IEC 62430 which provides guidelines for minimizing the adverse environmental impact of devices throughout their lifecycle. The publication defines environmentally-conscious design for all electrical and electronic products, for instance which materials are used, the quantity of energy consumed to make them and their rate of recyclability.

Complementing each other: standards and conformity assessment

Conformity assessment programmes also exist that allow manufacturers and suppliers of the electronic components used in all modern devices to ensure that their products have extremely limited amounts of hazardous substances or are hazardous substance-free.

A global solution

IECQ, the IEC Quality Assessment System for Electronic Components, established the IECQ hazardous substance process management (HSPM) scheme, which is a technically based management systems approach to implementing and maintaining hazardous substance-free products and production processes. It enables component manufacturers to give suppliers the means of demonstrating, through third-party assessment, that their electrical and electronic components and assemblies meet specific hazardous substance-free local, national and international requirements.



One of the targets of SDG 12 is to substantially reduce waste generation through prevention, reduction, recycling and reuse

Many companies work to attain IECQ HSPM Certification to IECQ QC 080000, IEC Quality Assessment System for Electronic Components (IECQ System) - HSPM System Requirements. The fourth edition clarifies how to manage hazardous substances other than by removing restricted substances and avoiding their use in products.

Some advantages to using IECQ QC 080000 include:

- → adaptation to global increasing hazardous substances legislation. For example, additional controlled substances, change control, product recall, as specified by the REACH regulation, the information communication within the supply chain, and notification to the European Chemical Agency (ECHA) about substances of very high concern (SVHC);
- → enhancement of documented information requirements in response to the applicable statutory and regulatory obligations. For example, requirements in the re-casted RoHS, such as compliance assessment, preparation of self-declaration, use of markings, etc. can now be managed through IECQ QC 080000;
- → alignment with ISO 9001:2015, Quality management systems – Requirements, and has adopted ISO Annex SL, defining the new high level structure for all ISO management systems standards.

Find out more: www.iecq.org

Tackling explosion and fire risks

IECEx-certified equipment helps protect rescue teams in the aftermath of natural or industrial disasters

By Claire Marchand

Natural disasters strike at regular intervals on our planet. Every year natural disasters leave huge areas totally devastated. Many experts point the finger at climate change for the increased intensity of storms, flooding and drought that affect millions of people throughout the world.

Increasing occurrences

The 21st century has already seen its share of major catastrophes – the 2004 Indian Ocean earthquake and tsunami, the 2010 earthquake in Haiti, the 2011 earthquake, tsunami and nuclear power plant explosion in Japan, Hurricane Sandy hitting the US East Coast in 2012, the 2015 earthquake in Nepal, or the cyclones, landslides and floods in the Philippines in 2018 and early 2019, to name a few.

This quick-deployment RXR-M80D-1 fire extinguishing robot can be used in disaster areas such as chemical plants, subway tunnels, gas leakage, and so forth (Photo: Beijing Topsky Century Holding Co. Ltd)

To make matters worse, natural disasters may trigger industrial or accidental disasters. While the former may be deadlier and more destructive, the succession of tragic events may lead to the total destruction of large areas and an even greater number of fatalities.

This occurred when heavy rainfall following a typhoon caused the collapse of the Banqiao dam in China in 1975, resulting in the immediate death of more than 25 000 people and, indirectly, of 250 000 later.

Explosion-proof gas leak detector (Photo: Direct Industry)

A category 4 or 5 hurricane or an earthquake of high magnitude will most certainly cause extensive damage to critical infrastructures: energy generation, transportation, food production and water supply, public health, telecommunications and the economic sector in general. This damage may result in gas or oil leaks, fires or explosions, increasing the number of casualties and the risk of further destruction and harm to the environment.

Accidents caused by explosions may also happen in chemical plants, grain silos, sugar refineries and many other sites, such as laboratories.

In the aftermath of such incidents, rescue teams are faced with the challenge of finding survivors in extremely harsh conditions. They have to protect themselves and their equipment from fires and explosions, going through the rubble which may be unsafe; always conscious of the risks they're exposed to.

The IEC at the forefront in standardization…

To prevent these accidents, specially designed and properly installed and maintained equipment and systems are essential. International standards for these are prepared by IEC TC 31: Equipment for explosive atmospheres. TC 31 has a complete series of international standards that cover all specific requirements for Ex electrical and non-electrical equipment and systems. These include general requirements and 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.

…and conformity assessment

Protecting installations and people against risks from explosive atmospheres is not only the result of comprehensive standardization work from IEC TC 31. It is also due, to a great extent, to the work of IECEx, the IEC System for Certification to Standards relating to Equipment for use in Explosive (Ex) Atmospheres.

IECEx in a nutshell

IECEx provides:

- → a robust and credible system for the operation of standardized certification schemes
- → a dedicated IECEx website
- → on-line certificates in real time
- → a forum for the industry and stakeholders to have a voice in the running of the IECEx schemes

IECEx has the mechanisms in place to help industry, authorities and regulators ensure that electrical and non-electrical equipment as well as the people working in Ex locations benefit from the highest level or 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.

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.

The global solution for Ex environments

Taken together, standardization work by IEC TC 31 and the IECEx system provide a global comprehensive solution to address many of the risks found in Ex environments. Their work is ongoing, as new risks arise and as new solutions are found.

This work is also relevant to the United Nations Sustainable Development Goal (SDG) 13: Climate action.

For more information: www.iecex.com

Protecting critical infrastructure: the importance of making power grids secure-by-design

IEC 62351 standards for secure-by-design power systems communications

By Moreno Carullo

For the second year in a row the World Economic Forum has listed cyber attacks as one of the top five global risks, and highlights that an attack on a country's electricity system could potentially have devastating effects. Power grid risk has increased due to expanded connectivity to IT and other systems, exposing them to more threats. As the same time, threat actors are focusing more on critical infrastructure attacks, and benefiting from the availability of malware toolsets on the internet.

Unfortunately, defending today's power systems is challenging because they typically use communication protocols optimized for bandwidth and efficiency, with zero or simple security protections. Furthermore, many grids have received little to no security enhancements post deployment.

To help counter this problem, in the early 2000s IEC Technical Committee (TC) 57, a group devoted to power system management standards, started working on how to make power grids secure-by-design. Working Group (WG) 15 was formed to evaluate the requirements from a technology perspective, and define a standard way to implement them.

I've been a member of WG15 since 2015, and led the Nozomi Networks hosting of the WG15 Winter '17 meeting in Lugano, Switzerland. As we approach the group's next meeting this spring, I thought it might be helpful to inform you about these standards and provide an update on their status.

Overview of WG15

First a brief overview of WG15. The group is made up of ICS operators, SCADA engineers, security specialists, and networking experts from 90 organizations worldwide. Members include ABB, Siemens, Schneider Electric, General Electric, Enel, IREQ, Nozomi Networks and others.

Together we have identified the components needed for a secure-by-design power system. These include the end-to-end encryption principle, the definition of roles for all users and identity management, and pervasive monitoring of the system itself.

Another duty of WG15 is to review other Working Group's documents to assess and validate cyber security aspects.

Status of the IEC 62351 Standards

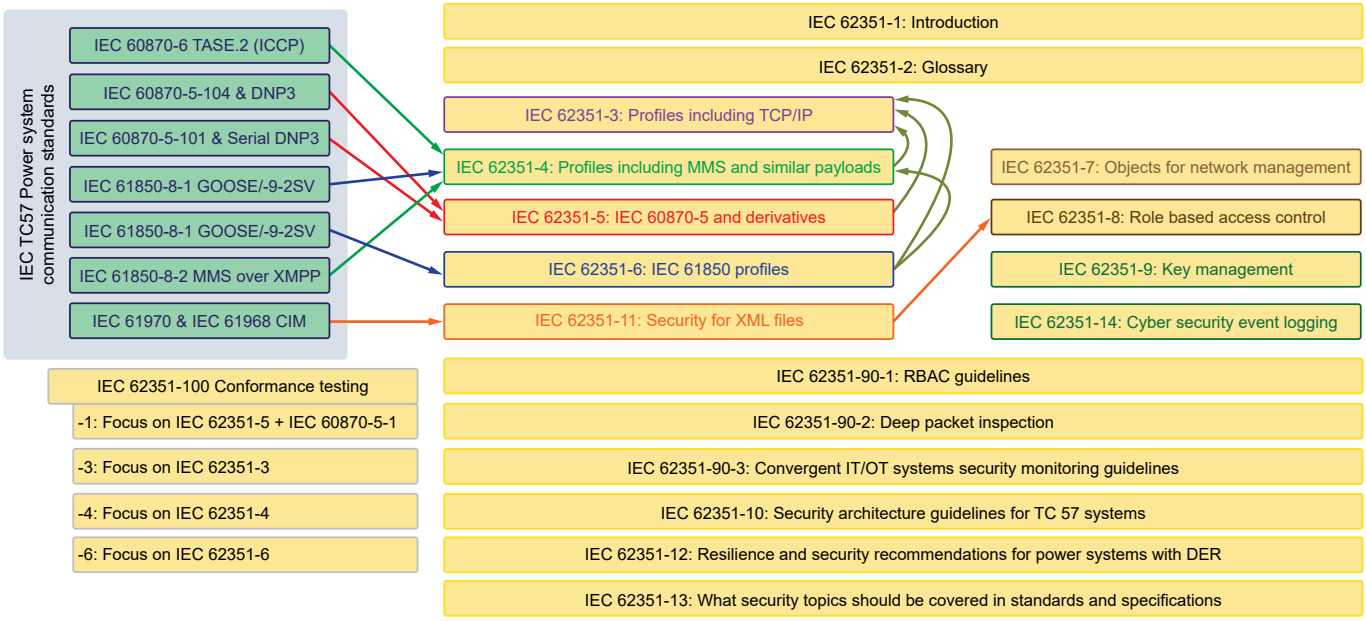
Currently, the 62351 family of standards (see *IEC 62351-1: Introduction* for an in-depth overview) depicts the architecture of a secure power system and standardizes its protocols and components. An interesting read for a better overview of it is: *IEC 62351-10: Security Architecture Guidelines for TC57 Systems*.

To truly obtain effective end-to-end security, secure protocols must:

1. establish secure connections based on some trusted private key of the actors, and
2. have a repository of actors allowed to act inside the system.

The former is standardized in *IEC 62351-9: Key Management*, while the latter is standardized in *IEC 62351-8: Role-based Access Control* (RBAC), and further reviewed and explained in *IEC TR 62351-90-1: RBAC Guidelines*.

IEC 62351 security standards and their interrelationships with IEC TC57 standards



Communication protocols play a key role when it comes to resolving “common OT protocol issues”, such as the lack of authentication, integrity checks, confidentiality, etc. Although some OT protocols already address these areas, it is very common within the OT world to have very low “protocol security”, that is *insecurity-by-design*. For this reason, the whole set of power system protocols designed under the IEC umbrella has been extended to provide end-to-end encryption, identity management and RBAC.

Of course, the role of existing secure protocols like transport layer security (TLS) play a big role, but many other aspects have been tackled to define all possible facets of a secure architecture. These include:

- → Using certificates for all devices
- → Standardizing how to behave with rare long-standing TLS sessions
- → Creating completely new encryption sub-protocols for specific use cases

Monitoring Power Systems with IEC 62351 Standards

In the IEC 62351 family of standards, end-to-end encryption is certainly an important feature, but system monitoring plays a key role as well. Several parts are in fact devoted to monitoring the healthy status of a power system:

- → Part 7 (IS, International Standard) is focused on the active monitoring of intelligent electronic devices (IEDs) and other power system components. A generic approach (via UML) has been used in the standard to define what needs to be monitored. Additionally, a pragmatic simple network management protocol (SNMPv3) is provided for monitoring a dedicated set of management information bases (MIBs).
- → Part 14 (in draft right now) is focused on the logs that power system components should generate. Standardizing the format and the semantics helps lower the cost of implementation and maintenance of power grid log management solutions.
- → Part 90-2 (TR, Technical Report) is focused on how deep packet inspection (DPI) of IEC 62351 encrypted channels can be carried out. The document explains the state of the art of existing DPI techniques and how they can be applied to monitor IEC 62351 channels today. It is also the reference work for analyzing changes to apply to protocols and technologies to enable easier and more secure DPI of communications.

A lot of discussion has occurred on this topic because of its controversial nature. Nonetheless, deep monitoring of encrypted communications in a machine-to-machine framework offers more advantages than not, including full visibility of ongoing activities.

- → Part 90-3 (in draft right now) is focused on putting the three parts above together. It aims to provide practical examples of how to monitor a power system in order to obtain deep visibility and support forensic analysis, consequently enabling a more dependable and resilient system.

Super cool cables

New standard to prepare the ground for the use of superconducting cables

By Catherine Bischofberger

IEC 63075 is a brand new standard which specifies tests methods for superconducting alternating current (AC) cables. The forward-looking document is published by IEC Technical Committee (TC) 20.

Energy-efficient transmission

Superconductors are materials which generate minimal energy losses when transmitting electrical power. Superconductivity occurs at extremely low temperatures and superconducting cables use liquid nitrogen as a coolant. The experts involved are dealing with temperatures ranging from 65 K to 80 K (-208 °C to -193 °C).

Superconducting cables are able to transmit large quantities of electrical power in a highly energy-efficient way. They have therefore become an attractive option to replace conventional cables. They are also lighter and more compact, making them easier to install. One of the drawbacks is that these cables cannot be used over long distances because of the problems implicit in supplying the nitrogen they require for cooling purposes. They are also more expensive to manufacture than conventional cables.

Testing superconducting cables at the Karlsruhe Institute of Technology (Photo: KIT)

On the other hand, their smaller dimensions and energy-efficient properties make them ideally suited for high-load centres, such as cities or dense business areas. A number of demonstration projects have already been successfully set up, in China, Japan, South Korea, Germany, the Netherlands, Russia and the US. But commercial implementation is lagging behind, mainly because of the cost of the technology.

A requirement for standards

International standards can help to lower the cost of superconducting cables by establishing benchmarks that can be used by the cable industry anywhere around the world. Guidelines would help to streamline manufacturing procedures making the whole production process less expensive. The IEC recently published IEC 63075, Superconducting alternating current (AC) power cables and their accessories for rated voltages from 6 kV to 500 kV- test methods and requirements. The 54-page document is a first in this area and is the result of the work of experts from two IEC

technical committees, IEC TC 20: Electric cables, and IEC TC 90: Superconductivity. "Several members of the project team which developed the standard were also active in different TC 90 working groups. TC 90 took the initiative to develop the standard and TC 20 then took over as the standard is specifically related to cables," explains Dr Mark Stemmle, who heads the IEC TC 20 project team.

IEC 63075 is based on the work of the International Council for Large Electric Systems (CIGRE). "CIGRE technical brochure (TB) 538 was the basis for discussions in the project team. Most of the test recommendations of the TB were transferred to IEC 63075 and we also introduced additional tests which were missing in the CIGRE work," said Stemmle.

IEC 63075 defines a wide number of tests for cables both before and after installation. They include voltage, bending and thermal cycle tests and heat invasion of cryostat. According to Stemmle, future editions of the standard could also include testing of the liquid nitrogen cooling systems. "There are more and more superconducting cable projects coming up and we will be monitoring the progress of these projects. Depending on requirements, we could include these additional tests in a new edition."

Stemmle does not think that superconducting cable technology will be used over long distances in the near future, as major technology hurdles still have to be overcome for that scenario to become viable. He agrees, however, that city centres are where superconducting cables could initially meet commercial requirements. "They are ideally suited for areas where there is not much space for installation. An example is the Ampacity project in Essen, Germany, where a medium voltage superconducting cable was used".

The project linked two Essen substations with a one km-long cable. After operating for three years, the analysis of the trial was published in a report issued during the summer of 2017. One of its main findings was that the technology was mature enough to operate under real grid conditions.

The business case for superconducting cables is gradually being made. IEC 63075 is helping by anticipating market requirements. "With this standard, there is now a unified approach to testing superconducting cables which should have a positive impact on costs," Stemmle concludes.

Smart devices

From VR headsets to agricultural robots, smart devices are being used in an increasing number of industries. In the upcoming issue of *e-tech* we look at some of the ways in which these devices are being used to make laborious tasks easier, or are helping in operations as diverse as urban planning and complex surgeries, making them more efficient and precise.

IEC 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