Future of transport

TECHNICAL COMMITTEES
Smart buildings for smart living
Evolving with digital transformation

INDUSTRY SPOTLIGHT
From driver to driven - and how to get there

TECHNOLOGY FOCUS
Protecting railway networks from cyber threats
Clean air moves boost interest in electric trucks
Harvesting energy from roads
Transport of the future
The future of transport

Could the next taxi you hail be a drone, or will it be a self-driving vehicle you order from your smartphone?

*By Antoinette Price*

**Though this scenario is still some way off, the first unmanned taxi drone had a successful maiden run in Dubai last September.**

Whatever the mode of transport, rapidly advancing technologies are changing our perceptions of how we will travel in the future.

Today, connected cars deploy diverse artificial intelligence applications, which will ultimately enable vehicles to become fully autonomous. It remains to be seen whether we will own our cars in the future, or if we will ride hail and ride share our way around town, as automobile manufacturers rethink business models.

As cities become smarter, infrastructure is becoming more intelligent. This is important for growing and aging populations which will rely on public transport more than ever before.

Faced with the need for greater public transport capacity, increased traffic congestion and pollution, transport authorities around the world are using new technologies to find solutions. For example, the digitalization of railway networks is enabling conflict-free schedules to be created more flexibly, the ability to adapt capacity to passenger requirements (peak and off-peak times), while saving costs and delivering more efficient, reliable services on the same train tracks.

However, at the same time, transport manufacturers and providers must ensure personal data privacy and the security of all their connected systems and devices. This will be vital to the success of self-driving vehicles.

This issue of *e-tech* looks at the status and future of vehicle communications and automated driving from business, technology and regulation perspectives, covering the role of connectivity, cyber security, artificial intelligence and more. It also examines what cyber security measures are being taken for modern railway networks.
FOCUS OF THE MONTH - The future of transport - Issue 2/2018

This issue of e-tech looks at how technology is changing transport and its infrastructures, including autonomous and electric vehicles, and the digitalization of railway networks.

Other themes cover the new European Union General Data Protection Regulation and examine the evolution of smart buildings.
New technology is revolutionizing the way we will consider transport in the near future. Flying cars are one of the options on the cards and a number of IEC Standards can help the various industries involved.

Congestion is the bugbear of every car driver, especially in big cities. Commuting to and from work often involves snail’s-pace progress through traffic jams, bumper to bumper with other cars. New technology is helping to transform the way we will use transport in the not so distant future. Various companies are hedging their bets on different scenarios.

For some, we will continue to own cars but these will gradually become more autonomous, taking over from us when we need them to, using artificial intelligence to guess our moods and, a bit like friendly robots, getting to know our preferences to enable them to adapt to our requirements. For others, we will cease to own cars, especially in big cities where parking space is at a premium, and instead, fleets of autonomous vehicles will be either rented or booked in the same way as a taxi. For yet a third group of visionaries, the future of transport will involve some form of flying. How better to avoid congestion than to be able to drive for part of the journey but then take off when necessary?

While huge legislation, insurance and safety certification issues must still be addressed, a number of companies have moved forward with the technology enabling car and aircraft to merge. Some of these developments were on show at the 2018 Geneva International Motor Show (GIMS).

Pie in the sky?

Pop Up is a project which was initially launched last year and results from the work of three different companies – a German automotive giant, an Italian design and engineering outfit and a major European aircraft manufacturer.

While the project remains conceptual, the technology behind it has greatly moved on from where it was a year ago. The aerodynamic design of the air module and the rotor ducts has been refined so as to improve performance and reduce fuel consumption in cruise mode. A functional locking and latching system has been designed to couple the ground capsule with the air module. “This is very complex because air and ground vehicles respond to completely different operating and safety dynamics,” explains one of the engineers involved in the project.

A lot of work has gone into making the device lighter, using a featherweight mesh material. Engineers at GIMS were also demonstrating a clever human machine interface inside the capsule, based on facial recognition and eye-tracking. “This is the second chapter in the story. We have worked with a third party to develop a personal assistant you will interact with in the capsule, using your eyesight to choose various travel and entertainment options,” explains Emanuele Rivella, a systems engineer at the Italian outfit. According to Rivella, the ground capsule will operate like most other autonomous vehicles, using sensors, cameras, radar and LIDAR (light detecting and ranging) technology. It will also be fully electric. Data protection issues are also being looked into. “We are researching quantum technology and its cryptography potential,” Rivella.
adds. He agrees that International Standards, such as the ones prepared by the IEC, should help move the project forward.

A number of IEC technical committees (TCs) and their subcommittees (SCs) prepare International Standards for the components found in these technologies. Among the most relevant, IEC TC 47: Semiconductors, issues IEC 62969 which deals with the general requirements of power interfaces for automotive vehicle sensors. IEC TC 100: Audio, video and multimedia systems and equipment, publishes Standards that relate to digital cameras. ISO/IEC Joint Technical Committee (JTC) 1: Information technology, includes several subcommittees which deal with the various technologies involved. ISO/IEC JTC1/SC 37 works on biometrics and publishes the ISO/IEC 19794 series on biometric interchange formats, for instance.

ISO/IEC JTC1/SC 38 deals with cloud computing, while ISO/IEC JTC1/SC 27 is looking at the thorny issues of data protection and cyber security. ISO/IEC JTC1/SC 42, which was set up in 2017, is dedicated to artificial intelligence. IEC TC 69: Electric road vehicles and industrial trucks, issues Standards pertaining to the power charging of EVs.

The flying Dutchman

A Dutch company was showing PAL-V Liberty at the Geneva show, claiming it is the first production model of a flying car. “We spent ten years developing the technology before getting to this stage,” says Carlo Maasbommel, the company’s vice-president of international business research and development. One of the main technical hurdles was creating a car that is light enough to fly, yet robust enough for the road. “Around 45 engineers have been working on the project. Half of them come from the automotive sector and the other half from the aeronautical industry,” he adds.
The dual engine propulsion drive train is based on two fully-certified aeroplane engines, produced by one of the leading manufacturers of aviation engines. According to Maasbommel, even if both engines fail, the device can still land using the rotors like a parachute. Unlike the Pop Up concept, the flying car is neither autonomous nor electric. It has a driver and a passenger seat. “Initially we are targeting it at government services such as police or fire-fighters. We already have sixty orders on our books,” he says. The PAL-V Liberty is expected to go into service in 2019, once all the various certifications have been obtained. According to Maasbommel, the device has been designed to meet the legislation requirements of most countries.

The IEC comprises several TCs that are relevant to the aviation industry. One of them is IEC TC 107 which develops process management Standards on systems and equipment used in the field of avionics. These include the electronics used in commercial, civil and military aerospace applications. IEC TC 97: Electrical installations for lighting and beaconing of aerodromes, prepares International Standards for power distribution systems adapted to the operational and safety needs of aeronautical ground lighting (AGL).

IEC TC 21: Secondary cells and batteries, includes maintenance team (MT) 60952, which deals with the maintenance of the IEC 60952 series of Standards on aircraft batteries. IEC TC 29: Electroacoustics, publishes Standards that measure noise levels. One of these is IEC 61265, Instruments for measurement of aircraft noise, which specifies requirements for devices used to measure sound for the purpose of aeroplane noise certification.

Autonomous drones

An entirely different approach is for autonomous drones to become flying taxis, a project which has already been tested, notably in Dubai. A trial flight already took place last year, using technology developed by a Chinese company.

All three projects are based on very different strategies and assumptions. While many issues still have to be resolved, they clearly demonstrate that flying to escape congestion is no longer merely the wishful thinking of commuters stuck in traffic.
How safe is your car from hackers?
Protecting connected cars against cyber attacks

By Michael A. Mullane

IHS Markit predicts that more than 70 million connected cars will be on the road by 2023. Connected cars enable drivers to receive updated traffic information, send messages or access personalized entertainment systems, but they are also vulnerable to sabotage.

The cyber threat

Official UK data suggests that vehicle theft has risen by around 30% as criminals use new technology to break into cars. For example, “relay car hackers” use radio transmitters to intercept the signal from a car key, often succeeding in gaining access to a vehicle in less than a minute.

Malware is another commonly used ploy. Falling victim can take no more than registering for a bogus free Wi-Fi service, which is all that is required for criminals to take complete control of your car.

What is really worrying is that criminals don’t need to acquire special expertise or invest in sophisticated equipment. The reality is that standard smartphones or cheap radio transmitters will provide hackers with all the technology they need to break into most vehicles.

Car theft is far from the only threat, however. A recent report warns that terrorists could hack into connected and autonomous vehicles in order to crash them deliberately.

So what is it that makes connected cars particularly vulnerable? “As cars continue to evolve, essentially becoming motorized computers, they are vulnerable to the very same threats and attacks as home computers, laptops and smartphones,” explains Carlos Moreira, the CEO of WiSeKey. “Unless appropriate cyber security measures are implemented, hackers can remotely access the vehicle’s computer system, manipulate the brakes, engine and transmission.”

Snapping turtle technology

One of the most quoted statistics about connected cars is that, collectively, all the built-in software systems contain more than 100 million lines of code. That is twice as many lines of code as CERN’s Large Hadron Collider, the world’s most powerful...
particle accelerator, and seven times more than the Boeing 787 Dreamliner.

“You can’t secure every line of code,” says Chuck Brokish of Green Hills Software, “but you can identify critical components.”

Brokish compares car security to the snapping turtles in his native Wisconsin. He claims that the amphibians combine powerful jaws with a shell so hard that cars can run over them without doing any damage.

Flip the turtles over, however, and their soft bellies make them extremely vulnerable, he says. Brokish likens this to the “medium robustness” security systems of connected cars, which offer protection against casual attacks but cannot cope with a targeted onslaught.

The experts say that connected cars should be fitted with security systems and mechanisms that provide the most stringent protection and rigorous security countermeasures. They are not.

“It’s like leaving your front door open,” says Manfred Kunz of Marvell, “and expecting someone in your living-room to protect your home.”

**Creating a security-conscious culture**

Promon founder Tom Lysemose Hansen says the lack of adequate protection can be hard to understand: “Various security-first practices, such as those for example already used in mobile banking, mobile payment or mobile authentication, could greatly reduce the risk of such an attack”.

All the experts we met agreed that protecting vehicles against cyber threats poses an enormous challenge that requires close and constant cooperation between a number of organizations, automotive and original equipment manufacturers (OEMs), software companies and security solution providers.

Alex Manea, the Chief Security Officer of BlackBerry, urges manufacturers to authenticate every chip and electronic control unit and ensure they are loaded only with trusted software. Regular health checks via analytics and diagnostics software are essential, but he argues that the critical factor currently lacking in the industry is a security-conscious corporate culture.

“Ensure that every organization involved in supplying auto electronics is trained in safety and security with best practices to inculcate this culture within the organization”, says Manea.

**The role of International Standards**

The message coming out of the Geneva International Motor Show is that more car makers should take responsibility for cyber security. The consensus among the analysts is that many manufacturers are only willing to do the minimum as security can be expensive.

In the end it will come down to whether consumers are prepared to pay more to move beyond snapping turtle technology. There are signs that this may be the case.

A recent report identifies consumer concerns about cyber security and safety as a significant barrier to continued growth in the connected car sector. Thirty-one per cent of respondents to Foley’s 2017 Connected Cars and Autonomous Vehicles Survey identified these concerns as the biggest obstacle to buying connected cars.

International Standards already provide manufacturers with the best practice guidelines they need to step up cyber security.

In this respect, the United Nations Economic Commission for Europe (UNECE) document on System Security Principles for Intelligent Transport System and Connected and Automated Vehicles highlights the important role played by the IEC in providing the tools to protect against cyber attacks. IEC develops International Standards for information technology, together with ISO. It lists no fewer than 11 ISO/IEC JTC 1 applicable Standards and guidance documents.
Protecting railway networks from cyber threats

Rail networks, as integral parts of critical infrastructure, continue to come under cyber attack

By Morand Fachot

Railways and metro systems have been the subject of a spate of cyber attacks in recent years. Although no major accidents or casualties have been reported so far, it is likely that the problem will get worse and affect safety. As train signalling and control systems move from what were essentially closed systems to open ones based on mobile communication and internet protocol (IP) technologies, cyber security becomes ever more important. IEC International Standards will play a major role in this sector.

Technological and cultural change

Railway systems form an integral part of the transport system and as such are seen as part of the critical infrastructure in many countries. Cyber threats to railway networks are assuming increased importance as the digitization of railway control systems grows.

Signalling and train control systems have relied on various types of switches for a long time. These are essentially closed proprietary systems protected by so-called air gaps.

The traditional air-gap protected systems are not immune to attacks. In 2008, a 14-year old Polish teenager used a modified TV remote control to interfere with the tram track and point system in the city of Lodz. Four vehicles were derailed and 12 people injured in the process.

The railway sector is now introducing open systems that are based on technologies such as general packet radio service (GPRS) and long-term evolution (LTE) for mobile communications, and IP. These systems, being open, represent a technological and a cultural shift. However, computer-based systems have introduced the additional dimension of cyber threats. This means that cyber security becomes a
concern and must be integrated from the beginning.

In November 2016, the San Francisco Municipal Transportation Authority (SFMTA) was the target of a ransomware attack. Its information systems were encrypted and the operator was forced to disconnect its fare gates and ticket vending machines, resulting in financial losses.

In May 2017, German rail operator Deutsche Bahn was affected by the WannaCry ransomware attack. While this resulted in its electronic boards being switched off in some stations, its train services were not disrupted.

Growing awareness of cyber threats to the railway sector has been highlighted by a range of international initiatives and conferences. A special session on Cyber Security in Rail within the framework of the Intelligent Rail Summit 2017 organized in Vienna in November 2017 by RailTech, a global platform for rail professionals, looked at a range of aspects. This session, attended by e-tech, listed issues in the cyber threat sphere and measures to address them, among them the use of IEC Standards.

Wide range of potential attackers

The main threat to railway (and other transport) systems does not come from the so-called script-kiddies, like the Polish teenager who hacked the Lodz tram system, but from four different groups of perpetrators in two categories:

1. Criminals who try to extort money, with ransomware being the main tool. This has become a business model with different types of malware being developed and either sold or rented.

2. Others who are determined to disrupt or damage operations. They include:
   - disgruntled or sacked employees with access (including physical) to computer systems
   - terrorists and politically-motivated groups
   - possible state actors

Physical attacks should not be discounted. In September 2016, the Chicago air traffic control centre was closed by a massive fire set by a disgruntled contractor. Thousands of flights were disrupted across the US. Attacks can take a hybrid form that combines physical and cyber attacks.

Prevention of physical attacks, which are often carried out through unauthorized access, can be ensured by applying International Standards developed by IEC Technical
Committee (TC) 79: Alarm and
electronic security systems, and by
ISO/IEC Joint Technical Committee
(JTC) 1/Subcommittee (SC) 17: Cards
and personal identification.

Enclosures containing electronic and
control equipment installed in remote
places along tracks present physical
and cyber vulnerabilities.

Protecting railway infrastructure
from cyber threats

The digitization of the railway sector
and the move from electromechanical
to digital IP-enabled technology is
being encouraged by the European
Union in the form of the European Rail
Traffic Management System (ERTMS).

ERTMS is a system of standards for
the management and interoperation
of signalling for railways, which is
being adopted not just in Europe, but
beyond: in several African countries,
in Brazil, Mexico, many Middle Eastern
and Asian countries including China
and India, and Australia.

Industrial automated control systems
(IACS), are no longer isolated from
the outside, and railway systems are
increasingly interconnected thanks
to automatic train operation (ATO)
and as part of intelligent transport
systems, François Hausman, Alstom
Main Line cyber defence manager and
Shift2Rail cyber security WP leader
told the conference. Cyber attacks on
industrial control systems increased
by more than 600% between 2012
and 2014, he said, bringing with them
severe financial and safety concerns.

Railway specifics, such as electronic
components scattered along tracks or
trains, a very long life cycle (in excess
of 25 years), diversity both of supply
chain and technology and other
characteristics make this a complex
domain.

Automated, wireless signals more
efficient, but open to new threats

“The automotive sector has woken
up to the critical need for cyber
protection. It’s time the railway
industry got on board as well,”
says Amir Levintal, CEO of Israel-
based specialized rail cyber security
company Cylus. “The current
approaches to cybersecurity do not
fit the architecture of railway networks
today,” Levintal told the Global Railway
Review.

Levintal sees new signalling systems
as especially vulnerable to hackers.
These systems “are the heart of
safety-critical train operations. They
have also become more and more
automated over the past few years –
and are now operated wirelessly,” he
explains.

“In the worst-case scenario, hackers
could send commands to the train
causing them to slow down, stop
completely, or even accelerate on
curves so that the train would be
unable to align itself with the switches
on the track. All of these scenarios
could lead to disaster,” Levintal warns.

IEC Standards for IACS central to
railways

Shift2Rail, an initiative that brings
together key European railway
stakeholders to achieve a single
European railway area, is looking
at defining how different aspects of
cyber security should be applied to
the railway sector. It has assessed
applicable standards and selected
the IEC 62443 series for the following
reasons (and others):

- it is a set of Standards dedicated
to IACS
- it addresses product and system
  life cycles
- it covers security risk assessment
  processes
- it defines security levels based on
  functional security requirements
- it is used by other critical
  infrastructures

The choice of IEC 62443 was also
highlighted by ERTMS Cyber Security
Lead Engineer Sharvind Appiah at a
workshop organized by the Railway
Gazette. “There’s no reason to
develop new standards for railways.
There are already many standards for
cyber security, whether they are NIST
[the US National Institute of Standards
and Technology] or ISO/IEC Standards
(…). The challenge is to see which of
these fit in the railway context. That’s
what we’re doing in Shift2Rail: we’re
looking at industry standards, which
means IEC 62443, a complete set of
Standards designed for IACS, but we
apply them in the railway context.”
"For me this is a smart way to bridge the gap. It avoids forcing us to go through the R&D phase, where we have to rewrite the standards. We have standards there; it’s a matter of adopting them and learning how to use them."

The fact that IEC 62443 is emerging as a core set of Standards for the railway sector was highlighted by other speakers at the Vienna conference, in particular by David Rogers of Siemens in his presentation: IEC 62443: A cyber security Standard approaching the Rail IoT.

The set of Standards involves the three major stakeholders in the protection of plants against cyber attacks: asset owners, system integrators and product suppliers, Rogers said. A key concept of IEC 62443 is that security requires a set of coordinated measures to be taken, an approach generally described as defence-in-depth.

The fact that IEC 62443 is being widely adopted is illustrated by the German standard DIN VDE V 0831-104; VDE V 0831-104:2015-10: Electric signalling systems for railways – Part 104: IT Security Guideline based on IEC 62443 (62443-3-3:2013)

All countries are introducing cyber security measures in the rail sector

The UK Department for Transport has issued a guidance document which is designed to support the rail industry in reducing its vulnerability to cyber attack. It is designed to be high-level and sets out the principles and general approach to cyber security as good practice. It does not provide detailed instructions.


In the US, NIST has published a paper on the performance evaluation of secure industrial control system design for a railway control system.

As railway systems will rely increasingly on mobile communication, connected devices and IP networks, the incidence of cyber attacks from a variety of actors is likely to increase.

International standards, in particular IEC Standards such as the IEC 62443 series, will provide an all-inclusive approach to information technology (IT) and operational technology (OT) security and will be central to protecting IACS from cyber threats.
International Standards provide toolkit for GDPR compliance

Organizations all over the world are being forced to comply with sweeping new EU data protection rules

*By Michael A. Mullane*

When the European Union’s General Data Protection Regulation (GDPR) comes into force, on 25 May, it will have a humongous impact on web properties all over the world. It will affect all organizations, wherever they keep their servers, if they provide EU citizens with any kind of information, content or service online.

The owners of web properties will need explicit permission from their users to continue collecting, storing, analyzing, or sharing personal information, as they do now, with analytics companies, advertising partners, marketing groups and numerous other third-party entities. It will likely transform the way data is treated everywhere as businesses will want to avoid the additional costs of managing different data regimes.

The GDPR will impose severe restrictions on the transfer of data outside the EU, both to other countries and international organizations. Full compliance will be a mandatory legal requirement to avoid severe sanctions, including fines of up to EUR 20 million – or 4% of global turnover, if the amount is higher.

Organizations across the world are racing against the clock to respect GDPR will likely transform the way data is treated everywhere
to guarantee privacy by design and default, but many online service providers remain concerned about compliance as the official guidelines are complex and sometimes difficult to relate to real world situations.

**The challenge**

The GDPR covers a broad range of personal data, including online identifiers such as IP addresses and cookies, as well as credit card and health information at the other end of the scale. It will transform the way that organizations collect personal data, how they store it and how they use it.

In order to comply with an individual’s “right to be forgotten”, for example, organizations will have to be able to delete personal data whenever requested. The GDPR also enshrines the right to “data portability”: the idea that citizens should be able to transfer personal data easily between different service providers.

The GDPR will ensure that personal data is kept only with a client’s explicit consent, used only for the purpose for which it was obtained and stored no longer than necessary. Not only will permission to use data have to be clear and concise, but also users will be able to revoke it at any time.

Organizations will have to follow strict guidelines to ensure that data is always accurate and processed in a fair and consistent manner. If there are any security breaches, organizations will have to inform the relevant supervisory authorities within 72 hours.

As 25 May draws closer, developers are rebuilding websites to ensure there is no automatic collection of data whenever visitors land on a page. They are tweaking all kinds of software to achieve GDPR compliance by minimizing the risk of a breach.

ISO/IEC 27001 identifies potential risks to client and stakeholder data and ensures that organizations implement the relevant controls to mitigate them. It takes in encryption, ongoing testing and risk assessment and the ability to restore access to personal data quickly in the event of an incident.

Currently under development, ISO/IEC CD 27552 will soon deliver an enhancement to ISO/IEC 27001 for privacy management requirements. It covers processes for protecting the capture, accountability, availability, and more.
integrity and confidentiality of data. ISO/IEC 19592-1 and ISO/IEC 19592-2, Information technology – Security techniques – Secret sharing, define best practices in the cryptographic techniques used to protect the confidentiality of messages (“secret sharing”) in terms of general requirements and fundamental mechanisms. These techniques can be used to store sensitive data securely in distributed systems.

ISO/IEC 29100, Information technology – Security techniques – Privacy architecture framework, identifies a framework and associated controls for the safeguarding of privacy in ICT systems that store and process PII.

With a focus on learning, education and training, ISO/IEC 29187-1, Information technology – Identification of privacy protection requirements pertaining to learning, education and training, takes into account the public policy requirements that control the creation, use and interchange of personal data, as well as information life cycle management. These include, but are not limited to, regulations for consumer protection, privacy and individual accessibility.

Conformity assessment

Because not all risks are technology-based, it is essential that the technical staff responsible for data management have the required training, knowledge and skills. The work of the Committee on Conformity Assessment (CASCO) - a joint effort by IEC and ISO - is vital to the process of determining whether an organization meets the requirements related to its technical competence in this area.

ISO/IEC 17024 sets out the general requirements for personnel certification, while ISO/IEC 17065 covers the requirements for certifying products, processes and services.

Adherence to the relevant International Standards ensures the effective implementation of best practices to protect personal data and to mitigate risks. Organizations can use them to build a new digital relationship with their customers, which is a cornerstone of the GDPR requirements.

International Standards can play an important role in helping to protect brand reputations and to minimize adverse publicity by giving clients confidence in the reliability of the systems to which they have entrusted their data. Against a backdrop of sweeping regulatory change, they provide the tools for implementing robust data security management systems that deal with sensitive information efficiently and effectively.
The electrification of commercial vans and trucks is being driven by a combination of technological advances in passenger electric vehicles and moves by governments and cities around the world to reduce greenhouse gas emissions by banning older diesel vehicles regarded as sources of pollution.

More than 300 million electric vehicles (EVs) will be in use around the world soon after 2040, according to the International Energy Agency (IEA). Improved battery technologies have reduced the cost and extended the operational range of passenger EVs.

These advances, along with official moves to reduce greenhouse gas emissions by creating ‘no-go’ zones for older diesel vehicles in cities in Europe, the US and China, are promoting the electrification of commercial vehicles, from light delivery vans to buses and heavy-duty freight trucks.

The greater use of electric trucks would help reduce the estimated 40% of road transport emissions produced by freight, a sector that is still expanding in many markets, according to the New Scientist. However, the lack of widespread recharging infrastructure and concerns over battery life, especially for long-distance trucks, could hold back growth in the next decade.

Several IEC technical committees (TCs) and subcommittees (SCs) draw up International Standards for a wide range of components used in electric trucks, including batteries and motors as well as electronic navigation, vehicle safety and driver assistance systems, such as collision mitigation technology and lane departure warning systems.

IEC TC 69: Electric road vehicles and electric industrial trucks, prepares Standards for motors and motor controllers, on-board electrical energy storage systems, power supplies and chargers.

China drives commercial EV growth

As more electrically-powered buses, vans and light delivery vehicles take to the roads, China is leading the way in promoting the growth of electric commercial vehicles.
to the world’s roads, established vehicle manufacturers as well as new start-ups are gearing up to produce medium- and heavy-duty electric trucks too. Growth in the electric bus sector is likely to reduce the cost of key components for electric trucks. China, which is forecast to become the largest market for all types of electrified trucks, is driving growth in the global commercial EV sector. Most buses in China are now electric, and there are plans for the country to have 4.5 million EV fast-charging stations in operation by 2020. The Chinese company BYD, the world’s leading manufacturer of electric buses, is increasing production of electric trucks both for export and domestic sale.

In 2017 Daimler, the world’s biggest commercial vehicle manufacturer, began delivering what it described as “the first series-produced all-electric light-duty truck” to customers in the US and Japan. The vehicle, known as the eCanter, has a permanent synchronous electric motor with an output of 185 kW and torque of 380 Nm. It is powered by lithium-ion battery packs and can travel up to 120 km before recharging, depending on the body, load and usage, according to Daimler.

Although Daimler is also developing “an all-electric heavy-duty truck concept” with a range of up to
350 km on a single charge and capable of carrying a payload of 11 tons, the company noted in October 2017 that “the electrification of long-haul trucks will still need considerable time”.

Major European manufacturers including Scania and MAN (both part of Volkswagen’s truck division) and Volvo Group (owner of the Renault and Mack truck businesses) all aim to have heavy-duty electric trucks on sale within the next two years. They face competing against smaller companies in Europe, the US and China, which have launched light electric trucks in local markets, as well as new entrants including US electric car specialist Tesla. Other players, among them Toyota and the US-based Nikola Motor Company, are focusing on hydrogen/electric heavy trucks.

Smaller plug-in electric vans used for shorter urban journeys and local deliveries have proved particularly popular in the European market. In this category, manufacturers including Citroen, Peugeot, Renault and Nissan offer models powered by lithium-ion battery packs in the 20-50 kWh range, which can be recharged at central depots. But when it comes to smaller inner-city deliveries, light electric vans face competition from electric scooters, three-wheelers and small autonomous vehicles.

**Battery, fuel cell or catenary wire**

Electric motors can be mounted either in a drivetrain before the transmission to provide energy to the driveshaft and then to the axles, or installed directly in the wheels of a truck or trailer. According to the IEA 2017 report on The Future of Trucks, electric trucks can reach powertrain-to-wheel efficiencies of as high as 85%, about three times greater than trucks powered by internal combustion engines. Electric drivetrains are also lighter and cheaper than conventional drivetrains.

Currently the three main types of all-electric propulsion options for long-range trucks are batteries, hydrogen fuel cells and overhead catenary systems.

IEC TC 21: Secondary cells and batteries, and its SCs prepare Standards for all secondary cells and batteries. This covers the performance, dimensions, safety installation principles and labelling of batteries used for the propulsion of electric road vehicles.

The International Council on Clean Transportation (ICCT) commented in a November 2017 report that “for long-haul applications specifically, one of our key conclusions was that there is no clear winner among the three options; each has both barriers and benefits.”

**Battery prices fall**

Costs of lithium-ion battery packs have dropped in recent years and are
projected to fall further as a result of economies of scale, improvements to battery design and production methods and competition among suppliers.

Research firm Frost & Sullivan reported in December 2017 that battery prices had decreased by about 50% since 2010 and were expected to halve again in the next four to six years. A key driver for cost-effectiveness would be battery pack costs dropping below USD 150 per kWh, the ICCT believes. However, disruptions to the supplies of the raw materials needed to increase production of lithium-ion batteries could overturn these forecasts.

Hydrogen fuel cells are another option, particularly for long-haul electric trucks, although the hydrogen fuel cell market is still in its infancy. Fuel cell electric vehicles are powered by pressurizing hydrogen with oxygen, creating a chemical reaction that generates electricity to power the vehicle. They offer longer ranges with shorter refuelling times, compared to battery-EV recharging.

IEC TC 105: Fuel cell technologies, prepares International Standards for fuel cell technologies which are increasingly deployed in the industrial and commercial EV sector.

A third solution is for trucks to pick up power from overhead wires using pantographs, similar to those used by trolley buses. These distribution systems are being tested in Europe and California to power electric trucks.

IEC TC 69: Electric road vehicles and electric industrial trucks, has developed the IEC 61851 series of International Standards to ensure that conductive charging systems are safe and reliable.

Wireless power transfer

Wireless power transfer (WPT) systems are an alternative way of charging EVs, either while they are stationary or in motion. WPT is based on high-power inductive energy transfer. The transfer takes place between sending components that are buried beneath the road surface and receiving equipment that is installed beneath the vehicle. Although the technology is still evolving, it has been used for some years to power electric city buses in countries including Belgium, Germany, South Africa and Sweden.

IEC TC 69 has a Working Group (WG), IEC TC 69/WG 7, which deals specifically with “Electric vehicle wireless power transfer (WPT) systems”.

IEC TC 69/WG 7 is working on IEC 61980, a three-part series of International Standards that applies to equipment used in WPT “from the supply network to electric road vehicles”. This series also applies to WPT equipment supplied from on-site storage systems (such as buffer batteries and so on).

ISO is also involved in the development of WPT through one of its TCs, which liaises with the corresponding IEC TC.

Lower running costs to boost sales

Analysts of the hybrid-electric and all-electric truck sectors differ significantly in their assessments of how the market will grow. Navigant Research forecast in 2017 that sales would grow by almost 25% annually, from 1% of the market in 2017 to 7% in 2027. A report by McKinsey Energy Insights is more optimistic, predicting that by 2030 electric trucks could account for 15% of all global truck sales. Frost & Sullivan estimate that annual global sales of all types of hybrid and full electric trucks could total more than 2.5 million units by 2025, with China accounting for 60% of global sales.

Although the upfront costs of electric trucks are currently high, future advances in battery technology, fast-charging options and charging infrastructure will reduce operational costs. With major van and truck manufacturers testing and launching an increasing range of new models powered by electric technology, this should promote their wider adoption.

StreetScooter WORK XL electric van jointly built by Deutsche Post DHL and Ford (Photo: Deutsche Post DHL Group)
Imagine using the millions of kilometres of paved roads around the world to harvest energy. Apart from the initial investment costs required for equipment and installation, this energy source is free to produce and has no adverse effect on the environment. Instead, it uses sunlight or the mechanical vibrations produced by vehicles to generate electrical energy.

Energy harvested from roads captures unused ambient energy and converts it to electric power. This electricity can then be used to power road infrastructure such as lights and signals. It can be stored in batteries for use when needed or fed into the electric power grid. And, because it makes use of the existing road network, no new land space needs to be allocated.

International Standards play a key role in the development of these solutions. IEC Technical Committee (TC) 47 develops International Standards for semiconductor devices including those that harvest energy. Batteries used to store electrical energy rely on the standardization work of IEC TC 21. IEC TC 8 and its Subcommittee (SC) 8A develop Standards for electricity supply systems, including the integration of power generated from renewable energy sources and fed into the electrical grid. A systems group, SyC Smart Energy, has recently been set up to provide systems level standardization, coordination and guidance in the areas of smart grid and smart energy.

Where the road meets the sun

Techniques have been developed to place photovoltaic modules directly on top of a road surface to capture solar power. Energy can be harvested from the over 16 million kilometres of paved roads around the world that are exposed to sunlight.

However, installing glass modules on roadways is no easy feat. Car tyres must be able to grip the road surface and glass panels must be durable and capable of withstanding heavy weights. Shading from trees, buildings and clouds can reduce exposure to the sun.

Despite these challenges, several companies have developed photovoltaic modules that can either replace asphalt or be placed directly on top of existing roadways. While these solutions are proprietary, they rely on International Standards developed by IEC TC 82, which is responsible for solar photovoltaic energy systems.

In the United States, Solar Roadways has developed solar modules that include microprocessors for intelligent communication and light emitting diode (LED) lights for lines and signage as well as heating elements to melt snow and ice. In France, the Wattway Solar Road is currently being trialled across the country, including at the entrance of a motorway toll booth to power the gates and payment machines. In China, a two kilometre road has been built in the Shandong province with the aim of powering street lights and containing a snow-melting system on the road. Roll-out, however, is limited given the high cost of these photovoltaic (PV) modules and the uncertainty regarding the actual levels of energy generated.
Piezo tiles (Photo: Branden Camp, Georgia Tech)
Alternatives have been suggested: placing PV panels alongside roads or in non-critical areas such as parking areas, bike paths and driveways.

Thermoelectric generators (TEGs) can also be used to harvest energy from roads. Based on the Seebeck effect, TEGs can convert geothermal energy – produced from the heat differential between the road surface and the layers beneath – into electrical energy. As the temperature differential increases, more electrical energy is produced, thus making this technology well suited to areas with extremely hot weather. In 2017, IEC TC 47 prepared the IEC 62830-2 series of Standards which provide methods for evaluating the thermal power of thin films used in thermoelectric energy harvesting devices.

Research is currently underway in the southwest of the United States to test this technology and potentially make use of it in rural areas and in airports to power lights and traffic sensors.

**Good vibrations**

The vibrations produced by a car driving on the road can be used to generate electricity.

Piezoelectricity is the electric charge produced by certain crystals when a mechanical stress is applied. First demonstrated in 1880 by the brothers Pierre and Jacques Curie, the piezoelectric effect has only begun to have practical applications in the past three decades. Standards for piezoelectric technology are developed by IEC TC 49, which addresses piezoelectric, dielectric and electrostatic devices.

Piezoelectric crystals can also be embedded beneath a layer of asphalt. As cars drive over the road, the wheels exert a force that causes these crystals to deform and generate electrical energy. This energy can then be used to power street lights or can be stored in batteries for later use. The IEC 62830-1 series, prepared by IEC TC 47, includes methods for evaluating the performance of vibration-based piezoelectric energy harvesting devices.

In the United States, the State of California has invested USD 2.3 million to fund two independent projects with the aim of determining the viability of embedding piezoelectric devices in roads to harvest energy. A similar trial is underway at Lancaster University in the United Kingdom. However, challenges remain. Factors that increase piezoelectric road efficiency are inversely related to the durability of a road. Roads with sizeable traffic flows from heavy-duty vehicles travelling at high speeds will generate a greater energy output compared to roads with little traffic, light-weight cars and slow speeds.

It has also not yet been confirmed whether the costs associated with installing and maintaining roads embedded with piezoelectric technology are offset by the electricity generated, given its relatively low energy conversion efficiency. Other energy harvesting solutions, such as PV modules alongside roads, may be cheaper to install and generate higher volumes of electricity.

**And down the road...**

Energy harvesting solutions making use of roads are still in their early stages. Because much of the current research and development has been undertaken by private companies, there is limited public availability of data. Costs remain high given the lack of mass production.

Some of these solutions may yet gain traction. Additional technologies such as sensors and microprocessors could be incorporated that monitor infrastructure and vehicular traffic conditions in real time. Such solutions will rely upon Standards developed by the ISO/IEC Joint Technical Committee, JTC 1/SC 25 for microprocessor systems and IEC TC 47 for sensors. It is not yet clear which technologies, if any, will be implemented. But the enthusiasm remains in the pursuit of renewable energies.

*What if our shoes could produce electricity? (Photo: www.instructables.com)*
The internet of things (IoT) – consisting of millions of “sensorized” connected devices and systems – and artificial intelligence (AI) – combining analytics, machine learning and algorithms – are making the world smarter and more connected. Together these disruptive technologies are changing how many industries operate, improving their products, systems and services, and saving costs, energy and time. The gathering, exchange and analysis of data from connected devices in real time offer many advantages. For example, smart lighting and heating systems make buildings more efficient, and connected medical wearables improve the quality of life for people with certain health conditions.

Rethinking the transport ecosystem

The transport industry is no exception. As the digitalization process continues, existing infrastructures are being updated to increase capacity for growing populations, improve safety and tackle congestion and pollution in cities by making services more green and efficient.

At the recent Geneva International Motor Show (GIMS), visitors got a taste of the latest connected, autonomous driving technology and advances in electric and hybrid vehicles. During the show, the International Telecommunication Union (ITU) and the United Nations Economic Commission for Europe (UNECE) organized their annual Future Networked Car symposium. Representatives of vehicle manufacturers and the automotive and information and communication technology (ICT) industries, as well as governments and their regulators gathered to discuss the status and future of vehicle communications and automated driving.

How will autonomous vehicles fit into existing infrastructures?

Russ Shields, Chair of ITU Collaboration on Intelligent Transport Systems Communications Standards said of the Geneva Motor Show, “You don’t see the hype we used to see, you actually see connected tech in the vehicles, so we have moved from ‘this is coming’, to ‘it is here’.”

In line with this shift, the ITU symposium also addressed one of the next big concerns: how to integrate autonomous vehicles (AVs) into a mixed environment. In other words,
how can fully autonomous vehicles be made to interact with people who are still driving vehicles which contain older technology? Without question, the transition phase will represent a big challenge.

**Enabling innovative transportation services**

Lissa Franklin, VP Business Development and Marketing, BestMile, Switzerland, addressed this question in her presentation: “Autonomous mobility is already in our streets and deployments of autonomous shuttles are blossoming worldwide, but the democratization of AVs will be impacted directly by the quality of mobility services and their integration in the existing transportation infrastructure”.

**The need for global coordination and real-time optimization**

In order to facilitate a smooth transition to autonomous vehicles, public transport agencies and smart cities, transport network companies, transport operators and on-demand private transport services will need to work together and develop new mobility services which integrate with autonomous vehicles. Services will include on-demand and fixed route, both of which will incorporate and need to manage a combination of human driven vehicles and AVs (hybrid fleets), as well as different brands of AVs (mixed fleets).

**High-tech mobility services**

IoT and AI technologies will contribute to producing the technical infrastructure required by this multi-modal transportation. It will need to consider: real-time analytics for predictive demand calculations, payment, apps, scheduling, traffic, passenger/user experiences, data intelligence, new revenue opportunities and shared autonomous services.

**Why future mobility services will need International Standards**

IEC has already produced many International Standards which are used to ensure the interoperability, quality, safety and reliability of many of the components of autonomous vehicles. Examples include audio, video and multimedia systems and equipment, batteries, electric vehicle charging, lighting and the all-important sensors, on which AVs rely.

IEC also works with ISO to develop Standards for information technology through its Joint Technical Committee (ISO/IEC JTC 1); many of them apply to AVs. They include cloud computing and distributed platforms and IoT and sensor networks. Most recently work has begun in the area of AI. JTC 1 has produced a series of Standards for IT security techniques which aim to protect information by addressing security and privacy aspects.

Additionally, a number of JTC 1 Standards are included in the UNECE Systems Security Principles document for Intelligent Transport Systems and Connected and Automated Vehicles.

**The future way**

As large car manufacturers rethink their business models and plan new
mobility products and services for an autonomous driving future, they face a number of complex issues.

Addressing the challenges through standardization

One of the great challenges in Europe lies in the fragmented nature of the markets. Each country has its own operators and service providers.

“For everyone in the industry, we need to be connected. We need networks and because we are a global company, we need networks all over the world, so obviously if we have standards we can apply everywhere, this will help accelerate this transformation”, said Pierre Masai, CIO of Toyota Motor Europe.

During his presentation, Masai stressed the need for Standards for 5G, for the mobile virtual network operators (MVNO) who will manage communications in multiple countries and jurisdictions and, very importantly, for preventing cyber attacks.

Mobility as a new service platform

Masai shared his company’s future vision of what it is doing to prepare for the next generation of connected cars.

As it moves ahead with its new mobility service platform, Toyota will be able to gather information from a digital communications module that will be installed in each new type-approved car, in other words, for cars which receive confirmation that production samples of a design will meet specified performance standards. All this information will be connected and allow interaction with the dealerships.

The global communications platform aims to offer automatic connections everywhere without needing to rely on roaming services and will enable the provision of stable, low cost, high quality services while adhering to all relevant regulations in each country and region.

A new global data centre currently being built will use the big data gathered and provide customers with all the services they want and agree to have. The global mobility services platform could eventually be leveraged to develop advanced vehicle and related mobility services for business applications.

So how will the future of driving really look?

At the same time as they move towards fully automated vehicles, key automotive manufacturers are developing high-tech, fully connected, mobility service fleet models. If the ultimate goal is to remove humans from behind the wheel, a number of questions still remain: what will AVs look like in another decade? Will urban dwellers still want to own their cars or will there be a cheaper, greener and completely new way of getting around town, perhaps along the lines of the ride hailing and ride sharing services we have already seen? Only time will tell.
Information technology has penetrated our homes, cities and workplaces, as billions of “sensorized” devices and systems that form part of the internet of things (IoT) help to simplify how we work, communicate and carry out daily tasks.

Surrounded by life-changing technology

Advances in digitization, analytics, artificial intelligence (AI), and automation are creating performance and productivity opportunities. They are also redefining how businesses and industries operate, from agriculture, automotive/transportation and energy management, to entertainment, healthcare, manufacturing and retail.

Examples are all around us. Predictive analytics, based on AI machine learning and algorithms, can improve business processes, enhance decision making and enable optimizing and automating decisions, on demand, to meet business goals. Predictive analytics is being applied in a number...
A more obvious form of AI is voice recognition technology, found in virtual personal assistants like Alexa or Siri. These assistants are being built into a growing number of smart devices and changing how we live. Replacing touch with voice, we will start to talk more to our smart appliances and ask them to do things for us, like find a specific TV channel, switch things on and off, and eventually tell the next generation of cars to drive us to our appointments.

Enhancing our world

This technology brings benefits. Voice recognition will make life easier for people living with certain physical disabilities. Additionally, smart devices and systems (heating, lighting) in homes and other buildings already save energy and costs, by automatically adjusting temperatures and lighting based on the presence or absence of people. As cars become more connected and autonomous, they will depend greatly on computing technology and contain more software programmes offering services, such as infotainment and road traffic information. Hundreds of sensors will gather huge amounts of data about the immediate surroundings, ultimately enabling cars to communicate with each other and road infrastructure, with the aim of improving safety and reducing congestion.

Where Standards fit in

In order for the different systems and platforms used across all these industries to function smoothly, they will need to ensure data privacy, cyber security and interoperability. This technology will make life easier for people living with certain physical disabilities. Additionally, smart devices and systems (heating, lighting) in homes and other buildings already save energy and costs, by automatically adjusting temperatures and lighting based on the presence or absence of people. As cars become more connected and autonomous, they will depend greatly on computing technology and contain more software programmes offering services, such as infotainment and road traffic information. Hundreds of sensors will gather huge amounts of data about the immediate surroundings, ultimately enabling cars to communicate with each other and road infrastructure, with the aim of improving safety and reducing congestion.
What do you hope to achieve?

There is a lot of work to do, but I would highlight three main points:

1. In order for our experts and national body delegations to productively develop Standards, we in JTC 1 must ensure that the directives, tools and approaches are conducive to their work, so we don’t fall short anywhere.

2. During the 30 years of JTC 1, IT has changed dramatically. Today IT is being applied in many industry sectors and affects just about everyone, everywhere, in many ways. In JTC 1, we call this the digital transformation phenomenon, and it means we need to think differently about how we develop information technology Standards. It is more important now for us to proactively engage with stakeholders who are underrepresented in our process, so that we can develop IT Standards that meet everyone’s needs.

3. Also related to digital transformation, some stakeholders are now more interested in IT standards than when JTC 1 was formed, like governments for whom the standards are very relevant. There is also substantial innovation in applications and services developed entirely in software, and that part of IT is a little less well represented at JTC 1. So it will be important for us to proactively engage with stakeholders who are underrepresented in our process, so that we can develop IT Standards that meet everyone’s needs.

What challenges do you see?

In an era of digital transformation, we need to work more cooperatively with other TCs at IEC and ISO and engage stakeholders who we think should be better represented in our work.

Another ongoing challenge for JTC 1 is to be aware of new trends and developments and be prepared to take appropriate action at the appropriate time. We have an emerging technology and innovations group called JETI, which assesses technology opportunities and proposes actions that JTC 1 should consider, for it to remain relevant also in the future.

What will the hot topics be for 2018?

Internet of things

In 2016 our IoT Working Group became JTC 1 Subcommittee (SC) 41. It’s very active and is part of the foundation of IoT for other sectors, whether automotive, healthcare or even smart cities. So it’s got a tremendous amount of important work to do.

Artificial intelligence

AI has quickly become a hot topic and we just formed JTC 1/SC 42 for AI. Its first meeting is in April and it will be important for this committee to begin its work. AI holds such promise for industry and society, but at the same time, some aspects of it concern people. It’s changing quickly and there’s so much innovation in this space. It would be a shame if regulations were put in place too early, which then reduced the opportunity to benefit from AI. This also means that there’s an opportunity for voluntary standards to help set the norms that we all agree should apply to AI and its applications.

Cyber security

It would be hard to overstate the importance of cyber security. Fortunately this has been a very active area of JTC 1 for many years and it will continue to be one of our hot topics. JTC 1/SC 27, is widely recognized as the best place for the development of International Standards for cyber security. The challenge for this extraordinarily busy group is that there’s so much to do in this area.

If an IoT device isn’t secure, and you don’t feel you can trust it, then it’s not very useful. For cars or medical devices, the threat of being hacked is a concern. That’s why cyber security and IT security need to be the underpinning of everything else.

Finally, even though Standards definitely play a significant role, they are not the total answer. Developers of products and services also have an important responsibility to ensure they incorporate security best practices in design and development.
Smart buildings for smart living

Open Sesame! Or the door to your home, using voice command

By Antoinette Price

Our world is getting smarter by the minute. Voice recognition allows us to tell devices to do things, such as find a specific TV channel or remind us of all our appointments for the day. Smart agriculture uses sensors, connected machinery and smartphone apps to tell farmers when to water their fields, while intelligent road infrastructure is improving road safety and congestion and all in real time.

Many industries, including construction, entertainment, healthcare, transport and retail, are using smart technology to add value to their products and services, in the form of connected devices and systems. These are all part of the internet of things (IoT). They gather, monitor, exchange and analyze data, in order to improve the user experience.

As cities become smarter, so are their infrastructures and buildings. Embedded technology can operate building access and security, data and energy management, water use, light and temperature.

Against this backdrop, IEC established the Standardization Evaluation Group (SEG) 9 for smart home/office building systems in February 2017.

Smart apps for homes can save energy and facilitate people with certain disabilities (Photo: Appsolutions)
The main aim of the Group is to:

- map technology trends and market evolution, assess current and future market segments
- develop indicative, general use cases
- look at current IEC Standards and others, to analyze gaps, overlaps and remediation paths if required
- identify best practice models, to coordinate work within IEC and with external bodies and ensure a longer term sustainable process. This will specifically address a number of identified areas of overlap between IEC technical committees.

The focus of IEC activities for smart homes and buildings

e-tech caught up with SEG 9 Convenor, Kim Craig, to find out more about the work and main trends for 2018.

What will the priorities be?

We’ve been going for just over a year and to date we have 64 registered members from 17 countries. We need to engage a wide range of experts to participate in the work, in order to get a truly representative view of the smart home/office building landscape. Initially, we’ll aim to get an accurate view of market trends and technology evolution for both current and future scenarios. Identifying gaps in standardization and also areas where standardization may not be required will be critical to our future recommendations to the IEC Standardization Management Board.

What big trends affect smart homes and buildings?

Interoperability, cyber security, data privacy

As buildings and homes become more intelligent, they contain more information and communication technology (ICT), audio, video and multimedia systems and diverse hardware.

IEC International Standards cover many aspects of these components, to ensure their quality and that they are safe and remain secure. Additionally, given that many devices and systems are manufactured by different parties, the Standards also consider the need for interoperability, so that the buildings incorporating this technology will be able to function reliably.

“The major trend is the rapid evolution of interoperability and interconnection between previously isolated components, communication protocols and sub systems, but cyber security and privacy are also top of mind”, said Craig.

The silver economy

The World Health Organization (WHO) estimates that the percentage of the world’s population aged over 60 will double from 11% to 22% between 2015 and 2050. WHO statistics show that the number of people 60 years and over is expected to increase from 900 million to two billion over the same period.

As populations continue to grow and age, buildings will need to be as efficient as possible and adapt to the needs of people who are more likely to require different levels of assistance on a daily basis.

One goal of smart cities is to ensure that people with disabilities can work, socialize and live independently for as long as possible, by providing human and technical support to manage chronic health conditions, ensure physical access to places, and guarantee the ability to move around easily within the home or city.
products and components. “A rapidly aging population (the ‘silver economy’) is a key element in smart homes and buildings where AAL aspects are becoming more pronounced as a lifestyle driver and enabler,” noted Craig.

**Energy efficiency**

The construction industry is already using smart technology to tackle the issue of energy efficiency. Buildings, whether homes, offices, factories, hospitals or other public and private spaces, are responsible for more than 40 percent of global energy use and one third of global greenhouse gas emissions, according to a report by the United Nations Environmental Programme (UNEP) Sustainable Buildings and Climate Initiative.

“A global focus on energy efficiency and the rapid growth of renewable energy sources and energy storage has major implications for SEG 9 work”, concluded Craig.

High-tech materials and smart systems save energy, costs and improve the quality of experience whether at home, work or in other buildings, such as a hospital or museum. For example, solar panels can sustain a building’s energy requirements, while systems using sensors to monitor light, temperature and room occupation, enable automatic adjustments to optimize the use of heating, cooling and lighting systems.
The International Energy Agency (IEA) Renewables 2017 Report highlights that new solar photovoltaic (PV) capacity grew globally by 50% in 2016, reaching over 74 GW. It also notes the significant point that for the first time, solar PV additions rose faster than any other fuel, surpassing the net growth in coal.

The IEA expects the renewable electricity forecast to expand by over 920 GW or 43% during the next five years, with solar PV representing the largest contribution.

Harnessing sun energy everywhere

Powering traffic lights and electronic road infrastructure, electric vehicle charging stations, residential, commercial and industrial sectors, solar PV use is expanding around the world as a leading renewable energy source.

Building trust while improving safety and quality

Manufacturers must be able to show that their products comply with required safety and performance.

By Antoinette Price
regulations. Since PV systems need substantial investment, manufacturers must also demonstrate that their products will perform for long periods, as promised, and be able to cope with the harsh conditions in which PV systems operate.

In order to achieve this, manufacturers in turn, must ensure the safety, resistance and performance of the components that comprise their PV products and systems.

The need for international certification

IECEE is the IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components. The different schemes test the safety, quality, efficiency and overall performance of electrical and electronic components, devices and equipment for homes, offices, workshops and health facilities, to ensure they comply with IEC International Standards. IECEE covers 23 categories of electrical equipment and testing services, including PV.

The great benefits of testing

IECEE Members use the principal of mutual recognition or reciprocal acceptance of test results to obtain certification or approval at national levels around the world, since IECEE certification offers proof of compliance to IEC International Standards. IECEE PV certification:

- saves costs and time, with fewer steps needed for international certification
- eliminates duplicate testing
- removes obstacles to international trade, such as different national certification or approval criteria
- allows faster product movement from plants to markets
- opens up access to more markets
- enables direct acceptance by regulators, retailers, buyers and vendors in many countries

For more information about IECEE: www.ieee.org

PV load testing simulates heavy snow which can accumulate on a sloping roof (Photo: TÜV Rheinland)
Faced with a “What-will-you-be-when-you-grow-up” question, a kid will choose rather conventional careers such as policeman/woman, astronaut, teacher, football player, actor, or singer; models and TV stars are more recent additions to the list. It’s pretty certain that no kid has ever said “I want to be an expert in explosive atmospheres!”

Explosive atmospheres: a chosen career path

Because the Ex sector is such a highly-specialized area, choosing that career path must definitely come at a later stage in life, while studying or joining a company that is active in that field. And often, those who have been exposed to it at some point in their career remain faithful to it until retirement and beyond.

The challenges of designing, manufacturing or even testing Ex-proof equipment are numerous. All electrical and non-electrical equipment installed in hazardous environments must meet very strict criteria to pass examination. This includes not only machinery, but also lighting fixtures, surveillance cameras, cell phones, computers, and so forth. The variety of equipment used in Ex areas is huge, even more so given the vast number of industry sectors involved. Oil, gas and mining are obvious, but sugar refineries, food processing plants, grain handling and storage, painting, to name but a few, also have to deal with hazardous environments.

A lifetime engagement

Gerhard Schwarz of Germany is a perfect illustration of this. After receiving a masters degree in engineering (Dipl-Ing, Electrotechnik) in Mannheim, he worked in sales, product management and design for...
products used in hazardous areas for close to 50 years.

Until the end of 2011, Schwarz was responsible for R&D explosion-protected light and switchgear at Cooper Crouse Hinds GmbH, where he was also in charge of the worldwide certification of hazardous area products. In 2012, he worked as senior technical consultant for Cooper Crouse Hinds, dealing with all general questions related to explosion protection, R&D, and certification. Since spring 2013, he has owned a consulting company in the explosion protection field.

Dedicated to standardization at the international level...

Complementing his professional career, he has also been active, at national, regional and international levels, in standardization and conformity assessment for explosive atmospheres.

Schwarz was a member of IEC Technical Committee (TC) 31: Equipment for explosive atmospheres, and was involved in numerous IEC working groups (WGs) dealing with electrical products used in hazardous areas, such as flameproof, increased safety and intrinsic safety. For a number of years he was Convenor of WG 40: Luminaires, and a member of several other WGs and maintenance teams (MT) that dealt with individual parts of IEC 60079, the series of International Standards on explosive atmospheres.

In 2005, Schwarz received the IEC 1906 Award in recognition of his significant and exceptional contribution to IEC TC 31.

...as well as in Europe and in Germany

At the regional level, within CENELEC, Schwarz was head of the German delegation in CLC/TC 31: Electrical apparatus for potentially explosive atmospheres, and was also involved in numerous WGs.

In Germany, he was Chair of the German committee on electrical equipment for use in hazardous areas at DKE, the German Commission for Electrical, Electronic and Information Technologies of DIN and VDE, and Chair of the WG on explosion-protected apparatus at ZVEI, the German Electrical and Electronic Manufacturers’ Association.

He was also involved in IECEx, the IEC System for Certification to Standards Relating to Equipment for Use in Explosive Atmospheres. He was a member of the special Working Group “WGEx” established some 25 years ago to consider the nucleus of a scheme dedicated to Ex equipment, the very origins of IECEx. He has maintained his involvement in the development and running of IECEx ever since, as an expert in the German delegation.

His expertise and experience in the Ex field made him a sought-after speaker. As such, he participated in IECEx international conferences, for example in 2012 in Dubai, United Arab Emirates, and in 2015 in Gdansk, Poland.

About IECEx

IECEx is the only truly international Conformity Assessment (CA) System to provide testing and certification for all items of electrical and non-electrical Ex equipment and installations as well as certifying the skills and competence of individuals working in hazardous areas.

The System addresses the inspection (location and other), installation,

maintenance and repair of equipment and systems and assesses the competence of personnel working in this highly-specialized area.

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

IECEx operates the following Schemes:

- IECEx Certified Equipment Scheme
- IECEx Certified Service Facilities Scheme
- IECEx Scheme for Certification of Personnel Competence (for Explosive Atmospheres)

The System also has the IECEx Conformity Mark Licensing System which provides on-the-spot evidence that products bearing the Conformity Mark are covered by an IECEx Certificate of Conformity.

More information: www.iecex.com
Avionics - a term coined from the merging of aviation and electronics - deals with all electronic devices and systems that perform specific individual functions on aircraft, satellites and spacecraft.

From WW II fighter planes to state-of-the-art aircraft

Modern avionics systems have their origin in World War II technological advances. This is the case for autopilot systems, for instance, which today equip any type of aircraft, from the smallest to the biggest passenger or cargo plane, and were developed during the war to help bomber planes fly steadily enough at high altitudes to hit their targets with precision. The radar was another engineering development of that era.

Post-WW II developments often continue to have their origin in the military, where a fair portion of the spending is allocated to avionics. In addition to benefitting from the new technologies trickling down from the defense industry, civil aviation has also seen a growing part of its R&D budget devoted to aircraft control systems and the like.
The second half of the 20th century saw very important breakthroughs in the electronics industry. These in turn had a major impact on the avionics sector which grew at a rapid pace. While new developments were usually made for the military and/or the space industry, they soon made their way into civil and commercial aviation as well.

In addition, the democratization of consumer flying followed by the emergence of low-cost airlines increased air traffic, tighter airspaces and, consequently, the need for more sophisticated methods of controlling and ensuring aircraft and passenger safety.

The cockpit, a concentration of avionics

The cockpit of an aircraft is a typical location for avionic equipment that consists of control, monitoring, communication, navigation, weather, and anti-collision systems. They include:

- **Automatic control**
  Automatic flight control systems lighten the pilots’ workload, especially at crucial times such as landing or when hovering, and help eliminate human errors that might otherwise prove fatal.

- **Monitoring**
  Display systems provide sensor data that allow the pilots to monitor flight parameters at all times and thus to fly the aircraft safely. Most of the information that used to be displayed on mechanical gauges in older aircraft now appears on electronic displays.

- **Communications**
  Communications connect the flight deck to the ground and to the passengers. On-board communications are provided by public address systems and aircraft intercoms.

- **Navigation**
  Navigation is the determination of position and heading (direction) on or above the surface of the earth. Avionics can use satellite-based systems, ground-based systems, or any combination of the two. Navigation systems calculate the position automatically and display it to the flight crew on moving map displays.

- **Anti-collision systems**
  As a complement to air traffic control, most large transport aircraft and many smaller ones use a traffic alert and collision avoidance system (TCAS), which can detect the location of nearby aircraft and provide instructions for avoiding a mid-air collision. Smaller aircraft may use simpler traffic alert systems which are passive and do not provide information for resolving potential problems. To help avoid collision with terrain, aircraft have systems such as ground-proximity warning systems (GPWS), of which radar altimeters are a key element.

- **Weather**
  Weather instrumentation, such as radar and lightning detectors, is important for aircraft which fly at night or in meteorological conditions in which pilots cannot see the weather ahead. Heavy precipitation (as sensed by radar) or severe turbulence (as sensed by lightning activity) are indicators of severe disturbances, and these weather instruments allow pilots to deviate around such areas.

- **Aircraft management systems**
  The trend today is to have centralized control of the multiple complex systems fitted to aircraft, including engine monitoring and management.

Specific requirements for avionics

While in the early days, a whole branch of the electronics sector designed and manufactured electronic components specifically for the aerospace/military industry, avionics today is mainly dependent on commercial off-the-shelf (COTS) electronic components. These are principally mainstream products, designed for all industries including consumer goods. But avionics has to meet its own requirements in terms of performance and durability.
IEC International Standards...

Although they may be subjected to severe conditions, such as the possible negative effects of atmospheric radiation at high altitude, or temperatures that may be outside the range specified for semiconductor devices by their manufacturers, avionics products must still perform reliably and safely during their working life.

IEC Technical Committee (TC) 107 develops process management Standards for these and other issues. Avionics original equipment manufacturers (OEMs) use increasing volumes of COTS electronic components, equipment and systems designed and manufactured for other industries in which they have limited control.

Many countries and regions are adopting legislation that restricts or eliminates the use of substances containing lead in most electrical and electronic equipment. As the avionics industry relies on COTS components, TC 107 provides a lead-free control plan that allows manufacturers to check the reliability of the components they use.

TC 107 also provides guidance for the avoidance, detection and mitigation of counterfeit electronic parts in avionics applications.

Other IEC TCs, such as TC 47: Semiconductor devices, or TC 110: Electronic display devices, prepare International Standards for components used in avionics applications.

...and certification crucial for avionics

IECQ, the IEC Quality Assessment System for Electronic Components, takes it one step further, testing and certifying the widest variety of electronic components. In addition, IECQ has a programme specifically designed for avionics, the IECQ Avionics Scheme.

The IECQ avionics parts and assembly management requirements are designed to evaluate commercial, military and aerospace equipment manufacturers’ and related organizations’ processes for compliance with the following Standards:

- IEC TS 62239-1, Process management for avionics – Management plan – Part 1: Preparation and maintenance of an electronic components management plan, developed by TC 107, and/or
- GEIA/ANSI 4899, Requirements for an Electronic Components Management Plan

Organizations holding IECQ avionics certification demonstrate that their organization and facilities comply with the requirements of the IECQ System and either IEC TS 62239-1 or GEIA/ANSI 4899 for their scope of activity.

Meeting all challenges

Electronic component manufacturers have other IECQ Schemes at their disposal to address counterfeit and hazardous substance issues.

IECQ has a Counterfeit Avoidance Programme (IECQ CAP) which ensures that equipment manufacturers or subcontractors used by an organization have processes for managing counterfeit avoidance in the selection and use of components according to IECQ CAP technical and quality management system requirements.

The IECQ Hazardous Substance Process Management (HSPM) Scheme is a technically based management systems approach to implementing and maintaining hazardous substance free products and production processes. IECQ HSPM was developed in response to component manufacturers’ needs 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.

United Launch Alliance (ULA)’s Vulcan Centaur rocket with a complete avionics package developed by L3. (Photo: ULA/Business Wire)
Obituary - Hans Gissel

IEC Past President Dr Hans Gissel has passed away

By Claire Marchand

It is with great sadness that we learned of the passing of IEC Past President Dr Hans Gissel, 86, on 6 March 2018.

Dr Gissel was IEC President from 1993 to 1995, serving as President-Elect in 1992 and as Immediate Past President in 1996-1997. He was also Vice-President of the German National Committee of the IEC and a consultant to the Steering Committee of DKE, the German Commission for Electrical, Electronic and Information Technologies of DIN and VDE.

A career in industry and research

Born in Rostock on 12 July 1931, Gissel studied electrotechnics at the Rheinisch-Westfälische Technische Hochschule in Aachen (RWTH Aachen), the largest technical university in Germany, where he obtained his PhD (Dr.-Ing.) in 1960. On completion of his studies, he joined AEG, the German conglomerate – AEG ceased to exist in 1996 but Electrolux gained the right to use the brand name on some of its products – where he spent about forty years and occupied managerial positions until 1993. Finally, he became a member of the AEG board with responsibilities for communications and defense engineering as well as research. Additionally, in 1985 Gissel was a constituent member of the advisory group on information technology of the Federal Ministry of Research (today’s Federal Ministry of Education and Research).

Gissel left his mark on the IEC

In his three years as President of the IEC, Gissel was instrumental in shaping the future of the Commission. Thanks to his professional career, Gissel perceived the major significance and influence of the semiconductor technology for all future IEC work. Early on, he referred to the “emerging and merging technologies”, as the big challenge of the second half of the 20th century.

IEC Masterplan

Under Gissel’s leadership, a first Masterplan was developed in the Lötschental, in the heart of the Swiss Alps, resulting in the streamlining of IEC structure and its National Committees (NCs) worldwide. It also led to a close examination of the numerous technical committees (TCs), with the consequence that some were disbanded and new ones established. Simultaneously, the President’s Advisory Committee on Future Technologies (PACT), set up by Gissel, worked as a think tank charged with the early identification of technology trends.

PACT

The role of PACT, as described in the IEC Bulletin (e-tech’s predecessor) of November/December 1994, was “to help the IEC fulfil industry’s future demand for standards in the areas of new and merging technologies, and of systems with major electrical/electronic content”. Members of the PACT think tank were presidents, vice-presidents and directors from major companies such as ABB, Alcatel Alsthom, Nokia, Philips, Rockwell, Siemens, or Toshiba, and leading organizations such as the China State Bureau of Technical Supervision,
the Italian National Broadcasting Enterprise and the UK Institution of Electrical Engineers. In a way, PACT was the ancestor of the IEC Market Strategy Board (MSB).

**Sector Boards**

In an effort to better tailor standardization efforts to market needs, under Gissel’s presidency, IEC made the decision to establish Sector Boards (SBs) to cover specific market segments and with representation not only from technical and national committees but also directly from industry to ensure relevance of the Standards produced by IEC.

Ultimately, four – now defunct – SBs were active for a number of years:

- **SB 1**: Electricity Transmission and Distribution
- **SB 2**: Healthcare systems
- **SB 3**: Industrial Automation Systems
- **SB 4**: Infrastructure and Telecommunications Networks

**Cooperation with CENELEC**

Gissel further developed the relationship with CENELEC, made official in 1991 under his predecessor Richard Brett with the signing of the Lugano Agreement. Gissel’s work led to the signing of the Dresden Agreement between IEC and CENELEC in 1996 (superseded by the Frankfurt Agreement of 2016) that ensure maximum harmonization and systems cooperation with IEC Standards underpinning European standards.

**…ISO and ITU**

With great foresight, Gissel undertook negotiations with ISO and ITU, the two sister organizations based in Geneva, with the objective of allocating competences and grouping technical and scientific resources and potentials. Interoperability was the absolute challenge, the key to the so-called merging technologies.

**Lord Kelvin Award**

It is also worth noting that it was also under the leadership of Hans Gissel that IEC created the IEC Lord Kelvin Award, first bestowed in 1995 on three experts for exceptional contributions to IEC work.

**Praise from his successor**

In his speech during Council in 1997, Bernard H. Falk, who succeeded Gissel as IEC President, paid tribute to the outstanding contribution and achievements of his predecessor:

“When I joined the IEC as President-Elect, a few years ago, I was, and I continue to be overwhelmed by Dr Gissel’s leadership abilities, and I must say it was a formidable task for me to follow the model of such an exemplary President. I learned immediately, during my first year as President-Elect, that I would take charge of the famous (and infamous) President elect task force and over the past two years, in his capacity as Immediate Past President, I can tell you, his guidance to me personally, to the Management Board, to the GPC, to the IEC in general, has been invaluable. Hans, you will be remembered by all of us for your enthusiasm and direct style. There was no hidden agenda for Dr Gissel: if he had something to say, he said it, unaffectedly. He always said exactly what he thought.

People perhaps did not always like what he said, but he said it! But I am sure you will remember that what he said sprang from his total devotion to the IEC and to the high standards he set for the Commission. It is very difficult to live up to these standards! But I know I speak for all of us, Hans, when I say we will remember the standards you have set and we will all try to reach them. So I wish to thank you on behalf of all of us and on behalf of the Commission.”

The President’s tribute to Dr Hans Gissel was supported by a long standing ovation and was officially part of the meeting report.

Dr Hans Gissel leaves behind his wife Ingeborg, his daughter Anne and his sons Ralf and Norbert, their children and grandchildren.
Cultivating the IEC experts and leaders of tomorrow

Registration to attend YP workshop opens in May

By Natalie Mouyal

The ninth IEC Young Professionals workshop will be held in Busan, Republic of Korea, on 22 to 24 October in conjunction with the IEC 2018 General Meeting. This workshop is an opportunity for the next generation of leaders to learn more about IEC and its work in standardization and conformity assessment.

The IEC Young Professionals (YP) Programme serves as a catalyst for the next generation of experts and leaders to become involved in IEC work. Developed for IEC and its National Committees to reach out to upcoming expert engineers, technicians and managers, the YP Programme helps to promote IEC standardization and conformity assessment activities. Young Professionals also bring a diversity of new voices to the organization. Since its launch in 2010, the Young Professionals Programme has welcomed a total of 468 participants from 50 countries.

IEC YP workshop

Each year, a new group of YPs is formally introduced to IEC at the annual Young Professionals workshop. Participants can network with the 3 000 IEC leaders and experts in standardization and conformity assessment attending the IEC General Meeting. The eighth edition of the YP workshop took place in Vladivostok, Russia in October 2017 and brought together 67 Young Professionals from 35 countries.

The YP workshop is an opportunity for Young Professionals to experience IEC in action. They can observe a meeting of the Standardization Management Board (SMB), the Conformity Assessment Board (CAB) or a technical meeting of their choice. Numerous breakout sessions provide participants with the opportunity to share their thoughts and, in one interactive session, to simulate a technical meeting.

A breakfast meeting is also held to foster the network between the Young Professionals and their National Committee Officers. Because National Committees serve as the gateway for Young Professionals to evolve in their
participation in IEC work, they are an essential element in the continued development and involvement of young experts and leaders.

**Ongoing support**

Once the YP workshop is completed, collaboration with the Young Professionals continues. Individual follow-up with all participants and their National Committees encourages further involvement at either the national or international level. Young Professionals are also invited to share their thoughts about future tools and services which will enable an enhanced and active participation in IEC work in the future.

Each year, the IEC Young Professionals Programme encourages the participants to join specific projects which contribute to their increased IEC involvement and to the development of the YP Programme. In previous years, these activities have included drafting a collection of business case studies and presenting IEC at local universities. Some YPs have been given the opportunity to take part in certain SMB and CAB groups as YP representatives. This year, a group of Young Professionals attended the IEC Future Leader’s Industry Forum in Munich to discuss cyber security in smart infrastructures, with the aim of producing a paper on the topic which will be submitted to the Market Strategy Board (MSB).

**National YP activities**

At the national level, a number of National Committees have begun organizing activities for their young experts.

In India, BIS launched its national equivalent IEC Young Professionals Programme in 2016 and has since organized three workshops. The most recent workshop was held in March in Bangalore. Similarly, China launched its first workshop in 2017 and is planning another one later this year. Other National Committees planning YP workshops in 2018 include Denmark, France, Germany, Italy, Japan, Mexico, Singapore, South Africa and the United Kingdom.

**Registration details**

Registration to participate in this year’s IEC Young Professionals workshop will be open from mid-May until the end of July. The YP workshop will take place in Busan, Republic of Korea from 22 to 24 October alongside the IEC General Meeting. It is expected that approximately 70 participants will attend from over 35 countries.

Prior to attending the YP workshop, upcoming Young Professionals are asked to complete an online pre-workshop training course to familiarize them with IEC work. It contains information slides, videos and a questionnaire for completion.

Further information about the IEC Young Professionals workshop can be found on the YP Programme web page. Details about the selection process in each country are available from National Committees.
The IEC family is growing

Peru and Côte d’Ivoire become IEC Members, São Tomé and Principe joins the Affiliate Country Programme

By Claire Marchand

In the past few months, IEC has welcomed two new Members, Peru in December 2017 and Côte d’Ivoire in March 2018, both countries joining IEC after about 15 years of participation in the IEC Affiliate Country Programme. In March as well, São Tomé and Principe became the latest participant in the Programme. Taking these changes into account, the IEC family now comprises 171 countries, of which 85 are Members and 86 Affiliates.

IEC welcomes Peru

Basic facts

Situated in Western South America on the South Pacific Ocean coast, Peru shares borders with Bolivia, Brazil, Chile, Colombia and Ecuador. It has a population of 31 million (July 2017 est.) and its capital is Lima. According to the World Bank Group, the GDP of the country in 2016 was USD 192 billion.

Peru’s topography, which ranges from the peaks of the Andes to the plains of the Pacific coastal regions and the tropical Amazon Basin rainforest.

Plaza Mayor and the Government Palace in Lima, Peru
and river, has a major impact on its economy. The Andes and the coastal areas are extremely rich in a variety of mineral resources, while the coast harbours many fisheries. The country is the world’s second largest producer of silver and copper.

Total electricity production amounts to 46.31 billion kWh while electricity consumption reaches approximately 41 billion kWh. The energy generated comes from fossil fuels for 62.6%, hydroelectric plants for 33.9% and other renewable sources for 4.3% (2015 est.).

**Peru and the IEC**

Peru joined the IEC Affiliate Country Programme in 2002 and, having adopted 50 or more IEC International Standards as national ones, as well as having set up a National Electrotechnical Committee (NEC), reached the Affiliate Plus status in 2010. In 2014, Rosario Uría, Director of the Standardization Department at INACAL, the Peruvian National Quality Institute, became Affiliate Leader, representing all Affiliate countries and liaising with IEC governing bodies. A year later, Peru took part in the Affiliate Mentoring programme, partnering with Mexico to increase the number of mirror technical committees in the country and participation in IEC work. Through ACAS, the Affiliate Conformity Assessment Status, Peru stakeholders, regulators in particular, were able to familiarize themselves with the IEC Conformity Assessment (CA) Systems and Schemes, thus learning how to verify the authenticity of IEC CA certificates.

Having gone through those stages, the natural next step was to apply for IEC membership, a formal request that was approved by Council in December 2017.

The electrotechnical interests of Peru are represented by the IEC National Committee (NC) of Peru. NC stakeholders are experts and professionals from different sectors, such as power generation (ENEL), power distribution (Luz del Sur, Distriluz Group), manufacturing, technology (including INACAL), academy, regulators and consumers. The President of the Peruvian NC is Orlando Chavez Chacaltana, Director, Direction of Electricity Regulation at the Ministry of Energy and Mines. The Vice-President is José Ortiz Ugarte, Commercial Manager at INDECO, a national leader in the cable industry. The Secretary is Rosario Uría and the Assistant Secretary Carmela Morgan Valencia, Standardization Executive at INACAL.

**IEC welcomes Côte d’Ivoire**

**Basic facts**

Côte d’Ivoire is situated in Western Africa, on the North Atlantic Ocean coast and bordered by Burkina Faso, Ghana, Guinea, Liberia and Mali. Its

![The plateau neighborhood, business district, in central Abidjan, Côte d’Ivoire (Photo: CNN)](image-url)
population is a little over 24 million. Yamoussoukro is its legislative capital and Abidjan its administrative and commercial capital. According to the World Bank Group, in 2016, the GDP of the country was USD 36 billion.

Agriculture engages about two-thirds of the Ivorian population. The country is the largest producer and exporter of cocoa beans as well as a major producer and exporter of coffee and palm oil. Climatic conditions and the fluctuation in international prices for these commodities may have a big impact on the economy. Outside agriculture, the country is developing its gold mining sector and is increasingly exporting electricity to neighbouring countries.

Total electricity production amounts to 8.2 billion kWh while electricity consumption reaches approximately 5.7 billion kWh. The energy generated comes from fossil fuels for 66.9% and from hydroelectric plants for 31.3 (2015 est.).

Côte d’Ivoire and the IEC

Côte d’Ivoire joined the IEC Affiliate Country Programme in 2003 and, having adopted 50 or more IEC International Standards as national ones, as well as having set up a National Electrotechnical Committee (NEC), obtained Affiliate Plus status in 2012. The NEC was established within CODINORM, the Ivorian Standardization Organization, and is now known as the National Committee of Côte d’Ivoire.

The NC has taken over from the NEC as host of the Economic Community of West African States (ECOWAS) Technical Harmonization Committee for Electrotechnical Standards (THC5) and, as did the NEC, will actively participate in the standardization work of the African Electrotechnical
Standardization Commission (AFSEC). The President of the NC is Serge Ahoussou, Director of Research and Planning at Société des Energies de Côte d’Ivoire (CI-Energies). The Secretary is Alain Constant Assa, Director of Standardization at CODINORM.

Stakeholders represent companies in the electricity sector, academia, telecommunications, air navigation, manufacturers and distributors of electrical equipment, ministries, government agencies, administration, professional and consumer associations.

São Tomé and Principe, a new Affiliate

Basic facts

São Tomé and Principe, which consists of two archipelagos around the main islands of São Tomé and Principe in the Gulf of Guinea, west of Gabon and just north of the Equator, joined the Affiliate Country Programme in March 2018.

The country has a population of 201,025 (July 2017 est.) and its capital is São Tomé. Total electricity production is 66 million kWh and electricity consumption 61.4 million kWh (2015 est.).

About the Affiliate Country Programme

The Affiliate Country Programme reaches out to developing countries, giving them the opportunity to get involved with IEC without becoming members. Participating countries benefit from free IEC International Standards for national adoption. IEC Central Office helps them become more aware of the benefits of using International Standards and more familiar with the work of IEC.
Trust in lab work

New edition of ISO/IEC 17025, the international reference for testing laboratories and calibration laboratories

By Claire Marchand

Since the publication of its first edition in 1999, ISO/IEC 17025 has become the international reference for testing laboratories and for calibration laboratories around the world. The Standard contains requirements for laboratories to enable them to demonstrate they operate competently and are able to generate valid results. The process ensures that a laboratory’s quality management system is thoroughly evaluated on a regular basis to guarantee continued technical competence and compliance with ISO/IEC 17025.

Changes in the third edition of ISO/IEC 17025

ISO/IEC 17025 is an International Standard developed according to the international best practices defined in the ISO/IEC Directives which includes circulation for voting to the national bodies of IEC and ISO, and approved by both organizations.

The third edition, published in November 2017, takes into account the numerous changes in market conditions that have occurred since 2005, when the second edition was issued. For instance, the Standard focuses on information technology, with a new section devoted to the use of computer systems and electronic records, as well as the production of electronic results and reports. The publication also puts the emphasis on the results of a process rather than on a detailed description of its tasks and steps.

The updated edition has also adopted a new structure aligned with the other Standards in the ISO/IEC 17000 series for conformity assessment.

The 2005 edition was split into two main sections: Management requirements and technical requirements. The 2017 version has five sections:

General requirements

Laboratories have to commit to impartiality and confidentiality in their activities.

The European Interoperability Centre tests interoperability between electric/hybrid vehicles and smart grids (Photo: European Interoperability Centre/EU 2015)
Structural requirements

The laboratory is a legal entity that is legally responsible for its activities. As such, the laboratory has to, among other things, identify management that has overall responsibility, define its organizational and management structure, the range of its activities, document its procedures and specify the role of anyone managing, performing or verifying work affecting the results of the laboratory.

Resource requirements

This section describes in many details all facets, processes and procedures linked to personnel, facilities and environment, equipment, metrological traceability as well as externally provided products and services.

Process requirements

Process requirements address the review of requests, tenders and contracts, the selection, verification and validation of methods, sampling, the handling of tests or calibration items, technical records, the evaluation of measurement uncertainty, ensuring the validity of results, reporting of results, complaints, nonconforming work and the control of data and information management.

Management requirements

A clause in the management requirement section addresses risks and opportunities associated with the laboratory activities, a first in the history of ISO/IEC 17025. Addressing risks can include “identifying and avoiding threats, taking risk to pursue an opportunity, eliminating the risk source, changing the likelihood or consequences, sharing the risk or retaining risk by informed decision”.

As for opportunities, they can “lead to expanding the scope of the laboratory activities, addressing new customers, using new technology and other possibilities to address customer needs.”

Benefits of using ISO/IEC 17025

ISO/IEC 17025 enables laboratories to demonstrate that they are technically proficient and able to produce precise and accurate test and calibration data, thus promoting confidence in their work at the national, regional or international level. It also helps facilitate cooperation between laboratories and other bodies by generating wider acceptance of results between countries. Having test reports and certificates issued in one country accepted and recognized in many others, without the need for further testing, also helps improve international trade.

For more on the ISO/IEC 17000 series of International Standards, please visit the IEC Webstore.
Simplifying the use of sound calibrators
New revised edition of IEC 60942

By Catherine Bischofberger

IEC Technical Committee 29: Electroacoustics, has issued a new redline version of IEC 60942, the International Standard for sound calibrators.

The IEC has published edition 4 of the International Standard for sound calibrators IEC 60942, prepared under the remit of IEC TC 29: Electroacoustics. It replaces the previous one issued in 2003, and is available as a redline version (RLV).

Noise levels in the workplace can be detrimental to workers' health (Photo: US department of defense)
IEC TC 29 publishes Standards relating to instruments and methods of measurement in the field of electroacoustics. This includes sound level meters and calibrators, but also hearing aids and equipment used for measuring aircraft noise.

“Sound calibrators should be used by anyone making a measurement with a sound level meter or a microphone. They are employed to check and adjust the overall sensitivity of acoustical measuring devices or systems,” explains Chair of TC 29, Susan Dowson.

**No manual corrections required**

The Standard was updated to take into account advances in modern-day electronic circuitry. Most calibrators can now automatically conform to environmental criteria requirements, for instance to the effects of static pressure, ambient temperature and humidity.

“Corrections for static pressure, ambient temperature or humidity used to be applied manually to ensure the sound calibrator met the specifications of the Standard. But now things are much more straightforward and in most cases there is no need for the user to worry about making these corrections,” says Susan Dowson.

In the new Standard, the class designations LS/C, class 1/C and class 2/C have been removed. These designations are applied to sound calibrators that required corrections for any static pressure (class LS/C and class 1/C), ambient temperature and ambient relative humidity (class 2/C), to meet the requirements of the Standard.

Two new class designations have been added, class LS/M and class 1/M, specifically for pistonphones, a type of calibrator which is operated mechanically and which still requires corrections for static pressure. “The changes in the new Standard really simplify the use of sound calibrators and makes specifications clearer for manufacturers at the design stage,” adds Susan Dowson. The Standard is maintained by MT17, a maintenance team of TC 29 of which Susan Dowson is also the Convenor.
Upcoming global events

On the agenda: Energy and utilities, IoT, energy storage, EV batteries and hydropower

By Claire Marchand

The IEC regularly supports key global and regional industry events, which can present the IEC endorsement on their website and materials.

Intellisub Europe 2018
Düsseldorf, Germany, 10-12 April 2018

120+ utility substation asset management, engineering, operations & maintenance, and cyber-security professionals will discuss investment drivers, new system architectures, operations & maintenance for new/refurbished substations in HV, MV and LV networks and more.

IoT Tech Expo Global 2018
London, UK, 18-19 April 2018

On the agenda: technology advancements, case studies, IoT ecosystem: smart energy & cities, connected industry, connected enterprise, data analytics for AI & IoT, connected transportation, privacy & security and more.

IEC participants benefit from a 20% special discount using the promo code: IEC20.

2018 Industrial Control Systems (ICS) - Cyber Security Conference
Singapore, 24-26 April 2018

Join the energy, utility, chemical, transportation, manufacturing, and other industrial and critical infrastructure organizations and get latest on ICSs, protection for SCADA systems, plant control systems, engineering workstations, substation equipment, programmable logic controllers (PLCs) and more.

IEC participants benefit from a 10% special discount using the promo code: IEC18.

Digital Utilities Europe 2018
Amsterdam, The Netherlands, 16-17 May 2018

Join key industry players to discuss swift digital transformation, EU regulations, case studies, cyber security, energy business models, e-mobility, energy efficiency and more.

IEC participants benefit from a 15% special discount using the promo code: EDUE3D15.

Berlin, Germany, 14-18 May 2018

This is Europe’s first conference for energy storage with over 250 utilities attending. In two separate forums, industry leaders and practitioners from utilities, EPCs and international regulators from 22+ countries will discuss large scale focus and residential energy storage.

IEC participants benefit from a 10% special discount using the promo code: IEC18.

European Electric Vehicle Batteries Summit 2018
Munich, Germany, 20-21 June 2018

Key industry stakeholders will discuss latest technologies, V2G, energy
storage, new business models, case studies, second life and recycled batteries and more.

IEC participants benefit from a 20% special discount until 28 February and 15% until 5 June using the promo code: EBAe1MKT.

**Hydrovision 2018**

**Charlotte, NC, US, 26-28 June 2018**

Global hydro experts will discuss asset resilience and sustainability, civil works and dam safety, operations and maintenance, policies and regulations, equipment and technology, marine and hydrokinetic energy and more.

**IoT Tech Expo Europe 2018**

**Amsterdam, The Netherlands, 27-28 June 2018**

On the agenda: smart building and facilities management, building the connected supply chain, intelligent city and transport management, smart grid data management and analytics, asset monitoring and management, delivering smart connected new products, and more.

IEC participants benefit from a 20% special discount using the promo code: IEC20

The complete list is on the IEC events & meetings webpage.
In a world abuzz with “innovative” products, services and business models it’s sometimes easy to forget that innovation is often a long process and one that is based on the inventions and innovations, successes and failures that came before.

In the forthcoming issue of e-tech we look at innovations that have changed the world over the past one hundred years and impacted IEC work, as well as the essential role that standardization plays in the innovation process and roll-out. From bar codes to drones and the IoT, we examine how innovation is often developed within one field, only to be taken up and adapted by another.

In the next issue:

**A century of innovations - Issue 3, 2018**