IEC role in the IoT
The physical world at large is now becoming an information system. Billions of devices and systems are “sensorized” and connected to the Internet to share relevant data with relevant systems often in real-time.

The term “Internet of Things” is believed to have been coined for the first time in 1999 by Kevin Ashton, Executive Director of the Auto-ID Center, in a presentation he made to Procter & Gamble. And while nearly 90% of the global population has never heard of IoT, its effect is starting to permeate every aspect of our lives. Everywhere you look devices are connected and many more will be added over the next years. Dog bracelets, pill boxes, fridges that communicate when a food item is missing or has expired, insulin pumps or a smart toothbrush that tracks how well you clean your teeth, thermostats, meters, and so much more.

Devices collect and send a myriad of data that are generated by the user and their environment. The IoT of the ordinary person will be constituted of hundreds of everyday objects running independently but communicating with each other directly, through smart phones, wearables or ways we have yet to imagine.

“Billions of devices and systems are “sensorized” and connected to the Internet...
Ongoing feedback loops

Connected devices are able to sense their environment and constantly provide feedback enabling instant and ongoing adjustments. Many of these systems work and communicate without the intervention of any human being. They sense occupation and turn lights or air-conditioners on and off, help manage water or energy consumption, turn on insulin pumps or manufacturing lines.

This constant feedback of data provides opportunities for many new information services. Those can include recommendations for improved viewing or reading, or pre-settings in devices that take into account preferences such as temperature or volume settings. It may also register food preferences and point to relevant menu items in a restaurant. The possibilities are near limitless.
When did the IoT start?

Contrary to what people think, the concept of the IoT is not new, only the acronym is. ATMs were among the first connected objects back in 1974. By 2008 more devices were connected to the Internet than people. This is largely due to a move from a desktop computer-driven Internet to a device-driven one.

The launch of smart phones, the fact that sensors are now incredibly cheap and smaller than ever before and the advent of smart algorithms have led to an acceleration of consumer-oriented IoT applications and with it new business opportunities. By 2020 an estimated 30 billion objects will be part of the IoT according to the most recent forecasts.

The next step is taking us to devices that are worn on the wrist, directly on the skin and soon under the skin. Before the advent of the “Internet of Everything”, the answer to the question “when were you last online?” was simple to answer: last time I logged in at my computer. Not anymore though. Now you are online with your e-reader, your smart watch or even your refrigerator.

But IoT is much broader than consumer devices. In industrial applications and power generation, digitization, connectivity and automation have been a reality for many years. The same is true for health and home care, buildings, mobility and much more. However, in the coming years, we will see a dramatic acceleration in the penetration of always connected devices and systems. The key drivers are efficiency gains, cost reductions as well as convenience to end users.

By 2020 an estimated 30 billion objects will be connected.
Why is standardization for IoT needed?

As with most disruptive technologies, IoT solutions are developed by a wide range of providers promoting their proprietary approaches. This can severely impact interconnectivity. With the expansion of the IoT, there is now an increased need for interoperability of many different systems and platforms. This can only be achieved through broad International Standards. Such Standards will establish common ground regarding topics such as terminology (ISO/IEC 20924, Definition and vocabulary for the Internet of Things) or reference architectures (ISO/IEC 30141, Internet of Things Reference Architecture) that will help product developers deploy an interoperable ecosystem. Without such Standards, the IoT will be stuck on isolated islands and this will hamper its expansion.

IEC work for IoT

Many different IEC Technical Committees support the advent of the IoT. Their work covers a broad range of technologies, including sensors, processors, displays, printed electronics, but also functional safety, automation, cyber security, cloud computing, fibre optics and all the surrounding hardware that enables the IoT.

Sensors and IoT

Sensors and micro-electromechanical systems (MEMS) are key components of the IoT. Essentially, anywhere you have a system with added intelligence you are likely to find a sensor.

A decade ago, sensors were much less common in electronics. They were generally reserved for cameras and most were used in airbags. Since then the cost for sensors has dramatically decreased. Today, there is not a single technology where sensors don’t play a major role. They have literally invaded everything: enabling measuring,
data capture and constant feedback. Any smart phone today has multiple digital microphones to capture voice, and cancel environmental noise, one or more cameras, motion sensors, and more.

Sensors make driverless cars possible, are behind the latest wave of wearables and are able to collect vital information in a non-invasive way, changing our approach to healthcare. The fact is: a sensor can be used in a multitude of systems and devices. The field of application is as wide as that of the IoT.

There is not a single technology where sensors don’t play a major role

IEC work for sensors

The rules that guide sensors and their work are an integral part of many IEC International Standards, for example the IEC 61508 Functional Safety series developed by IEC Subcommittee (SC) 65A; or IEC 61757 on fibre optic sensors developed by IEC SC 86C. IEC Technical Committee (TC) 47 prepares publications that relate to semiconductor devices, including sensors. IEC TC 76 covers sensors that rely on lasers and the list could go on.

Nanotechnology and the IoT

Sensors are tiny, but they are now getting even smaller. Two-dimensional materials such as graphene allow further miniaturization of sensors; two-dimensional because they are only one atom thick. Work on graphene and carbon nanotube materials is coordinated in IEC TC 113. Graphene is an ideal material for sensors due to its attractive thermal and electrical conductivity, electrical properties and a large surface to volume ratio.

What is a sensor?

Basically a sensor is a device that responds to a physical stimulus such as heat, light, sound, pressure, magnetism or motion and transmits information that is used to generate an action, such as on/off, open/close or start/stop.
Big Data and the cloud

While sensors collect data autonomously, they need processors to pull out the information contained in this data. The accessibility of increasingly affordable computing power is a key element in making sense of these increasingly large data streams.

The shift to digital has massive ramifications for data. We are surrounded by an explosion of data. Experts estimate that 90% of the world’s data has been generated between 2013 and 2016. As digitization continues, data generation accelerates. As data grows, we need new ways to create order from increasing chaos and extract meaningful, actionable information. The IEC and ISO work together in ISO/IEC Joint Technical Committee (JTC) 1/WG 9 on Big Data to scope the role of standardization in this area and identifying gaps that need to be addressed.

Whereas data used to be exclusively stored on devices, much of it is now kept in the cloud. This offers a near infinite data storage capacity that can be accessed from anywhere. The IEC via ISO/IEC JTC 1/SC 38 works among other things on Standards for cloud computing and distributed platforms.

90% of the world’s data has been generated between 2013 and 2016.
Cybersecurity and IoT

Big Data opens many new market opportunities but it also generates new risks including that of cyber attacks or questions around the ownership of information as well as privacy concerns.

Experts feel that the biggest problem facing IoT will not be the communication between devices or the collection and ability to share data but rather the safe-keeping of data. Global vulnerability to malicious acts in cyberspace is growing. The failure to secure one device can have a direct impact on many others and there is an increasing need to apply strong security techniques to avoid that risks are passed onto more important systems. The exploitation of cyber vulnerabilities of infrastructure systems is becoming an increasing threat to business and society’s overall security.

New risks: cyber attacks, ownership of information, privacy concerns

The IEC has published over 200 International Standards that very directly address cybersecurity and privacy of health, business and critical infrastructure systems.

The IEC Conformity Assessment Systems are also active in cybersecurity; the IEC Conformity Assessment Board Working Group 17 is focused on home automation, smart devices as well as medical devices.

ISO/IEC 27001 and ISO/IEC 27002 provide a common language to address governance, risk and compliance issues related to information security. ISO/IEC 27031 and ISO/IEC 27035 help organizations to effectively respond, diffuse and recover from cyber attacks. There are also ISO/IEC Standards that ensure the protection of personally identifiable information, define encryption and signature mechanisms that can be integrated into products and applications to protect online transactions, credit card use and stored data.

Safe and secure IoT platforms

How data is collected and implemented will determine how transformational the IoT can become. Security grows exponentially in importance as devices that where once isolated become interconnected and more and more information is collected. Bringing the ambitious visions expressed by the IoT to reality will require significant efforts in standardization.

The IEC Market Strategy Board has worked with Fraunhofer Institute for Applied and Integrated Security as well as SAP to prepare a White Paper that provides an overview of key requirements for smart and secure IoT platforms.

It aims to provide an overview of current IoT limitations and deficiencies in the area of security, interoperability and scalability. It also discusses next generation platform-level technologies and provides important recommendations to IoT stakeholders and for IoT standardization work.
Energy is another area where IoT plays a crucial role.

In the consumer energy space, IoT is frequently used to provide feedback that allows consumers to adapt and change their behaviour with regard to electricity consumption. While this approach increases awareness regarding conservation, savings are relatively small at around 3%. It is much more efficient to build efficiency controls directly into appliances and use automation.

The IoT is an integral part of the Smart Grid. It helps increase the visibility of where energy is used or lost and allows to identify cost saving potentials. With the IoT energy can be managed based on immediate data rather than historic patterns of energy use.

Real-time awareness of local conditions allows for immediate detection and action. The IoT is indispensable to optimize the integration of renewables and distributed energy generation.

Data mining and social networking can help increase the comfort of end users, overall energy efficiency and facilitate diagnostics and maintenance. The IoT also opens the door to energy services and payment tariffs that can dramatically reduce energy costs, increase performance visibility and boost sustainability.

The IoT in energy applications allows for more real-time operations, increasing control and decreasing the time it takes for information to travel and corrective actions to be taken.

Going forward, connected devices such as fridges, air-conditioners, thermostats, smart meters, washing machines, etc. are all expected to become an integral part of the energy IoT as a means to balance the larger grid.

The IoT is indispensable to optimize the integration of renewables and distributed energy generation.

The IEC prepares the large majority of all technical Standards for the Smart Grid and the automation, safety and security of energy generation and distribution.
Sensorization and interconnectivity of medical devices is not a new concept – this has been a vital part of care within the hospital environment for years. However, until recently it has not been a viable option for personal monitoring outside highly centralized care settings.

Societal trends such as ageing populations have resulted in a need for personal monitoring based on sensor systems outside these traditional in-patient care settings. A new generation of sensors and connected devices represents an enabling technology for a more patient-centric, decentralized health care system. To satisfy the needs of this relatively new business sector, the IEC has put in place a Systems Committee on Active Assisted Living (AAL). It brings together many different stakeholders and is an excellent example for broad collaboration between the IEC, fora and consortia with an objective to ensure the interoperability of different systems from different vendors.

International Standards are a key element of the IoT in healthcare and IEC TC 62: Electrical equipment in medical practice, is pivotal to this work. But as we move into an environment of “sensors everywhere”, other IEC TCs will be called upon to make a contribution.

For example, the work of TC 21: Secondary cells and batteries, is important for power, as is that of TC 119: Printed electronics, for production technologies. Wireless communication Standards support systems placed on (or in) the patient whilst enabling patient mobility and ensuring the security of their highly personal data.

The fabrication technologies of TC 21 and TC 119 bring the technology into ever cheaper and smaller domains, facilitating systems ranging from disposable adhesive patches to reusable on-body devices. And in this mix we may soon see smart medical dressings making possible the real-time monitoring of wounds for infection and the rate of healing.

Data and healthcare

Data will transform healthcare by customizing treatments and empowering patients.

Next-generation medicine will utilize more complex models of physiology and more sensor data than any doctor could comprehend. Much of what physicians do – check-ups, testing, diagnosis, prescriptions, behaviour modifications – can be done by automated systems, which passively and actively collect and analyze data.

Any of the rudimentary tests like blood pressure, insulin levels and heart rate can be conducted without the need to visit a doctor.

Additionally, instead of providing a one-time limited view, there will be a wealth of continuous data available that can be sent to the physician, alerting him in case of need.

With an ageing population and increasing number of chronic conditions such as diabetes and hypertension, digital data will allow doctors to know more about their patients and enable them to provide increasingly customized care, more efficiently.

IoT and personal safety

The IoT is also likely to become much more widespread in the personal safety sector and in hazardous environments. Human performance and wellness monitors are being developed for the military, pilots and emergency service personnel using wearable technologies. They require biosensor technologies looking at early warning signs of stress, fatigue or injury.
IoT in smart buildings, homes
The concept of smart buildings and home automation has been around for quite some time and is just another example for what we call today the IoT.

In smart commercial buildings, the IoT enhances the capability of building management systems to automate control functions and optimize efficiencies. The connectivity provided by the IoT allows for the integration of disparate automated systems and intelligent devices.

Sensors for detecting motion, noise, moisture, temperature, humidity, fire and smoke, carbon dioxide and hazardous gases, security and access control systems all supply data and analytics in real-time. The resulting fast responsiveness allows buildings to adapt to changing conditions and make real-time alterations that result in increased efficiency and reduced operating costs. With this information, building managers are able to anticipate the needs of tenants, preferences for lighting, heating or ventilation and oversee security systems, utility meters or water and waste disposal, to name but a few.

**IEC work for smart buildings**

Electricity and electronics as well as processors, sensors and other hardware are indispensable for the operation of smart buildings. Standardization is a fundamental principle here.

Many IEC TCs and SCs coordinate on the development of International Standards that apply to smart buildings. The emphasis is on safety and interoperability among the broad range of systems, equipment and applications used in the construction and maintenance of smart buildings. They include for example ISO/IEC JTC1/SC 25, which develops International Standards for smart homes and buildings.

**IoT for building efficiency**

Energy efficiency and sustainability are major features of a smart building. Buildings on average consume about 30% of the world's energy, and savings of up to a quarter of costs could be achieved by using advanced building management systems and analytics to optimize performance in areas such as ventilation, temperature, lighting and air quality.

Heating, ventilation and air conditioning systems are intended to detect automatically and respond intelligently to variables such as weather conditions, time of day and occupancy of the building, with the help of sensors and other data gathering equipment. For example, HVAC systems in smart buildings should be able to switch off lights automatically in areas where there are no occupants, or adjust the temperature according to weather conditions and the number of occupants in a room.

**Advanced building management systems can achieve savings of up to 25%**

**IoT and cities**

As buildings become incorporated into the wider networks of smart cities and linked to other aspects such as transport, water and air quality, the increasing intelligence and automation of buildings will play a key role in the smart cities of the future.

Two IEC White Papers are relevant to buildings and cities in particular. The first surveys the role of wireless sensor networks in the evolution of the IoT. It assesses the need for Standards to achieve interoperability among wireless sensor networks from different vendors and across varied applications, in order to unleash the full potential of the IoT. The other focuses on how to orchestrate the infrastructure that is needed for smart and sustainable cities.

The IEC has also put in place a Systems Committee on Smart Cities, which prepares relevant International Standards.
IoT and lighting

Smart street lighting is a first “killer app” that uses the IoT. With an annual growth rate of 20.4%, smart street lamps are expected to reach 6.8 million units by 2023.

Such lamps integrate a large number of services that can themselves be further connected to other devices and systems. They include for example:

- On-demand light levels, fully dimmable and responsive to ambient lighting
- Announcement systems for public, traffic or emergency transmissions
- Image and proximity sensors, for example to count foot traffic or identify missing persons
- Digital signage for traffic information, alerts, advertising or street signs
- Emergency or push to talk systems
- Internet access and transceivers

And here, as elsewhere, much of the hardware and protocols are guided by IEC International Standards made by many different IEC TCs.
IoT and mobility

Transportation systems of every kind will benefit from the IoT. Vehicle-to-infrastructure and vehicle-to-vehicle communication systems will help improve the safety, efficiency and environmental performance of public and private transportation. They will also help reduce congestion in cities, improve space management and reduce accidents and resulting health costs.

Drivers of connected cars benefit from a large number of services, including navigation, real-time traffic and parking information, infotainment and an integration of smart phones with dashboards and wearable devices. All of the systems that drive these services rely on IEC work in standardization and conformity assessment.
IoT and industry
Smart manufacturing or Industry 4.0 will cover the whole value chain and life cycle of a product from idea to order, construction and development, delivery, recycling including all related services as well as real-time integration of user or consumer input and feedback.

Information and collected data will allow continuous optimization of cost, availability and resource consumption beyond company borders up to and including mass customization.

IEC work for Industry 4.0

Standardization is of central importance for smart manufacturing. Industry 4.0 requires an unprecedented integration of systems across domains, hierarchic boundaries and life cycle phases. In the IEC standardization work for automation and the digitalization of industrial processes and related technologies was initiated long before the term Industry 4.0 was coined.

Today the Standards domain of the process and plant floor is largely covered by IEC TCs, while management systems are addressed by ISO.

For a very long time

IEC TC 65, for example published some of the most important International Standards that cover wireless communication networks and communication profiles that rely on industrial protocols such as HART, Fieldbus or real-time Ethernet. The aim is to enable wireless interoperability of intelligent measurement and control devices from different vendors and to support the full range of communication, monitoring, control, safety, security applications in field and plant automation for:

- Equipment and processes
- Regulatory compliance and energy consumption
- People management, health, safety, environment
- Asset management
- Predictive maintenance and advanced diagnostics

Many technical committees

But there are many other IEC TCs that contribute the essential know-how and expertise to the many individual technologies and protocols that enable Industry 4.0.

IEC work covers everything from:

- energy consumption, including for example piezoelectrics or batteries in all forms and shapes, to electric motors, actuators, data transfer and cloud storage or computing in general
- Acoustic, ultrasound, gyroscope, temperature, pressure and many other types of sensors
- Localization and tracing technologies such as RFID or global navigation satellite systems
- 3D printing, printed electronics, lasers, robotics, access control but also risk management, privacy and security, cyber security, to name but a few.

IEC systems approach to Industry 4.0

One of the most fundamental changes in manufacturing is the need for a systems approach. It is no longer enough to look at the devices and small systems that are used on the plant floor. Smart manufacturing will need to integrate a top-down systems perspective. For this very reason, the IEC has put in place the Systems Evaluation Group: Smart Manufacturing to provide a platform where industry can sit and drive what is needed for Industry 4.0. The aim is to connect experts from around the world and share know-how beyond traditional boundaries, integrating expertise also from outside organizations.

In this context, the IEC published the White Paper Factory of the future to assess the potential global needs, benefits, concepts and pre-conditions for smart manufacturing. It identifies business trends in related technologies and markets as well as their impact on data, people, technologies and Standards. The White Paper was developed in cooperation with the Fraunhofer Institute for Manufacturing Engineering and Automation IPA.

Another IEC White Paper that also applies to smart manufacturing is entitled Internet of Things: Wireless Sensor Networks. In the context of smart manufacturing it focuses on infrastructure technologies, applications and standards featured in wireless sensor network designs. The White Paper also assesses the potential global needs, benefits, concepts and pre-conditions for the factory of the future. It was developed in cooperation with NIST, the US National Institute of Standards and Technology.
Low voltage direct current (LVDC) technology will open the path to bringing IoT to the less developed world. It will enable the connection of devices in an energy efficient way in rural areas.

Solar PV generates direct current. And yet – even in rural settings – this energy is transformed into alternating current. This is a nonsense that results in unnecessary efficiency losses. LEDs, cell phone chargers and PCs can all function perfectly fine with direct current.

The IEC is now preparing the Standards that are needed to make direct current perfectly safe for off-grid use for almost all electrical applications, including in rural homes.

The IEC is addressing the challenges of LVDC, including voltage, design, equipment and rules of installation.

LVDC: the path to bringing the IoT to developing countries
Further information

Please visit the IEC website at www.iec.ch for further information. In the “About the IEC” section, you can contact your local IEC National Committee directly. Alternatively, please contact the IEC Central Office in Geneva, Switzerland or the nearest IEC Regional Centre.

**Global**

**IEC – International Electrotechnical Commission**

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

T +41 22 919 0211
Fax +41 22 919 0300
info@iec.ch
www.iec.ch

**Asia Pacific**

IEC-APRC – Asia-Pacific
Regional Centre
2 Bukit Merah Central #15-04/05
Singapore 159835

T +65 6377 5173
Fax +65 6278 7573
dch@iec.ch

**Latin America**

IEC-LARC – Latin America
Regional Centre
Av. Paulista, 2300 – Pilotis Floor – Cerq.
César
São Paulo - SP - CEP 01310-300
Brazil

T +55 11 2847 4672
as@iec.ch

**North America**

IEC-ReCNA – Regional Centre for North America
446 Main Street, 16th Floor
Worcester, MA 01608
USA

T +1 508 755 5663
Fax +1 508 755 5669
tro@iec.ch

**IEC Conformity Assessment Systems**

—

**IECEE / IECRE**

c/o IEC – International Electrotechnical Commission
3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
secretariat@ieceee.org
secretariat@iecre.org
www.iecree.org
www.iecre.org

**IECEx / IECQ**

The Executive Centre
Australia Square, Level 33
264 George Street
Sydney NSW 2000
Australia

T +61 2 4628 4690
Fax +61 2 4627 5285
chris.agius@iecex.com
chris.agius@iecq.org
www.iecex.com
www.iecq.org

**IEC Regional Offices**

—

**Africa**

IEC-AFRC – Africa Regional Centre
7th Floor, Block One, Eden Square
Chiromo Road, Westlands
PO Box 856
00606 Nairobi
Kenya

T +254 20 367 3000 / +254 20 375 2244
M +254 73 389 7000 / +254 70 493 7806
Fax +254 20 374 0913
eod@iec.ch
fya@iec.ch

**Europe**

IEC – International Electrotechnical Commission
Central Office
3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
Fax +41 22 919 0300
info@iec.ch
www.iec.ch

**IEC Regional Offices**

—

**Asia Pacific**

IEC-APRC – Asia-Pacific
Regional Centre
2 Bukit Merah Central #15-04/05
Singapore 159835

T +65 6377 5173
Fax +65 6278 7573
dch@iec.ch

**Latin America**

IEC-LARC – Latin America
Regional Centre
Av. Paulista, 2300 – Pilotis Floor – Cerq.
César
São Paulo - SP - CEP 01310-300
Brazil

T +55 11 2847 4672
as@iec.ch

**North America**

IEC-ReCNA – Regional Centre for North America
446 Main Street, 16th Floor
Worcester, MA 01608
USA

T +1 508 755 5663
Fax +1 508 755 5669
tro@iec.ch

**IEC Conformity Assessment Systems**

—

**IECEE / IECRE**

c/o IEC – International Electrotechnical Commission
3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
secretariat@ieceee.org
secretariat@iecre.org
www.iecree.org
www.iecre.org

**IECEx / IECQ**

The Executive Centre
Australia Square, Level 33
264 George Street
Sydney NSW 2000
Australia

T +61 2 4628 4690
Fax +61 2 4627 5285
chris.agius@iecex.com
chris.agius@iecq.org
www.iecex.com
www.iecq.org

**IEC Regional Offices**

—

**Africa**

IEC-AFRC – Africa Regional Centre
7th Floor, Block One, Eden Square
Chiromo Road, Westlands
PO Box 856
00606 Nairobi
Kenya

T +254 20 367 3000 / +254 20 375 2244
M +254 73 389 7000 / +254 70 493 7806
Fax +254 20 374 0913
eod@iec.ch
fya@iec.ch