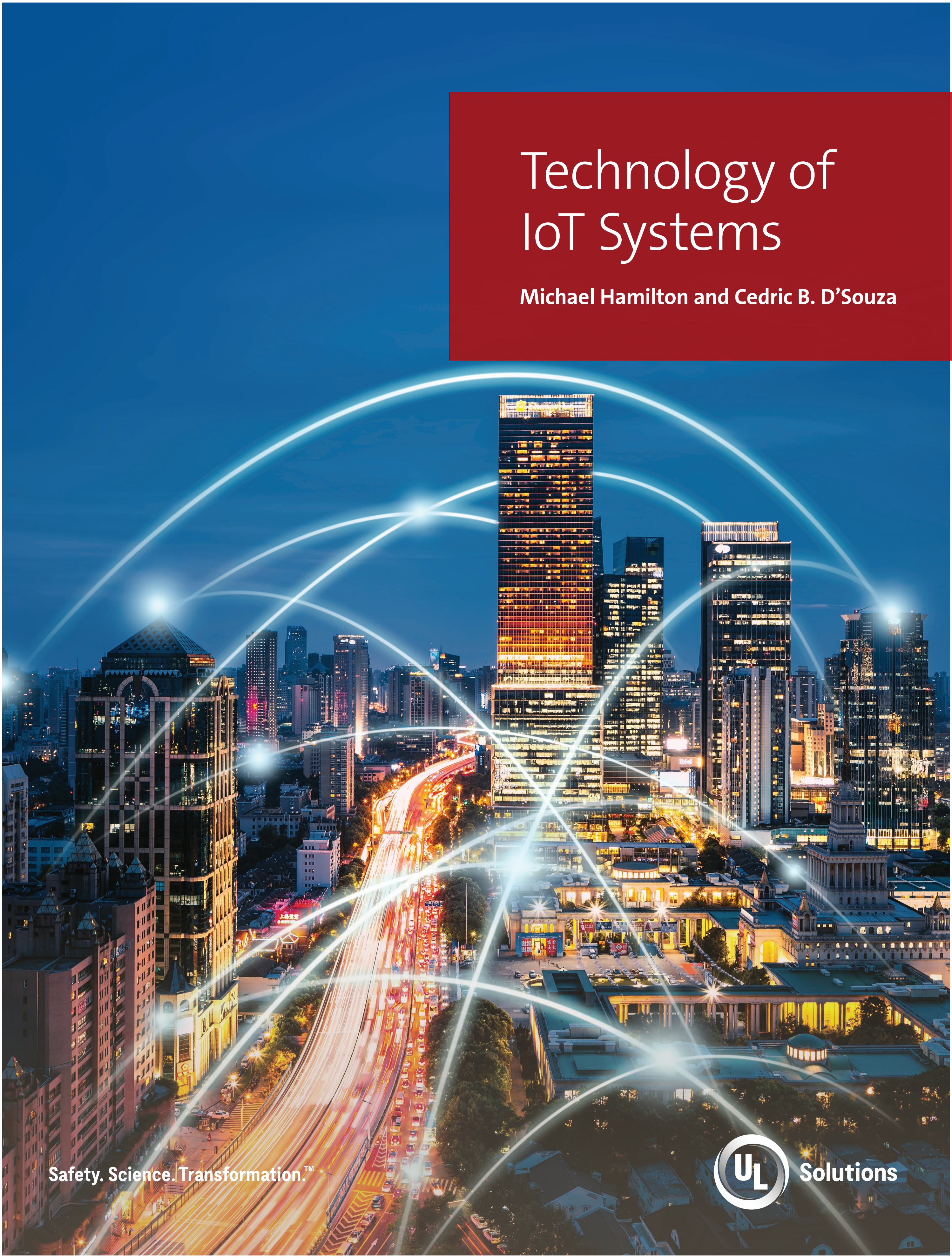
Technology of IoT Systems

Michael Hamilton and Cedric B. D’Souza



Safety. Science. Transformation.™

UL Solutions

Executive summary

This paper discusses the technology and usages of Internet of Things (IoT) systems in general, as well as specific concerns with respect to human factors, interoperability and resiliency. We present a general overview of IoT systems, followed by a more in-depth examination of smart cities with a focus on smart grids, bridge monitoring and drones as they relate to the smart city and IoT systems. This paper then examines the IoT services UL Solutions currently offers, followed by a systems-oriented approach to complex IoT system evaluation and how the system development life cycle (SDLC) may be used to approach such a complex evaluation by applying the V-model. Finally, this paper looks at some of the future growth areas in IoT — namely, security and interoperability.

Table of contents

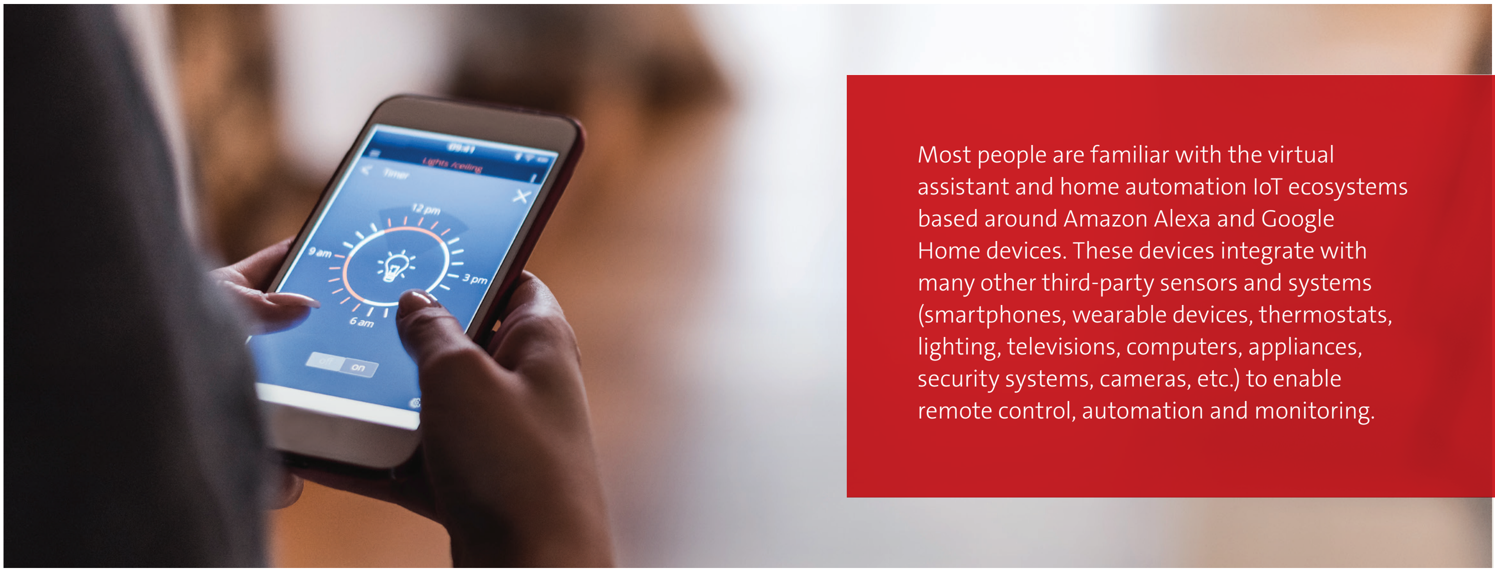
Overview

The term Internet of Things was coined in 1999; in its broadest definition, it is the network of physical objects that contain embedded technology to communicate, sense or interact with their internal states and the external environment (Gartner, 2019). Simply put, these "things," i.e., devices, can send and receive data and connect to the internet via various protocols: Wi-Fi, LPWAN, Zigbee, Bluetooth®, GSM/5G, proprietary networks and others (Badii et al., 2020). A typical IoT system consists of components such as devices, network connections, data management (cloud or premises) platforms and applications. IoT systems are complex in terms of hardware and software, supported by a continuously growing ecosystem of original equipment manufacturers (OEMs), suppliers, system integrators and users.

There are many different categories of IoT, including building automation, industrial, agricultural, smart city, medical and military. Most people are familiar with the virtual assistant and home automation IoT ecosystems based around Amazon Alexa and Google Home devices. These devices integrate with many other third-party sensors and systems (smartphones, wearable devices, thermostats, lighting, televisions, computers, appliances, security systems, cameras, etc.) to enable remote control, automation and monitoring.

On a larger scale, an industrial IoT system (see Industry 4.0 in the glossary) may link various machinery and power distribution in a manufacturing facility. A smart city may integrate parking, autonomous vehicles (AVs), street lighting, renewable energy sources, traffic and bridge monitors in an urban area. A smaller-scale IoT ecosystem might include an implanted medical device, such as a pacemaker with a wearable smartwatch for monitoring, or a sensor in a hospital bed linked with the nurse's station. IoT is not limited to urban settings, either — IoT in agriculture can be used for monitoring crops, weather conditions and soil quality, all to promote higher yields and protect the environment (IoT World Congress, 2019).

Each system can include a multitude of devices and connection methods, and each comes with its own set of challenges for integration and operation. Security is one concern and is usually a top priority — the attack surface increases as more devices are connected to network infrastructures. Malicious actors have used printers, voice over Internet Protocol (VoIP) phones, video decoders and other IoT devices to penetrate targeted computer networks (Goodin, 2019). There are also many concerns with respect to the systems' human factors, interoperability, reliability and resiliency. This paper will look at the specific example of the smart city and how human factors, interoperability and resiliency may be affected at various levels of the system. This paper discusses the concept of the "smart city" in more detail later.



Most people are familiar with the virtual assistant and home automation IoT ecosystems based around Amazon Alexa and Google Home devices. These devices integrate with many other third-party sensors and systems (smartphones, wearable devices, thermostats, lighting, televisions, computers, appliances, security systems, cameras, etc.) to enable remote control, automation and monitoring.

Characteristics

Before delving into any specific examples, we must first understand some key attributes of an IoT system. There are many characteristics that one can consider: design, safety, security and privacy, storage, control, sustainability and many others. This paper will focus on three specific attributes relevant to product safety: human factors, interoperability and resiliency. We will look at these terms in general and with an eye toward their specific application in an IoT system example.

Interoperability refers to a system's ability to operate with other devices or systems, even if they are designed and manufactured by different companies at different times.

Human factors

"Human factors is the scientific discipline that studies how people interact with devices, products and systems" (Human Factors and Ergonomics Society, 2018). With respect to IoT devices, this can affect a device's safe operation based on human error in operation or design. Examples of these include:

- Errors in coding
- Poorly designed human-machine interfaces (HMIs)
- Operator selecting an incorrect setting
- Operator responding incorrectly to a prompt
- Errors in sequencing or timing

(Swain and Guttmann, 1980)

Any of the above may make it difficult to control the device or result in unintended operation. This can present a serious safety concern, depending on the device and the hazards of misuse. If a smart appliance like a washing machine isn't configured correctly and doesn't send the operator a notification that their laundry is done, the hazard is minimal. However, if a drone is used to monitor traffic on a busy highway, an error in operation could result in a crash to the ground, into a moving vehicle or, worse yet, cause a multivehicle collision. At the least, the monetary cost would be high; at worst, it would endanger people's lives.

Interoperability

Interoperability refers to a system's ability to operate with other devices or systems, even if they are designed and manufactured by different companies at different times. The effect interoperability has on safety can vary. In some cases, interoperability may not be a safety concern. However, it is a critically important design and performance concern for manufacturers. If a customer purchases a high-end washing machine or refrigerator with connected capabilities, then discovers it won't connect to their home Wi-Fi or connect to their cell phone, the customer would be understandably upset, and the brand image could sustain damage. Yet, for other types of smart products, interoperability may indeed pose a critical safety concern. In a fire control system, a damper may connect to an actuator and a controller, and all three of these must work together to prevent the spread of a fire. In this application, there is no margin for error.

Smart devices need to work with a wide range of other systems out of the box since one of the main functionality criteria of IoT devices is to share data with other devices. This interoperability concern may apply to any systems that exchange information.

In a home automation system, interoperability concerns may present themselves when attempting to link a smart device, such as an LED lamp, manufactured by a different company than the home automation hub. Some lamps may only work with their own proprietary control software or require a third-party application to bridge the two. In a city, there may be a system to monitor traffic conditions on a highway, but this system might not share any information with vehicles in the vicinity. Ideally, the data should be shared so drivers or autonomous vehicle control systems can avoid congestion and take alternate routes.

Resilience and reliability

The National Institute of Standards and Technology (NIST) defines *information system resilience* as the ability of an information system to continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs (NIST, 2011). Adverse conditions range from cyber incidents to power and data network outages. An organization with a resilient system can rapidly detect adverse events, absorb the impacts, quickly recover and guarantee business continuity to its stakeholders. Examples of systems that need to be resilient include control systems for industrial processes, the electric grid, healthcare communication networks and control systems for air traffic control.

Reliability may be considered a direct result of resiliency. Reliability is the outcome a service provider or device manufacturer strives for. Resiliency is the ability of the device or service to withstand failure and remain functional from the customer's perspective. "In other words, reliability is the outcome, and resilience is the way you achieve the outcome" (Bills, 2014). The following example will examine these factors as they pertain to the smart city IoT ecosystem.

Smart city

Example of an IoT ecosystem

The smart city is one example of an IoT ecosystem that contains many devices currently used on a daily basis. The smart city also contains subsets of IoT ecosystems such as homes with digital assistants and automation, factories with industrial IoT networks, lighting controls for streetlights, municipal transportation, autonomous vehicles, energy monitoring and many others. These systems may interact with each other or work only within their own ecosystems. Figure 1 on page 7 shows a list of IoT systems typical of a smart city.

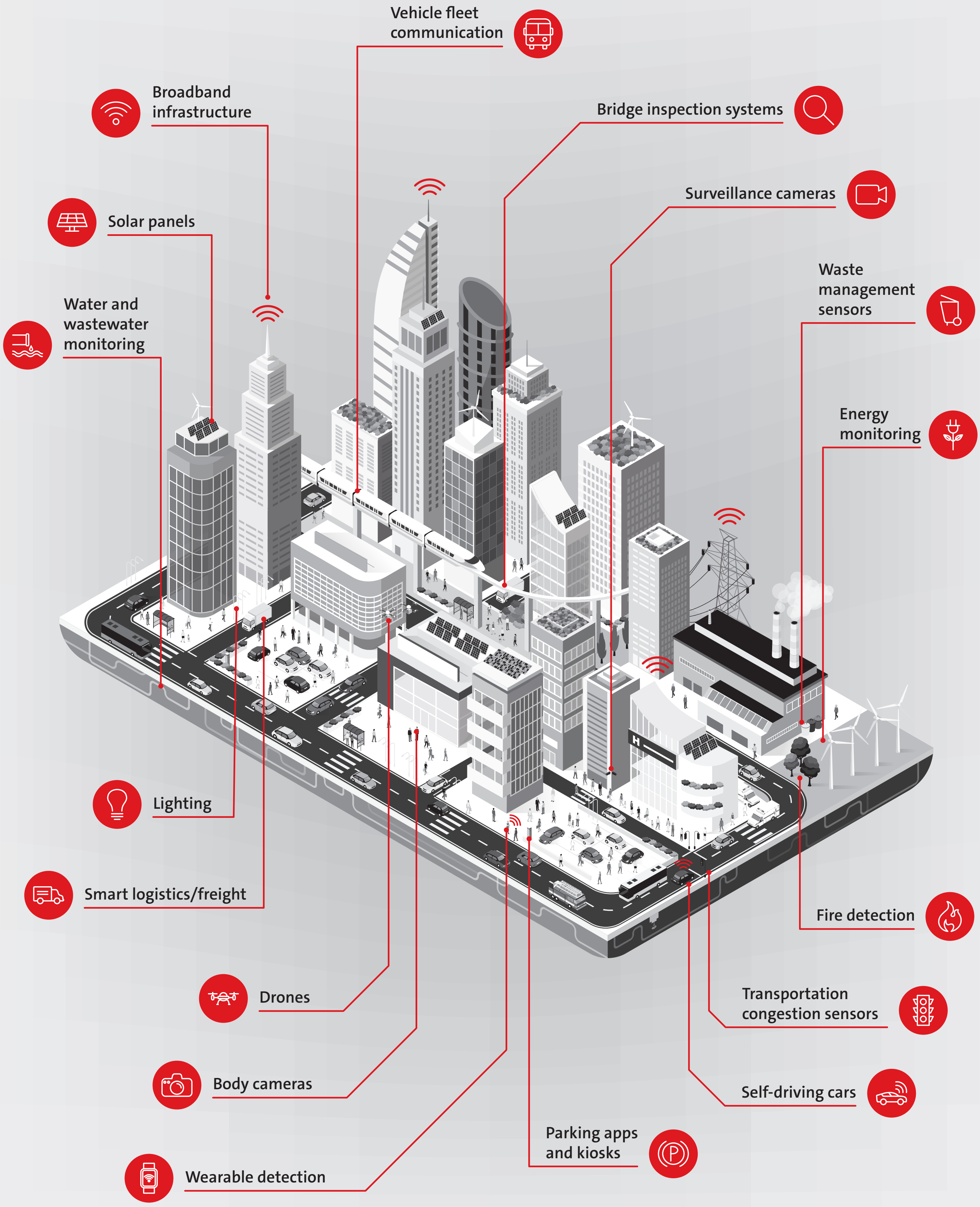


Figure 1. Example of a smart city IoT ecosystem

Each of these applications can be considered IoT systems in themselves and how they relate to the above characteristics. Let's take a look at a few of them in more detail:

Smart grid

The smart grid uses IoT devices to monitor the power grid to help with tasks such as fault monitoring, predicting usage, automating demand response, reducing greenhouse gas emissions from power production plants and improving security, efficiency, reliability and resiliency of the grid itself (Ghasempour, 2019). Smart meters can be used to monitor usage at customer sites, providing grid operators with data on usage and demand and allowing operators to notify customers about issues and outages. Monitoring generating equipment, substations, transformers or power lines can help warn operators about attacks on a grid and can potentially help isolate problems to smaller locations. Linking microgrids and renewable energy sources can boost efficiency. Some work is already under way to allow interoperable communications and controls between plug-in electric vehicles (EV) and EV support equipment (U.S. Department of Energy, 2017).

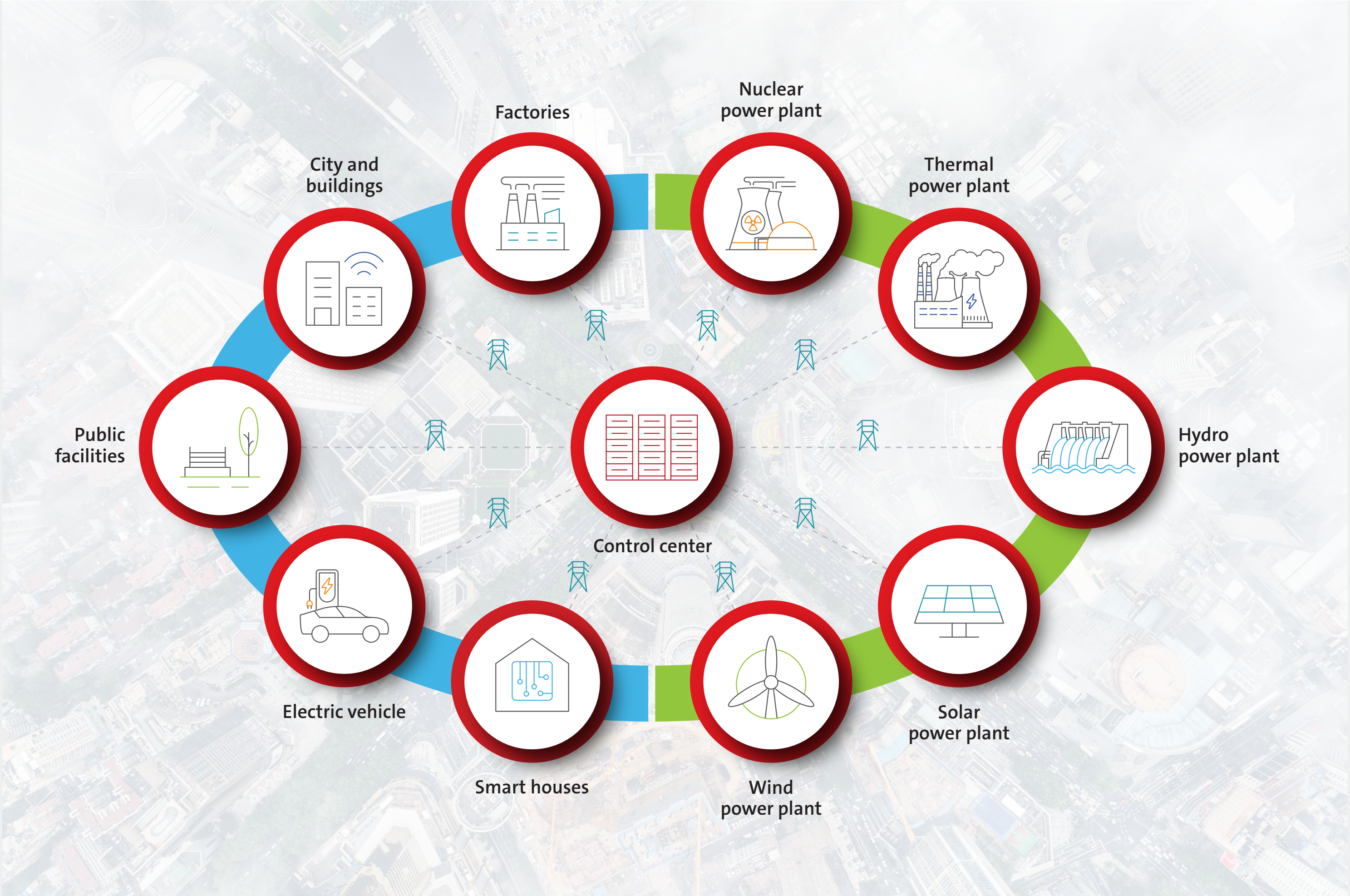


Figure 2. Example of the interconnectivity and applications of the smart grid (Jones, 2020)

Presently, some of the bigger issues with smart grids lie in their interoperability with each other (IEEE, 2019). "The lack of communications standards and common protocols continues to hamper interconnectivity efforts." The Smart Electric Power Alliance (SEPA) represents a nonprofit group dedicated to carbon-free power generation; its goal is "to aid the industry in developing open standards to make interoperability among power-generating microgrids easier and less expensive" (Castagna, 2019).

> *As with any networked environment, security must be a key consideration for IoT-based renewable energy installations. Given the criticality of the services they deliver, any compromise to the integrity of IoT renewable energy grids could be disastrous, potentially causing power shortages and even blackouts across interconnected power grids.*
> *(Castagna, 2019)*

These are just some of the benefits and issues that will need to be resolved as smart grids become more prevalent and integral to power delivery.

Smart parking

IoT systems can help improve ordinary day-to-day tasks, such as helping drivers find a parking space in a congested city.

> *Unavailability of free parking spaces is one of the major reasons for traffic jams in urban locations. Congestion and parking are interrelated because searching for a free parking spot creates additional delays and increases local circulation. In the center of large cities, 10% of the traffic circulation is due to cruising, as drivers spend nearly 20 min searching for a free parking space.*
> *(Ali et al., 2020)*

With smart parking, sensors embedded in parking spaces can detect whether a spot is occupied or available. This IoT data is transmitted wirelessly to the cloud, where data is collected and analyzed in real time to produce a map of available spaces. Drivers can use applications on their smart phones — or potentially in infotainment systems integrated into vehicles — to locate spaces that are free, some with the ability to reserve and pay for parking. (MobiDev, 2020)

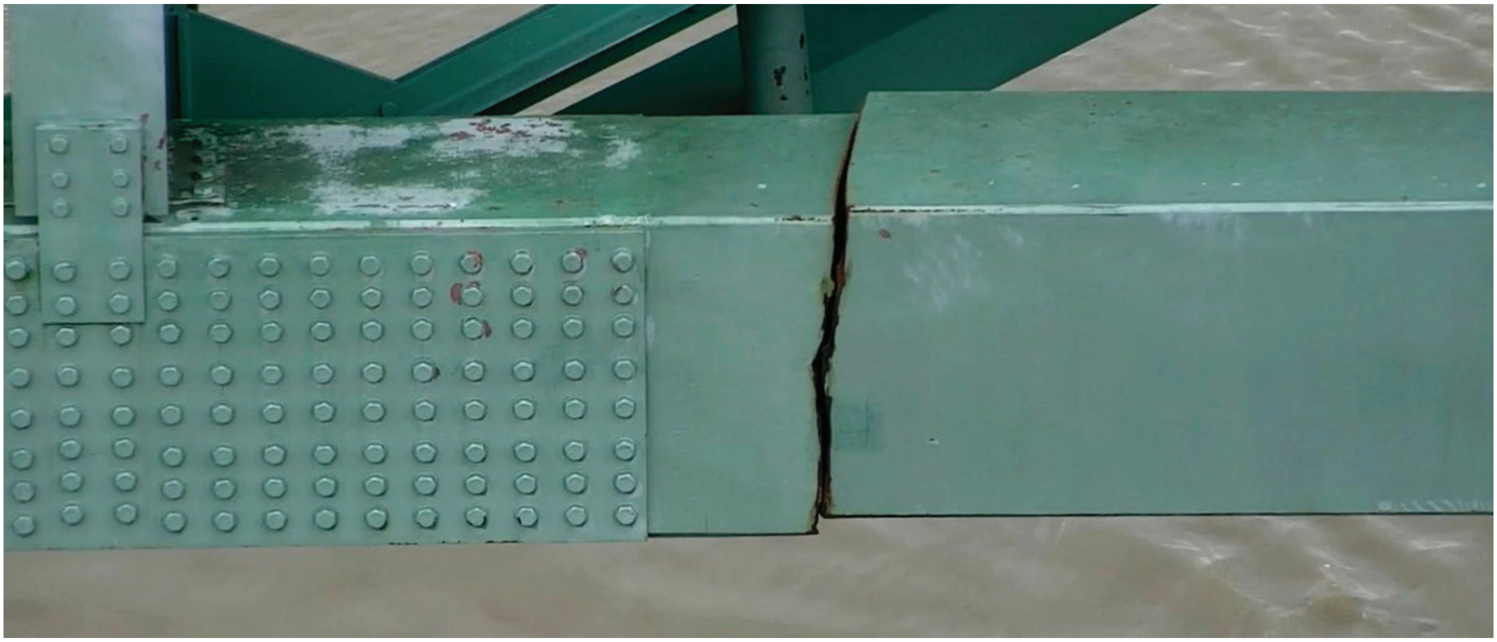


Figure 3. Hernando de Soto Bridge structural member fracture. This is just one example that combines the subjects of human error factors, bridge-monitoring sensors and drones. Photo courtesy of the Tennessee Department of Transportation

Bridge monitoring

Monitoring bridges' structural integrity is a necessary task for today's infrastructure. All structures have a design lifespan. This is especially crucial for bridges and roadways where failure can result in devastating loss of life in addition to major social and economic impacts. Many jurisdictions require certain inspection intervals for bridges and infrastructure (Hillhouse, 2020). In the past, maintenance personnel have inspected bridges. This has some major shortcomings:

> *Monitoring is typically not regular, and some results are obtained by empirical estimation; due to the limitation of data collection frequency, testing results often lag behind the damage of the bridge, and there are no early warnings of damage; due to the lack of real-time monitored data, it is difficult to understand the development of damage. (Tong, 2019)*

One recent example of this is the Hernando de Soto Bridge, which carries six lanes of interstate traffic across the Mississippi River between Arkansas and Tennessee. On May 11, 2021, this bridge was shut down due to the discovery of a large crack in one of the tension members. This was found during a required hands-on annual inspection and had been overlooked in prior remote inspections (Figure 3 above). (Hillhouse, 2021)

Although it would be imprudent to say that sensors will solve all bridge inspection issues, IoT sensors can certainly be used to supplement scheduled manual inspection by providing real-time data, monitoring infrastructure for defects and alerting maintenance personnel to potential issues as they occur and before they become major failures.

Drones

Drones or, more formally, unmanned aerial vehicles (UAVs), are technological tools with a wide variety of uses, including traffic and crowd monitoring, civil security, merchandise delivery, infrastructure inspection (as mentioned previously) and more. Further, when integrated with other IoT innovations, UAVs could help drivers find parking spaces, map out metro projects, create more efficient bus transit routes and even identify the best areas for bike paths and other forms of green transport. It is expected that the use of unmanned aerial vehicles will provide important and diverse contributions to the evolution of smart cities. (Browning, 2020)

> *The integration of drones, IoT, and AI (artificial intelligence) domains can produce exceptional solutions to today's complex problems in smart cities. A drone, which essentially is a data-gathering robot, can access geographical areas that are difficult, unsafe or even impossible for humans to reach. (Alsamhi et al., 2019)*

But human error still poses an issue. The use of drones for bridge inspection is a noteworthy example: Drones may help access difficult locations, but the data acquired often still requires human analysis. In other use cases, if the operator flying the drone presses the wrong button on a controller, loses communication or loses line of sight, the drone may fly into the side of a building, fall out of the sky, damage property or injure a person. Security is also a significant consideration; consider the scenario where a cybercriminal or bad actor takes control of a UAV to cause harm or incorrect operation. Controlling UAVs has been a topic of considerable research and legislation for many decades now and will likely continue to be an issue well into the future. (Hobbs, 2016)

Present capabilities

UL Solutions currently offers a multitude of services related to IoT, interoperability, security and human factors in addition to having evaluated many types of IoT sensors and devices going back almost 40 years: home automation assistant hubs, automotive infotainment systems and their compatibility with other connected devices, specific wireless carriers' handset/headset interoperability programs, Bluetooth Special Interest Group (SIG), Zigbee and Thread certifications, wireless coexistence testing and many others (consumer, medical and information technologies (CMIT), home security devices, smoke detectors (built environment (BE)), smart meters (energy and industrial automation (E&IA)), smart thermostats, lighting controllers and other connected appliances (appliances, HVAC and lighting (AHL)). UL Solutions has the technical expertise and understanding to evaluate newly designed sensors for bridges, AV systems, smart factories and many others.

Many UL Standards already incorporate requirements for functional safety, interoperability and human factors (UL 60730, the Standard for Automatic Electrical Controls; UL 61058, the Standard for Switches for Appliances; and others). UL Standards & Engagement has independent Standards for cybersecurity (UL 2900, the Standard for Software Cybersecurity for Network-Connectable Products) and remote software updates (UL 5500, the Standard for Remote Software Updates). Table 1 shows just a handful of the current service offerings related to IoT.

Table 1. Current IoT and related service offerings available from UL Solutions

SPIRE™ Smart Buildings services	TIA and UL Solutions will additionally focus on benchmarking, measurements, assessments, certification and registration in the areas of connectivity, interoperability, safety, security (both cyber and physical), resiliency and sustainability for buildings. And coming soon, the SPIRE Verified Assessment and Rating offers a complete smart building evaluation with the opportunity to earn a Smart Building Verified Mark.	https://spiresmartbuildings.ul.com/
IoT Security Rating Certification	UL Solutions has created a rating system that measures the security of connected products. With this IoT Security Rating, we test and classify products into one of five security levels, ranging from the lowest level, bronze, to the highest level, diamond.	https://ims.ul.com/iot-security-rating-levels

Table 1. Current IoT and related service offerings available from UL Solutions

IoT Security and Industry 4.0	UL Solutions can help you understand and mitigate the particular risks associated with Industry 4.0. We can work with you to identify gaps and deploy a risk-based cybersecurity approach that functions as an integral part of your business strategy and operations. Cybersecurity offerings for Industry 4.0 include IEC 62443 solutions (ISA/IEC 62443 Cybersecurity Certificate Programs), UL Supplier Cyber Trust Level, UL Cybersecurity Assurance Program (UL CAP), Common Criteria for Information Technology Security Evaluation and FIPS 140-2.	https://www.ul.com/services/solutions/cybersecurity/industry-40-cybersecurity
SAR and Interoperability for IoT Devices	For IoT devices intended for use near or on the human body, such as wearables, you will need SAR (Specific Absorption Rate) testing, an IEEE/FCC requirement. Interoperability plays an important role in helping IoT reach its full market potential. IoT devices rely on various protocols to "talk" to each other and the internet. Currently, there is no universal IoT standard to satisfy all market needs. Though interoperability is invisible to the consumer, manufacturers must ensure that their IoT devices can communicate seamlessly.	https://ctech.ul.com/en/industries/internet-of-things
Wireless Device EMC Testing and Certification	Unintended interactions and signal interference among electronic products, as well as equipment emissions, can have adverse impacts on electronic devices and radio systems. For this reason, in many countries, new products must comply with electromagnetic compatibility (EMC) requirements before launch.	https://www.ul.com/services/consumer-technology-emc-testing
Internet of Things (IoT) Testing Services	We help you protect your brand's reputation by offering you interoperability and connectivity testing services that assess whether your products perform in accordance with your claims. This is a critical component in driving consumer trust and confidence in your brand.	https://www.ul.com/services/internet-things-iot-testing-services
IoT Security and Interoperability	As your center of excellence for trusted security, UL Solutions serves the entire ecosystem of connected devices. We help you innovate successfully and securely, allowing you to build more reliable and secure IoT products. To strengthen security, UL Solutions helps our customers ensure confidentiality and integrity of data on IoT devices. We have the expertise to identify the best security implementation while also ensuring that security does not constrain system functionality.	https://ims.ul.com/trusted-security-identity-management/end-end-expertise/ul-iot-expertise
Cybersecurity Assurance and Compliance	Building cybersecurity into connected products represents a critical component needed to unlock the vast potential of IoT innovation. We help innovators create safer, more secure products and technologies by guiding them through the growing complexities across the supply chain.	https://www.ul.com/services/cybersecurity-assurance-and-compliance
Smart Meter Interoperability	The interoperability of smart meter devices is critical to their effectiveness and ability to function as the core IoT device for electric power. Thus, a relatively new standard, IEEE 2030.5, has emerged among utilities as the most relevant and applicable set of requirements to safeguard two-way communication.	https://www.ul.com/news/tower-babel-making-sure-smart-meters-speak-same-language

Table 1. Current IoT and related service offerings available from UL Solutions

Cybersecurity Risk Assessment for Medical Devices	The Cybersecurity Assurance Program (CAP) supports manufacturers, end users, system installers and integrators in promoting good cybersecurity hygiene in designing, manufacturing, installing and maintaining products and systems. Based on the UL 2900 Series of Standards and other industry standards, the full suite of cybersecurity services helps organizations manage their cybersecurity risks and validate their cybersecurity capabilities to the marketplace.	https://www.ul.com/services/healthcare-cybersecurity-solutions
Cybersecurity for Physical Security Systems	It is imperative that life safety and physical security systems undergo evaluation for cybersecurity to help ensure performance and reliability, prevent damage to assets, mitigate risk, improve security and maintain health and safety. While many often do not think about it, we would all like the peace of mind that comes from knowing that these systems will work as intended when called upon in an emergency. The Cybersecurity Assurance Program (CAP) for electronic physical security systems utilizes UL 2900-2-3, the Standard for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems, to offer testable cybersecurity criteria to help assess software vulnerabilities and weaknesses, minimize exploitation, address known malware, review security controls and increase security awareness to help mitigate risk.	https://www.ul.com/services/cybersecurity-physical-security-systems
IoT Device Interoperability Verification	We test for interoperability and ease of customer use at the same time that we test for compliance, making the entire process as efficient as possible. More importantly, UL Solutions helps you protect your brand's reputation by offering you testing services that confirm that your products perform in accordance with your claims, a critical component in driving consumer trust and confidence in your brand.	https://www.ul.com/services/interoperability-solutions-internet-things
KNX and DALI Protocols Testing	As lighting systems, appliances, heating, ventilation and air-conditioning (HVAC) systems and other electronics become increasingly connected, interoperability protocols prove more important than ever. In addition to EMC and wireless testing such as Bluetooth®, Zigbee and Thread, UL Solutions has recently added capabilities to test to KNX and Digital Addressable Lighting Interface (DALI) protocols. We test end products, components and gateways of building control systems that connect electronic devices, including lighting and appliances.	https://www.ul.com/services/knx-and-dali-protocols-testing

UL Solutions also has an emerging business offering for systems evaluation, which involves concept and systems assessments. Such systems do not always fit one product or system category in the traditional sense of the word due to multiple regulations, standards and guidelines. Examples include hydrogen processing plants, chemical refineries, fuel cells and large-scale vertical farms. UL Solutions can assist with regulatory mapping and other aspects of system safety via this new offering: Regulatory Assessment Services for Industrial Systems. See the next section for a brief overview and explanation of the V-model for systems evaluation.

V-model application for IoT systems

To evaluate IoT systems (or any systems) that are complex or do not fit one particular standard or category, several life cycle models can be used to break these systems down into smaller components and design phases. From the previous example, a smart city could not be evaluated as a whole, but could instead be broken down into constituent parts such as cameras, drones, parking sensors, etc., similarly to smart factories or any other large system.

Known as a system development life cycle (SDLC), various frameworks can be utilized, including the V-model, waterfall, prototyping, spiral and agile. The V-model uses a robust requirements-based approach, with specific, measurable deliverables at different phases of the development cycle.

The V-model shown in Figure 6 represents the stages of a product or system development cycle, where the left and right sides relate to the verification and validation steps. The right side ensures that the modules and the system are verified and validated to the requirements on the left side. Table 2 below describes a very high-level overview of this process as it applies to an IoT system.

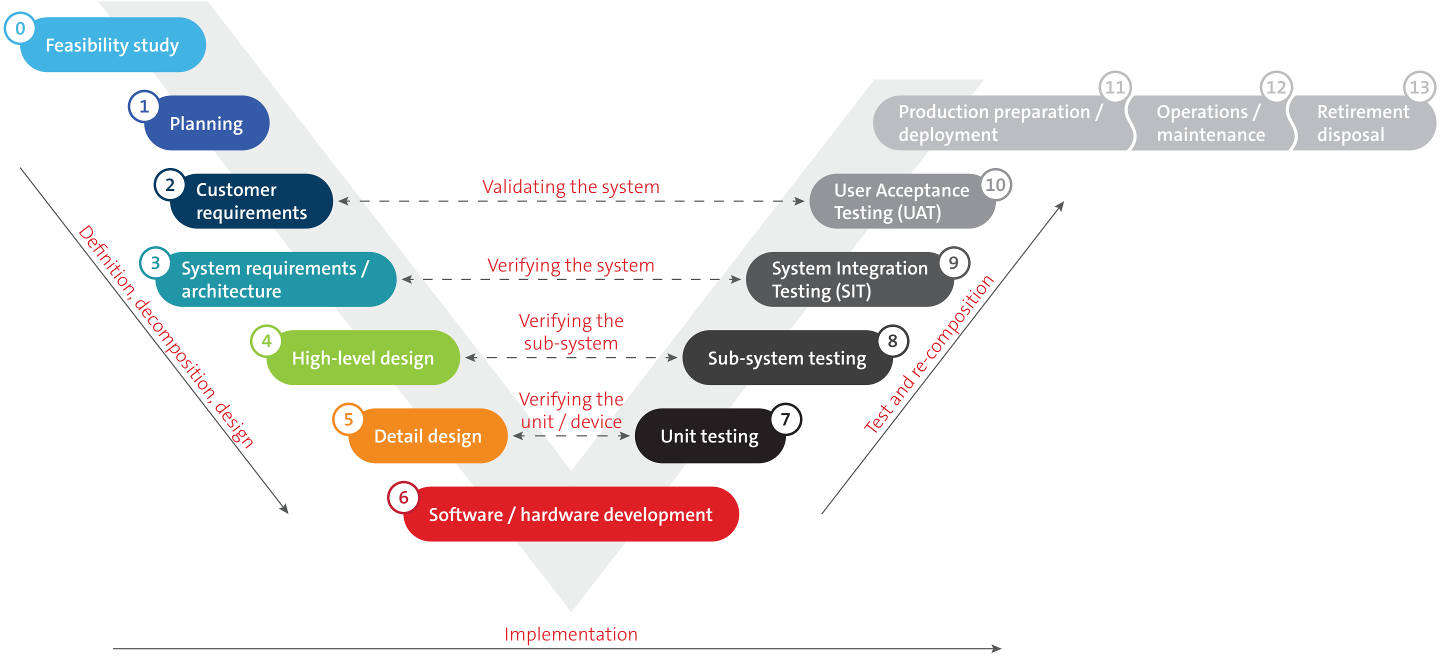

0 Feasibility study
1 Planning
2 Customer requirements
3 System requirements / architecture
4 High-level design
5 Detail design
6 Software / hardware development
7 Unit testing
8 Sub-system testing
9 System Integration Testing (SIT)
10 User Acceptance Testing (UAT)
11 Production preparation / deployment
12 Operations / maintenance
13 Retirement disposal
Validating the system
Verifying the system
Verifying the sub-system
Verifying the unit / device
Definition, decomposition, design
Test and re-composition
Implementation

Figure 6. SDLC V-model

Table 2. High-level overview of the steps in the V-model as they apply to IoT system evaluation

	V-model step	Description
0	Feasibility	The feasibility study helps ensure that the strategic goals of the business are met in project development. During this phase, the purpose of the product, the problems it should solve, the user and usage profiles and the product's input/output are also documented.
1	Planning	Documents the project scope, time, cost, objectives, deliverables and constraints

Table 2. High-level overview of the steps in the V-model as they apply to IoT system evaluation

	V-model step	Description
2	Customer requirements	The end user's operational needs, technology, frameworks and interface requirements are documented during this phase. Security standards and compliance requirements are identified. Hardware requirements include requirements for mandatory certifications.
3	System requirements/ architecture	The documentation describes the general organization of the system, definition of functions, user interface elements, including dialogs and menus, workflows, menu structure, data structures and use cases. During this phase, the system test specifications are also completed.
4	High-level design	Focuses on the system-level architecture and its physical and functional decomposition into subsystems
5	Detailed design	Each component is described in detail, including its functionality, internal logic and database tables. The interface relationships with other components are described, including dependencies with the inputs and outputs of each component. Component tests are also prepared based on the functional description and interface specification of the components.
6	Software/ hardware development	Coding and building of hardware: Preparations are under way to certify the hardware to the compliance and safety requirements identified in the system requirements phase.
7	Unit testing	This testing verifies that each unit of the software code performs as expected and helps eliminate software bugs at the code or unit level (the smallest component of any system).
8	Subsystem testing	Components are integrated into subsystems (hardware) and modules are combined into applications (software). The integration tests verify that the assembly of components, which have been developed and tested independently, can integrate with each other and communicate as expected.
9	System integration testing	Verifies the interactions between the subsystems (hardware) and modules (software) — the test deals with verifying the high- and low-level software requirements specified in the system requirement specifications. The test also verifies each software system's compatibility with upstream and downstream systems.
10	User acceptance testing	Checks that the system behaves as per requirements articulated in the customer requirements phase. This is where parameters such as performance, security, usability, connectivity, interoperability, compatibility and product safety/regulations are all assessed for final acceptance.
11	Production preparation/ deployment	Security control assessments (Dempsey, 2020) for high-risk areas of the hardware, software, system configurations, controls and any other customizations are performed prior to placing the system into production.
12	Operations and maintenance	Through the product life, the manufacturer may fix bugs, upgrade applications and add new features to existing software. Routine security operation and system administration and maintenance are performed following established security practices. Products are continuously updated to maintain security and compatibility with new tools.
13	Retirement and disposal	During this phase, the information contained in enterprise-wide systems and applications must be protected once a system has reached the end of its life and the end of support. Any residual vulnerabilities from application and infrastructure are assessed, documented and mitigated. (NIST, 2014)

Key takeaways from the V-model analysis:

- The system can be decomposed into its physical and functional architecture, showing the different technologies integrated into the system.
- The V-model enables mapping of the different risks posed by the technologies to the physical architecture, which leads to the identification of applicable technical regulations and standards.
- The V-model can be used to tailor the requirements and advisory service offerings to satisfy the customer's needs depending on what stage of the process the project is in.

Future of IoT and UL Solutions

IoT is seen as a huge area of growth — today, there are approximately 14.4 billion internet-connected devices worldwide (Security Today, 2020), and there are expected to be 27 billion IoT devices by 2025 (Verma, 2021). Looking at where IoT is going in the future, some of the biggest areas among technology leaders include security, analytics and device management (Mordor Intelligence, 2020).

Security is an issue predicted to stand at the forefront of connected devices. "The threat is ongoing and evolves constantly, so cybersecurity should not be viewed as a one-time 'project' with a defined beginning and end. Since there is no such thing as being fully secure, the preferred approach should also be ongoing." (Resnick, 2020). Cybersecurity studies show an ever-increasing number of cyber threats and incidents.

> *Rapidly increasing cybersecurity incidents and regulations requiring their reporting are driving the cybersecurity market. The global cybersecurity market was valued at $150.37 billion (USD) in 2021, and it is expected to reach a value of $317.02 billion (USD) by 2027, registering a CAGR of 13.37% during the forecast period 2022-2027. According to the Center for Strategic and International Studies (CSIS) and McAfee, cybercrimes, which include damage and destruction of data, stolen money, lost property, intellectual property theft and other areas, currently cost the world almost $600 billion (USD) each year, or 0.8% of the global GDP. (Mordor, 2020)*

IoT is seen as a huge area of growth — today, there are approximately 35 billion internet-connected devices worldwide (Security Today, 2020), and there are expected to be 70 billion IoT devices by 2025 (Verma, 2021).

Regarding interoperability, GE has highlighted the Open Process Automation™ Forum (OPAF), a collaboration of industry leaders who are in the process of developing requirements to aid the interoperability of IoT devices:

> *The OPAF [was] established to identify and select appropriate standards for technology and systems to support interoperability, avoid technology obsolescence and deliver more business value. The goal of this collaboration is to accelerate creation of a standards-based, open, interoperable and secure automation architecture that addresses both technical and commercial challenges of current systems. (Resnick, 2020)*

Smart cities are another projected area of growth in which UL Solutions has already started to gain a foothold with offerings that include smart meters and the UL Safety Index, mentioned previously. There are many new aspects and possible inroads into this field:

> *With IoT technologies now being used to monitor traffic, operate public amenities and manage buildings, smart cities are no longer a thing of the future. There are countless applications of IoT in the automation of cities. We anticipate that this IoT emerging trend will continue to grow as local governments realize smart cities are more resilient and better equipped to deal with unforeseen large-scale crises.*
>
> *Two areas where this shift will be very visible is smart public transport and energy management. For example, IoT technologies are expected to provide a better understanding of the need of citizens and their patterns of movement. (Burbach, 2021)*

UL Solutions is currently developing more system analyses to help customers with large and complex products. A systems engineering approach can be used to examine the integration of various IoT systems, as shown previously, using the SDLC V-Model to examine the risks and hazards. A deeper dive into this topic would require a separate research paper in itself, but in short, it takes a look at every stage from design to end of life for a system and can be used to help identify safety risks and applicable requirements.

Conclusion

IoT is a mature technology from the device point of view, and current service offerings at UL Solutions cover safety certification for these types of products. UL Solutions also offers a wide variety of performance and verification service offerings for security, reliability, human factors and interoperability, among many others.

With the ever-increasing number of new technologies and devices on the market, there will continue to be a large demand for device certification, systems integration and interoperability testing. There is also potential to offer performance verification services related to product lifetime and cybersecurity, which are growing and evolving areas of business. Further study may help determine how much these areas will grow in the future. Presently, UL Solutions is poised to help customers with the numerous facets of IoT device performance and safety, and we plan to continue researching and growing to support new areas of technology.

Contact us at UL.com/sales-inquiries.

Sources

1. A. D. Swain and H. E. Guttmann (1980). Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Sandia National Labs.

2. Ali, Ghulam, Ali, Tariq, Irfan, M., Draz, U., Sohail, M., Glowacz, A., Sulowicz, M., Mielnik, R., Faheem, Z, & Martis, C (Oct. 15, 2020). IoT Based Smart Parking System Using Deep LongShort Memory Network. MDPI. https://www.mdpi.com/2079-9292/9/10/1696

3. Alsamhi, Saeed, Ma, Ou, Ansari, Mohammad, & Almalki, Faris (Aug. 13, 2019). Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities. IEEE Access. https://ieeexplore.ieee.org/abstract/document/8795473

4. Badii, C, Bellini, P, Difino, A, & Nesi, P (2020). Smart City IoT Platform Respecting GDPR Privacy and Security Aspects. IEEE Access. https://ieeexplore.ieee.org/abstract/document/8966344

5. Bills, David (March 2014). Reliability Series #1: Reliability vs. Resilience. Microsoft. https://www.microsoft.com/security/blog/2014/03/24/reliability-series-1-reliability-vs-resilience

6. Browning, Daniel (Oct. 13, 2020). UAVs Can Play a Vital Role in The Future of Smart Cities. Smart Cities Dive. https://www.smartcitiesdive.com/news/uavs-can-play-a-vital-role-in-the-future-of-smart-cities/586857

7. Burbach, Björn (Jan. 14, 2021). What are the IoT Trends in 2021? Siemens-Advanta. https://www.siemens-advanta.com/blog/what-are-expected-iot-trends-2021

8. Castagna, Rich (Aug. 29, 2019). How Smart Grid Technology Is Driving Renewable Energy. IoT World Today. https://www.iotworldtoday.com/2019/08/29/how-smart-grid-technology-is-driving-renewable-energy

9. Gartner Inc. (Aug. 29, 2019). Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020. https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io

10. Ghasempour, Alireza (March 26, 2019). Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges. MDPI.

11. Goodin, D. (August 2019). Microsoft Catches Russian State Hackers Using IoT Devices to Breach Networks. Ars Technica. Page accessed on August 18, 2020: https://arstechnica.com/?post_type=post&p=1546303

12. Hillhouse, Grady (June 09, 2021). What Really Happened at the Hernando de Soto Bridge? Practical Engineering https://practical.engineering/blog/2021/6/9/what-really-happened-at-the-hernando-de-soto-bridge

13. Hobbs, A., & Lyall, B. (2016). Human Factors Guidelines for Unmanned Aircraft Systems. Ergonomics in Design. https://human-factors.arc.nasa.gov/publications/Hobbs_Lyall_Ergonomics_Design_prepub.pdf

14. Cyber Security Market Trends, Size, Share (2022-27) | Industry Growth https://www.mordorintelligence.com/industry-reports/cyber-security-market

15. Human Factors & Ergonomics Society (2018). What is Human Factors and Ergonomics? Human Factors & Ergonomics Society. https://www.hfes.org/About-HFES/What-is-Human-Factors-and-Ergonomics

16. IEEE Innovation at Work (2019). The Smart Grid and Renewable Energy. https://innovationatwork.ieee.org/smart-grid-transforming-renewable-energy

17. IoT World Congress (April 22, 2019). IoT Transforming the Future of Agriculture. IoT World Congress. https://www.iotsworldcongress.com/iot-transforming-the-future-of-agriculture

18. Jones, Quinn (April 1, 2020). What Is the Smart Grid and How Is It Enabled by IoT? Digi. https://www.digi.com/blog/post/what-is-the-smart-grid-and-how-enabled-by-iot

19. MobiDev (April 14, 2020). How To Use IoT For Smart Parking Solution Development. https://www.iotforall.com/how-to-use-iot-for-smart-parking-solution-development

20. Mordor Intelligence (2020). IoT Device Management Market - Growth, Trends, Covid-19 Impact, and Forecasts (2022 - 2027). https://www.mordorintelligence.com/industry-reports/cyber-security-market

21. National League of Cities (2016) Trends in Smart City Development. https://www.nlc.org/wp-content/uploads/2017/01/Trends-in-Smart-City-Development.pdf

22. NIST (March 2011). Computer Security Resource Center. Page accessed on July 15, 2021: https://csrc.nist.gov/glossary/term/resilience

23. Resnick, Craig (2020). Key Technology Trends for 2020. GE. https://www.ge.com/digital/blog/key-technology-trends-2020

24. Security Today (Jan. 13, 2020). The IoT Rundown For 2020: Stats, Risks, and Solutions. https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2

25. Tong, Xinlong., Yang, H., Wang, L. & Miao, Y. (March 11, 2019). The Development and Field Evaluation of an IoT System of Low-Power Vibration for Bridge Health Monitoring. MDPI https://www.mdpi.com/1424-8220/19/5/1222

26. U.S. Department of Energy (June 1, 2017). Internet of Things-enabled Devices and the Grid. https://www.energy.gov/articles/internet-things-enabled-devices-and-grid

27. Verma, Sanjeev (Feb. 17, 2021). Looking Past the Industrial Future with AI, IoT and Blockchain. IBM. https://www.ibm.com/blogs/blockchain/2021/02/looking-past-the-industrial-future-with-ai-iot-and-blockchain

Glossary

Botnet	Also called a "zombie army," a botnet is a large number of compromised computers used to generate spam, relay viruses or flood a network or web server with excessive requests to cause it to fail (see denial-of-service attack). The computer is compromised via a Trojan that often works by opening an internet relay chat (IRC) channel that waits for commands from the person in control of the botnet. (PCmag)
Cobot	A cobot, or collaborative robot, is a robot intended for direct human-robot interaction within a shared space or where humans and robots are in close proximity. (https://www.techopedia.com/definition/14298/collaborative-robot-cobot)
Fault-tolerant	A system with the built-in capability to provide continued, correct execution of its assigned function in the presence of a hardware and/or software fault. (NIST, 2015)
Industry 4.0	The Fourth Industrial Revolution (4IR or Industry 4.0) refers to the ongoing automation of traditional manufacturing and industrial practices using modern smart technology. Large-scale machine-to-machine communication (M2M) and the Internet of Things (IoT) are integrated for increased automation, improved communication and self-monitoring and production of smart machines that can analyze and diagnose issues without the need for human intervention. (https://www.ibm.com/topics/industry-4-0)
Industrial control system	An information system used to control industrial processes, such as manufacturing, product handling, production and distribution — industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes. (NIST, 2013)
Industrial Internet of Things (IIoT)	Refers to the application of instrumentation and connected sensors and other devices to machinery and vehicles in the transport, energy and industrial sectors (NIST, 2019)
Infotainment system	Information + entertainment system — the infotainment system runs all of a car's communication and entertainment functions, from phone calls and navigation to music and podcasts. (https://www.cr.org/infotainment-systems/screen-stars-in-car-infotainment-systems)
Interoperability	The ability for a device from one manufacturer to work with one from another (Gartner)
Legacy system	Business application system currently in use within the enterprise (CISA, 2006)
Malware	Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity or availability of an information system (NIST, 2013)

Glossary

Reliability	The ability of a system or component to function under stated conditions for a specified period of time (Harrington, 1999)
Resilience	The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs (NIST, 2013)
Sensor	A device that produces a voltage or current output that is representative of some physical property being measured, e.g., speed, temperature, flow (NIST, 2015)
System	A combination of interacting elements organized to achieve one or more stated purposes (NIST, 2015)
System development life cycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and, ultimately, its disposal, which instigates another system initiation (NIST, 2015)
System integrator	An organization that customizes — e.g., combines, adds, optimizes — components, systems and corresponding processes (NIST, 2015)
Zigbee	A global wireless mesh networking technology based on the IEEE 802.15.4-2003 standard (Gartner)
5G	The fifth-generation technology standard for broadband cellular networks (https://www.qualcomm.com/5g/what-is-5g)

UL Solutions

UL.com/Solutions