From prototype to production: fast track IOT adoption with secure and seamless connectivity

UL Solutions

Safety. Science. Transformation.™

Internet of Things (IoT) devices are everywhere, from smart medical devices to connected cars. Statista reported that there were 7.7 billion connected IoT devices in 2019. Business Insider predicted that the number of IoT-connected devices will grow to nearly 31 billion by 2025, for a combined annual growth rate (CAGR) of over 26%. Business Insider further projected the entire market of IoT devices and internet connectivity at over $2.7 trillion (USD) annually by 2027. The growing interest in IoT from governments, businesses and consumers represents a huge market potential for manufacturers of connected devices.

This massive growth of IoT devices is, unfortunately, attracting cybercriminals. IoT devices greatly expand the attack surface for cybercriminals to penetrate a secure network. Each IoT device provides a potential non-secure entry point into a network that had previously been advertised as secure. The Washington Post reported that hackers circumvented a casino's network through an IoT thermostat in one of the fish tanks. Newsweek described how over 1,000 home cameras (including baby monitors) were hacked and their live feeds posted to a website titled "Big Brother Is Watching You."

Interoperability and cybersecurity are key enablers for IoT adoption. On the regulatory level, manufacturers need to comply with safety, electromagnetic compatibility (EMC) and wireless requirements for access to desired markets. On the consumer level, buyers look for IoT products that work securely in real-world environments. Efforts by UL Solutions help manufacturers in their journey to meet compliance and safe IoT requirements, from Wi-Fi to Bluetooth to 5G millimeter wave.

Business Insider predicted
IoT-connected devices
that the number of
will grow to nearly
31 billion by 2025

Changing the way we live and work

More and more, digital-savvy consumers are incorporating IoT devices into their homes. A prime example is the voice-activated smart home assistant that helps to simplify everyday tasks from ordering groceries to managing a playlist.

For enterprise businesses, IoT can help optimize business processes and uncover new opportunities. In manufacturing, IoT sensors collect and analyze operational data to minimize downtime. Other IoT business applications include vehicle sensors, which insurers use to assess driving behavior.

The GSM Association (GSMA) estimated that there will be 11 billion IoT connections in the Asia Pacific region by 2025, representing 43% of the world's total number of connected devices. Smart cities such as Tokyo and Singapore want to improve citizens' lives with the help of IoT.

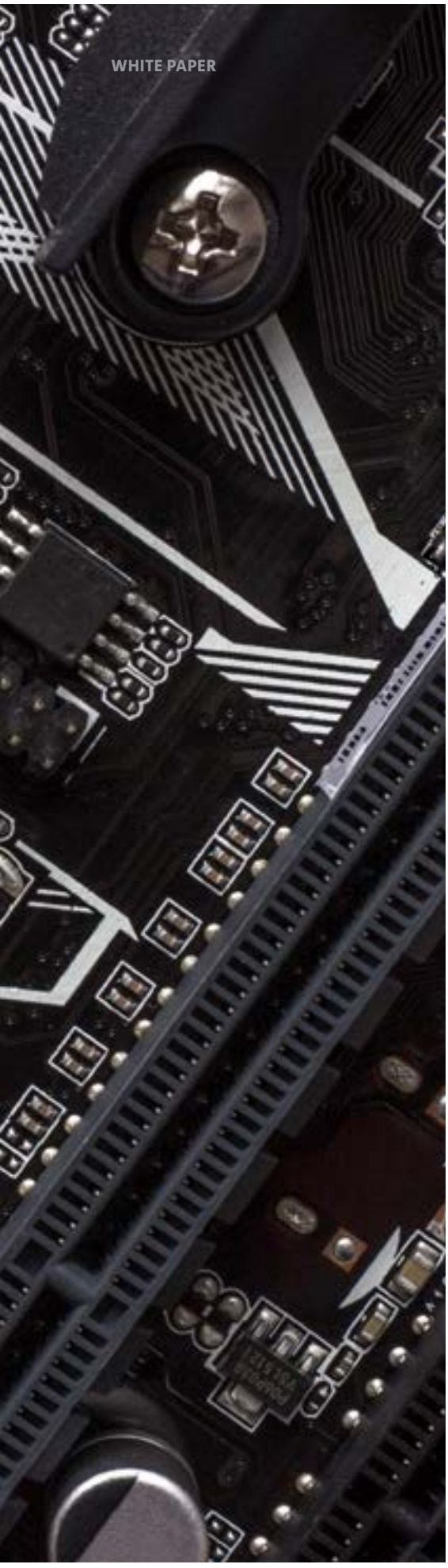
Trains on the Tokyo Yamanote subway line depart every two to four minutes, carrying 34 million passengers a week. Any maintenance closures are a real problem. An IoT-based smart maintenance system is used to minimize disruption. Sensors collect data, identify weak points, predict equipment failures and determine when and where maintenance is required.

Singapore's first smart-enabled public housing estate, Punggol Northshore Residences, is equipped with smart appliances and smart energy sockets. Just one feature of these smart homes is sensors to detect low water pressure so homeowners are alerted about a potential water leak on their smartphone app. This smart-enabled public housing estate is one of many government-led IoT projects in Singapore's smart nation initiative.

In the automotive industry alone, the market for IoT devices and sensors will reach more than $540 billion (USD) by 2025. Some leading applications include fleet and driver management, real-time vehicle telematics, predictive maintenance and infotainment.

For IoT to reach its full potential, we need to analyze and gather insights from massive amounts of data. Imagine millions of connected sensors and devices sharing information about events with their central IoT application every second. Businesses need to process that data at speed to take specific actions in real-time, whether activating lights in the driveway or detecting temperature changes in products during delivery.

Improving cybersecurity in IoT



IoT data is attracting the attention of cybercriminals. High-profile hacking incidents highlight the need for device manufacturers to make cybersecurity a top priority. In 2016, the Mirai botnet compromised more than 5 million IoT devices to launch distributed denial of service (DDoS) attacks. Security vulnerabilities in IoT devices in industrial and public sectors can result in financial losses and disrupt critical infrastructure.

Governments around the world are establishing IoT security initiatives to tackle cyberthreats. California is one of the first U.S. states to pass an IoT security law. Device manufacturers are required to adopt cybersecurity standards during product development and design stages, not as an afterthought.

The EU Cybersecurity Act promotes the adoption of certification and other end-user guidance tools such as security labels to improve IoT security awareness and help consumers make informed decisions. Countries in the Asia Pacific region followed suit with IoT security regulations such as a cybersecurity labeling scheme in Singapore and Korea KISA IoT Privacy by Design in South Korea. Manufacturers should consider testing IoT products to robust security guidelines.

The good news is that customers are willing to pay for security. According to global consulting firm Bain & Company, consumers will spend an average of 22% more for secure IoT devices and buy an average of 70% more IoT devices if they are secure.

We help manufacturers overcome IoT security challenges with two IoT security certification programs: **UL Cybersecurity Assurance Program** and CTIA Cybersecurity Certification for IoT Devices. Additionally, **UL's IoT Security Ratings** system and Marks will help consumers differentiate products based on their levels of security.

UL 2900-1, the Standard for Software Cybersecurity for Network-Connectable Products, is recognized by the U.S. Food and Drug Administration (FDA) and widely used for certifying connected healthcare devices.

IoT testing for market success

To accelerate time to market, consider these four questions when assessing your product readiness.

1. **Does your IoT device meet wireless/cellular, EMC and safety compliance requirements to be sold in desired markets?** Manufacturers who conduct internal testing using an industry-standard application program interface (API) and toolset may find that such testing is limited in scope. As an accredited testing laboratory for many IoT and wireless standards, we can help you test for regulatory compliance, pre-compliance and retest for wireless devices.
2. **What product certification marks should you consider for your IoT device to gain customer confidence?** We offer independent third-party testing and certification to product safety standards relevant to electrical products.
3. **Can your IoT device connect out of the box, stay connected and deliver the right functionalities in its intended ecosystem?** For example, compatibility with voice assistants such as Amazon's Alexa and Apple's Siri is a must for smart home devices.
4. **Is your IoT device secure for use?** Smart home manufacturers such as GE Appliances, Midea and LG participated in UL Solutions IoT Security Rating to demonstrate their IoT products' security capabilities with security labels.

5G and IoT go hand-in-hand

The rollout of 5G, with speeds 10 times faster than 4G, will boost IoT adoption across homes, businesses and cities. However, widespread IoT adoption requires manufacturers to offer consumers and businesses reliable and secure products that they can trust. We offer the science and expertise to evaluate connected device manufacturers' products and innovations to the latest regulatory requirements and standards.

Learn more at UL.com/IOP or contact us today.

Why UL Solutions?

UL Solutions is a global safety science leader that can support you with interoperability and cybersecurity testing and certification for your connected products. We can help evaluate whether your products comply with regulatory standards and operate seamlessly with other devices and major connectivity/IoT platforms. This will help you deliver more reliable, safer and more secure connected products to consumers, improving customer experience and brand reputation.

- UL Solutions has approved testing laboratories for many IoT and wireless standards bodies, such as Bluetooth Special Interest Group (SIG), Thread Group, Connectivity Standards Alliance (CSA), Matter and the Open Connectivity Forum (OCF).
- We can perform real-world interoperability testing for most connected products, mobile app testing, Wi-Fi reconnection robustness testing, feature testing, long-term connection performance and more.
- We can develop customized testing solutions to meet your specific requirements.
- UL Solutions is your single-source service provider. We offer a comprehensive suite of services, including end-product testing, certification and validation, that can help you access your target markets more quickly.

Applicable services include testing and certification to:

- Connectivity standards and platforms.
- Wireless cellular devices standards.
- Cybersecurity standards and ratings.

Endnotes

1. Statista. (Mar. 2022). Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030. www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
2. Business Insider. (Mar. 2020). The Internet of Things 2020. www.businessinsider.com/internet-of-things-report?IR=T
3. IoT Now. (Jun. 2020).5 challenges still facing the Internet of Things. www.iot-now.com/2020/06/03/103228-5-challenges-still-facing-the-internet-of-things/#
4. GSMA Intelligence. (2018). The Internet of Things By 2025. www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf
5. Raconteur. (Feb. 2020). Tokyo on track for smartest Olympics ever. www.raconteur.net/technology/internet-of-things/iot-tokyo-2020/?zephr_sso_ott=LDtWzN
6. GlobeNewswire. (Jan. 2020). Automotive IoT Market Worth $541.73 Billion by 2025. www.globenewswire.com/en/news-release/2020/01/15/1970769/0/en/Automotive-IoT-Market-Worth-541-73-Billion-by-2025-Exclusive-Report-by-Meticulous-Research.html
7. Contus. (Dec. 2020). 5 Major Applications of IoT in The Automotive Industry. blog.contus.com/iot-in-automotive-industry/
8. Hacker News. (Oct. 2016). www.thehackernews.com/2016/10/mirai-source-code-iot-botnet.html
9. Bain and Company. (Jun. 2018). www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things/
10. PRN Newswire. (Jan. 2020). www.ul.com/news/ul-announces-ge-appliances-first-household-appliance-brand-test-connected-devices-new-iot
11. PRN Newswire. (Jun. 2020). www.prnewswire.com/news-releases/midea-recognized-as-first-company-in-china-to-achieve-uls-iot-security-rating-301069572.html
12. PRN Newswire. (Dec. 2015). www.lg.com/sg/about-lg/press-and-media/lg-webos-3-receives-ul-verification-for-smart-home-readiness

UL.com/Solutions

CS348127 (0722)