# It’s Complicated: Five Challenges of Developing Connected Products

Connected Ecosystems Research Report

UL Solutions

Safety. Science. Transformation.™

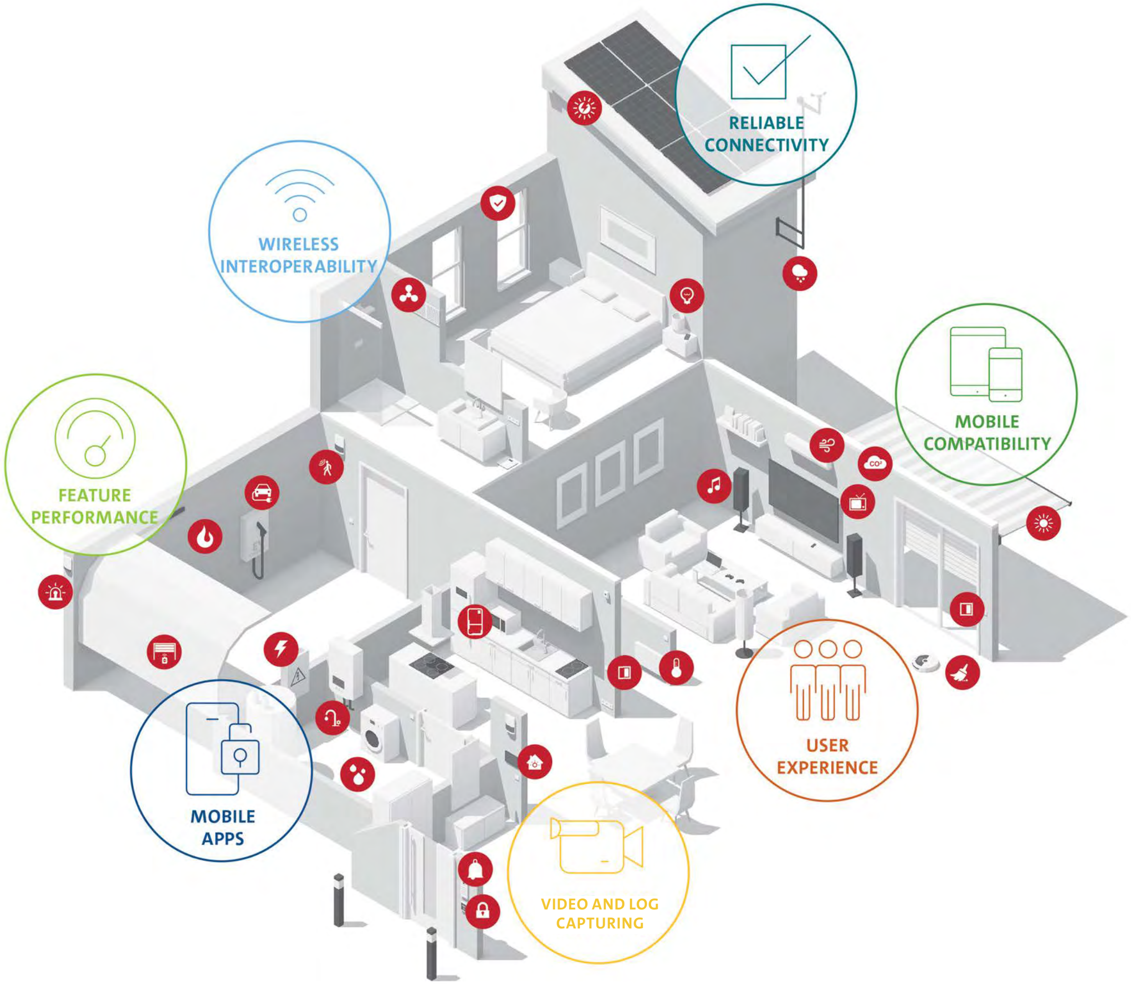
Introduction
Development
Features
Cybersecurity
Intentions
Compliance
Conclusion
Why UL Solutions?
Sources

It’s no secret that the Internet of Things (IoT) has transformed the world with its connectivity. From simple objects such as a smartwatch to a smart city with sensors across all its regions, IoT automation benefits us all.

However, studies show that the IoT market is developing more slowly than analysts predicted. How is this possible, given its vast potential?

Here’s a snapshot of key challenges manufacturers face when developing connected products.

*The second you add a* **SMART** *feature to an object, the list of complexities grows.*



## What is IoT?

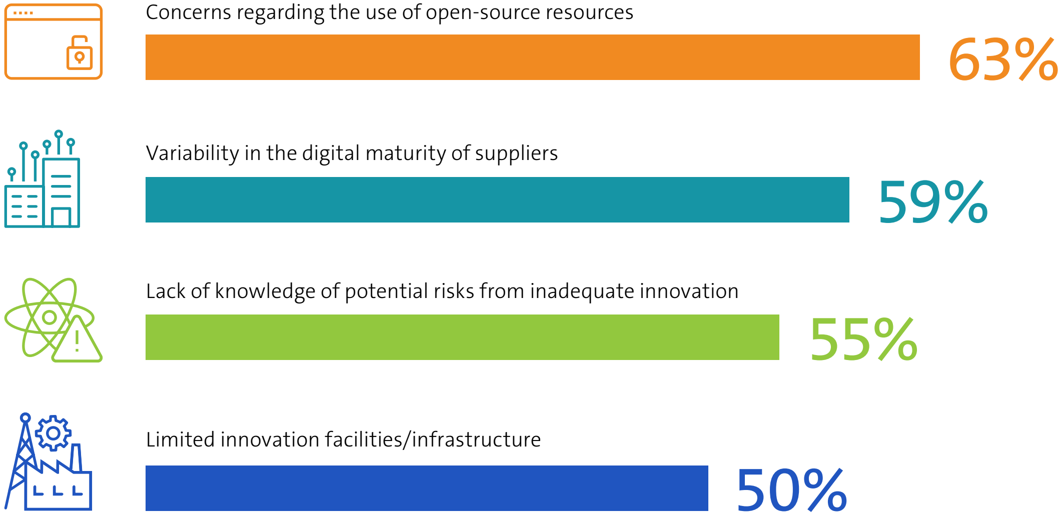
IoT refers to a collection of functions with at least one physical component that can connect over a switched or wireless network. These include physical components, the resident software inside the devices’ various computing elements, and any software residing in a mobile app or cloud instance.

## Challenge #1

# Developing connected products is harder than it looks

IoT innovation may look easy, but getting connected products to market can prove more difficult than you may think. With a myriad of technologies, devices, applications and management platforms, manufacturing even one device can prove complicated. Building IoT functionality into connected products will take time and will require organizations to rethink their current operations.

When asked which challenges keep organizations from pursuing greater levels of innovation, executives said:[1]



Introduction
Development
Features
Cybersecurity
Intentions
Compliance
Conclusion
Why UL Solutions?
Sources

## Challenge #2
# Product features fail in real-world settings

Manufacturers know that the number, type and purpose of IoT devices expands each year, yet many consumers have had less-than-stellar experiences. Consumers have expressed concerns about potentially fatal consequences if and when glitches occur with IoT devices in their homes and lifestyles. Keep in mind that people buy solutions, not products, which are part of a connected ecosystem of solutions. Each product needs to work with all the solutions.

83%

of consumers worry about losing control of their smart home due to **performance problems.**[2]

62%

of consumers worry that connectivity issues will increase as IoT becomes **more prevalent.**[2]

46%

of companies consider product reliability the most important buying criteria for technology **purchase decisions.**[3]

21%

of consumers abandon wearables due to the devices' **limited functionality and use.**[4]

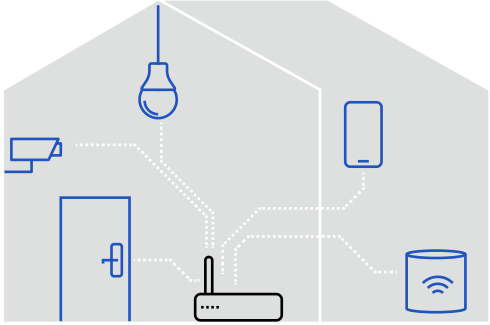
*IoT technology can* ***FALL SHORT*** *of the convenience it promises, with*

**ONE IN THREE**

**people struggling**

*to operate their smart gadgets.*[5]

# Why features fail in real-world settings



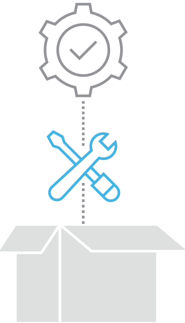
### Connectivity

A lack of signaling or bidirectional communication between products for collection and routing purposes can contribute to device failure and user frustration.

**Always ask:**
*Does the device seamlessly connect? Does it stay connected? If power surges occur, does it reconnect quickly? Does it connect seamlessly for data transmission at the appropriate speed?*

### Device configuration

Many products still require manual configuration, which users can find problematic. As the connected ecosystem evolves, auto-configuration becomes a must-have.

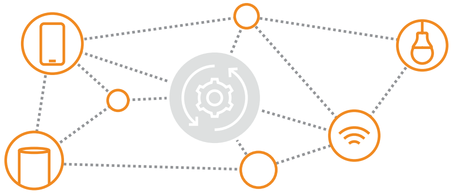


**Always ask:**
*Does the device set up easily out of the box?*

### Device load

As the volume of connected products increases along with increased project activity, server farms become a necessity for handling large amounts of data.

**Always ask:**
*Does processing allow for the seamless transfer of data between products and servers?*



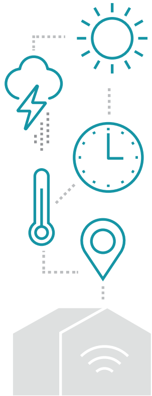
### Integration problems

Connected product apps typically integrate with various routers, smart hubs or other systems.

**Always ask:**
*Does the device adapt to operating system upgrades, new apps and new devices in its connected ecosystem?*

### Operating environment

Connected products operate in a wide range of environments and conditions.



**Always ask:**
*Under what conditions will users operate the product?*

# Challenge #3

# Cybersecurity risk entrenched in daily life

With the need for interconnected systems to communicate and share data frequently, the attack vector for hacking connected products has increased significantly. Cyberattacks are real, and any connected product — from refrigerators to pacemakers — can face hacking threats. Once cyber criminals gain control, they can take over an object's functionality in seconds or pivot to other products or systems on the network. Instead of leaving security as an afterthought, embed it in the way you build products.

**Why we need to stay one step ahead, by the numbers:**

**5 minutes**
How long it takes before the average IoT device experiences an attack after it goes live[6]

**38,182**
The number of IoT-based malware attempts in March 2020 alone[8]

**7 days**
The average cost in time due to a malware attack[7]

**$3.86 million**
The average cost of a malware attack on a company

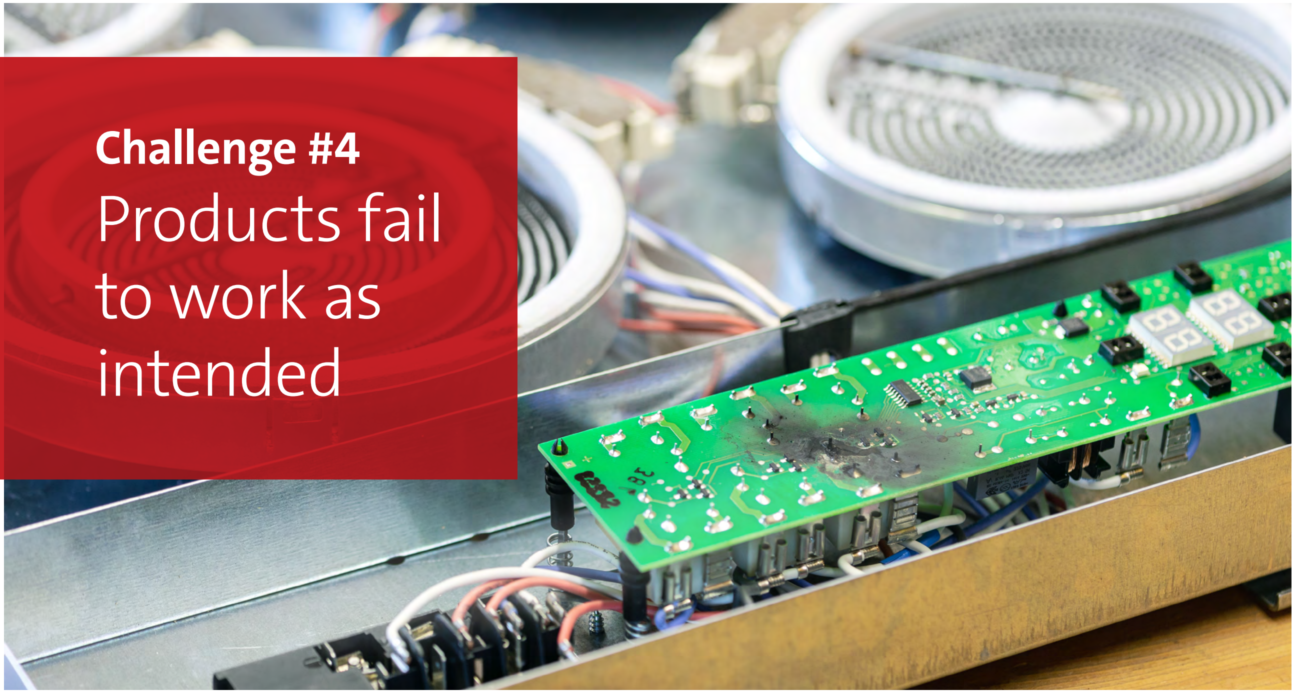
(includes customer turnover, increased customer acquisition, loss of reputation and diminished goodwill)[9]

Cybersecurity vulnerabilities in connected systems and devices most frequently result from a lack of security best practices built into product design and implementation. The most common causes generally fall into one of the following five areas:

- Poor product design
- Non-secure communications protocols
- Inadequate authentication procedures
- Limited software updating
- Improper implementation or device/application use

**57%**
*of IoT devices are vulnerable to medium- or high-severity attacks, making them easy targets for attackers.*[10]

Introduction
Development
Features
Cybersecurity
Intentions
Compliance
Conclusion
Why UL Solutions?
Sources



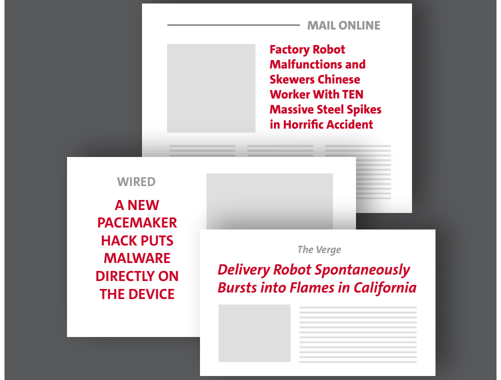
## Challenge #4

# Products fail to work as intended

### What risk management says about safety risks

> *"With the rise of autonomous vehicles, industrial IoT, smart homes and more, a technology failure has the potential to cause physical harm to people and property. Forward-thinking companies should ensure they are covered for this growing liability."*
>
> Marsh & McLennan Companies

### From the headlines



MAIL ONLINE

**Factory Robot Malfunctions and Skewers Chinese Worker With TEN Massive Steel Spikes in Horrific Accident**

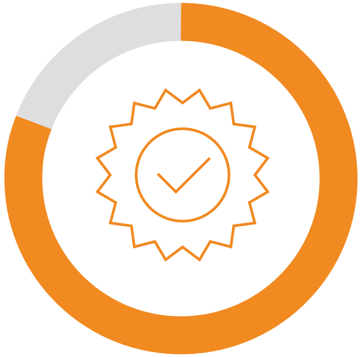
WIRED

**A NEW PACEMAKER HACK PUTS MALWARE DIRECTLY ON THE DEVICE**

*The Verge*

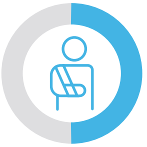
***Delivery Robot Spontaneously Bursts into Flames in California***

Many connected products play vital roles in sensitive sectors like fintech, medtech and healthtech, which prioritize physical safety and the protection of personal data needs. The moment a product reaches the customer, it must be flawless. Poorly functioning or poorly managed products can negatively affect brand reputation at best, and in a worst-case scenario, harm the user. Safety should not be limited to end products; safe manufacturing processes should be kept in mind as well.



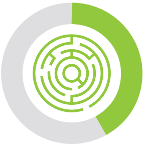
81%

of consumers said that they need to be able to trust a brand to buy from them.[13]



50%

of end users are increasingly concerned with the risk of bodily harm from IoT devices.[11]



42%

of executives expect that the risk of IoT failures will grow in complexity.[12]

Introduction
Development
Features
Cybersecurity
Intentions
Compliance
Conclusion
Why UL Solutions?
Sources

# Challenge #5
## Growing uncertainty around regulatory compliance

*Whether cybersecurity, safety, interoperability or wireless, there's always a global market access component as region-specific requirements vary from country to country.*

Uncertainty is growing as regulatory interest in IoT increases globally. Companies are concerned and expect regulations to take precedence over innovation. Current legislative actions focus on securing IoT devices and protecting consumer privacy and data. As safety regulations and requirements can differ from country to country, it's always advisable to learn about market-specific regulations.

66%

of companies are setting aside money to comply with laws and legislation.[14]

40%

of executives expect compliance risks to grow in complexity over the next three to five years.[15]

## Conclusion

# With connected products, the challenge is the complexity

As IoT adoption grows, so does the importance of implementing solutions, best practices and controls that can protect the safety, functionality and security of not only devices but the entire connected ecosystem. Companies need to understand what they are making, buying and using. Incorporating connectivity and security into product development along with processes for handling vulnerabilities and managing life cycles and support is critical.

**Initial questions to consider**

- Where will this product be sold?
- Which standards apply to my product?
- How do we provide consumers with a great user experience?
- How do I reduce problems with connectivity?
- How can I check to make certain that my device connects, stays connected and delivers on its intended functionality?
- What are the best practices for developing safe and secure products?
- What level of security is right for my product?

**To learn more about IoT interoperability and connectivity testing services, visit UL.com/IOP**

Introduction
Development
Features
Cybersecurity
Intentions
Compliance
Conclusion
Why UL Solutions?
Sources

# 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 assess that your products operate seamlessly with other devices and major connectivity/IoT platforms and standards. This can help you deliver reliable, safe and secure connected products to consumers, improving customer experience and brand reputation.

- UL Solutions has helped develop more than 1,600 standards to define safety, security, quality and sustainability.
- 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) and the Open Connectivity Forum (OCF).
- We can perform testing for real-world interoperability for most connected products, mobile apps, Wi-Fi reconnection robustness, features, 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, with a comprehensive suite of services including end-product testing, certification and verification, which can help you access your target markets more quickly.

**Contact us today.**

Applicable services include testing and certification to:

**Smart assistants**

- Google assistant
- Amazon Alexa

**Connectivity standards and platforms**

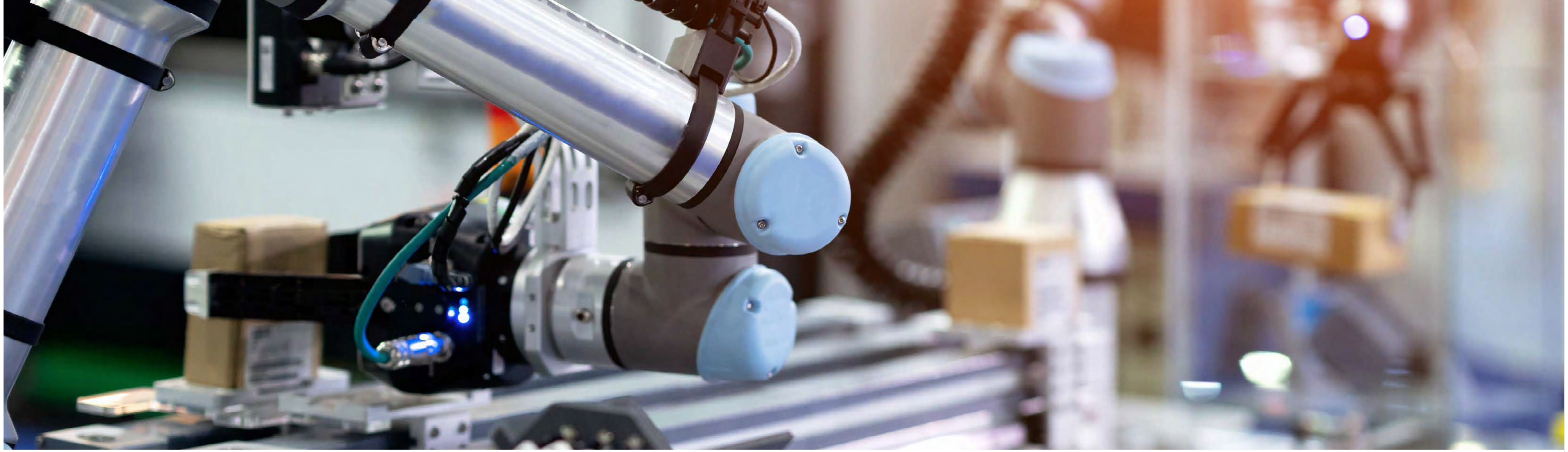
- Samsung SmartThings
- Matter
- MFi
- Thread
- CSA (Zigbee)
- OCF
- Bluetooth®
- USB IF

**Wireless cellular devices standards**

- Global Certification Forum (GCF)
- PTCRB

**Cybersecurity standards and ratings**

- UL Verified IoT Device Security Rating[16,17]
- UL 2900-2-1, the Standard for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems
- 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
- IEC 62443



# Sources

1. UL. (April 2020). Innovation and Safety in a New Decade.

2. Dynatrace. (August 2018). Consumer Confidence Report.

3. Statista. (September 2020). Most important buying criteria for tech purchases (COVID-19 Context). https://www.statista.com/statistics/1169718/worldwide-it-purchase-buying-criteria-covid/

4. Ericsson. (May 2019). Wearable technology and the IoT. https://www.ericsson.com/en/reports-and-papers/consumerlab/reports/wearabletechnology-and-the-internet-of-things/

5. ADT. (August 2019). Home is where the smart is.

6. NETSCOUT. (August 2019). Dawn of the Terrorbit Era.

7. Purplesec. (February 2020). 2020 Cyber Security Statistics.

8. Symantec. (April 2019). ISTR 2019: Internet of Things Cyber Attacks Grow More Diverse.

9. Purplesec. (February 2020). 2020 Cyber Security Statistics.

10. Palo Alto. (March 2020). Unit 42 IoT Threat Intelligence Report. https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat%20Intelligence%20Report%202H%202018.pdf

11. Marsh & McLennan Companies. (October 2018). Internet of Things: Limitless Connections and Ways to Fail. https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2018/dec/IoT--Limitless-Connections-and-Ways-to-Fail/Internet-of-Things_%20Limitless%20Connections.pdf

12. Marsh & McLennan Companies. (March 2020). A New Definition of Catastrophic Risk: Technology Industry Risk Study.

13. Edelman. (February 2019). Edelman 2019 Trust Barometer.

14. Marsh & McLennan Companies. (March 2020). A New Definition of Catastrophic Risk: Technology Industry Risk Study.

15. Marsh & McLennan Companies. (March 2020). A New Definition of Catastrophic Risk: Technology Industry Risk Study.

16. https://www.ul.com/resources/Iot-security-rating-levels-guide

17. https://www.ul.com/services/ul-verified-iot-device-security-rating

Introduction
Development
Features
Cybersecurity
Intentions
Compliance
Conclusion
Why UL Solutions?
Sources

Back to the first page

UL Solutions

**UL.com/IOP**