



The future of electronics

A manufacturer's guide to safe, secure and compliant products



Contents

3	Foreword	9	The Internet of Medical Things (IoMT)
4	Consumer electronic devices	10	Sustainability and carbon footprint
5	The Internet of Things (IoT)	11	The power of remanufacturing
8	Industrial Internet of Things (IIoT)	12	References



Foreword

When manufacturing electronic products, safety is paramount. Guidelines and international standards have been put in place to protect consumers and maintain their trust in electrical products, and through testing and certification, manufacturers can ensure their products meet these guidelines. Manufacturers that place a mark of trust on their electrical products will enhance consumer confidence and, ultimately, achieve better outcomes for their business.

As technology evolves, new challenges and obligations on manufactures are emerging. With the rise of the Internet of Things (IoT), there are more products entering the market that are connected to the internet, and therefore need to meet multiple standards to ensure they meet both electrical safety and cybersecurity requirements.

The Industrial Internet of Things (IIoT) encompasses a different set of standards and regulations as it involves a different set of risks associated with complex, industrial processes and a wide range of data including commercially sensitive information.

Separate standards also apply to the Internet of Medical Things (IoMT), which is concerned specifically with connected devices relating to healthcare.

In addition to ensuring consumer, worker and patient safety, manufacturers of these products must have measures in place to maintain a low carbon footprint and align with the United Nations goal of achieving global Net Zero by 2050.¹



Consumer electronic devices

Electrical equipment spans a wide spectrum, from small devices such as doorbells and thermostats to larger items including washing machines and electric vehicle (EV) chargers.

Before electrical equipment products can be placed on the market in Great Britain, they must meet the requirements set out by the Electrical Equipment (Safety) Regulations 2016 (Low Voltage Directive).²

The Low Voltage Directive states that a manufacturer of electrical equipment must ensure it is designed and manufactured in accordance with the principal elements of a defined set of safety objectives.³

By collaborating with regulatory bodies, manufacturers can enhance the safety and quality assurance of their products. This partnership ensures products meet established benchmarks and rigorous safety criteria, leading to a marketplace with innovative, functional, and, most importantly, safe products.

BSI offers CE marking as a Notified Body for many electrical and electronic products under the Low Voltage Directive and the Machinery Equipment Directive.

Where Notified Body involvement is not required, BSI can also support manufacturers in product self-declaration, providing Third Party Type Testing and a comprehensive technical file assessment service.



Visit bsigroup.com to learn about independent testing and certification of electrical products with BSI.

The Internet of Things (IoT)

By 2030, the number of IoT devices worldwide is projected to be over 32.1 billion – almost doubling from 18 billion in 2024.⁴


BSI offers testing and certification of connected devices to ensure that a wide range of smart devices, including smart locks, doorbells, security cameras, Wi-Fi home-hubs, and CO2 and fire alarms, are safe and secure.

In recognition of long-standing cybersecurity and privacy vulnerabilities in consumer products connected to the internet or a network, the UK Product Security and Telecommunications Infrastructure (Product Security) regime (UK PSTI)⁵ has been introduced.

Manufacturers of consumer connectable products must ensure their products are in compliance with this legislation, for example by having their products tested, before placing them on the UK market.



Visit bsigroup.com to learn about third-party UK PSTI Compliance Testing with BSI.



“For businesses in the age of digital and AI, maintaining the trust of customers and workforces is an essential priority, meaning security and privacy must be at the top of the agenda when building networks of smart devices and connected technology.”⁶

Forbes

Radio Equipment Directive (RED)

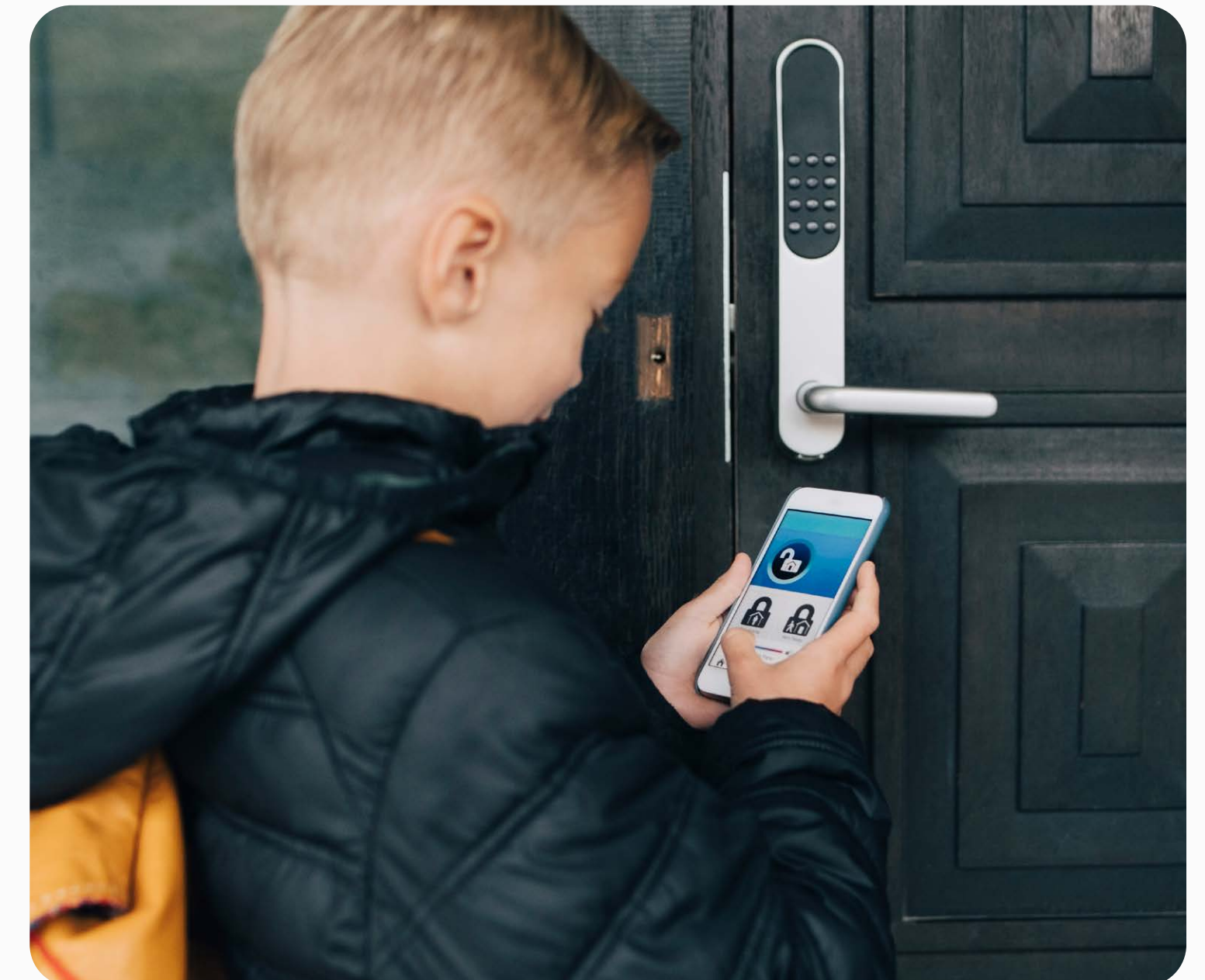
From 1 August 2025, all internet-connected radio equipment placed on the EU market must comply with the enhanced cybersecurity requirements of the Radio Equipment Directive Delegated Act (EU) 2022/30,⁷ which is supported by the new EN 18031 standards. This landmark regulation ensures that devices meet stringent criteria for network protection, data security, and fraud prevention.

RED's scope encompasses a broad range of products across industries, highlighting the critical role of compliance in the modern marketplace. Consumer devices, such as smartphones, smartwatches, and tablets, are primary examples, reflecting the directive's focus on safeguarding devices central to daily life.

Additionally, IoT devices—ranging from smart home products like thermostats and lighting systems to connected appliances and wearable health monitors—are key categories. As these devices collect, transmit, and process sensitive user data, ensuring compliance is vital for protecting consumer trust and privacy.

Beyond consumer applications, RED applies to industrial and infrastructure-focused devices that underpin critical operations. Examples include IoT-enabled industrial monitoring systems, connected fire safety equipment, and vehicle telematics solutions. Payment systems, such as wireless point-of-sale terminals and devices supporting cryptocurrency transactions, face particularly stringent requirements under RED, given their potential exposure to fraud risks.

BSI is at the forefront of supporting manufacturers in meeting RED and EN 18031 requirements. Capabilities include a comprehensive suite of services, such as gap analysis, conformity testing, and technical file assessment, ensuring that devices comply with RED standards and can be successfully placed on the EU market.



Visit bsigroup.com to learn about RED testing with BSI.

Industrial Internet of Things (IIoT)

The Industrial Internet of Things refers to the extension and use of IoT in industrial sectors and related applications. With a strong focus on machine-to-machine (M2M) communication, big data, and machine learning, the IIoT enables industries and enterprises to run more efficient and reliable operations.

An example of a business that has significantly enhanced business operations through IIoT is IKEA, which has implemented the use of industrial sensors to manage logistics via drone technology and artificial intelligence (AI). Drones are set up with algorithms designed to carry out stock checks in warehouses and maintain up-to-date records, which can then be communicated to customers.⁸

IIoT is the premise for the next industrial evolution. The connection of devices within an industrial environment enables complete operational visibility, allowing the best real-time decisions to be made, with or without human intervention – transforming how we will manufacture for years to come.



As demand for automation grows, however, the risk of cyber threats increases. The adoption of industrial security standards with certification is essential to the advancement of IIoT because it ensures the security not just of individual assets but also of larger systems, and systems of systems.

There are well established strategies and techniques that automation professionals across many different industries can employ, to discover and mitigate security vulnerabilities and improve the inherent security of their products and systems, as defined in the IEC 62443 series of standards.

To implement systems like the one used by IKEA, organizations need a structured approach, assessing numerous threats at various levels. They are processing large amounts of data, so it is essential they are designed and maintained with the highest levels of cybersecurity. The improvement of contemporary digital attacks on IIoT solutions is such that IT and OT experts need to work seamlessly to create secure frameworks customized to conditions.

The Internet of Medical Things (IoMT)

The Internet of Medical Things (IoMT) is the collection of medical devices and applications that connect to healthcare information technology systems through different online connectivity technologies. The basis of IoMT is medical devices equipped with different radio IoT technologies, such as Bluetooth, Wi-Fi, NFC and Cellular, enabling machine-to-machine⁹ communication.

The advent of IoT has revolutionized the healthcare industry. A notable increase in wearables for purposes such as patient monitoring and health vitals monitoring has led to robust growth in healthcare IoT devices and applications.

The increasing development of connected medical devices presents many benefits, including providing reliable and accurate diagnosis that leads to improved patient management. However, these devices can also be subject to cybersecurity threats including Distributed Denial-of-Service (DDoS) and Denial-of-Service (DoS) attacks, Man-

in-the-Middle (MITM) attacks, and malware injections, amongst others. It is therefore essential that effective measures are in place to protect patient privacy and data.

Some examples of IoMT devices are:

- Connected devices and related software applications, produced by active medical device original equipment manufacturers (OEMs):
 1. Wearable external devices: connected skin patches, blood glucose monitoring devices, insulin pumps and remote patient monitoring devices.
 2. Stationary devices: home monitoring devices, CPAP devices, connected imaging devices, scanning machines, MRI devices, X-ray and scanners.
- Digital health applications and platforms.
- Telehealth platforms: remote health monitoring, healthcare automation and hospital infrastructure monitoring.

BSI can support manufacturers of connected medical devices with cybersecurity testing services, encompassing global cybersecurity requirements set out by bodies such as the FDA and meeting relevant requirements of Annex I

of the Medical Devices Regulation (MDR) and In-vitro Diagnostic Medical Devices Regulation (IVDR). Hardware and software components can be tested against standards such as UL2900, IEC 62443, IEC/TR 60601-4-5, OWASP, IEC 82304, IEC 81001-5-1 and IEC 62304.

We also partner with active medical devices manufacturers to provide electrical safety testing and certification, helping them to reach international markets with the IECCE CB programme.



Learn how BSI helps medical device manufacturers ensure patient safety at bsigroup.com.

Sustainability and carbon footprint

As with all industries, it is important that manufacturers of electrical products design and distribute their products in a sustainable manner, minimizing their carbon footprint.

To become carbon neutral, an organization must absorb from the atmosphere the same amount of carbon as it emits. This means an organization must have measures in place to ensure that any of the greenhouse gases it produces in the creation and distribution of its products or services are offset by some other means. Alongside this, the organization must have in place effective tools for both measuring and reducing its carbon footprint.

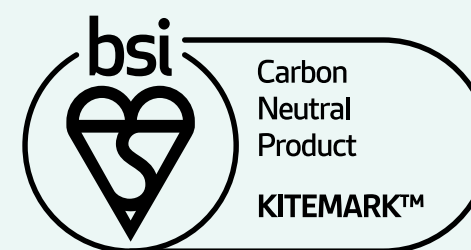
Carbon neutrality is a key objective for organizations looking to help combat climate change, enhance their sustainability credentials and increase resilience. It helps them align with the United Nations Sustainable Development Goals (UN SDGs) and gain a competitive edge by offering customers greener products and services.

One organization putting significant measures in place to reduce its carbon footprint is global technology company Lenovo, who achieved the BSI Kitemark™ for Carbon Neutral Products for its ThinkBook 13x G4 IMH and ThinkBook X IMH.¹⁰

The BSI Kitemark for Carbon Neutral Products is a symbol of trust, demonstrating that a product has been independently assessed against international standards and has met rigorous testing criteria confirming its carbon-neutral claims.

53%

A 2023 YouGov survey found that 53% of consumers would spend more on a product with the BSI Kitemark for Carbon Neutral Products.¹¹



Discover more about the BSI Kitemark for Carbon Neutral Products at bsigroup.com.

The power of remanufacturing

There are many ways an organization can improve its carbon credentials. One example is using remanufactured products to support development of a circular economy.

Remanufacturing involves disassembling a discarded product, restoring and re-testing the individual parts then using these to recreate a product which is as good as, if not better than, new.

Circular Computing was the first organization to achieve BSI Kitemark Certified Remanufacturer status. As part of the remanufacturing process, every laptop goes through its Circular Remanufacturing Process, a 360-step journey that returns a used product to at least its original performance, with a warranty that is better than, or at least equivalent to new.¹²

The Irish government recently signed a four-year contract worth EUR 30 million to procure around 60,000 refurbished laptops from Circular Computing. These can be purchased by any public body, accounting for around 12% of Ireland's laptop market.¹³



“Our work with BSI means that the industry is empowered to change the way that ICT products are purchased. We can now finally, after all these years, provide an alternative to new, that is in full compliance with the circular economy, and all the benefits that society needs.”

Scott Mac Meekin, CEO, Circular Computing



Discover more about manufacturing safe and sustainable electronic products at bsigroup.com

References

1. For a livable climate: Net-zero commitments must be backed by credible action, United Nations, un.org
2. Electrical Equipment (Safety) Regulations 2016: Great Britain, GOV.UK, gov.uk
3. The Electrical Equipment (Safety) Regulations 2016, legislation.gov.uk, legislation.gov.uk
4. Number of Internet of Things (IoT) connections worldwide, statista, statista.com
5. The UK Product Security and Telecommunications Infrastructure (Product Security) regime, GOV.UK, gov.uk
6. 2024 IoT And Smart Device Trends: What You Need To Know For The Future, Forbes, forbes.com, October 2023
7. Radio Equipment Directive, European Union, eur-lex.europa.eu
8. How IKEA has Committed to Global Digital Transformation, Technology Magazine, technologymagazine.com, August 2024
9. machine-to-machine (M2M), TechTarget, techtarget.com, August 2019
10. Lenovo certified BSI Kitemark™ for Carbon Neutral Products, The British Standards Institution, bsigroup.com
11. YouGov 2023. Sample – 5390 adults across UK, China, US and India
12. The world's First & Only BSI Kitemark for Remanufactured Laptops, Circular Computing, circularcomputing.com
13. Irish Government signs framework agreement for the purchase of remanufactured laptops, European Circular Economy Stakeholder Platform, circulareconomy.europa.eu, June 2024





To find out more about how BSI can help you, visit bsigroup.com