Connected toys: Safety for a modern world

An e-guide for toy manufacturers and retailers

UL Solutions

Safety. Science. Transformation.™

Overview

- Quick safety guide: Connected toys and children's products
- Connected toys fast facts
- Key risks of connected toys
- Minimize risk in connected toys and children's products
- What to evaluate before launching a connected toy or children's product
- How UL Solutions can help

Back to overview

Quick safety guide: Connected toys and children's products

Connected toys and children's products can provide hours of fun and intellectual stimulation for children of all ages. Due to an increase in demand for intelligent and interactive connected toys, the potential benefits that connecting to the internet and Internet of Things (IoT) can bring are unparalleled in the history of toy manufacture. However, connectivity also brings new challenges to toy manufacturers of electronic and wireless devices for learning and gaming.

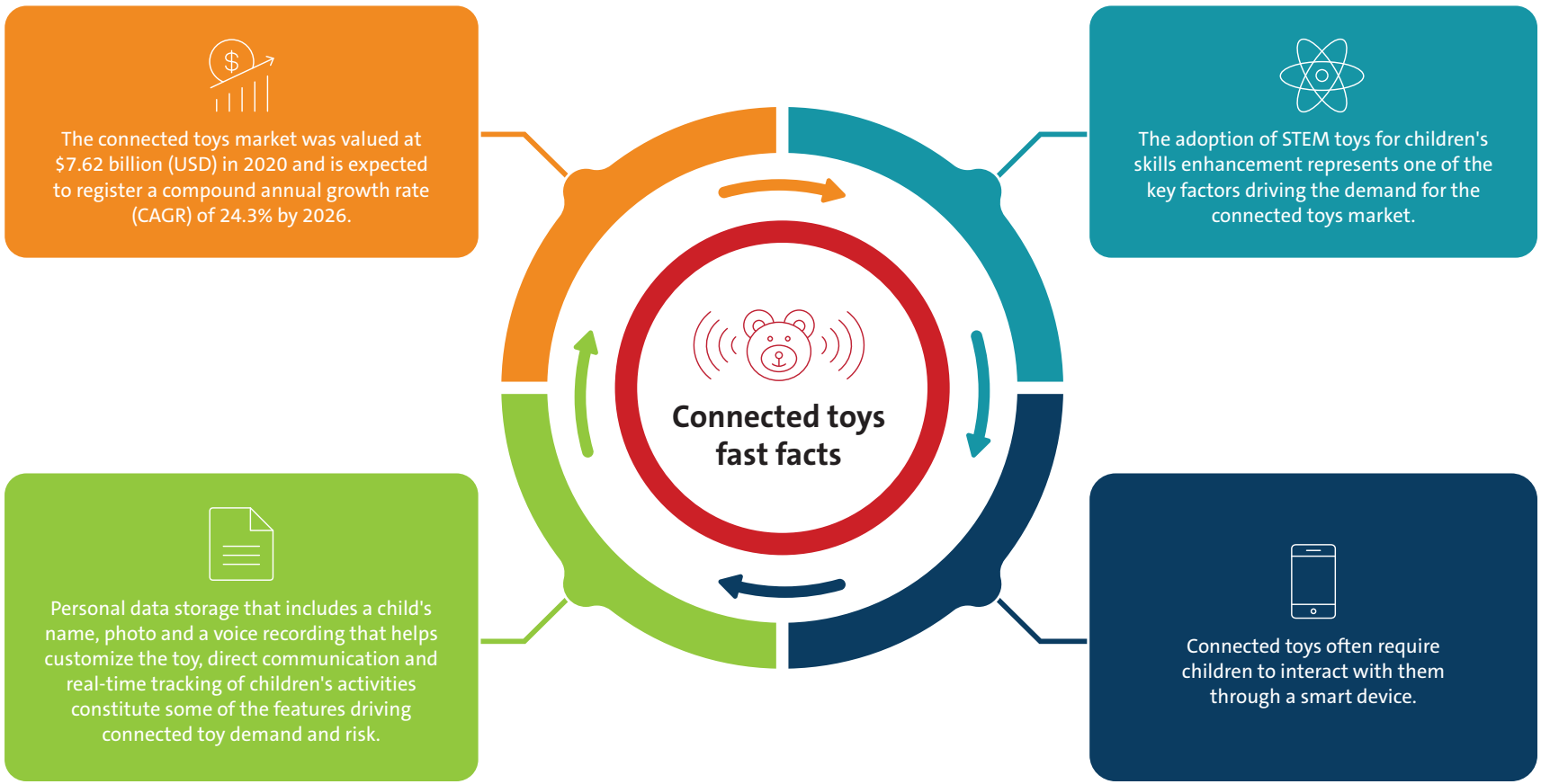
Parents who want to provide their children a learning opportunity might turn to toys that promote STEM — science, technology, engineering and math. Some toy robots allow kids to program the robot's movements, teaching the basics of coding. Some IoT devices can help kids stay healthy, with fitness trackers and smart toothbrushes.

These digital toys and devices present many benefits for children.

The toy and children's product industry is highly regulated to protect the safety and health of the young consumers who use them. Toys and children's products entail very specific safety concerns since their intended users may play with them in unintended but foreseeable ways. Plus, parents have understandable concerns about the health and safety of their children.

In addition, connected toys bring even greater potential risks, including privacy and security concerns. Toys and children's products that contain cameras, microphones and GPS locators can expose children to threats that were unimaginable when the most advanced feature of a toy was an adjustable handle on a jack-in-the-box.

UL Solutions



Source: Connected Toys Market - Growth, trends, Covid-19 impact and forecasts (2022 - 2027) - MondorIntelligence

Key risks of connected toys

Toy manufacturers are well aware of the most traditional safety risks that toys bring, such as choking hazards and sharp edges, and they are also well-versed in the key product safety requirements, including chemical and physical/mechanical safety, depending on the target countries where they launch their products. They also know about the battery safety risks and those inherent in radio frequency (RF) exposure. However, connected toys and children's products now bring new dangers like data privacy risks that can prove just as harmful to both children and their families.

To avoid RF exposure risks, manufacturers measure the specific absorption rate (SAR) from their connected toys as well as other toys exposed to RF sources. SAR measures the rate at which a human body absorbs energy per unit mass when exposed to an RF electromagnetic field.

Maintaining battery safety requires evaluating specific risks when electronic toys draw power from batteries or wall plugs to operate. For example, when a circuit board, motor or battery compartment increases the temperature of exposed surfaces to high levels, it can pose a burn hazard to children upon contact.

Let's focus now on data privacy risks, which represent a new type of risk and for which regulations aren't always clear.

Back to overview

First, it's important to highlight the different kinds of information that hackers can collect from children using these devices:

- Date of birth, name and gender
- Profile pictures
- Voice messages, chat messages and photos sent by children
- Account passwords
- Physical location
- Chat history
- Internet browsing history[1]

They can also collect information from parents:

- Email address and mailing address
- Gender
- Profile pictures
- Voice messages, chat messages and photos sent by parents
- Account passwords and password retrieval questions
- Credit card information
- Phone number
- Wi-Fi passwords and IP addresses[2]

[1]Nelson, Bill 1942-. 2016. "Children's Connected Toys: Data Security and Privacy Concerns." Homeland Security Digital Library. Retrieved April 13, 2017 (https://www.hsdl.org/?abstract&did=797394).

[2]Nelson, Bill 1942-. 2016. "Children's Connected Toys: Data Security and Privacy Concerns." Homeland Security Digital Library. Retrieved April 13, 2017 (https://www.hsdl.org/?abstract&did=797394).

UL Solutions

Hackers can collect information during product registration, during play or through hacking home Wi-Fi systems to which the toys and children's products are connected. Also, even if a consumer's home network is secure, the connected product's manufacturer and retailer, who store this data on their servers, may experience cyberattacks and data breaches. When this happens, in addition to exposing manufacturers and retailers to criminal and civil penalties for the breach, their brand loyalty among consumers can take a potentially fatal hit.

Consumers should also understand whether and to what extent manufacturers will share the data that connected toys collect. Even if the goal of such data sharing is to improve features such as voice recognition, manufacturers must disclose to consumers the risks inherent in retaining and sharing non-anonymized data.

The Children's Online Privacy Protection Act of 1998 (COPPA) imposes requirements on operators of websites or online services directed at children under 13 years of age, and on operators of other websites or online services that know they are collecting personal information online from a child under 13 years of age.[3] Toys that connect to the internet fall under this regulation's purview.

[3]https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Back to overview

Minimize risk in connected toys and children’s products

Toys and children’s products that incorporate wireless, artificial intelligence (AI) and computing components come with risks and regulatory requirements that may be unfamiliar to manufacturers.

In addition to testing connected toys and children’s items for safety risks, manufacturers can take steps to reduce further risks to consumers and their brands. For example, a toy should only collect data necessary for the functioning marketed features and purpose of the toy. This data should not be shared or sold for any reason.

They need to design privacy and security into the toy as part of the manufacturing process, just as they do physical safety. They need to strengthen interoperability and secure connection features to control how toys pair to prevent unauthorized access to the toy and home networks.

What to evaluate before launching a connected toy or children's product

Wireless components and connectivity engines:

Connected products that contain wireless components or connectivity engines are subject to an entirely new set of regulatory requirements that vary by region. For example, the Radio Equipment Directive (RED) in the EU requires many kinds of testing to verify the safety of wireless devices. The Federal Communications Commission (FCC) oversees similar standards in the U.S.

To sell wireless toys in these markets, companies must demonstrate compliance with regional requirements. Understanding the relevant regulations that apply in each market represents a demanding but essential step in gaining global market access.

Some of the most critical testing in this area includes:

- Electromagnetic compatibility (EMC) testing – Assessing electronic devices' ability to operate as intended when in proximity to other electronic devices or in the presence of electromagnetic phenomena.
- RF testing – Testing to help ensure that radio broadcasts use their space on the spectrum efficiently; RF tests cover most kinds of broadcasts, including Bluetooth®, Wi-Fi, cellular devices and more.
- SAR testing – Measuring the electromagnetic energy absorbed by a body in proximity to wireless devices helps assess whether a device exceeds a country's established RF exposure limits.
- Bluetooth® Special Interest Group (SIG) qualification – Satisfying the requirements to use Bluetooth® technology as well as its intellectual property and the associated logo.
- Over-the-air (OTA) testing – Many standards organizations and wireless carriers require accurate predictions of real-world wireless device performance capabilities.
- Interoperability (IOP) testing – Helping to ensure that products connect and function as intended.

Back to overview

As with any connected products, data privacy and cybersecurity risks present a formidable challenge to companies. Top of mind among consumers, cybersecurity breaches could expose one of the most vulnerable populations: children. The prudent course of action for companies to take is to establish a healthy cybersecurity culture, including sufficient cybersecurity testing and monitoring to identify and address potential vulnerabilities. Some of the most critical testing in this area includes:

- Regulatory requirements and marks – Depending on the technologies used in the product, it must demonstrate conformity with regulatory requirements before its market launch — a critical element for earning brand trust.
- Security by design – Building security into the organization's governance processes by building cybersecurity into the product's fundamentals rather than relegating it to the status of afterthought.
- Penetration testing vulnerability analysis – Applying required standards and best-practice principles to ensure that products and their ancillary services, such as mobile applications and web interfaces, do not represent easy targets for individuals with malicious intent.
- Back-end protection – Any cloud infrastructure or back-ends require protection to address both security concerns and data transfer privacy.

In addition to the goal of designing and manufacturing toys and children's products that are as safe as possible, manufacturers also have to navigate complex and varying global regulations. Understanding how compliance requirements impact products on a global scale, removing market entry barriers and solving critical challenges to country- and region-specific regulations comprise the most important steps for successfully launching connected toys and children's products.

Back to overview

How UL Solutions can help

UL Solutions, a global safety science leader, is a trusted name in safety and performance testing and third-party certifications. We have the experience, worldwide facilities and expertise to help toy companies navigate the complexities of introducing smart toys and children's products to the market. Our toy safety tests can assess whether your products comply with applicable U.S., EU and other international standard consumer safety specifications, as well as all applicable safety standards for connecting to the IoT.

Our wide range of testing and certification services includes EMC, SAR, product safety, Bluetooth® conformance, cybersecurity and radio testing. Manufacturers who can demonstrate a truly safety-first approach to their products will build more solid relationships with parents and children alike.

Back to overview

To learn more, visit
ul.com/smart-toys-solutions

UL Solutions

UL.com/Solutions

Safety. Science. Transformation.™