



Designation: F3463 – 21

Standard Guide for Ensuring the Safety of Connected Consumer Products¹

This standard is issued under the fixed designation F3463; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ϵ) indicates an editorial change since the last revision or reapproval.

INTRODUCTION

This guide is intended to provide direction for the design and manufacture of connected consumer products to help ensure that the connected functionality of such products does not pose physical hazards to consumers. This guidance should provide considerations for designing connected functionality that neither poses nor introduces product safety hazards.

The focus of this guide is limited to consumer products. While the Internet of Things (IoT) presents one system for connecting products, this proposed guidance also covers other types of network-connected systems such as Bluetooth, WiFi, or other communication protocols used with consumer products.

1. Scope

1.1 This guide provides guidance for connected consumer products, as defined in 1.1.1, as it relates to physical product safety hazards created by virtue of their connectivity. It applies to connected products that need testing and evaluation to prevent cybersecurity vulnerabilities and weaknesses that could compromise the safety-related performance of the product, create a physical safety hazard in the product or its operation, or result in a noncompliance to the underlying end product safety standard.

1.1.1 Connected consumer product or Internet of Things (IoT) consumer device means any consumer device or physical object that is capable of connecting to the internet or other network, directly or indirectly, and is assigned an internet, Bluetooth, or other communication protocol address or identifier. A non-exhaustive list of examples includes:

1.1.1.1 Connected children's products such as toys and juvenile products such as baby monitors;

1.1.1.2 Connected safety-related products such as smoke alarms and door locks;

1.1.1.3 Connected TVs and speakers;

1.1.1.4 Wearable connected health trackers and smart apparel;

1.1.1.5 Connected home automation, security or surveillance cameras, and alarm systems;

1.1.1.6 Connected appliances (for example, washing machines and refrigerators); and

1.1.1.7 Connected smart home assistants.

1.2 Safety, for this guide, is defined as the freedom from an unreasonable risk of physical injury or illness resulting from mechanical contact, hazardous energy release, or exposure to hazardous chemicals from the connected product. Physical injury or illness may include burns, lacerations, strains, contusions, suffocation, strangulation, poisoning, disease, seizures, internal injuries, shock, or other injuries to the body. Property damage related to non-functionality of the connected device is only included to the extent that such property damage leads to a safety issue. Safety, for this standard, does not include privacy or personal data security, or physical harms potentially resulting from privacy or personal data breaches.

1.3 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.4 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Referenced Documents

2.1 *Federal Standard.*²

15 USC 2025(a)(5) Consumer Product Safety Act

¹ This guide is under the jurisdiction of ASTM Committee F15 on Consumer Products and is the direct responsibility of Subcommittee F15.75 on Connected Products.

Current edition approved Sept. 1, 2021. Published November 2021. Originally approved in 2020. Last previous edition approved in 2020 as F3463 – 20. DOI: 10.1520/F3463-21.

² Available from U.S. Government Printing Office, Superintendent of Documents, 732 N. Capitol St., NW, Washington, DC 20401-0001, <http://www.access.gpo.gov>.

3. Terminology

3.1 Definitions:

3.1.1 *connected consumer product, n*—any consumer device or physical object that is capable of connecting to the internet or other network directly or indirectly and is assigned an internet, Bluetooth, or other communication protocol address or identifier.

3.1.2 *consumer product, n*—as defined in 15 USC 2052(a)(5) of the CPSA; any article, or component part thereof, produced or distributed (i) for sale to a consumer for use in or around a permanent or temporary household or residence, a school, in recreation, or otherwise, or (ii) for the personal use, consumption or enjoyment of a consumer in or around a permanent or temporary household or residence, a school, in recreation, or otherwise; such term does not include:

(A) any article which is not customarily produced or distributed for sale to, or use or consumption by, or enjoyment of, a consumer;

(B) tobacco and tobacco products subject to FTC and/or FDA regulation;

(C) motor vehicles or motor vehicle equipment subject to NHTSA regulation;

(D) pesticides subject to EPA registration, except to the extent that the Poison Prevention Packaging Act may apply;

(E) firearms, their accessories, and ammunition subject to BATFE regulation;

(F) aircraft, aircraft engines, propellers, or appliances subject to FAA regulation;

(G) boats, vessels, appurtenances to vessels, and accessories and other equipment subject to US Coast Guard regulation;

(H) drugs, medical devices, or cosmetics subject to FDA regulation, except to the extent that the Poison Prevention Packaging Act may apply;

(I) food subject to FDA and/or USDA regulation.

3.1.3 *cyber security, n*—protection against network-based threats that could lead to criminal or unauthorized access to the connected consumer product or to data obtained from the connected consumer product that could result in an introduced hazard to the product or noncompliance with an underlying standard, including the measures taken to achieve this.

3.1.4 *firmware, n*—machine instructions (programs) installed on the memory chip or other programmable component of a connected consumer product intended to provide instructions for the execution of the product's operating functions.

3.1.5 *hazard, n*—potential source of physical injury.

3.1.6 *Internet of Things, IoT, n*—system of connected products (consumer and non-consumer) that transfer data at local, national, and global levels.

3.1.7 *remote update, n*—update of a consumer connected product in which its embedded software, firmware, or configuration data is changed through a connection to the Internet.

3.1.8 *reasonable and foreseeable future, n*—use of a connected consumer product in a manner that may result from reasonably predictable human behavior.

3.1.9 *safety controls, n*—features (for example, systems, devices, and processes) within a connected consumer product or system designed to mitigate one or more specific safety risks.

3.1.10 *vulnerable sub-populations, n*—groups identified as often less able to perceive or avoid certain hazards associated with a consumer product or in the home environment.

3.1.10.1 *Discussion*—U. S. Consumer Product Safety Commission (CPSC) regulations identify children, the elderly, and the handicapped as vulnerable sub-populations.

3.2 Definitions of Terms Specific to This Standard:

3.2.1 *authenticated user, n*—user granted access to the product's operating systems through a qualified logon process that verifies the user credentials and authentication factors, such as a password, personal identification number (PIN), keychain fobs, smartphone two-factor codes, biometrics, or other similar measures.

3.2.2 *authorized user, n*—user-granted express or implied legitimate access or permission to operate a connected consumer product.

3.2.3 *failure mode and effects analysis (FMEA), n*—structured approach to identifying potential failures that may exist within the design of a product or process that result in a physical safety hazard or non-compliance with an end product safety standard.

3.2.3.1 *Discussion*—Failure modes are the ways in which a process can fail. Effects are the ways that these failures can lead to defects, or harmful outcomes for the customer.

3.2.4 *fault tree analysis, n*—deductive procedure used to determine the various combinations of hardware and software failures and human errors that could cause undesired events at the system level.

3.2.5 *safety-by-design principle, n*—concept intended for product designers to apply in order to achieve a safe product through implementing hazard identification, risk assessment, and risk control processes at each stage of the design process by considering and documenting reasonably foreseeable use of the product and taking measures to either eliminate hazards or minimize risks as early in the design life cycle as possible or provide a default on-product fail-safe mode.

3.2.6 *smart, adj*—term indicating that an item is a connected product.

3.2.7 *software patch, n*—publicly released software update to repair one or more known bugs or issues.

4. Significance and Use

4.1 This guide is intended to apply in conjunction with applicable end-product specific performance or design standard requirements to address the overall system safety of a connected consumer product. Designers and manufacturers of a connected consumer product, with assistance from conformity assessment bodies, or others, as deemed desirable, should identify applicable and relevant product standards. They should assess and document if or how connectivity potentially affects the ability of such products to meet overall product-safety requirements, as well as conflicts or requirements, if any,