UL 5500

STANDARD FOR SAFETY

Remote Software Updates

UL Standard for Safety for Remote Software Updates, UL 5500

First Edition, Dated September 6, 2018

Summary of Topics

This First Edition of the Standard for Safety for Remote Software Updates, ANSI/UL 5500, covers the remote updating of software via the manufacturer's recommended process. It is limited to software elements having an influence on safety and on compliance with the particular end product safety standard.

The new requirements are substantially in accordance with Proposal(s) on this subject dated November 10, 2017, May 25, 2018, and July 27, 2018.

No Text on This Page

UL 5500

Standard for Safety for Remote Software Updates

First Edition

September 6, 2018

This ANSI/UL Standard for Safety consists of the First Edition.

The most recent designation of ANSI/UL 5500 as an American National Standard (ANSI) occurred on September 6, 2018. ANSI approval for a standard does not include the Cover Page, Transmittal Pages, and Title Page.

Comments or proposals for revisions on any part of the Standard may be submitted to UL at any time. Proposals should be submitted via a Proposal Request in UL's On-Line Collaborative Standards Development System (CSDS) at https://csds.ul.com.

No Text on This Page

CONTENTS

STANDARD FOR SAFETY FOR REMOTE SOFTWARE UPDATES

1 Scope

This standard covers REMOTE software updates taking into account the manufacturer's recommended process. It is limited to software elements having an influence on safety and on compliance with the particular end product safety standard.

This standard additionally covers hardware compatibility necessary for safety of the REMOTE software update.

NOTE 1 This standard does not cover:

– Functional SECURITY such as premises, physical, and other similar SECURITY purposes;

– Safety related availability or connectivity of REMOTE communications;

– Field updates done with physical access by qualified personnel;

– Software development lifecycle and maturity;

– Cryptographic techniques for the purposes of user data confidentiality and consumer privacy;

– Insider threat (corporate espionage); and

– REMOTE control operation of the product.

NOTE 2 This standard is intended to be used in conjunction with the appropriate end product safety standard.

2 Normative references

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies:

FIPS 140-2, *(Annexes A, B and C) Security Requirements for Cryptographic Modules*

IEEE 802.3, *Standard for Ethernet*

IEEE 802.11, *Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*

IEEE 802.15.4, *Standard for Low-Rate Wireless Networks*

ISO/IEC 9796, *Information Technology – Security Technologies – Digital Signature Scheme Giving Message Recovery*

ISO/IEC 9797-1, *Information Technology – Security Technologies – Message Authentication Codes (MACs)*

ISO/IEC 9798 (all parts), *Information Technology – Security Technologies – Entity Authentication*

ISO/IEC 10118-1, *Information Technology – Security Technologies – Hash-Functions – Part 1: General*

ISO/IEC 14888-1, *Information Technology – Security Technologies – Digital Signatures with Appendix – Part 1: General*

ISO/IEC 15946-1, *Information Technology – Security Technologies – Cryptographic Techniques Based on Elliptic Curves – Part 1: General*

ISO/IEC 18033-1, *Information Technology – Security Technologies – Encryption Algorithms – Part 1: General*

ISO/IEC 29192-1, *Information Technology – Security Techniques – Lightweight Cryptography – Part 1: General*

ISO/IEC 19772, *Information Technology – Security Techniques – Authenticated Encryption*

NIST SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*

NIST SP 800-57, *Recommendation for Key Management, Part 1: General*

3 Terms and definitions

For the purposes of this standard, the following definitions apply.

3.1
AUTHENTICATION
the process of verifying the identity of an ENTITY.

3.2
AUTHORIZATION
the process of permitting an authenticated ENTITY to access or manipulate the product or the product property to the extent the ENTITY has such permission.

Note to entry: In this context, manipulation means the downloading, installation and verification of software.

3.3
ENTITY
a person, device, product or service which interacts with another via a network.

3.4
INCIDENT
an occurrence that actually or potentially results in adverse safety consequences in the end device application.

Note to entry: INCIDENT is modified from: https://niccs.us-cert.gov/glossary#I

3.5
REMOTE
a term defined by the end product standard.

Note to entry: In the end product application, the term potentially addresses, but is not limited to the following conditions:

– supervision;

– intervention;

– whether the presence of the hazard is detectable;

– distance from the device; and

– physical access to the device or devices.

3.6
SECURITY
the state of having acceptable risk, as determined by the end product standard, that particular SECURITY threats do not exploit a particular SECURITY vulnerability leading to safety hazard(s).

Note to entry: This term is also known as cybersecurity.

3.7
SOFTWARE DOWNLOAD PACKAGE
element that could include software, firmware or safety parametric data.

4 Remote Software Update Process

4.1 General

4.1.1 The REMOTE software update process shall not result in a risk of fire, electrical shock, injury to persons, loss of one or more safety functions, or other hazard as specified in the relevant end product standard. The remote software update process, including any AUTHENTICATION and encryption processes, shall include means to prioritize hardware and software interrupts of the operational firmware.

Compliance is checked by applying the requirements of 4.1.2 and 4.2 to 4.9

4.1.2 The software update process shall implement a suitable means for connection between a host and one or more target end devices for the SOFTWARE DOWNLOAD PACKAGE.

Validation of the REMOTE software update process in accordance with the requirements of this standard and the relevant end product standard shall include the following process steps. The steps may be discrete or combined and may be reordered by the end product requirements:

– Establish REMOTE Connection (see 4.2)

– AUTHENTICATION (see 4.3)

– AUTHORIZATION (see 4.4)

– Hardware/Architecture/SOFTWARE DOWNLOAD PACKAGE Compatibility Check (see 4.5)

– Download/(Re-)Transmission (see 4.6)

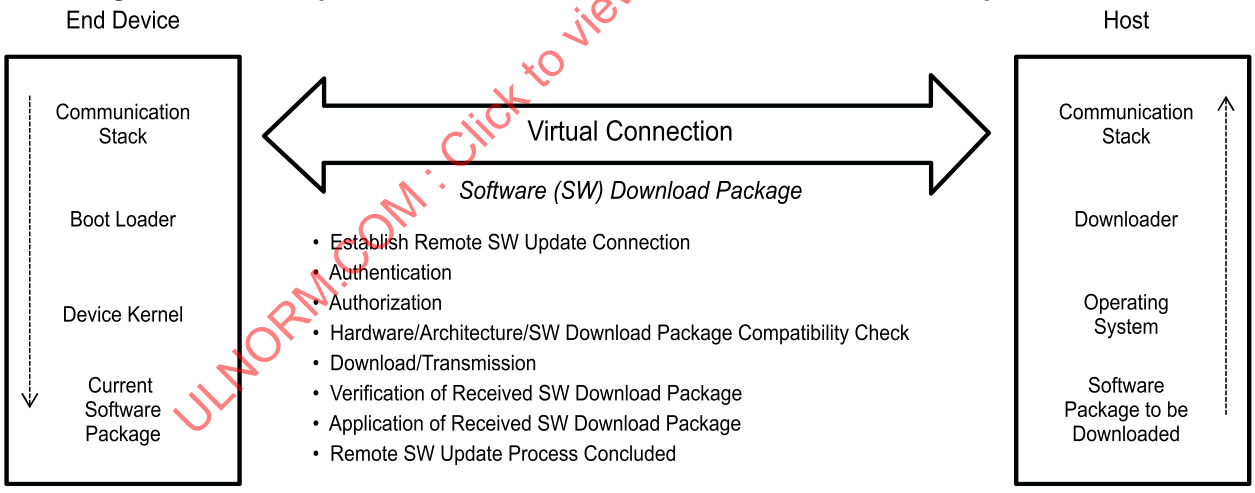
– Verification of Received SOFTWARE DOWNLOAD PACKAGE (see 4.7)

– Application of Received SOFTWARE DOWNLOAD PACKAGE (see 4.8)

– Software Update Process Concluded (see 4.9)

Compliance is checked by inspection.

Figure 4.1 – Example of REMOTE Communication Path for Software Update Process



su2888

4.2 Establish remote connection

4.2.1 The manufacturer shall identify a communication protocol for establishing a REMOTE connection between the host and end device.

Compliance is checked by inspection. Suitable technologies that may be used include, but are not limited to:

– IEEE 802.3;

– IEEE 802.11;

– IEEE 802.15.4;

– Other open source and proprietary methodologies.

NOTE: Link and transport layer cryptographic techniques for these protocols may be used to fulfill the requirement of 4.6.

4.2.2 The REMOTE software download process shall include means to identify the host and end device entities. Unless otherwise specified in the end product standard or by regulation, the manufacturer shall specify the means for unique identification of the end product.

Compliance is checked by inspection.

4.3 Authentication

The AUTHENTICATION process shall

– Establish the respective identities of the host and end device(s); and

– Include suitable means for verifying the host and end device entities are, by design, those intended to be engaged in REMOTE software update.

AUTHENTICATION attributes shall be encrypted.

NOTE: Suitable means may include digital certificates, device IDs, serial numbers, white listing and known-answer tests.

Compliance is checked by inspection.

4.4 Authorization

The AUTHORIZATION process shall:

– Include suitable means for verifying that the host ENTITY has the manufacturer specified REMOTE software update rights; or

– Include suitable means for verifying that the end device may engage the host ENTITY in the receipt and installation of a REMOTE SOFTWARE DOWNLOAD PACKAGE.

Compliance is checked by inspection.

4.5 Hardware / Architecture / Software Download Package Compatibility Check

Means for a hardware / architecture / SOFTWARE DOWNLOAD PACKAGE compatibility check shall be provided. Such means shall be one of the following:

– An end device means that demonstrates its hardware and software architecture is compatible with the SOFTWARE DOWNLOAD PACKAGE;

– The SOFTWARE DOWNLOAD PACKAGE is on a pre-selection list of manufacturer-specified SOFTWARE DOWNLOAD PACKAGES previously found compatible.

NOTE: Software previously found to meet the necessary criteria is also known as a “whitelisted application.”

Compliance is checked by inspection.

4.6 Download/Transmission

Data transmission shall be encrypted. Suitable means for encryption shall be industry standard cryptographic techniques as described in one or more of the following:

– ISO/IEC 9796;

– ISO/IEC 9797-1;

– ISO/IEC 9798-1;

– ISO/IEC 10118-1;

– ISO/IEC 14888-1;

– ISO/IEC 15946-1;

– ISO/IEC 18033-1;

– ISO/IEC 29192-1;

– ISO/IEC 19772;

– NIST SP 800-56A;

– NIST SP 800-57; or

– FIPS 140-2, (Annexes A, B and C)

Other suitable cryptographic techniques shown to be equivalent to the industry standard cryptographic techniques fulfill these requirements.

Compliance is checked by inspection.

4.7 Verification of Received Software Download Package

The detailed requirements for verification of the received SOFTWARE DOWNLOAD PACKAGE to end devices are device-specific and are as described in the end product standard.

Verification of the received SOFTWARE DOWNLOAD PACKAGE process shall include a check for authenticity of the SOFTWARE DOWNLOAD PACKAGE with respect to the version management process (Clause 6), SOFTWARE DOWNLOAD PACKAGE data integrity and hardware / architecture / SOFTWARE DOWNLOAD PACKAGE compatibility. However, a check for compatibility is not required where incompatibility affecting safety is precluded by the end product design.

Compliance is checked by inspection.

4.8 Application of Received Software Download Package

The detailed requirements for the application to end devices of the received SOFTWARE DOWNLOAD PACKAGE are device-specific and are as described in the end product standard.

Application of the received SOFTWARE DOWNLOAD PACKAGE process shall:

– Include a means to verify suitable conditions are present to apply the received SOFTWARE DOWNLOAD PACKAGE to the end device; or

– If the end device is operable during application of the received SOFTWARE DOWNLOAD PACKAGE, the device shall continue to comply with the requirements of the end product standard during this application.

Compliance is checked by inspection.

4.9 Conclusion of Remote Software Update Process

The REMOTE software update process conclusion shall:

– Include reporting the SOFTWARE DOWNLOAD PACKAGE identity of the end device and, upon host ENTITY verification, terminate REMOTE software download process, or

– Abort at any point of the REMOTE software update process in response to the failure / status identification conditions of 5.2.

Process termination may be as specified by the manufacturer if not otherwise specified in the requirements of the end product standard.

Compliance is checked by inspection.

5 Remote Software Update Validation

5.1 General

At any point during REMOTE software update the end device shall remain in compliance with the requirements of the end product standard and, when the REMOTE software update process is concluded, the end device shall:

– Resume its intended function with the new SOFTWARE DOWNLOAD PACKAGE installed; or

– Revert to its intended function under the old SOFTWARE DOWNLOAD PACKAGE; or

– Exist in a fail-safe condition (e.g. ″bricking″), as specified in the end product standard; or

– Continue to retry the REMOTE software update process.

Compliance is checked by inspection and functional test, both successful and failed update attempts, of the end product simulating the REMOTE software update process taking into account the requirements of 5.2 to 5.4.