UL 5500

STANDARD FOR SAFETY

Remote Software Updates

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER
REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

UL Standard for Safety for Remote Software Updates, UL 5500

First Edition, Dated September 6, 2018

Summary of Topics

This revision of ANSI/UL 5500 dated July 24, 2026 includes changes in requirements, incorporating inclusive language, in 4.9.

Text that has been changed in any manner or impacted by ULSE's electronic publishing system is marked with a vertical line in the margin.

The revised requirements are substantially in accordance with Proposal(s) on this subject dated April 10, 2026.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical photocopying, recording, or otherwise without prior permission of ULSE Inc. (ULSE).

ULSE provides this Standard "as is" without warranty of any kind, either expressed or implied, including but not limited to, the implied warranties of merchantability or fitness for any purpose.

In no event will ULSE be liable for any special, incidental, consequential, indirect or similar damages, including loss of profits, lost savings, loss of data, or any other damages arising out of the use of or the inability to use this Standard, even if ULSE or an authorized ULSE representative has been advised of the possibility of such damage. In no event shall ULSE's liability for any damage ever exceed the price paid for this Standard, regardless of the form of the claim.

Users of the electronic versions of UL's Standards for Safety agree to defend, indemnify, and hold ULSE harmless from and against any loss, expense, liability, damage, claim, or judgment (including reasonable attorney's fees) resulting from any error or deviation introduced while purchaser is storing an electronic Standard on the purchaser's computer system.

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

No Text on This Page

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

SEPTEMBER 6, 2018
(Title Page Reprinted: July 24, 2026)

ANSI/UL 5500-2026

1

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 including revisions through July 24, 2026.

The most recent designation of ANSI/UL 5500 as an American National Standard (ANSI) occurred on July 24, 2026. 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 ULSE at any time. Proposals should be submitted via a Proposal Request in the Collaborative Standards Development System (CSDS) at https://csds.ul.com.

Our Standards for Safety are copyrighted by ULSE Inc. Neither a printed nor electronic copy of a Standard should be altered in any way. All of our Standards and all copyrights, ownerships, and rights regarding those Standards shall remain the sole and exclusive property of ULSE Inc.

© 2026 ULSE Inc. All rights reserved.

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

No Text on This Page

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

CONTENTS

1 Scope 5
2 Normative references 5
3 Terms and definitions....6
4 Remote Software Update Process....7
4.1 General 7
4.2 Establish remote connection....8
4.3 Authentication 9
4.4 Authorization....9
4.5 Hardware / Architecture / Software Download Package Compatibility Check 9
4.6 Download/Transmission....9
4.7 Verification of Received Software Download Package 10
4.8 Application of Received Software Download Package 10
4.9 Conclusion of Remote Software Update Process 11
5 Remote Software Update Validation 11
5.1 General 11
5.2 Failure/Status Identification Detection 11
5.3 Response to Error Detection....12
5.4 Software Download Package Version....12
6 Documentation & Tracking....12

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

No Text on This Page

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

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*

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

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;

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

– 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.

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.