JOINT CANADA-UNITED STATES
NATIONAL STANDARD

ANSI/CAN/UL 2900-2-1:2023

STANDARD FOR SAFETY

Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems

Approved American National Standard

UL 2900-2-1-2023

SCC FOREWORD

National Standard of Canada

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization, in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development, and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

UL Standard for Safety for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems, ANSI/CAN/UL 2900-2-1

First Edition, Dated September 1, 2017

Summary of Topics

This revision for ANSI/CAN/UL 2900-2-1 dated January 30, 2023 includes the following changes in requirements:

– Addition of Inclusive Language; 12.4.3.16, 12.4.3.17 and Annex A

– Updated note about Threat Modeling; 12.1.1

Text that has been changed in any manner or impacted by UL'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 August 12, 2022 and November 18, 2022.

No Text on This Page

ANSI/UL 2900-2-1-2023

SEPTEMBER 1, 2017
(Title Page Reprinted: January 30, 2023)

ANSI/CAN/UL 2900-2-1:2023

Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems

First Edition

September 1, 2017

This ANSI/UL Standard for Safety consists of the First Edition including revisions through January 30, 2023.

The most recent designation of ANSI/UL 2900-2-1 as an American National Standard (ANSI) occurred on January 27, 2023. ANSI approval for a standard does not include the Cover Page, Transmittal Pages, Title Page, Preface or SCC Foreword.

This standard has been designated as a National Standard of Canada (NSC) on January 30, 2023.

No Text on This Page

CONTENTS

No Text on This Page

Preface

This is the First Edition of the ANSI/CAN/UL 2900-2-1, Standard for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems.

UL is accredited by the American National Standards Institute (ANSI) and the Standards Council of Canada (SCC) as a Standards Development Organization (SDO).

This Standard has been developed in compliance with the requirements of ANSI and SCC for accreditation of a Standards Development Organization.

This ANSI/CAN/UL 2900-2-1 Standard is under continuous maintenance, whereby each revision is approved in compliance with the requirements of ANSI and SCC for accreditation of a Standards Development Organization. In the event that no revisions are issued for a period of four years from the date of publication, action to revise, reaffirm, or withdraw the standard shall be initiated.

In Canada, there are two official languages, English and French. All safety warnings must be in French and English. Attention is drawn to the possibility that some Canadian authorities may require additional markings and/or installation instructions to be in both official languages.

Only metric SI units of measurement are used in this Standard. If a value for measurement is followed by a value in other units in parentheses, the second value may be approximate. The first stated value is the requirement.

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 http://csds.ul.com.

To purchase UL Standards, visit UL Standards Sales Site at
http://www.shopulstandards.com/HowToOrder.aspx or call tollfree 1-888-853-3503.

This Edition of the Standard has been formally approved by the UL Standards Technical Panel (STP) on Software Cybersecurity for Components of Healthcare Systems, STP 2900-2-1.

This list represents the STP 2900-2-1 membership when the final text in this standard was balloted. Since that time, changes in the membership may have occurred.

STP 2900-2-1 Membership

Name	Representing	Interest Category	Region
Ahmadi, Mike	M Ahmadi	General	USA
Alvarez, Edison	Becton Dickinson	Producer	USA
Barker, David	D Barker	General	USA
Biggs, Doug	UL Solutions	Testing & Stds Org	USA

STP 2900-2-1 Membership Continued on Next Page

STP 2900-2-1 Membership Continued

Name	Representing	Interest Category	Region
Cosman, Eric	OIT Concepts LLC	Non-voting member	USA
Dawson, Joe	EWA-Canada (an Intertek Co.)	Testing & Stds Org	Newfoundland, Canada
Dischert, Larry	Johnson Controls, Inc./ Building Solutions North America	Commercial/Industrial User	USA
Finnegan, Anita	NOVA LEAH	Supply Chain	Ireland
Fitzgerald, Brian	Food & Drug Administration	Government	USA
Fogleman, Greg	Department of Veterans Affairs	Government	USA
Francois, Guy	Sekon Enterprise	General	USA
Fuchs, Kenneth	Draeger Medical Systems, Inc	Producer	USA
Garrett, Michael	Garrett Technologies Inc	General	USA
Glasgow, Ian	Health Canada	Government	Ontario, Canada
Goldman, Julian	Massachusetts General Hospital	Consumer	USA
Griffith, Steve	NEMA	Non-voting member	USA
Ivey, James	Tektone Sound & Signal Mfg Inc	Producer	USA
Leinonen, Juuso	ECRI	Supply Chain	USA
Li, Xiaodong	Lenovo (Beijing) Ltd	Producer	China
Lubadel, Joern	B Braun Medical Inc	Producer	USA
Martin, Robert	The Mitre Corporation	Commercial / Industrial User	USA
Prince, Deborah R.	UL Standards & Engagement	STP Chair – Non-voting	USA
Rowland, Michael	IAEA	Government	Austria
Shkolnik, Moti	Firedome	Supply Chain	USA
Srivathsa, Karthik	Rauland-Borg Corp	Producer	USA
Tran, Phat	BC Safety Authority	Non-voting member	British Columbia, Canada
Treuthardt, Caroline	UL Standards & Engagement	STP Project Manager – Non-voting	USA
Vance, Matthew	HCA Healthcare Inc	Commercial / Industrial User	USA
Vasserman, Eugene	Kansas State University	General	USA
Wang, Hui	CNCERT/CC	General	China

International Classification for Standards (ICS): 35.030, 35.110, 35.240.50, 35.240.80

For further information on UL standards, please contact:

Underwriters Laboratories Inc.
Telephone: (613) 755-2729
E-mail: ULCStandards@ul.com
Web site: ulse.org

This Standard is intended to be used for conformity assessment.

The intended primary application of this standard is stated in its scope. It is important to note that it remains the responsibility of the user of the standard to judge its suitability for this particular application.

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE

INTRODUCTION

NOTE: This Standard for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems, is to be used in conjunction with the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1. The requirements for network connectable components of healthcare systems are contained in this part 2 standard and UL 2900-1. Requirements of this Part 2 standard, where stated, amend the requirements of UL 2900-1. Where a particular subclause of UL 2900-1 is not mentioned in UL 2900-2-1, the UL 2900-1 subclause applies. This standard has been developed in accordance with IEC Guide 120, Security aspects – Guidelines for their inclusion in publications.

1 Scope

1.1 This security evaluation standard applies to the testing of network connectable components of healthcare systems. It applies to, but is not limited to, the following key components:

a) Medical devices;

b) Accessories to medical devices;

c) Medical device data systems;

d) In vitro diagnostic devices;

e) Health information technology;

f) Wellness devices; and

g) All software components used for the secure operation of the device, wherever they may reside, including remote assets.

Note – Combinations of the technologies listed here may be applied to such solutions as “telemedicine,” where a single solution may contain both regulated and unregulated components.

2 Normative References

2.1 The Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, shall be applied as specified in this standard.

2.2 The Standard for Medical Devices – Application of Risk Management to Medical Devices, ISO 14971:2007, shall be applied as specified in this standard.

2.3 The Standard for Medical Devices – Quality Management Systems – Requirements for Regulatory Purposes, ISO 13485:2003, shall be applied as specified in this standard.

2.4 The Standard for Medical Device Software – Software Life Cycle Processes, IEC 62304:2006+AMD1:2015, shall be applied as specified in this standard.

2.5 The Standard for Health software – Part 1: General requirements for product safety, IEC 82304-1:2016

2A Informative References

AAMI TIR57, Principles For Medical Device Security – Risk Management (2016)

AAMI TIR75, Factors to Consider When Multi-Vendor Devices Interact Via an Electronic Interface: Practical Applications and Examples (2019)

AAMI/UL 2800-1, Medical Device Interoperability

ANSI/NEMA HN 1-2019, Manufacturer Disclosure Statement for Medical Device Security

IEC/TR 80001-2-8:2016, Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

IEC TR 80001-2-9:2017, Application of risk management for IT-networks incorporating medical devices – Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities

IEC/TR 60601-4-1:2017, Medical electrical equipment – Part 4-1: Guidance and interpretation – Medical electrical equipment and medical electrical systems employing a degree of autonomy

IEEE/UL DTSec, Standard for Wireless Diabetes Device Security (DTSec)

IEEE/UL DTMoST, Diabetes Technology Society Mobile Platform Controlling a Diabetes Device Security and Safety Standard

ISO/IEC 15408-1:2009, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

MEDICAL DEVICE AND HEALTH IT JOINT SECURITY PLAN;
https://healthsectorcouncil.org/wp-content/uploads/2019/02/HSCC-MEDTECH-JSP-v1.2.pdf

3 Glossary

3.1 BASIC SAFETY – Freedom from unacceptable risk, for those risks that are not directly related to the intended use of the product.

3.2 ESSENTIAL PERFORMANCE – Performance, other than that related to BASIC SAFETY, whose loss or degradation beyond the limits specified by the MANUFACTURER results in an unacceptable risk. [IEC 60601-1 Ed3.1]

3.3 MANUFACTURER – See VENDOR

3.4 RISK MANAGEMENT FILE – Set of records and other documents that are produced by risk management [EN ISO 14971: 2012]

DOCUMENTATION FOR PRODUCT, PROCESSES, AND USE

4 Product Documentation

4.1 Product documentation shall meet the requirements of the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, except as noted in this standard.

5 Process Documentation

5.1 Process documentation shall meet the requirements of the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, except as noted in this standard.

6 Documentation for Product Use

6.1 Safety-related security considerations for product use

6.1.1 Intended use of the product as indicated in the Risk Management File (RMF)

6.1.1.1 A statement of the product's intended use shall be included in the Risk Management File.

6.1.1.2 Jurisdiction-specific definitions for 'intended use' and 'indications for use' shall be provided in the Risk Management File.

6.1.1.3 The product's intended use statement shall indicate essential performance that may be impacted by security breach.

6.1.2 Environment in which the product is intended to be used

6.1.2.1 The product's assumptions regarding the environment within which it is intended to be operated shall be enumerated.

6.1.2.2 The product's indications for use statement shall identify security capabilities and constraints relative to assumptions regarding the environment within which it is intended to be operated.

6.2 Instructions

6.2.1 Instructions on means to over-ride security measures when necessary for patient safety per 12.4.1.7 and 12.4.2.6 shall be communicated to intended stakeholders with security controls as described in the Risk Management File.

SECURITY CONTROLS

7 General

7.1 The product shall comply with the requirements of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1, Section 7, except as noted in this standard.

8 Access Control, User Authentication, and User Authorization

8.1 The product shall comply with the requirements of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1, Section 8, except as noted in this standard.

9 Remote Communication

9.1 The product shall comply with the remote communication requirements of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1, Section 9, except as noted in this standard.

10 Cryptography

10.1 The product shall comply with the cryptography requirements of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1, Section 10, except as noted in this standard.

11 Product Management

11.1 The product shall comply with the product management requirements of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1, Section 11, except as noted in this standard.

PRODUCT ASSESSMENT

12 Safety-Related Security Risk Management

12.1 Risk analysis

12.1.1 The product shall comply with the applicable requirements of the Standard for Medical Devices – Application of Risk Management to Medical Devices, ISO 14971, or the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, Section 12, Vendor Product Risk Management Process.

NOTE 1: Information Technology network risks per the Standard for Application of Risk Management for IT-Networks Incorporating Medical Devices – Part 1: Roles, Responsibilities and Activities, IEC 80001-1, should be considered as part of product risk management.

NOTE 2: Threat Modeling should be performed following the principles of AAMI TIR 57 to generate an abstracted representation of the product / system that is to be decomposed into the components listed in a Software Bill of Materials (SBOM). The threat model should identify assets, attack surfaces, vulnerabilities, attack vectors, risk controls, and residual risk in the context of objects, processes, interfaces, dataflows, and trust boundaries within specific use environments and use cases. The level of threat modeling detail should align with the component decomposition granularity provided by Software Composition Analysis.

12.1.2 A risk management file shall be constructed in accordance with the Standard for Medical Devices – Application of Risk Management to Medical Devices, ISO 14971, risk management process, or equivalent, and it shall specifically include the following elements with regard to security:

a) Security risk analysis;

NOTE: The security risk analysis should consider defense-in-depth also known as layer of protection analysis (LOPA)[1].

b) Security risk evaluation;

c) Security risk control;

NOTE: Security risk controls should consider a defense-in-depth strategy to minimize impact of a breach.

d) Production and post-production changes in security risks that may change over time;

NOTE: See also the post market surveillance requirements of ISO 13485, ISO 14971, TIR57 and 20.4.

e) Verification and validation of security risk controls; and

NOTE: Validation demonstrates that the specification and resulting implementation satisfies user needs through acceptance and suitability testing.

f) Analysis of the acceptability of residual security risk.

[1] See the IEC 61511, Functional Safety – Safety Instrumented Systems for the Process Industry Sector standards.

12.1.3 Processes for Quality Management (QM) shall reflect:

a) Allocation of adequate security resources to product development;

NOTE: Compliance can be determined by demonstrating compliance with Clauses 13 – 20 of this standard.

b) Establishing policies and criteria for security risk acceptability for the product based on applicable international, national or regional regulations; and

c) Ongoing re-assessment of the continued suitability of the security risk management process at planned intervals, including documentation of decisions and actions taken.

12.2 Risk evaluation

12.2.1 The risk evaluation shall be conducted in accordance with 12.3 and 12.4 in the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1.

12.3 Risk control

12.3.1 The risk controls identified in Sections 7 – 11 of the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, and the security capabilities of the Application of Risk Management for IT-Networks Incorporating Medical Devices – Part 2-2: Guidance for the Disclosure and Communication of Medical Device Security Needs, Risks and Controls, IEC/TR 80001-2-2, or equivalent, shall be considered for risk management.

12.3.2 Any security measures contraindicated by the risk analysis are to be designated as Not Applicable (NA) with justification(s) in the Risk Management File or explanation of alternative measures.

12.3.3 A security risk management plan shall be constructed and documented to reflect the following processes, including rationale for any qualitative or quantitative measures used:

a) Identification of assets, threats, and vulnerabilities;

b) Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;

c) Assessment of the likelihood of a threat and of a vulnerability being exploited;

d) Determination of risk levels and suitable mitigation strategies; and

e) Assessment of residual risk and risk acceptance criteria.

f) Security-relevant data logging when applicable

12.3.4 The vendor shall provide a risk management artifact to reflect hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with the product, including:

a) A specific list of all cybersecurity risks that were considered in the design of the product;

b) A specific list and justification for all cybersecurity risk controls that were established for the product;

c) A means of demonstrating traceability that links product cybersecurity risk controls to the cybersecurity risks that were considered;

d) A summary describing the plan for providing validated software updates and patches as needed throughout the lifecycle of the product to continue to assure its safety and effectiveness;

e) A summary describing cybersecurity risk controls that are in place to assure that the product software will maintain its integrity (e.g. remain free of malware) from the point of origin to the point at which that product leaves the control of the vendor; and

f) Product instructions for use and product specifications related to recommended cybersecurity risk controls appropriate for the intended use environment (e.g. anti-virus software, use of firewall).

12.3.5 The organization shall identify all security-related safety and non-safety security-related requirements for the product in the risk management file or in separate documents referenced by the risk management file (see also 12.4.1.1, 12.4.2.1, and 12.4.3.1).

12.3.6 The security risk controls shall be based on requirements derived from the risk evaluation.

12.3.7 The security risk controls shall be derived from relevant product requirements including requirements not stated by the customer, but necessary for the security and safety of the product during its intended use.

12.4 Coverage of security analysis and testing

12.4.1 Protection of inputs

12.4.1.1 Security measures protecting inputs to the product shall be specified when applicable (e.g. encryption of input data).

12.4.1.2 Any specific inputs to the risk controls derived from the product inputs shall be specified (e.g. threshold values for safety interlocks).

12.4.1.3 Data security (e.g. authenticated encryption) shall be specified for inputs.

12.4.1.4 Metadata security comparable to that in 12.4.1.3 shall be specified for inputs (e.g. patient identifying information).

12.4.1.5 Security measures to protect confidentiality of the contextual meaning of any exposed input data (e.g. wirelessly transmitted data as opposed to data securely entered locally at an HMI) shall be specified.

NOTE: An example of such a measure would be de-identification of patient identifiable data.

12.4.1.6 Security measures protecting assets against transitional vulnerabilities exploited through input manipulation during product state changes shall be specified (e.g. exception handling for out-of-range values, see SANS top 25).

NOTE: Triggers for state machine changes should be considered.

12.4.1.7 Secured means to over-ride input security measures (e.g. “break-the-glass”) when necessary for patient safety shall be specified.

12.4.1.8 All security-relevant assumptions and constraints, related to the product inputs, imposed during the development of the product shall be specified.

12.4.2 Protection of outputs

12.4.2.1 Security measures protecting outputs of the product shall be specified.

12.4.2.2 Data security (e.g. encryption) shall be specified for outputs.

12.4.2.3 Metadata security shall be specified for outputs.

12.4.2.4 Security measures to protect confidentiality, integrity, and availability of the contextual meaning of any exposed output data (e.g. wirelessly transmitted data) shall be specified.

NOTE: An example of such a measure would be de-identification of patient identifiable data.

12.4.2.5 Security measures protecting assets against transitional vulnerabilities exploited through output manipulation (e.g. falsification of security credentials) during product state changes shall be specified.

12.4.2.6 Secured means to over-ride output security measures (e.g. “break-the-glass”) when necessary for patient safety shall be specified.

12.4.2.7 All security-relevant assumptions and constraints, related to the product output(s), imposed during the development of the product shall be specified.

12.4.3 Design and Development Process-related Risk Controls

NOTE: Compliance is to be determined by inspection of the risk management file.

12.4.3.1 Security controls shall be implemented during the design and development process as required by the risk assessment, where the following subclauses (12.4.3.2 – 12.4.3.20) constitute a minimum set of design and development process security controls to be considered, with the nonuse of any of these considerations justified in the Risk Management File.

12.4.3.2 “Random” number seeds shall be evaluated during design for suitability per the security risk assessment and documented in the Risk Management File.

12.4.3.3 Software processes and their authorized users shall be granted only those privileges required for them to carry out their specified function(s). See UL 2900-1, Clause 8.8.

12.4.3.4 Unless contraindicated by the product risk assessment, all inputs shall be validated prior to being processed.

12.4.3.5 Where such constraints do not introduce new hazards, programs shall be deterministically constrained (i.e. use of programming constructs controlled) to avoid vulnerabilities including, but not limited to:

a) Buffer overflow;

b) Use of undefined or uninitialized programming constructs (e.g. null pointer dereference);

c) Use of unmanaged resources (e.g. use after free);

d) Use of uninitialized memory; and

e) Improper use of resource management functions (e.g. illegal free of an already freed pointer or improper use of buffered data).

f) Use of exception handling techniques with catch-all implementation that allows exceptions to arise through the call stack without affecting the core functionality of the device, if possible, or with documented fallback functionality in the case it is affected by exceptions.

12.4.3.6 The use of memory safe languages shall be considered during risk assessment.

12.4.3.7 The use of language subsetting shall be considered during risk assessment.

12.4.3.8 The use of automated memory safety error mitigation and compiler-enforced buffer overflow elimination shall be considered during risk assessment.

12.4.3.9 The use of secure coding standards shall be considered during risk assessment.

12.4.3.10 The use of automated thread safety analysis shall be considered during risk assessment.

12.4.3.11 The use of proven cryptographic algorithms and implementations shall be considered during risk assessment.

12.4.3.12 The use of modified condition decision coverage for functional testing shall be considered during risk assessment and test planning.

12.4.3.13 Unused functions/features shall be removed based on analysis of operational use cases and if deemed necessary not to be removed, the presence of such unused functions shall be justified in the Risk Management File.

12.4.3.14 Digitally signed software and firmware shall be used.

12.4.3.15 Software and firmware updates shall be validated using digital signatures prior to re-initiation of the product.

12.4.3.16 An allow-list shall be used to ensure only authorized software is executed unless such use introduces new hazards.

12.4.3.17 Proactive endpoint malware protection shall be used when technically feasible (e.g. a list of permitted processes/ports). Reactive malware protection (e.g. antivirus, intrusion detection) shall be used when proactive protection is not feasible. If no tool or method is available for endpoint protection, this should be captured in the risk assessment and documented accordingly.

NOTE: See 12.4.3.16.

12.4.3.18 Storage (e.g. memory) shall be monitored with an integrity monitor to ensure that the code and data sections are not unintentionally modified.

12.4.3.19 Software (including sensitive data) interfacing directly to hardware shall be protected against unauthorized modifications or access via either software or hardware means as prescribed by the manufacturer's risk management process.

12.4.3.20 The use of perfect-forward secrecy in the encryption protocol shall be considered during risk assessment.

13 Known Vulnerability Testing

13.1 The product shall contain no known vulnerabilities unless otherwise stated in the vendor's risk management file, based on CVSS metrics or adaptation of CVSS metrics or equivalent, used in the vendor's risk management process.

13.2 The product shall be tested for known vulnerabilities in accordance with the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, Section 13.

13.3 The vendor's process for handling security related vulnerability reports shall be documented.

14 Malware Testing

14.1 The product shall be tested for malware in accordance with the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, Section 14.

15 Malformed Input Testing

15.1 The product shall undergo malformed input testing in accordance with the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, Section 15, to identify unknown vulnerabilities within the defined testing parameters and in accordance with 12.3.5 through 12.4.1.8 of this standard.

Note: Malformed input testing is also known in the industry as fuzz testing.

15.2 Upon conducting the Malformed Input Testing and Structured Penetration Testing according to Sections 15 and 16 of the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, the product shall continue normal operation, per its intended use, or transition to a defined risks addressed (RA) state, as specified in the product Risk Management File (RMF).

16 Structured Penetration Testing

16.1 During the Structured White-box Penetration Testing of the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, Section 16, the product shall be assessed for unauthorized use via the potential for Elevation of Privilege (EoP) under the specified testing conditions.

16.2 Protection against EoP shall be tested by targeting inputs, and output characteristics of the product (i.e. structured penetration testing) per 12.4.1.1 through 12.4.2.1 of this standard.

16.3 Protection against EoP shall be evaluated for software processes that may not be directly accessible via external interfaces. This shall be determined through the evaluation of 16.4 through 16.12 using the structured penetration testing approaches specified in Section 16 of the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1.

16.4 Security measures protecting the product's internal safety-critical software processes (e.g. logic and state transitions) shall be tested (i.e. for software-to-software interfaces).

16.5 Any safety-related and security-related software processes within the product affected by outputs from other software processes within the product shall be tested.

16.6 Data security (e.g. encryption) shall be tested to evaluate software processes within the product that may interact with other unsecured software processes within the product (e.g. multicore processing).

16.7 As an alternative to 16.6, such interactions may be viewed as inputs to the secured process per 12.4.1.1.

16.8 Metadata security shall be tested to evaluate software processes within the product that may interact with other unsecured software processes within the product (e.g. multicore processing).

16.9 Security measures to protect confidentiality of the contextual meaning of any exposed input data (e.g. shared between secured and unsecured cores) shall be tested to evaluate software processes within the product that may interact with other unsecured software processes within the product (e.g. multicore processing).

NOTE: An example of such a measure would be de-identification of patient identifiable data.

16.10 Security measures protecting assets against transitional vulnerabilities exploited through software process manipulation during product state changes shall be tested.

16.11 Means to over-ride software process security measures internal to the product when necessary for patient safety shall be tested.

16.12 Upon conducting the Structured Penetration Testing of Section 13 of the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, the product shall continue normal operation, per its intended use, or transition to a defined Risks Addressed (RA) state, as specified in the product Risk Management File (RMF) with no EoP.

17 Software Weakness Analysis

17.1 The product shall undergo software weakness analysis per Sections 17, 18, and 19 of the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1.

17.2 The product shall contain no known weaknesses unless otherwise stated in the vendor's risk management file and also satisfying the CWSS score established as part of the risk management process.

18 Static Source Code Analysis

18.1 The product shall comply with the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, Section 18.

19 Static Binary and Bytecode Analysis

19.1 The product shall comply with the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, Section 19.

ORGANIZATIONAL ASSESSMENT

20 Lifecycle Security Processes

20.1 Quality management processes

20.1.1 The product shall be developed under a Quality Management System per the Standard for Medical Devices – Quality Management Systems – Requirements for Regulatory Purposes, ISO 13485, or equivalent.

20.1.2 The software development lifecycle shall comply with the applicable requirements of the Standard for Medical Device Software – Software Life Cycle Processes, IEC 62304, or equivalent.

20.2 General procurement processes

NOTE: Compliance is to be determined by inspection of the Risk Management File.

20.2.1 For software components integrated into the product, the vendor's Quality Management System shall address security considerations in the procurement process.

20.2.2 For components to be integrated into the product, the vendor (i.e. product developer) shall establish documented procurement procedures that include review of supplier security specifications for compatibility with organizational security policies and procedures.

20.2.3 The vendor (i.e. product developer) shall plan the supplier selection, establish selection, evaluation and re-evaluation criteria, and establish a supplier qualification process based on the supplier's ability to address defined security criteria and provide products that satisfy the vendor's security requirements.

20.2.4 The vendor (i.e. product developer) shall perform ongoing surveillance of the supplier's compliance to the security requirements. The vendor (i.e. product developer) shall also:

a) Perform periodic requalification of the supplier, as appropriate per this surveillance; and

b) Manage software updates (e.g. patches) as part of the ongoing supplier surveillance.

20.3 Procurement risk management process

20.3.1 The supplier shall comply with the requirements of Section 12, Safety-Related Security Risk Management.

20.3.2 Where contractual constraints or IP considerations preclude the disclosure of the items in Section 12, Safety-Related Security Risk Management, directly to the vendor (i.e. product developer), demonstrated conformance to this standard may be used instead.

20.3.3 The vendor (i.e. product developer) shall document the vendor’s defined end-of life and communicate to the customer that supplier support for security aspects of the component will be provided only until the product's expected end-of-life.

20.3.4 As an alternative to 20.3.3, the vendor (i.e. product developer) shall demonstrate the ability to address ongoing component security without supplier support.

NOTE: An example would be compensating controls that are part of a defense-in-depth security strategy.

20.3.5 Software development tool chains shall be considered as part of purchasing controls of the quality management system.

20.4 Product update release and patch management process

20.4.1 The product shall comply with the requirements of the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, Clause 11.

20.4.2 Patches and fixes shall be deployed to the affected populations within 14 days of the validated fix and the manufacturer's infrastructure shall permit this.

20.5 Decommissioning process

20.5.1 For products intended to be part of a larger system, decommissioning procedures shall be provided to allow for the product to be removed from the system (and replaced if performing a security-critical function) without compromising system security during the product decommissioning process.

NOTE: A compromise of system security would be, for example, leaks of PHI / PII from the overall system whether via communication channels or improper disposal of a system component.

20.6 Packaging and shipment

20.6.1 The product packaging and distribution processes shall maintain the integrity of the security measures specified in Section 5, Process Documentation, using techniques of 12.4.3.5 or 12.4.3.16 or equivalent, unless contraindicated by the risk management process.

20.6.2 The measures employed shall be described in the Risk Management File.

ANNEX A (Informative) – Rationale for the Requirements

A1.1 This Annex provides informative documentation on how a clause is intended to operate and rationale for inclusion of the clause in the standard.

Table A1.1 Rationale for the Requirements

Reference	Description	Rationale
6.1.1.1	A statement of the product's intended use is included in the Risk Management File	Safety related security considerations for product use should be aligned with intended use considered in the relevant Risk Management File (RMF). A product may have multiple intended uses, which should be included in the RMF. Further, as noted in ISO 14971:2012, the intended use shall be documented and maintained in the RMF. Documentation of the intended use allows the manufacturer to identify and document relevant qualitative and quantitative characteristics that could affect the safety of a medical device. An RMF is not a discrete or singular document, but rather any documentation that describes the mitigation of product risk.
6.1.1.2	Jurisdiction-specific definitions for 'intended use' and 'indications for use' are provided in the Risk Management File	Product sold into multiple jurisdictions may have differing intended uses and indications for use due to limitations imposed by regulators or payors. Further, the differences may include new risks or different risk levels. Therefore, in conjunction with the rationale listed for 6.1.1.1, jurisdiction-specific definitions for intended use and indications for use must be considered in the RMF.
6.1.1.3	Essential performance that may be impacted by a security breach is documented in the product's intended use statement	Essential performance of a device may be affected by a breach. Further, in accordance with IEC 60601-1, essential performance must be maintained during both normal operation and failure of any one component. Thus, it is important to identify in the intended use statement how essential performance could be impacted by a security breach. Notably – while IEC 60601-1 defines and incorporates the concept of essential performance, this is not a defined term, but could be aligned with the functional safety concept in IEC 61010-1.
6.1.2.1	Assumptions regarding the environment in which product is intended to be operated are documented	The product's environment, may increase or decrease the potential for certain types of cybersecurity breaches. If the product is intended to be used on a network with robust cybersecurity controls, the potential for cybersecurity breaches could be decreased. Assumptions one way or another must be defined so that end uses/facilities know that they are expected to apply controls.
6.1.2.2	Security capabilities and constraints relative to assumptions regarding environment within which it is intended to be operated are identified	Similar to the safety-related security considerations in 6.1.1.3 and the assumptions rationale provided for 6.1.2.1, the product user should be made aware of the intended product environment so that they can assess and, if warranted, implement additional cybersecurity safeguards. Further, the user should be made aware of how security capabilities and constraints impact the product's intended use, and more specifically, the essential performance. The threat model should be driven by the threat environment.
6.2.1	Instructions on means to over-ride security measures when necessary for patient safety shall be communicated to intended stakeholders with security controls as described in the Risk Management File	For all safety/patient critical functions of the device, a mechanism must be in place to override security measures of the device in order to be able to deliver time critical patient care, e.g. such as during an emergency. Instructions on secured means to override the input and output security measures should be prepared and documented in advance because the existence of the security measure could lead to the

Table A1.1 Rationale for the Requirements Continued on Next Page

Table A1.1 Rationale for the Requirements Continued

Reference	Description	Rationale
		deterioration of patient safety, for example, in case a clinician is not able to deliver time critical patient care.
12.1.2	A compliant Risk Management File exists	Risk management processes should be documented as the risk management file following ISO 14971 or similar risk management standards. They should consider not only safety but also security. Some important elements which should be included in the risk management file are listed in terms of security risk management.
12.1.3(a)	QM processes reflect allocation of adequate security resources to product development	Cybersecurity shall be considered as early as possible in the product development process to mitigate cybersecurity risks. The normative reference to ISO 13485 provides for top management commitment, which in turn drives adequate implementation resources. Insight applied at the earliest point possible in the product development process can avoid wasteful rework, the need for last minute fixes to remove known types of flaws and mistakes and minimize the number of post-deployment fixes for quality escapes that impact reliability, safety, and security.
12.1.3(b)	QM processes establish policies and criteria for security risk acceptability for the product based on applicable international, national or regional regulations	Consistent policies and criteria for decisions are needed to address the variety of impacts that errors have and to guide the identification of which errors need mitigations.
12.1.3(c)	QM processes include ongoing re-assessment of the continued suitability of the security risk management process at planned intervals, including documentation of decisions and actions taken	While the natural laws remain constant over time, the ability of software errors to cause harm or for them to be activated and manipulated by attackers can change as new techniques for influencing systems emerge and made more repeatable. Re-assessment needs to include changes in intended use and changes in use environment.
12.3.2	Risk Management File reflects assessment of security measures contraindicated by the risk analysis	Contraindication is sometimes missed in the security risk management process, but it should take priority over anything else in medical devices. Therefore alternative measures should be presented or the measure should be noted as Not Applicable or contraindicated based on situational risk context. (See AAMI TIR57.)
12.3.3	An adequate security risk management plan exist	A security risk management plan that is periodically updated is important for downstream risk management activities (See ISO 14971, AAMI TIR57 or AAMI TIR97.)
12.3.4	Vendor has performed hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with the product	A top level hazard and threat analysis is important to ensure system level security hazards are identified, recorded and mitigated. This should include both top down and bottom up analysis.
12.3.5	Risk management file identifies all security-related safety and non-safety requirements for the product	A version controlled repository of requirements is important to drive downstream design, verification and validation (V&V) and recovery activities.
12.3.6	Security risk controls are based on requirements derived from the risk evaluation	Cybersecurity related requirements stemming from the risk and threat evaluation phase should have corresponding risk controls.
12.3.7	Security risk controls are derived from relevant product requirements including requirements not stated by the customer, but necessary for the security and safety of the product during its intended use	Cybersecurity related requirements stemming from the review of product requirements (including those derived from regulatory guidance, industry best practices, and emerging risks) should have corresponding risk controls.
12.4.1	Protection of inputs (combine in testing protocol with UL 2900-1 15.1 & 16.1)	Inputs should not alter the intended risk profile of the device. Protection of input over communications protocols or user interfaces should include measures such as specifying appropriate data inputs and data security.

Table A1.1 Rationale for the Requirements Continued on Next Page