UL 2800-1

STANDARD FOR SAFETY

Medical Device Interoperability

Standard for Safety for Medical Device Interoperability, UL 2800-1

Second Edition, Dated June 10, 2022

Summary of Topics

This is the Second Edition of ANSI/UL 2800-1, the Standard for Medical Device Interoperability, dated June 10, 2022.

The new requirements are substantially in accordance with Proposal(s) on this subject dated November 5, 2021.

No Text on This Page

AAMI
AAMI 2800-1
Second Edition

Underwriters Laboratories Inc
UL 2800-1
Second Edition

Standard for Medical Device Interoperability

June 10, 2022

Approved American National Standard

ANSI/UL 2800-1-2022

Commitment for Amendments

This Standard is issued jointly by the Association for the Advancement of Medical Instrumentation (AAMI) and Underwriters Laboratories Inc. (UL). Comments or proposals for revisions or any part of the standard may be submitted to AAMI and/or UL at any time. Revisions to this Standard will be made only after processing according to the Standards development procedures of AAMI and UL.

This ANSI/UL Standard for Safety consists of the Second Edition. The most recent designation of ANSI/UL 2800-1 as an American National Standard (ANSI) occurred on June 10, 2022. ANSI approval for a standard does not include the Cover Page, Transmittal Pages, Title Page (front and back), or the Preface.

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.

To purchase UL Standards, visit UL's Standards Sales site at http://www.shopulstandards.com/HowToOrder.aspx or call toll-free 1-888-853-3503.

CONTENTS

Preface

This is the joint AAMI/UL Standard for Medical Device Interoperability, AAMI/UL 2800-1. It is the second edition of AAMI 2800-1 and the second edition of UL 2800-1.

This Joint Standard was prepared by the Joint Committee for Medical Device Interoperability, JC 2800. The standard was formally approved by the Joint Committee and the efforts and support of the Joint Committee are gratefully acknowledged.

This standard has been approved by the American National Standards Institute as an American National Standard.

AAMI/UL Joint Committee for Medical Device Interoperability, JC 2800

Name	Representing
Dave Arney	CIMIT (MGH Anesthesia & Biomedical Engineering)
Oliver Christ	Prosystem AG
R Cooper	Eurofins E&E North America
Holly Drake	Dexcom Inc.
Sherman Eagles	SoftwareCPR
Scott Eaton	Mindray DS USA Inc
Kenneth Fuchs	Draeger Medical Systems Inc.
Julian Goldman	Massachusetts General Hospital
Pamela K. Gwynn	UL LLC
John Hatcliff	Kansas State University
Jacob Johnson	Kaiser Permanente
Diana Pappas Jordan	Underwriters Laboratories Inc.
Edmund Kienast	National E-Health Transition Authority (NEHTA)-Australia
Todd Konieczny	Intertek Testing Services
Patty Krantz	Medtronic Inc.
Insup Lee	University of Pennsylvania
Marina Lee	Staubli Electrical Connectors, Inc.
Ovidiu Munteanu	AAMI
Steve Nichols	GE Healthcare
Geetha Rao	Springborne Life Sciences
Tracey Rausch	DocBox Inc.
Daniel Rubery	NxStage Medical, Inc.
Patricia A. Sena (JC Project Manager)	Underwriters Laboratories Inc.
Elliot Sloane	Center For Healthcare Information Research & Policy
Erin Sparnon	ECRI
Sandy Weininger	US FDA/CDRH

This list represents the membership at the time the Committee balloted on the final text of this edition. Since that time, changes in the membership may have occurred.

No Text on This Page

1 Introduction

1.1 The AAMI/UL 2800 series of standards covers the interoperability of medical products. AAMI/UL 2800-1 is the general standard that specifies a baseline set of requirements for assuring safe and secure interoperability for interoperable medical systems. The requirements in the AAMI/UL 2800-1 standard are supplemented by the requirements in additional AAMI/UL 2800 standards. These additional standards are intended to be used in conjunction with the general standard and applied as needed. While this introduction applies to all of the AAMI/UL 2800 series of standards, the scope section of each additional standard describes what is covered by that standard.

1.2 Multiple stakeholders may participate in the development, deployment, assembly, and operation of a medical system with interoperable elements. Such a system, referred to as an interoperable medical system, should minimize patient risks, maintain clinical effectiveness, ensure timely and adequate access to data while protecting its security, and enable adequate provision of care. In order to facilitate alignment of stakeholders around these aims, the AAMI/UL 2800 series of standards establishes a baseline set of requirements for assuring safe and secure interoperability.

1.3 Each stakeholder will need to determine the specific level and manner in which interoperability will be specified and assured for its interoperable medical products. However, a specific system may be developed, assembled, deployed, and operated through a range of processes undertaken by multiple stakeholders. Specific activities in these processes assure interoperability. In order for stakeholders to collectively accomplish this, the processes need to be linked effectively.

1.4 Effective linkage of processes across multiple stakeholders is a core focus of the AAMI/UL 2800 series of standards. This first requires that each stakeholder adequately assesses and manages safety, security and essential performance vulnerabilities of its interoperable medical products. Secondly, it requires that each stakeholder understands and conforms with interoperability aspects of disclosed specifications of an interoperable medical product which it acquires or with which it interoperates, including the consequent safety and security characteristics. Finally, it requires that each stakeholder clearly communicates to the other stakeholders the information required to assure interoperability.

1.5 The requirements in the AAMI/UL 2800 series of standards are intended to apply to medical devices, as well as other connected infrastructure elements, and interoperable medical systems constructed from these. The AAMI/UL 2800 series of standards is intended to be used by individual stakeholders.

1.6 The AAMI/UL 2800 series of standards employ a lifecycle process approach to organizing requirements. In addition to a set of broad management functions, the standards provide for a set of interoperability planning, realization, deployment, and monitoring activities. These activities also incorporate cross-cutting requirements for security and risk management. The standards recognize that a given organization may be responsible for only a part of the full range of activities required for an interoperable medical system. Furthermore, the organization's interoperable medical products may provide only a specific or limited functionality. To accommodate this, the standards provide for flexibility in the scope, sequence, and interaction of these activities. Finally, the standards provide requirements and supplementary guidance on key clinical and engineering properties of an interoperable medical system that are essential to assuring safe and secure interoperability and provide guidance on lifecycle activities.

1.7 The requirements provide a baseline for assuring safe and secure interoperability throughout the lifecycle of the interoperable medical system. In order to meet these requirements, a set of lifecycle processes needs to be established. It is anticipated that many organizations in the interoperability ecosystem will also have requirements for formal quality and risk management processes, as well as those related to specific aspects of product development, such as usability, software development, electrical and biological safety. The lifecycle processes in the AAMI/UL 2800 series of standards may be integrated into the organization's processes previously established for meeting quality and risk management and product-specific requirements.

1.8 As part of complying with the AAMI/UL 2800 series of standards, an organization will need to understand its specific role in the interoperability ecosystem, as well the role of the various other stakeholders. It is essential that responsibilities for meeting specific requirements are unambiguously communicated to other stakeholders. The standards include requirements for disclosure and other communications. These may be helpful in for identifying contractual requirements with other stakeholders.

1.9 The establishment of processes for assuring safe and secure interoperability should take into account the role of the organization in the interoperability ecosystem, and regulatory requirements applicable to the organization's activities. It is not the intent of the AAMI/UL 2800 series of standards to imply the need for uniformity in the structure of different processes for assuring interoperability, uniformity of documentation or alignment of documentation to the clause structure of these standards.

1.10 The above approach enables an organization to establish processes that are consistent with the role it plays in the interoperability ecosystem. It also enables the organization to manage its activities in a manner appropriate to the scope of its interoperable medical products.

2 Scope

2.1 This Standard is applicable to interoperable medical products, including assembled systems of interoperable medical products that comprise or are intended to be incorporated into interoperable medical systems within an interoperable environment.

2.2 This Standard specifies a baseline set of interoperability lifecycle requirements for assuring safe and secure interoperability for interoperable medical systems.

3 References

3.1 Any undated reference to a code or standard appearing in the requirements of this Standard shall be interpreted as referring to the latest edition of that code or standard.

3.2 The following standards are referenced in this Standard:

AAMI TIR57, *Technical Information Report: Principles for Medical Device security – Risk Management*

AAMI/UL 2800-1-1, *Standard for Risk Concerns for Interoperable Medical Products*

AAMI/UL 2800-1-2, *Standard for Interoperable Item Development Life Cycle*

AAMI/UL 2800-1-3, *Standard for Interoperable Item Integration Life Cycle*

ASTM F2761, *Standard for Medical Devices and Medical Systems – Essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE) – Part 1: General requirements and conceptual model*

IEC 60601-1, *Standard for Medical Electrical Equipment – Part 1: General Requirements for Basic Safety and Essential Performance*

IEC 60601-1-8, *Standard for Medical Electrical Equipment – Part 1-8: General Requirements for Basic Safety and Essential Performance – Collateral Standard: General Requirements, Tests and Guidance for Alarm Systems in Medical Electrical Equipment and Medical Electrical Systems*

IEC 61508, *Functional Safety Of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 1: General Requirements*

IEC 62304, *Standard for Medical Device Software – Software Life Cycle Processes*

IEC 80001-1, *Standard for Application of Risk Management for IT-Networks Incorporating Medical Devices – Part 1: Roles, Responsibilities and Activities*

IEC/TR 80002-1, *Medical device software — Part 1: Guidance on the application of ISO 14971 to medical device software*

ISO 14971, *Standard for Medical Devices – Application of Risk Management to Medical Devices*

ISO/IEC 15026-3, *Systems and software engineering – Systems and software assurance – Part 3: System integrity levels*

ISO 26262-1, *Road vehicles – Functional safety – Part 1: Vocabulary*

ISO/IEC/IEEE 42010, *Systems and software engineering – Architecture description*

ISO/IEE Guide 51, *Safety aspects – Guidelines for their inclusion in standards*

4 Terms and Definitions

4.1 ACTOR – An active or passive entity, human or non-human, capable of initiating action or providing data, potentially in response to commands.

NOTE 1: An interoperable item is a special case of non-human actor.

NOTE 2: Health IT systems including Electronic Medical Record systems or Physician Order Entry systems are examples of non-human actors that may not be interoperable items.

NOTE 3: Medical devices are examples of non-human actors (which may or may not comply with the requirements of this Standard, i.e., may or not be interoperable items).

NOTE 4: Operators and patients are examples of human actors.

NOTE 5: Actors may be distinguished by context of use including development context of use actors (e.g., interoperable medical system manufacturers), deployment context of use actors (e.g., clinicians, bio-medical engineers, etc.)

4.2 ALARM CONDITION – State of the alarm system when it has determined that a potential or actual hazardous situation exists for which operator awareness or response is required.

NOTE 1: An alarm condition can be invalid, i.e. a false positive alarm condition.

NOTE 2: An alarm condition can be missed, i.e. a false negative alarm condition.

4.3 ALARM LIMIT – Threshold used by an alarm system to determine an alarm condition.

4.4 ALARM SETTINGS – alarm system configuration, including but not limited to:

a) Alarm limits;

b) The characteristics of any alarm signal inactivation states; and

c) The values of variables or parameters that determine the function of the alarm system.

NOTE: Some algorithmically-determined alarm settings can require time to be determined or re-determined.

4.5 ALARM SIGNALING – Action taken by the alarm system to generate an alarm signal at the operator's position.

4.6 ALARM SIGNAL – Type of signal generated by the alarm system to indicate the presence (or occurrence) of an alarm condition.

4.7 ALARM SYSTEM – Parts of ME equipment or a ME system that detect alarm conditions and, as appropriate, generate alarm signals.

4.8 ARCHITECTURE VIEW – Artifact within the interoperability architecture expressing the architecture from the perspective of specific set of concerns.

4.9 ARCHITECTURE VIEWPOINT – Constraints establishing the conventions for the construction, interpretation, and use of an architecture view to frame a specific set of concerns.

4.10 ASSURANCE – Grounds for justified confidence that a claim has been or will be achieved.

NOTE: Assurance activities include verification and validation activities that provide objective evidence for claims reflected in interoperable item SSOs and interoperability specification.

4.11 AUTHENTICATION/AUTHENTICATED/AUTHENTICITY – The process of verifying the identity of an entity.

4.12 AUTHENTICATION OF INFORMATION – Sensitive data is any critical security parameter that can compromise the use and security of the product such as passwords, keys, seeds for random number generators, authentication data, personally identifiable information and any data whose disclosure could jeopardize the security properties of the product.

4.13 AUTHORIZATION/AUTHORIZED – [Source: CNSSI-4009 via AAMI TIR57]

4.14 AVAILABILITY/AVAILABLE – [Source: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542 via AAMI TIR57]

4.15 CLINICAL CARE – Patient contact and/or management, which corresponds to a block of activity (session) directly related to:

a) Diagnosis of disease or other conditions,

b) Cure, alleviation, mitigation, treatment/therapy, or prevention of disease,

c) Compensation for an injury or handicap,

d) Replacement or modification of the anatomy or of a physiological process, or

e) Intended to affect the structure or any function of the body of the patient.

4.16 COMPUTATIONAL VIEW – An aspect of the interoperability architecture that provides a decomposition in terms of logical functional as interactions between those functions.

NOTE 1: The Computational View is based on concepts from the ISO/IEC 10746 RM-ODP Computational View. However, this Standard does to require compliance to ISO/IEC 10746.

NOTE 2: The Computational View captures what is commonly referred to as a functional architecture, where interactions between functional elements are captured in terms of programmatic interfaces.

NOTE 3: For an overview of the notions of architectural view and viewpoint see ISO/IEC/IEEE 40210.

4.17 CONFIDENTIALITY – The property that data, information or software is not made available or disclosed to unauthorized individuals, entities, or processes.

4.18 CONSTITUENT INTEROPERABLE ITEM – A member of the collection of interoperable items integrated to form the realization of an encompassing interoperable item [see definition of interoperable item(b)].

4.19 DEPLOYMENT CONTEXT OF USE – Actors, processes, and health-delivery objectives that may impact the safe and secure use of the interoperable medical product as part of deployment activities.

NOTE 1: Deployment context of use activities are summarized in Annex A.

NOTE 2: In typical cases, the deployment context of use refers to the context of use in a Health Delivery Organization and addresses the use of the interoperability solution to support medical functions as well as the configuration, deployment, and maintenance of the interoperability solution.

4.20 DEVELOPMENT CONTEXT OF USE – Organizations, processes, technologies, interoperability frameworks, and business relationships that may influence or use the interoperable medical product as part of development activities.

NOTE: Development context of use Activities are summarized in Annex A, and detailed in AAMI/UL 2800-1-2 and AAMI/UL 2800-1-3.

4.21 DISCLOSURE – Planned and managed release of information between the organization originating the interoperable item and stakeholder organizations to support the safe and secure use of the interoperable item in its development context of use or deployment context of use.

NOTE 1: See the Annex for Guidance on Interoperability File of AAMI/UL 2800-1-2 and the Annex for Guidance on Disclosure of AAMI/UL 2800-1-2.

NOTE 2: ISO 14971 Information for Safety, IEC 80001 Responsibility Agreements and Information for Assurance are addressed by the disclosures of this Standard.

NOTE 3: Disclosures support "risk hand-offs" between organizations and are key element of supporting cross-organization risk management for interoperable medical systems.

4.22 EFFECTIVENESS – Ability to produce the intended result for the patient and the responsible organization. Reasonable assurance that a device is successful in producing a desired or intended result

when it can be determined, based upon valid scientific evidence, that in a significant portion of the target population, the use of the device for its intended uses and conditions of use, when accompanied by adequate directions for use and warnings against unsafe use, will provide clinically significant results.

4.23 ERROR – Deviation from an item interoperability specification that is observable on an interface of the interoperable item.

NOTE 1: An error originating in an interoperable item's context may propagate into the interoperable item through its interface inputs.

NOTE 2: An error may propagate out of an interoperable item over an interface due to either:

a) A fault internal to the interoperable item; or

b) An error propagating into the interoperable item from its context that is passed through the interoperable item or transformed into an error of different character.

4.24 ERROR PROPAGATION SPECIFICATION – Summary of inward and outward flowing interoperability-related errors that may manifest on the interoperable item's interfaces.

NOTE: See Annex D of AAMI/UL 2800-1-2 the purpose of the error propagation specification in the context of broader risk management activities. See the Annex for Guidance on Interoperability File of AAMI/UL 2800-1-2 for relationship of the error propagation specification to other work products.

4.25 EXTERNAL MEASURE – Measure separate and distinct from the interoperable item that reduces or mitigates the risks resulting from the interoperable item or usage of the interoperable item within its development context of use or deployment context of use.

NOTE 1: The means by which an external measure is to be achieved will typically be communicated through instructions for use and will typically coincide with ISO 14971 Information for Safety.

NOTE 2: Interoperable item SSOs and external measures are designed in concert with the intent that the interoperable item will be able to achieve its SSOs if the external measures are achieved.

NOTE 3: External measures represent obligations of the agents in the context of the interoperable item whereas SSOs represent obligations on interoperable item, given that external measures are achieved. The organization producing the interoperable item also has the obligation of communicating the external measures clearly.

4.26 EXTERNAL PRODUCT – An anticipated non-human actor or specified interoperable item with which the interoperable medical product interacts but is not provided with the interoperable medical product.

NOTE – An external product may be specified as an accessory to be provisioned by the user of the interoperable medical product (such as a sensor device) or be a part of the interoperable environment within which the interoperable medical product is used (such as an electronic medical record system).

4.27 EXTERNALLY SOURCED PRODUCT – Either a constituent interoperable item in an interoperable medical product or an external product that is specified as necessary to proper use of the interoperable medical product that is placed on the market by an external party that is not part of the organization.

4.28 FUNCTIONAL SAFETY CONCEPT – Design of functional safety including independence aspects, allocation to items within the architecture, risk controls, and their interaction necessary to achieve SSOs.

4.29 HAZARDOUS SITUATION – Circumstance in which people, property, or the environment are exposed to one or more hazard(s).

4.30 IDENTIFICATION/IDENTIFIED – See authenticated.

4.31 IDENTIFIER – *[Source – Adapted from RFC 2828 (referring to data, but is generalized for this document)]*

4.32 IDENTITY – A particular presentation of an operator or interoperable item. An identity may be a unique reference to the operator or interoperable item, especially binding when proved through authentication.

4.33 IDENTITY CLAIM – Assertion or statement of the state or fact of being the same one as described.

4.34 INFORMATION VIEW – An aspect of the interoperability architecture that describes:

a) The primary data elements exchanged between constituent interoperable items and between the interoperable item and its context; and

b) Operations on those data elements.

NOTE 1: The information view is based on concepts from the ISO/IEC 10746 RM-ODP information view. However, this Standard requires compliance to ISO/IEC 10746.

NOTE 2: The information view may also capture important internal state of an interoperable item that is necessary to specify constraints on the interoperable item's interoperability behavior.

NOTE 3: For an overview of the notions of architectural view and viewpoint see ISO/IEC/IEEE 40210.

4.35 INTEGRATOR – Natural or legal person carrying out the activity of interoperable item integration. See Annex A.

4.36 INTEGRITY – The assurance that data can only be altered by authorized entities.

4.37 INTENDED USE [intended purpose] – Use for which a product, process or service is intended according to the specifications, instructions and information provided by the manufacturer.

4.38 INTERACTION – An action between an interoperable item and its context taking place over one of the interoperable item's interfaces. See the Annex for Interoperability Architecture Specification of AAMI/UL 2800-1-3.

NOTE: An interaction involves the participation of both the interoperable item and an actor in its context. When the actor in the context is an another interoperable item, the interaction occurs over an interoperability interface.

4.39 INTERACTION BEHAVIORAL SPECIFICATION – Constraints on the interactions between an interoperable item and its context over its interfaces specified in terms of interface contracts.

NOTE: Specifications of interactions over the interoperability interfaces of an interoperable item are stated in terms of interface contracts.

4.40 INTERACTION PARAMETER SPECIFICATION – Part of an interaction specification that specifies the parameters and accompanying characteristics of a particular interaction. See the Annex for Interoperability Architecture Specification of AAMI/UL 2800-1-3.

4.41 INTERACTION POINT – Interoperability architecture feature defined for the purpose of stating constraints and assumptions on data and control [information] that flow across an interoperable item's boundary.

Each interaction point is specified as exactly one of the following types:

a) Physiological – Supports machine-to-patient interactions associated with sensing or actuation capabilities related to the physiology of the patient;

b) Operator – Supports machine-to-human interactions for commands or information exchange between the interoperable item and operator; or

c) Interoperability – Supports machine-to-machine interactions.

An interoperability interaction point consists of one or more related interoperability interfaces.

4.42 INTERACTION SPECIFICATION – Characteristics of an interaction given at a level of precision that are sufficient to:

a) Determine if interoperable items participating in the interaction comply with the specification; and

b) Exclude undesirable behaviors leading to violations of safety-related and security-related properties. See the Annex for Interoperability Architecture Specification of AAMI/UL 2800-1-3.

Interaction specifications are accompanied by interface contracts that constrain the behavior of interactions over interfaces.

4.43 INTERFACE CONTRACT – Behavioral constraints on the interactions between an interoperable item and its context over one of its interoperability interfaces.

NOTE 1: An interface contract imposes obligations on both the interoperable item and its clients. An Interface contract will typically establish pre-conditions that clients of the interoperable item must achieve before or at the initiation of an interactions, and post-conditions that the interoperable item must achieve given that associated pre-conditions are satisfied.

NOTE 2: An interface contract may include constraints on data exchanged during an interaction, temporal ordering of interactions on the interoperability interface, timing constraints on the interaction or sequence of interactions, and exceptional behavior and error return codes.

4.44 INTERFACE SPECIFICATION – Collection of interaction specifications, associated interface contracts, and engineering and technology aspects of the interface realization.

4.45 INTEROPERABILITY ARCHITECTURE – Constraints and rules determining the organization of a set of interoperable items, their designed interoperable interactions with each other, and their intended interactions with environment. The interoperability architecture provides a decomposition at the granularity at which interoperable items may be exchanged and reused according to their designed interoperability.

NOTE 1: An interoperability architecture may be defined using a variety of methods including annotated graphical models or textual constraints as long as the precision is sufficient to determine compliance to this Standard. The interoperability architecture may be incorporated into a more comprehensive architecture description that addresses non-interoperability-related aspects.

NOTE 2: The rules and constraints of an interoperability architecture capture designed interoperability variabilities that allow multiple interoperability architecture instances to be compliant with an interoperability architecture. This concept enables a set of related interoperability architecture instances to be addressed determining compliance to this Standard.

4.46 INTEROPERABILITY ARCHITECTURE CONFIGURATION – Specific restriction of one or more interoperability variabilities of an interoperability architecture.

NOTE: An interoperability architecture configuration is a refinement of an interoperability architecture that restricts the set of conformant interoperability architecture instances for a particular purpose. Examples of common restrictions include bounding the number or types of medical devices that can connect with a platform, or restricting the applications that may be executed simultaneously with a high-criticality application. Such restrictions may be useful for scoping the use of an interoperability framework for a particular set of related applications whose assurance will be addressed collectively.

4.47 INTEROPERABILITY ARCHITECTURE INSTANCE – An interoperability architecture configuration where no interoperability variabilities remain.

NOTE 1: An interoperability architecture instance represents a concrete realization whose behavior can be accessed via testing.

NOTE 2: An instance of an interoperability architecture for an interoperable medical system may be executed at the point-of-care to provide a particular clinical function.

NOTE 3: Compliance of an interoperable item to this standard addresses the safety and security properties of all interoperability architecture instances that conform to the interoperable item's interoperability architecture.

4.48 INTEROPERABILITY BINDINGS – Planned association of two or more interoperable items over designated interoperability interfaces of the interoperable items.

4.49 INTEROPERABILITY ECOSYSTEM – Stakeholders whose products and services enable interoperability.

4.50 INTEROPERABILITY FILE – One or more information repositories either containing or referencing records generated to demonstrate compliance to the requirements of this Standard.

4.51 INTEROPERABILITY FRAMEWORK – Consists of a managed collection of interoperability assets including:

a) Items designed to be integrated in different configurations in conformance with a interoperability architecture;

b) Processes conforming to life-cycle objectives of this Standard for coordinating life-cycle activities across the framework items to increase effective and trustworthy reuse of items and associated specification, risk management, and assurance results; and

c) Assets, shared across the development of the framework items, for supporting interoperability-related aspects of development and assurance.

NOTE: The notion of an INTEROPERABILITY FRAMEWORK supports the notions of platform-based development, product lines and product families (e.g., as described in ISO/IEC 26550), and families of items developed around a common interoperability interfacing framework (e.g., IEEE 11073).

4.52 INTEROPERABILITY INTERFACE – An engineered mechanism for information exchange that provides all or part of a realization of an interoperability interaction point.

NOTE 1: An interoperability interaction point will often be realized in terms of multiple interfaces that address different levels of abstraction. For example, an interoperability interaction point for reporting physiological data from a medical device may include network transport layer interfaces, middleware service interfaces, and data description interfaces.

NOTE 2: The granularity of an interface specified for the purposes of compliance with this Standard may be determined by following guidance in the Annex for Architecture Definition Guidance of AAMI/UL 2800-1-3 and the Annex for Interoperability Architecture Specification of AAMI/UL 2800-1-3.

4.53 INTEROPERABILITY SCENARIOS SPECIFICATIONS – Partial specification of an interoperable medical system or family of related interoperable medical systems describing an intended application of interoperability that may be evaluated under this Standard.

NOTE 1: An interoperability scenario specification may serve to normalize use cases, requirements, and architectural approaches for the purpose of establishing community consensus for particular applications.

NOTE 2: An interoperability scenario specification may be used as input to the later design and realization of an interoperable medical system which may benefit from reuse of the artifacts developed in and may claim compliance to the interoperability scenario specification. See Annex B.

NOTE 3: An interoperability scenario specification may include as aspects of use specification, interoperability architecture, interoperable, and the like.

4.54 INTEROPERABILITY VARIABILITY – Designed feature within the INTEROPERABILITY ARCHITECTURE allowing variations in the set of conforming instances.

4.55 INTEROPERABLE APPLICATION SPECIFICATION – A summary of the important characteristics related to the use of the interoperable medical product within stated interoperability scenario specifications.

4.56 INTEROPERABLE ENVIRONMENT – The managed collection of interoperable products and associated services that can be integrated in one or more configurations to enable interoperable use of a specific interoperable medical product.

4.57 INTEROPERABLE ITEM (ITEM) – A realization of an item interoperability specification for interoperable hardware, software or system to which the contents of this Standard are applied. This may take one of two forms:

a) It may not be further decomposed with respect to interoperability and compliance with this Standard; or

b) It may be a collection of interoperable items integrated in accordance with integration life-cycle activities.

NOTE: A member of the collection of the integrated interoperable items in (b) is referred to as a constituent interoperable item.

4.58 INTEROPERABLE ITEM BOUNDARY – The division between the realization of the interoperable item and external actors, as defined by the interoperable item's interaction points.

NOTE: The boundary may help scope the assurance, risk management, and disclosure responsibilities of the interoperable item manufacturer by indicating the engineering features under the interoperable item manufacturer's direct control.

4.59 INTEROPERABLE ENVIRONMENT – The managed collection of interoperable products and associated services that can be integrated in one or more configurations to enable interoperable use of a specific interoperable medical product.

4.60 INTEROPERABLE MEDICAL PRODUCT – Output that is intended for, or required by, a customer, for supporting the development and deployment of an interoperable item for medical purpose.

NOTE: Common examples of interoperable medical products include:

a) An interoperable item supporting a medical purpose;

b) An interoperable medical system (as a special case of interoperable item);

c) An interoperability framework; and

d) Work products or services related to the stakeholder activities in Annex A.

4.61 INTEROPERABLE MEDICAL SYSTEM – An item consisting of one or more integrated (sub)-items (and is therefore decomposable) with a clinical intended use.

4.62 INTEROPERABLE USE SPECIFICATION – A summary of the important characteristics related to the context of use of the interoperable medical product that serves as input for determining item interoperability specifications.

4.63 ITEM INTEROPERABILITY SPECIFICATION – Collection of artifacts which are necessary and sufficient to:

a) Define the item's interoperability-related functionality and interfaces;

b) Integrate the interoperable item with or as part of another interoperable item and to carry out associated safety and security assurance activities, including those that determine that the item's conditions of acceptability have been satisfied; and

c) Specify controls that are required to ensure safety and security during the deployment, operation, and maintenance of the item.

NOTE: Specification artifacts may include requirements, interface specifications including interface contracts that capture conditions of acceptability, technical instructions, risk management information, and operating instructions, and constraints on the technical, clinical, and operating environment needed to achieve safety.

4.64 IT-NETWORK [INFORMATION TECHNOLOGY NETWORK] – A system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes.

Adapted by UL from IEC 61907:2009 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved

NOTE: The scope of the IT-NETWORK in this document is defined by the responsible organization based on where the health software in the IT-NETWORK is located and the defined use of the IT-NETWORK. It can contain IT infrastructure, home health, or general computing components or systems not intended by design to be used in a healthcare setting. See also 7.2.

4.65 MANUFACTURER – Natural or legal person with responsibility for the design, manufacture, packaging, or labelling of ME equipment, assembling and configuring an ME system, or adapting ME equipment or an ME system, regardless of whether these operations are performed by that person or on their behalf by another person(s).

Adapted by UL from IEC 60601-1:2020 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.66 MEDICAL ELECTRICAL EQUIPMENT [ME EQUIPMENT] – Electrical equipment having an applied part or transferring energy to or from the patient or detecting such energy transfer to or from the patient and which is:

a) Provided with not more than one connection to a particular supply mains; and

b) Intended by its manufacturer to be used:

1) In the diagnosis, treatment, or monitoring of a patient; or

2) For compensation or alleviation of disease, injury or disability, or other condition.

NOTE 1: In some jurisdictions, ME Equipment may meet the definition of a medical device as defined in a particular jurisdiction.

NOTE 2: Equipment, when mentioned in this Standard, should be taken to include ME equipment.

4.67 MEDICAL ELECTRICAL SYSTEM [ME SYSTEM] – Combination, as specified by its manufacturer, of items of equipment, at least one of which is ME equipment to be inter-connected by functional connection or by use of a multiple socket-outlet.

4.68 OBJECTIVE EVIDENCE – Data supporting the existence or verity of something.

NOTE: OBJECTIVE EVIDENCE can be obtained through observation, measurement, testing, or other means.

4.69 ORGANIZATION – An entity with responsibility for placing on the market an interoperable medical product intended to be used in accordance with an interoperable application specification.

4.70 OPERATIONAL CONTEXT OF USE – A sub-context of the deployment context of use related specifically to the point-of-care. Actors, processes, and health-delivery objectives and use cases that may impact the safe and secure use of the interoperability solution [generic term encompassing both item and interoperability framework] as part of delivery of care to the patient in interoperable item operation activities.

4.71 OPERATOR – Someone who, under authority of the responsible organization, controls the function of a machine, process or system in a specified manner.

NOTE 1: Different categories of operator include:

a) A medical professional;

b) A patient if appropriately authorized; and

c) Service personnel if appropriately authorized.

NOTE 2: An operator may take control or receive information from the machine, process, or system in a venue outside of the responsible organization (i.e., in home care).

4.72 OPERATOR IDENTITY/IDENTIFICATION – Person-specific information used to distinguish an individual operator. Operator identifiers include username, badge number, and/or other identifiers generated by ADT or EMPI.

4.73 PASSWORD – Sensitive data is any critical security parameter that can compromise the use and security of the product such as passwords, keys, seeds for random number generators, authentication data, personally identifiable information and any data whose disclosure could jeopardize the security properties of the product.

4.74 PATIENT – Living being (person or animal) undergoing a medical, surgical or dental procedure.

NOTE: A patient can be an operator.

4.75 PATIENT ASSOCIATION – The process of establishing a patient identity within an interoperable item for the purpose of identifying the patient under care.

4.76 PATIENT DISASSOCIATION – The process of dissolving the logical relationship between an interoperable item and the patient under care previously established by a patient association process.

NOTE: Patient disassociation will likely involve clearing patient identity information and medical information linked to the patient identity.

4.77 PATIENT EPISODE – The period of time between and patient association and patient disassociation during which the medical functions of the interoperable item are dedicated to care-giving for the patient under care.

4.78 PATIENT ID – The identity claim of a patient.

4.79 PATIENT IDENTIFICATION – The process of matching the patient with the patient identifier information (see also patient identity verification).

4.80 PATIENT IDENTIFIER – An item of person-specific information used to distinguish an individual patient. Patient identifiers include name (given name, family name, and/or middle name), DOB, MRN, location, other identifiers generated by ADT or EMPI.

4.81 PATIENT IDENTITY – Selected data elements associated with a patient to uniquely identify that patient among other patients within a Health Delivery Organization. Selected data elements (patient identifiers) – usually the name (given name, family name, and/or middle name), birth date, SSN, MRN, and sometimes the gender for a single patient. Patient identity can be either verified or un-verified. (See patient identity verification.)

4.82 PATIENT IDENTITY VERIFICATION – The process of matching patient identifiers that were input to the ME system with a trusted source of patient information (ADT/EMPI) to ensure the patient is accurately identified.

4.83 PATIENT UNDER CARE – The particular patient whose care is being addressed by the interoperable item while it is performing its clinical function.

4.84 PHYSIOLOGICAL ALARM CONDITIONS – Alarm condition arising from a monitored patient-related variable.

4.85 POTENTIALLY HAZARD CONDITION – Conditions on the state of an interoperable item that may lead to a violation of the interoperable items interoperability specification and/or indirectly to patient harm.

NOTE 1: The term potentially hazard condition generalizes the notion of fault or root cause to address the fact that an interoperable item may not know the potential patient harms associated with interoperable medical systems into which it is integrated. In such cases, the objectives of interoperable item development center around (a) developing technical specifications (captured in the interoperable item interoperability specification) that are appropriate for the intended use of the interoperable item and (b) mitigating potentially hazard conditions that could lead to violations of the technical specification.

NOTE 2: A potentially hazard condition may represent a precondition for a risk concern.

4.86 PROTECTED HEALTH INFORMATION (PHI) – Protected health information (PHI), also referred to as personal health information, generally refers to demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and any information about health status, provision of health care, or payment for health care that is created or collected by an entity, or their representative, and can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

Source: https://www.hhs.gov/hipaa/for-professionals/faq/2042/what-personal-health-information-do-individuals/index.html

4.87 PROVENANCE – A record of the original source and chain of possession of data – combination of authenticity, integrity, and no-repudiation for every entity that has processed the data – a chain of authentication of information.

4.88 REFERENCE ARCHITECTURE – An interoperability architecture for an interoperability framework that serves a schema and establishes constraints on interoperable item and interoperable medical system instances that are compliant with the interoperability framework.

4.89 RELEASE CRITERIA – Conditions and traceability relationships on the interoperable item interoperability specification, interoperable item realization and associated work products and disclosures that are to be achieved and substantiated with objective evidence before the interoperable item is released.

NOTE 1: Release criteria include primary conditions and relationships to be assessed when determining compliance to this Standard. release criteria for the primary development activities of the Standard are presented in the Annex for Guidance on Release Criteria of AAMI/UL 2800-1-2.

NOTE 2: Though not required by this Standard, release criteria may be used to inform the contents of a risk management file or the design of an assurance case for the interoperable item.

4.90 RESPONSIBILITY AGREEMENT – One or more documents that together fully define the responsibilities of all relevant stakeholders.

NOTE: This agreement can be a legal document, e.g. a contract.

4.91 RESPONSIBLE ORGANIZATION – Entity accountable for the use and maintenance of an ME equipment or an ME system

NOTE 1: The accountable entity can be, for example, a hospital, an individual clinician or a layperson. In home use applications, the patient, operator and responsible organization can be one and the same person.

NOTE 2: Education and training is included in “use”.

4.92 RISK CONTROL – Process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels.

4.93 RISK MANAGEMENT – Systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling and monitoring risk.

4.94 SAFETY – Freedom from risk which is not tolerable.

4.95 SAFETY and SECURITY OBJECTIVES [SSO] – An objective for the interoperable items design, functionality, performance, and risk controls that characterizes the interoperable item's intentions and obligations for achieving a safety and security – related property.

NOTE 1: Interoperable item SSOs and external measures are designed in concert with the intent that the interoperable item will be able to achieve its SSOs if the external measures are achieved.

NOTE 2: External measures represent obligations of the agents in the context of the interoperable item whereas SSOs represent obligations on interoperable item, given that external measures are achieved.

NOTE 3: AAMI/UL 2800-1-1 provides candidate system-level SSOs to consider when forming interoperable item SSOs.

NOTE 4: SSOs are refined into requirements on the interoperable item, which are in turn refined to interface contracts that constrain the interactions of the interoperable item with its context over its interoperability interfaces.

4.96 SECURITY – The process of having acceptable levels of confidentiality, integrity, authenticity and/or availability of product data and/or functionality through risk analysis.

4.97 TECHNICAL ALARM CONDITIONS – Alarm condition arising from a monitored equipment-related or alarm system-related variable.

4.98 TECHNICAL SAFETY CONCEPT – Design of the realization of the functional safety concept in terms of the interoperability architecture and technical requirements used in the realization of the interoperable item.

4.99 VALIDATION – Confirmation, through the provision of objective evidence, that the interoperable item is fit for purpose as expressed in the interoperable use specification and interoperable application specification.

4.100 VERIFICATION – Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

5 (Leadership) Management Responsibility

5.1 Top management shall provide evidence (see the NOTE in 5.2) of its commitment to assuring safe and secure interoperability by:

a) Establishing policy for determining criteria for safe and secure interoperability;

b) Ensuring that objectives (see SSOs of AAMI/UL 2800-1-1) specific to the interoperability of its products with respect to safety and security are established and met;

c) Ensuring that processes required by this Standard are established and maintained; and

d) Ensuring the availability of resources to effectively implement the processes.

5.2 Top management shall provide evidence (see NOTE) of its commitment to collaboration within the interoperability ecosystem, by ensuring that:

a) Roles and needs of stakeholders in the Interoperability ecosystem are determined and understood;

b) Risks and opportunities that can affect the ability of stakeholders in the interoperability ecosystem to assure safe and secure interoperability are determined and addressed;

c) Ongoing communication, including provision of timely disclosures (see 6.3) and focus on enhancing stakeholder collaboration is maintained.

NOTE: Evidence of management commitment may be maintained separately or relevant parts incorporated into a Risk Management or Quality Management System documentation.

6 Interoperability Information

6.1 Controlled information

6.1.1 The identity claim of a patient interoperability ecosystem shall maintain controlled information (see NOTE 1) to:

a) Provide evidence that the required processes are being established and carried out; and

b) Provide evidence of compliance to this Standard.

Controlled information shall be maintained in a manner so as to be unambiguously referenced and accessed in a timely fashion when required.

NOTE 1: Controlled information may be maintained in documents or in electronic information management systems. Information can be maintained in distributed repositories, including information contained within the interoperable medical product (e.g., machine readable information).

NOTE 2: Controlled information required by this Standard can be maintained as part of other documentation required, for example, by a manufacturer's quality management system.

6.2 Interoperability file

6.2.1 One or more files shall be established and maintained, either containing or referencing information for demonstrating compliance with the requirements of this Standard, including required processes as applicable.

6.2.2 For each type or family of interoperable medical products the content of the file(s) shall include, but is not limited to:

a) Description of the interoperability of the interoperable medical product;

b) Scope of the interoperable environment and anticipated external products;

c) Interoperable use specifications for the interoperable medical product (see 9.1.4);

d) Interoperability specifications for the interoperable medical product;

e) Description of the interoperability of anticipated and specified external products;

f) Interoperable application specification for the interoperable medical product (see 13.2); and

g) Information necessary for demonstrating traceability and adequacy of safety and security evidence with respect to interoperability-related release criteria for specified application.

NOTE: See the Annex for Guidance on Interoperability File of AAMI/UL 2800-1-2 for more information.

6.3 Disclosure and communication

6.3.1 General

6.3.1.1 Information required for assuring safe and secure interoperability for any specified application of the interoperable medical product shall be disclosed as appropriate to relevant stakeholders in the interoperability ecosystem.

6.3.1.2 Disclosed information shall be communicated through appropriate means.

NOTE: Appropriate means of communicating disclosed information can include:

a) Accompanying documents containing information on safety (see IEC 60601-1);

b) Autonomous machine-to-machine communication;

c) Human readable disclosures conveyed through software; and

d) Business interfaces.

6.3.2 Information to be disclosed

6.3.2.1 Information disclosed to stakeholders in the interoperability ecosystem shall include, as appropriate, information about the product required by the stakeholder for:

a) Correct use of the interoperable medical product for a specified application within the interoperability ecosystem (see 13.2.1);

b) Technical integration of the interoperable medical product into other products or systems within the interoperability ecosystem;

c) Performance of integration testing of the interoperable medical product when integrated into other products or systems within the interoperability ecosystem;

d) Performance of provisioning and installation of the interoperable medical product when integrated into other products or systems within the interoperability ecosystem;

e) Operating and maintenance activities related to the interoperable medical product when integrated into other products or systems within the interoperability ecosystem; and

f) Decommissioning and disposal activities related to the interoperable medical product within the interoperability ecosystem.

6.3.2.2 Information disclosed to a provider of externally sourced product (see Section 10, Interoperability of Externally Sourced Products) shall include applicable information required by the organization for:

a) Determining interoperable use specifications (see 9.2) relevant to the correct use of the externally sourced product when integrated into the interoperable medical product or used with the interoperable medical product;

b) Technical integration of the externally sourced product into the interoperable medical product;

c) Integration testing of the externally sourced product when integrated into the interoperable medical product;

d) Provisioning and installation of the externally sourced product when integrated into the interoperable medical product;

e) Operating and maintenance activities related to the externally sourced product when integrated into the interoperable medical product or used with the interoperable medical product; and

f) Decommissioning and disposal activities related to the externally sourced product when integrated into the interoperable medical product or used with the interoperable medical product.

NOTE: See the Annex for Guidance on Disclosure of AAMI/UL 2800-1-2 for more information.

6.3.3 Required disclosure

6.3.3.1 The interoperable medical product's interoperable application specification (see 13.2) shall be disclosed as part of market release of the interoperable medical product or provision of the interoperable medical product for specified application.

6.3.3.2 Disclosures for purchasing or acquisition of externally sourced product, shall include as appropriate:

a) Specifications for externally sourced product; and

b) Responsibility agreement (See Section 10).

7 Interoperability Management

7.1 Scope of interoperability management

7.1.1 The organization shall determine the scope of interoperability of its interoperable medical products and potential application by the interoperability ecosystem that affect the ability to assure safe and secure interoperability. (See NOTE 1 of 7.1.2.)

7.1.2 The organization shall monitor information relevant to the scope, including any emergent aspects, after deployment and during operation of the interoperable medical product by the interoperability ecosystem that incorporates its interoperable medical products.

NOTE 1: The scope of interoperability management should include consideration of the roles played by the organization in an interoperability ecosystem, as well as the manner in which its interoperable medical products are used in the interoperable environment.

NOTE 2: See Annex A for more information on the various potential stakeholders and their roles in an interoperability ecosystem.

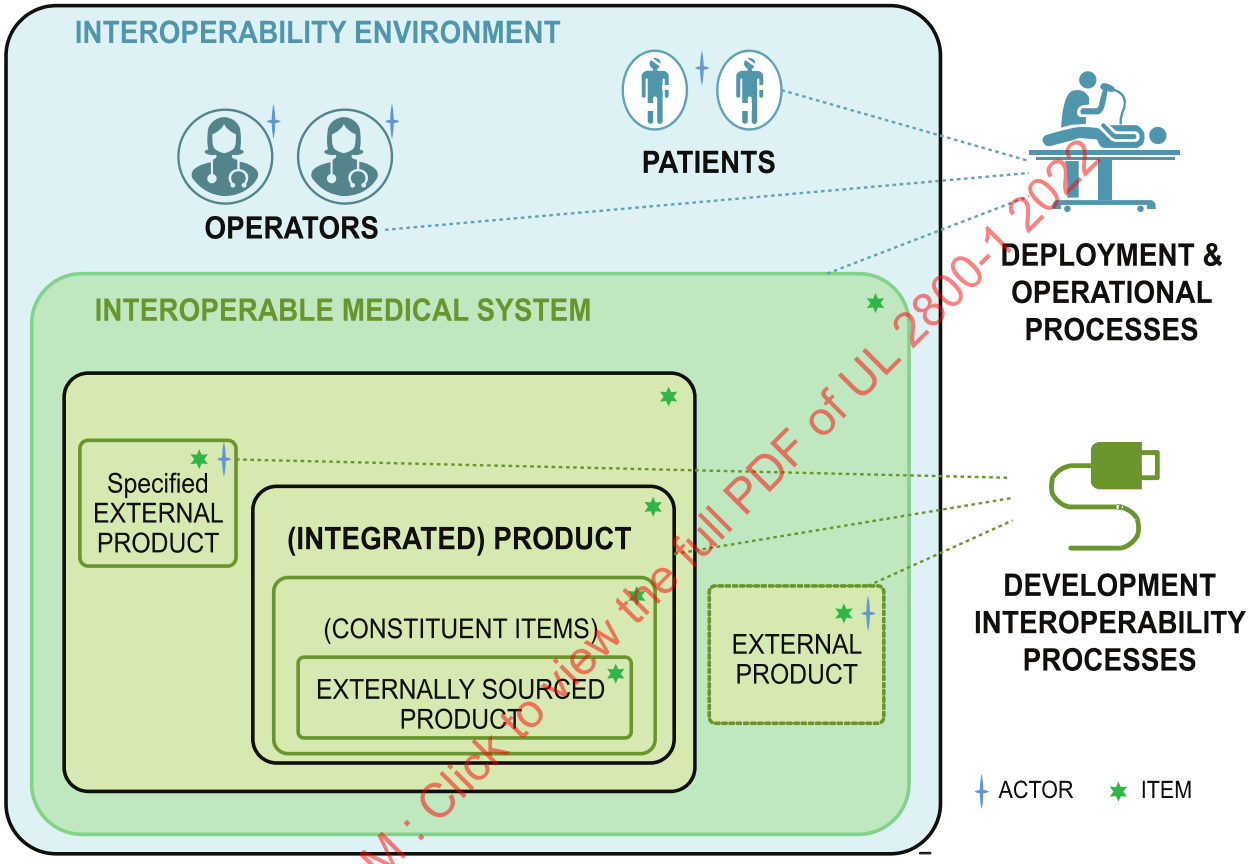
7.2 The interoperable environment

7.2.1 The organization shall determine the scope of the interoperable environment for its interoperable medical products. See Figure 7.1 for a schematic representation of the interoperable environment.

NOTE: The interoperable medical product may be in the form of a single contained interoperable item, or a platform comprising a collection of reusable interoperable items, or specific configurations of items or instantiations of platforms for specified clinical applications.

Figure 7.1

Interoperable environment ontology



su3403

7.2.2 In determining the interoperable environment, the following shall be considered:

a) Other interoperable medical products that incorporate or interact with the organization's interoperable medical products and their interoperability needs;

b) External products, including anticipated and specified external products, needed for application of the interoperable medical product;

c) Externally sourced products that are incorporated into the organization's interoperable medical products and information, including disclosed information about them; and

d) Any other products or services, including emergent aspects, in the interoperability ecosystem relevant to the ability to assure safe and secure interoperability.

7.2.3 Based on the above, the interoperable environment shall be determined, including the external infrastructure and resources that are relevant to the organization's ability to assure safe and secure interoperability.

7.3 Processes for assuring safe and secure interoperability

7.3.1 The organization shall determine the processes that assure safe and secure interoperability.

7.3.2 When determining the processes, the following shall be considered:

a) The scope of interoperability management referred to in 7.1;

b) The interoperable environment referred to in 7.2;

c) The interoperable medical products of the organization; and

d) Risk management process for assuring safe and secure interoperability (see 8.2).

7.3.3 All of the requirements of this Standard shall apply when they are applicable within the determined scope. Justification shall be provided for any requirement that is determined as not applicable.

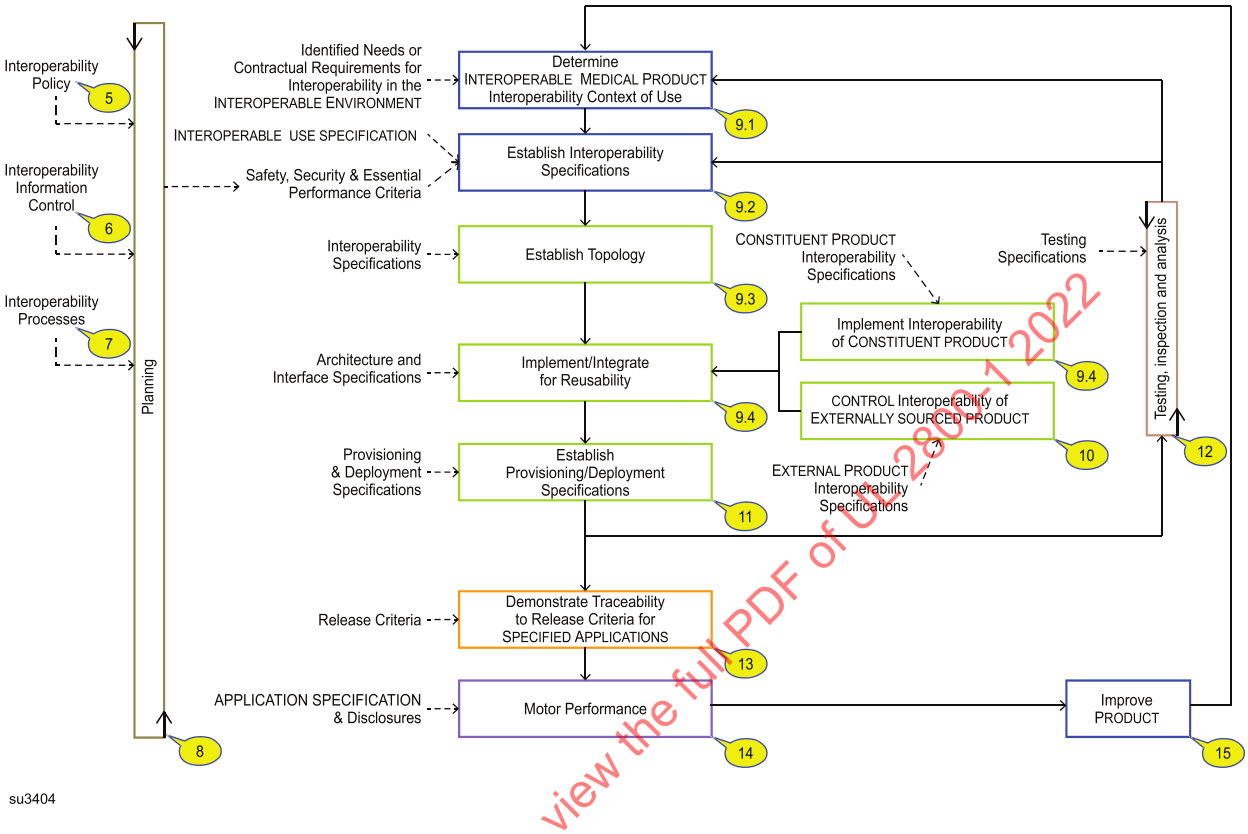
NOTE: See Annex B for more information.

7.3.4 The methods used shall be suitable to the type and scope of the interoperable medical product.

A schematic representation of interoperability realization processes (along with corresponding section numbers of this Standard) is shown in Figure 7.2. Depending on the type of interoperable medical product, individual elements of realization can have varying emphasis. Realization activities can be performed iteratively or in multiple steps as appropriate to the interoperable medical product.

Figure 7.2

Schematic of interoperability realization lifecycle



NOTE to Figure 7.2: Numbers in yellow circles correspond to clause numbers in the Standard.

7.3.5 Information on the organization's interoperability realization processes shall be controlled and maintained. (See 6.1.)

NOTE: Controlled information on processes for assuring safe and secure interoperability may be maintained separately or relevant parts incorporated into the organization's Risk Management or Quality Management System documentation.

7.3.6 Compliance with this Standard may only be claimed if the requirements determined as not being applicable do not affect the organization's ability to assure safe and secure interoperability.

8 Interoperability Realization Processes

8.1 Interoperability realization planning

8.1.1 The organization shall plan the realization of interoperability for the interoperable medical product, including:

a) Design, development, and implementation of interoperability for the interoperable medical product (see Section 9, Design, Development and Implementation of Interoperability);

b) Control of externally sourced products (see Section 10, Interoperability of Externally Sourced Products);

c) Provisioning and deployment of the interoperable medical product within the interoperable environment (see Section 11, Provisioning, Deployment, and Operation);

d) Testing for interoperability (see Section 12, Testing and Review);

e) Release of interoperability for specified application (see Section 13, Traceability and Release);

f) Monitoring and incident response during use of its interoperable medical product within the interoperable environment (see Section 14, Interoperability Performance Monitoring and Control of Changes);

g) Improvement of interoperable medical product (see Section 15, Improvement of Processes);

h) Risk Management (see 8.2); and

i) Communication with stakeholders in the interoperability ecosystem, including disclosure (see 6.3).

NOTE: AAMI/UL 2800-1-2 and AAMI/UL 2800-1-3 contain a more detailed description of the steps in the interoperability realization process.

8.1.2 Realization activities shall ensure that:

a) Interoperability objectives (see SSOs in AAMI/UL 2800-1-1) are met by:

1) Identifying applicable interoperability properties (see SSOs in AAMI/UL 2800-1-1) relating to interoperability objectives;

2) Establishing safety and security criteria with respect to the interoperability properties; and

3) Ensuring that the interoperable medical product meets the safety and security criteria.

b) Ensuring that the interoperable medical product meets release criteria (see Section 13, Traceability and Release); including criteria for risk acceptance;

c) Usability of interoperable medical product interoperability is acceptable, including ensuring that:

1) Unsafe control actions are avoided, such as when settings and configurations are changed;

2) Communications to and from the interoperable environment occur in a timely and correct fashion; and

3) Appropriate information on the current state of the interoperable medical product is provided to operators and external products, as appropriate.

NOTE 1: See the Annex for Interoperability Usability in UL 2800-1-1 for more information.

d) Security of interoperable medical product interoperability is acceptable, including ensuring that:

1) Cyber and physical threats are identified;

2) Vulnerabilities are identified; and

3) Mitigations are identified, implemented and tested.

NOTE 1: See the Annex for Security Properties in AAMI/UL 2800-1-1 for more information.

8.2 Risk management

8.2.1 Risk management shall be incorporated throughout interoperability realization and ensure that:

a) Potential hazardous situations associated with the use or reuse of the interoperable medical product in the interoperable environment and related potentially hazardous conditions of the interoperable medical product are identified (See NOTE 1);

b) The level of risk associated with each hazardous situation or the potentially hazardous conditions is estimated based on the probability of occurrence and the severity of harm that may result;

c) The level of risk is evaluated using risk acceptance criteria;

d) Risk control requirements that reduce risk sufficiently to meet risk acceptance criteria are identified, implemented, and are effective;

e) Controls required for specified application are included in disclosures (see 6.3), as appropriate include information on potentially hazardous conditions; and

f) Information from integration and application of the interoperable medical product in the interoperable environment that is relevant to risk management is monitored and reviewed for impact on previously conducted risk management activities.

NOTE 1: In order to identify hazardous situations, the organization needs to have a good understanding of the clinical context of use (see 9.1.2). For general purpose interoperable medical products, specific information on clinical use may not be available. In such cases, the technical context of use (see 9.1.3) should be analyzed and potentially hazardous conditions of the product identified. These may include operating states in which the product fails to perform or goes outside specified performance limits. Risk management activities may then be performed with respect to potentially hazardous conditions. Both hazardous situations and potentially hazardous conditions can be addressed as part of risk concerns (see ISO 14971).

NOTE 2: See Annex D for more information.

9 Design, Development, and Implementation of Interoperability

9.1 Interoperability context of use

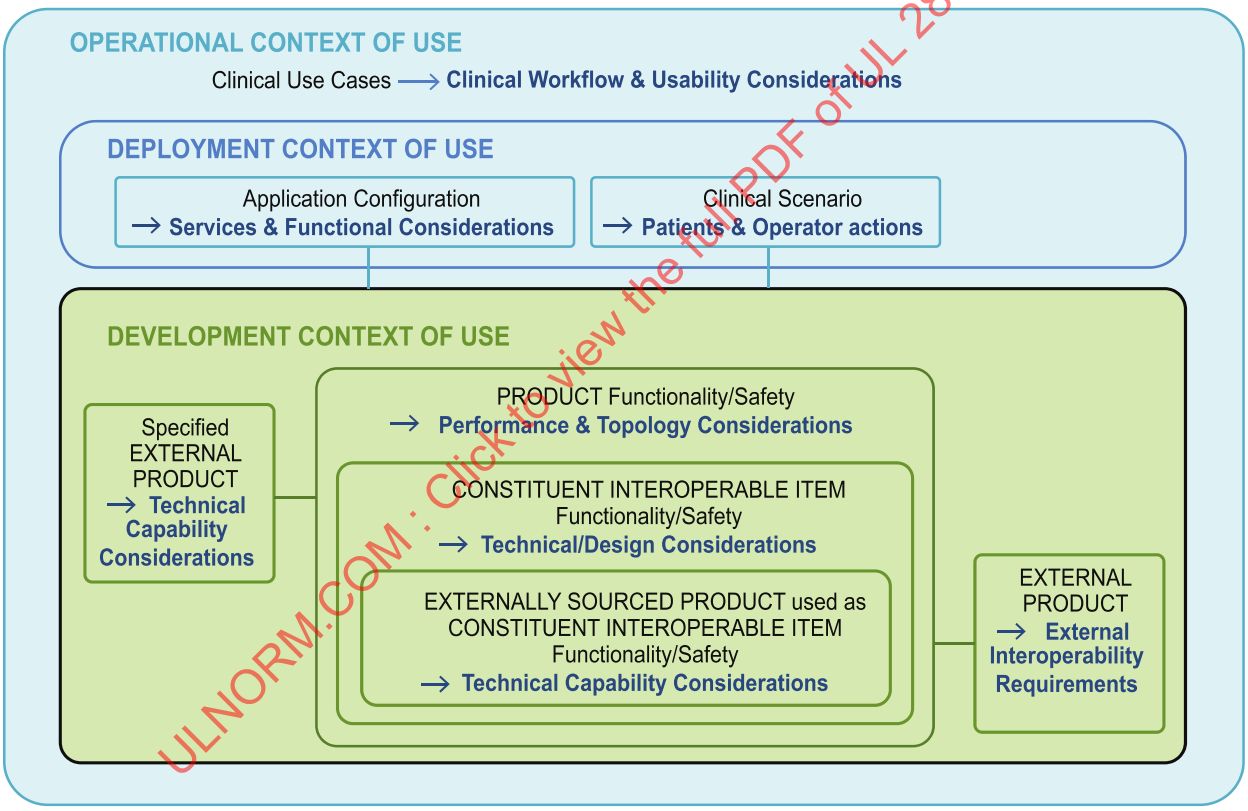
9.1.1 General

9.1.1.1 The organization shall determine the interoperability context of use and reuse for the interoperable medical product. Figure 9.1 schematically shows the potential contexts of use and their relationships.

NOTE: Depending on the nature of the interoperable medical product, the context of use or reuse may include deployment or development aspects or both.

Figure 9.1

Interoperability contexts of use



su3405

9.1.2 Deployment aspects in context of use

9.1.2.1 When applicable, interoperability aspects relevant to deployment shall include:

a) Intended clinical or medical uses and situations for which the interoperable medical product is intended to be deployed, including anticipated activities for the clinical workflows within which the interoperable medical product is intended to be used. (See NOTE 1)

b) Relevant clinical indications and scenarios and the associated application configurations of the interoperable medical product required for them.

c) Operations aspects such as services and functionality required for the interoperable medical product for set up, preparation or integration, and deployment prior, during, after clinical use including:

1) The type or category of clinical staff (See NOTE 2);

2) Potential changes or new/novel equipment or workflow that could improve the clinical workflow in the future; and

3) Benefits of the proposed clinical workflow.

d) Impact of the interoperable medical product on the clinical workflow when used as intended, including usability considerations.

e) Interoperability aspects for assuring that any patients associated with the interoperable medical product are correctly identified and are consistent with care-giving intent (i.e., care is being provided to the "right patient").

f) Interoperability aspects for assuring that any operators associated with the interoperable medical product are correctly identified and trusted to control the interoperable medical product.

g) Interoperability aspects for providing and controlling access based on operator roles.

h) Hazardous situations, breach of security, or use error (including foreseeable misuse) related to interoperability (see NOTE 3), that could potentially be introduced during application of the interoperable medical product and potential resulting harm.

i) Potential risk controls, such as operator actions available in the deployment context of use.

j) Any other aspects of interactions with the interoperable medical product in the deployment context relevant to assuring safe and secure interoperability.

NOTE 1: It might be helpful to consider the current state standard of clinical practice, the clinical challenge/function intended to be addressed by the interoperable medical product, as well as the instructions for operation and management of the components according to clinical lifecycle phases.

NOTE 2: Examples of clinical staff include surgeons, intensivists, anesthesia providers, chief nurse, nursing assistant, respiratory therapists, etc.

NOTE 3: A fault tree or similar analysis may be used to provide a more detailed representation of potential hazardous situations arising at various points in the clinical workflow or through combinations of conditions from multiple points in the workflow.

9.1.3 Development aspects in context of use

9.1.3.1 When applicable, aspects relevant to development shall include:

a) Product boundaries at the granularity at which product interoperability will occur;

b) External products and technical processes in the interoperable environment for the product (see NOTE 1);

c) Semantic interoperability aspects, including data elements, nomenclature and frameworks for identification of external products;

d) Interoperability needs of the interoperable environment, including external products, including:

1) Known or contractually provided requirements for interoperable functions of the product, and

2) Known or contractually provided requirements for interoperability performance levels and interface characteristics of the product.

e) Product interfaces with the interoperable environment, including with external products, patients, and, operators with which the product interfaces, and their characteristics;

f) Functional and performance constraints of the interoperable environment (see NOTE 2);

g) Potentially hazardous conditions of the product that could result in potential hazardous situations in the interoperable environment, including those resulting from:

1) Control actions of the product;

2) Data or operational instructions communicated to operators by the product; and

3) Data and commands communicated to external products by the product.

h) Usability and security considerations in the interoperable environment;

i) Potential risk controls, such as actions by external products available in the development context of use; and

j) Any other aspects of interactions with the product in the technical context relevant to assuring safe and secure interoperability.

NOTE 1: External products may include existing technology platforms, electronic medical records systems, pharmacy management systems, and other interoperable products used in the clinical environment.

NOTE 2: Interoperability constraints may include data constraints, temporal ordering constraints, input/output relationships, exceptional behaviors, fault propagations, mitigations, and appropriate identification of attributes relevant to interoperability of the interoperable medical product within the interoperable environment.

Also see AAMI/UL 2800-1-2.

9.1.4 Interoperable use specification

9.1.4.1 Information on the interoperability context of use and reuse shall be controlled and maintained as interoperable use specifications and include:

a) A summary description of the scope of interoperability of the interoperable medical product;

b) A summary description of the interoperable environment (including external products) within which the interoperable medical product is intended to be used; and

c) Important constraints of the interoperability of the interoperable medical product (see 9.1.2 and 9.1.3), including constraints related to SSO (see the SSO in AAMI/UL 2800-1-1) and release criteria with respect to them [see 13.1.2(a)].

NOTE 1: Interoperable use specification may include statements of user needs or specific market requirements for the product. In some cases this information may be captured in a Market Requirements Document.

NOTE 2: The interoperable use specification is an input to interoperability realization activities and in determining the interoperable application specification (see Section 13). Statements related to intended use may be included in the interoperable application specification.

9.2 Interoperability specification

9.2.1 The organization shall establish specifications for interoperable items that comprise the interoperable medical product related to the scope and purpose of the interoperability of the interoperable medical product.

NOTE: Interoperability specifications may be developed and refined as realization activities for the interoperable medical product proceed (see Sections 9 – 11).

9.2.2 Interoperable Item Interoperability Specifications shall include specifications related to the context of use and reuse determined in 9.1, including:

a) Interoperability functional and performance specifications required to meet the interoperable use specifications (see 9.1.4) of the interoperable medical product, including:

1) Specifications derived from the clinical interoperability aspects determined for the interoperable medical product (see 9.1.2), including the clinical purpose and function and actual conditions under which the product is intended to be used; and

2) Specifications derived from technical interoperability aspects determined for the interoperable medical product (see 9.1.3), including application, function, and performance of the interoperable medical product and situations in which the interoperable medical product is intended to be integrated into operational contexts.

b) Specifications or criteria for meeting interoperability SSO (see AAMI/UL 2800-1-1) and the role of the interoperable medical product in supporting interoperability in interoperable medical systems;

c) Specifications to meet statutory and regulatory requirements applicable to the interoperable medical product;

d) Specifications to meet external references (See NOTE);

e) Specifications arising from release criteria;

f) Specifications arising from risk controls or risk acceptance criteria; and

g) Any other specifications related to meeting SSOs of the interoperable medical product in the interoperable environment.

NOTE: External references may include external reference architectures, nomenclature frameworks, design standards or codes of practice.

9.2.3 Interoperable Item Interoperability Specifications shall include contractual or other requirements of the interoperable environment; including those related to:

a) Design, development, and integration of interoperability function and performance; and technical characteristics of the interoperable medical product required by the interoperable environment;

b) Provisioning and deployment of the interoperable medical product required for application in the interoperable environment;

c) Installation, maintenance, monitoring and incident response during operation of the interoperable medical product in the interoperable environment;

d) Testing, including qualification and acceptance testing for the interoperable medical product; and

e) Traceability to release criteria specifically required by the interoperable environment.

9.2.4 Interoperability specifications shall be adequate for realization purposes, complete, and unambiguous, and include as applicable:

a) Interoperable use specification (see 9.1.4);

b) Architecture, interface, and interaction specifications (see 9.3);

c) Sourcing specifications (see Section 10, Interoperability of Externally Sourced Products);

d) Provisioning and deployment specifications (see Section 11, Provisioning, Deployment, and Operation); and

e) Interoperable application specification (see Section 12).

9.2.5 Conflicting specifications shall be resolved.

9.3 Interoperability topology

9.3.1 General

9.3.1.1 The interoperability topology of the interoperable medical product shall be developed and specified and include the architecture, boundaries, and interaction points of the interoperable medical product and anticipated and specified external products within the interoperable environment.

NOTE: The topology may be developed at a high level initially and determined with greater granularity as realization activities proceed.

9.3.1.2 In developing the topology, the following shall be considered:

a) Interoperability context of use and interoperable use specifications (see 9.1);

b) Interoperability specifications (see 9.2);

c) Boundary requirements;

d) Applicable or required external reference architectures;

e) Statutory and regulatory requirements;

f) Standards or codes of practice that the organization has committed to implement; and

g) Requirements arising from risk concerns (see SSOs in AAMI/UL 2800-1-1) and risk controls, usability, and security.

9.3.2 Architecture specification

9.3.2.1 Information on the interoperability architecture shall be controlled and maintained as one or more product architecture specifications and include:

a) Specification of the interoperable medical product boundary;

b) The organization of relevant architectural elements including the interoperable medical product, external products, and constituent interoperable items;

c) The identification of reusable architectural elements and the manner of reuse;

d) The interaction points (see 9.3.2.2) and scope of interactions among the architectural elements and actors (see 9.3.4);

e) Any aspects that are dynamically configured during deployment or operation, including those for reusable elements;

f) Aspects that are derived from risk concerns (see SSOs in AAMI/UL 2800-1-1); and

g) Aspects required to demonstrate traceability to release criteria.

9.3.2.2 Product architecture specifications shall ensure responsibilities and governance rules for dynamic configuration are unambiguous and provide for resolution of conflicts. See the Annex for Architecture Definition Guidance in AAMI/UL 2800-1-3 for more information.

9.3.3 Interface specification

9.3.3.1 Information on interfaces shall be controlled and maintained as one or more product interface specifications and include:

a) Identification and characteristics of interfaces between the interoperable medical product and the interoperable environment, including external products and actors;

b) Identification and characteristics of interfaces between constituent interoperable items;

c) Identification and characteristics of reusable interfaces and interaction points; and

d) Specification of interface contracts.

NOTE: See AAMI/UL 2800-1-2 for details.

9.3.3.2 Interface specifications shall ensure unintended interference among the architectural elements are restricted. See the Annex for Interoperability Architecture Specification in AAMI/UL 2800-1-3 for more requirements.

9.3.4 Interaction specifications

9.3.4.1 Interaction specifications shall include:

a) Identification of interaction points;

b) The initiator of interactions;

c) The temporal characteristics of interactions, including:

1) The periodicity or aperiodicity of the interaction; and

2) Anticipated bounds on response times.

d) Authorization of entities to participate in interactions;

e) The characteristics of data and control information exchanged;

f) Changes in item states or modes that result from interactions; and

g) Conceptual assumptions and guarantees for pre- and post-interaction conditions.

9.3.4.2 Interaction specifications shall ensure that unintended interactions are controlled, including by restricting interactions to specified interfaces (see 9.3.3).

9.4 Implementation for reusability

9.4.1 General

9.4.1.1 Design and development of interoperability of the interoperable medical product shall include, as appropriate:

a) Development of interoperable medical products that are reusable and can interface with external products in an interoperable environment;

b) Development of constituent interoperable items required for reuse;

c) Integration of constituent interoperable items into the interoperable medical product;

d) Development and deployment of applications, including configurations and settings for the interoperable medical product;

e) For applications intended to be assembled (see NOTE), specification of specified external products that are reusable with the interoperable medical product in an interoperable environment; and

f) Assembly of reusable interoperable medical products, including specified external products, and other anticipated external products into the interoperable environment.

NOTE: Applications may be deployed using a base interoperable medical product and various reusable external products. In such cases, the interoperable medical product may be referred to as a "platform" interoperable medical product.

9.4.1.2 Externally sourced products that are constituent interoperable items shall be controlled (see Section 10, Interoperability of Externally Sourced Products).

9.4.1.3 Design and development for reusability shall ensure that:

a) The interoperable medical product meets its interoperable use specifications (see 9.1.4);

b) The interoperability characteristics of the interoperable medical product meet interoperability specifications (see 9.2);

c) Constituent interoperable items support the interoperable medical product scope;

d) Specified and anticipated external products support the interoperable medical product scope; and

e) The interoperable medical product, constituent interoperable items, and anticipated and specified external products are consistent with applicable architectures and meet the Interface Specifications (see 9.3).

9.4.2 Reusability

9.4.2.1 Design and development of interoperability of the interoperable medical product shall ensure that:

a) Mechanisms are provided for [element, operator, and code] partitioning, protection, isolation, and resource reservation (e.g., memory, time, bandwidth, and all other necessary resources for application execution and communication).

b) Communication mechanisms are provided that have the reliability, timeliness, and quality of service necessary to meet specifications.

c) The process model (model of the state of the interoperable environment) of the interoperable medical product is accurate.

d) Means to maintain integrity and authenticity of data and code (in transit) and protects it from unauthorized alteration.

e) Interactions are limited to declared interfaces to eliminate interference between components.

f) Means are provided to expose timeliness information to external products and operators.

9.4.2.2 Data management for interoperability of the interoperable medical product shall ensure that:

a) The name space of data and objects is appropriately managed; and

b) Data and objects are correctly and unambiguously identified and verified to originate from the claimed source (the identity of the correctly and unambiguously identified source is authenticated, as well as the authorship of the source of the data or objects).

9.4.2.3 Identification controls for interoperability of the interoperable medical product shall ensure that suitable means are provided to identify appropriate elements.

9.4.2.4 Access controls for interoperability of the interoperable medical product shall ensure that:

a) Suitable means are provided to identify operational accounts;

b) Role-based access and secure login is provided; and

c) Logout, including automatic logout after set time is provided.

9.4.2.5 Data protection for interoperability of the interoperable medical product shall ensure that suitable factory-set defaults are provided along with options to change default settings.

9.4.2.6 Design and development of interoperability of the interoperable medical product shall ensure adequate controls for risk arising from faults, including ensuring that:

a) Unsafe control actions are avoided;

b) Failure modes including fail-safe (fail-stop) or fail-operational (fault tolerant) exhibit determinism with respect to their risk-associated state (all failures result in a risk-addressed states);

c) Time synchronization mechanisms assure that the response time of the interoperable medical product is adequate to control the development of a hazard into an unsafe control action;

d) Failure of application execution and communication are logged and communicated to the operator (explicitly or implicitly); and

e) Mechanisms are provided for establishing traceability of adverse event to root causes.

10 Interoperability of Externally Sourced Products

10.1 Control of externally sourced products

10.1.1 The organization shall control interoperability from externally sourced products when:

a) Externally sourced products are incorporated into the organization's interoperable medical products;

b) Externally sourced products are provided directly to user(s) by external providers on behalf of the organization; and

c) Externally sourced products are used as a result of a decision by the organization (see NOTE).

NOTE: This may happen for example when the organization specifies the use of a particular product of type of product in the product's interoperable application specification (See Section 12, Testing and Review).

10.2 Sourcing specifications

10.2.1 Specifications relevant to interoperability of the externally sourced product shall be developed, reviewed for adequacy, and communicated to external providers, including:

a) Topology specifications relevant to the externally sourced product (See 9.3);

b) Connectivity of externally sourced product with the interoperable medical product (see 9.4, Implementation for reusability);

c) Communications technologies to be used by the externally sourced product (see 9.4, Implementation for reusability);

d) Specifications relevant to Integration of the externally sourced product (see 9.4, Implementation for reusability);

e) Provisioning and deployment of the externally sourced product (see Section 11, Provisioning, Deployment, and Operation);

f) Testing specifications required for qualification of externally sourced product (see Section 12, Testing and Review), including specifications for:

1) Conformance testing, and

2) Integration testing;

g) Specifications related to performance monitoring of externally sourced product; and

h) Ongoing responsibilities for operation and maintenance (see 10.4).

10.3 Verification and validation of externally sourced products

10.3.1 Externally sourced products shall be appropriately verified and validated (see 12.1.2 and 12.2.2).

10.4 Responsibility for ongoing operation and maintenance

10.4.1 General

10.4.1.1 For externally sourced products with potential for emergent risks during operation and maintenance, a responsibility agreement shall be established with external providers as appropriate to the risks associated with the externally sourced product.

10.4.2 Responsibility agreement

10.4.2.1 Disclosed information in a responsibility agreement shall include, as appropriate:

a) The planned context of use or reuse for the externally sourced product;

b) The intended use cases and environment, including if applicable the clinical application phase(s), if appropriate;

c) The required interoperability capabilities and performance levels (see NOTE 1);

d) Requirements relevant to installation, configuration and settings, deployment, and maintenance;

e) Requirements for handling and controlling data;

f) Requirements for maintenance and contingency actions, including:

1) Incident response; and

2) Mechanisms for secure code updates.

g) Other requirements relevant to assuring safe and secure interoperability of interoperable medical product.

NOTE 1: Capabilities may include specific features such as required modes or operation, compatibility, and data logging capabilities. Performance levels may include quantitative metrics such as data transmission rates, image resolution, memory capacity, and response times.

NOTE 2: See the Standard for Application of Risk Management for IT-Networks Incorporating Medical Devices – Part 1: Roles, Responsibilities and Activities, IEC 80001-1, for more information on Responsibility Agreements.

11 Provisioning, Deployment, and Operation

11.1 Provisioning, deployment, and operation specifications

11.1.1 The organization shall determine specifications for provisioning, deployment, training, and operation of its interoperable medical product taking into consideration:

a) The interoperability characteristics of the interoperable medical product;

b) The use of suitable or specified infrastructure or other elements for the deployment and operation of the interoperable medical product within an interoperable environment;

c) The authorization of competent operators, including any required qualification;

d) The implementation of actions to prevent human error;

e) The implementation of release, setup, and de-installation activities, include maintenance and normal operation, upgrades, change-outs to components or devices; and

f) Resource conflicts/resolution, resource sharing for multiple applications.

11.2 Clinical deployment

11.2.1 Clinical deployment shall consider:

a) Procurement specifications for the interoperable medical product and any required external products, including contracted configurations;

b) Acceptance specifications, including implementation of representative configurations and testing requirements;

c) Installation in accordance with the interoperable application specifications of the interoperable medical product;

d) Application readiness requirements; and

e) Deployment and monitoring.

11.3 Operation

11.3.1 Operation of the interoperable medical product in the interoperable environment shall ensure that:

a) The communication mechanisms in the interoperable environment have the reliability, timeliness, and quality of service necessary for specified applications, including management of alarms and timely display of data;

b) Timeliness, availability and reliability of the interoperable medical product in an interoperable environment is adequate for specified applications and information on the performance on these aspects is communicated within the interoperable environment, as appropriate;

c) Provenance of data provided to the interoperable medical product is verified;

d) The integrity, authenticity, confidentiality, and privacy of data, including protected health information, provided to the interoperable medical product is maintained during operation, including in transit and protected from unauthorized alteration;

e) Identification is verified for patients, operators and external products that interact with the interoperable medical product; and

f) Physical and electronic access to the interoperable medical product is controlled, including adequate management of access by operators, and for updating the interoperable medical product through patches.

See the Annex for Services for Interoperable Medical Systems in AAMI/UL 2800-1-1 for more information regarding operation of alarm management systems.

12 Testing and Review

12.1 Testing to interoperability specifications

12.1.1 Verification of product

12.1.1.1 Testing, inspection, or analyses shall be performed to verify that interoperability of the interoperable medical product meets interoperability specifications for the interoperable medical product (see 9.2).

12.1.1.2 Testing to interoperability specifications shall ensure the following:

a) All Interaction points (see 9.3) are exercised by test interactions; and

b) All interactions trace to relevant interaction points.

12.1.2 Verification of constituent interoperable items

12.1.2.1 Testing, inspection, or analyses shall be performed to verify that interoperability of any constituent interoperable item meets its interoperability specifications (see 9.2).

12.1.2.2 Verification shall include suitable stages of integration of constituent interoperable items into the interoperable medical product.

12.1.3 Verification of configurations with external products

12.1.3.1 Testing, inspection, or analyses of external products shall be performed to verify that interoperability of external product meets provisioning specifications.

12.1.3.2 Verification shall include sufficiently representative specified and anticipated external products and their applicable configurations.

12.1.4 Verification of externally sourced product

12.1.4.1 Testing, inspection, or analyses of externally sourced products shall be performed to verify that interoperability of externally sourced product conforms to specifications for the externally sourced product (see 10.2.1) prior to use.

12.1.4.2 Verification shall include applicable configurations of externally sourced products.

12.1.5 Verification of applications

12.1.5.1 Testing, inspection, or analyses of applications and their configurations shall be performed to verify that the application has met interoperable application specifications prior to deployment.

12.1.5.2 Testing shall be conducted on configurations using representative provisioning of the interoperable medical product.

12.1.5.3 Readiness of application configurations shall be verified prior to deployment.

12.1.5.4 Readiness testing of shall be conducted using representative settings of the interoperable medical product.

12.2 Testing for suitability to context of use

12.2.1 Validation of product

12.2.1.1 Testing for suitability to context shall be performed to assure that the interoperability of the interoperable medical product is suitable for the context of use (see 9.1) and meets its interoperable use specifications (see 9.1.3).

12.2.1.2 Testing for suitability for the context shall be conducted on representative interoperable medical product in a representative interoperable environment and include all the medical and interoperability functional goals are exercised by the interactions, and interactions trace to relevant functional goals.

12.2.1.3 validation testing shall include confirmation that traceability of adequate evidence to release criteria for specified applications has been met when the interoperable medical product is deployed in an interoperable environment.

12.2.2 Validation of external products

12.2.2.1 Performance of external products shall be validated to be suitable for specified technical and functional performance.

12.2.2.2 Validation shall include representative configurations of the interoperable medical product.

12.2.3 Validation of externally sourced product

12.2.3.1 Performance of externally sourced products when integrated into the interoperable medical product shall be validated to be suitable to specified functional or technical performance (see 10.2.1).

12.2.3.2 Validation of externally sourced products shall include representative configurations of the product.

12.3 Interoperability implementation review and change control

12.3.1 At suitable stages, evaluation of the interoperability of the interoperable medical product shall be performed to assess whether interoperability specifications are being met and establish that traceability to Release Criteria is being met for specified applications.

12.3.2 Changes made during, or subsequent to, the interoperability of the interoperable medical product, any sourcing, provision and deployment aspects, including changes to specifications and release criteria, shall be identified, reviewed, and controlled, to the extent necessary to ensure that there is no adverse impact on the ability to assure safe and effective interoperability.

12.3.3 Controlled information on changes shall be maintained (see 6.2) and include the following:

a) The results of reviews;

b) The authorization of the changes; and

c) The actions taken to prevent adverse impacts.

12.3.4 Information on changes made after market release or release for specified application shall be disclosed (see 6.2) as appropriate or in accordance with responsibility agreements (see 10.4).

13 Traceability and Release

13.1 General

13.1.1 Prior to market release of the interoperable medical product, or release for specified application in the interoperable environment, the organization shall establish adequate evidence of traceability demonstrating that the interoperability of the interoperable medical product meets interoperability objectives for SSOs in AAMI/UL 2800-1-1 for the specified application.

13.1.2 Release criteria shall be established, including detailed criteria with respect to applicable interoperability objectives (see the SSOs in AAMI/UL 2800-1-1).

13.1.3 Adequate and objective evidence through a traceability analysis that the interoperability of the interoperable medical product meets release criteria shall be established.

13.1.4 For any specified application or intended use of the interoperable medical product, release criteria shall be established to include:

a) Interoperability capabilities and performance claims stated in an interoperable application specification (see 13.2);

b) Systematic argumentation regarding the claims, including traceability to SSOs in AAMI/UL 2800-1-1 and interoperability specifications (see 9.2);

c) Relevant evidence to support the argumentation;

d) Assumptions made in the argumentation; and

e) The decision that the implementation is acceptable with respect to applicable SSOs.

13.1.5 To the extent appropriate, traceability and release information shall be included in the interoperable application specification (see 13.2).

NOTE 1: See the Annex for Guidance on Release Criteria in AAMI/UL 2800-1–2 for more information.

NOTE 2: Traceability to release criteria may be used to demonstrate compliance with regulatory requirements.

13.2 Interoperable application specification

13.2.1 As part of market release, communications with stakeholders that use or specify the use of the organization's interoperable medical product shall include an interoperable application specification.

13.2.2 Disclosed information in an interoperable application specification shall include, as appropriate:

a) Information on key features of the interoperable medical product;

b) Information on interoperability capabilities, including any claims of capabilities;

c) The specified application of the interoperable medical product, including as appropriate:

1) Clinical applications; and

2) Technical applications.

d) Context for appropriate or specified application, including as appropriate:

1) Clinical indications; and

2) Technical functions.

e) Information required for safe, secure and effective use, as applicable, including but not limited to:

1) Requirements for provisioning with external products, including anticipated and specified external products;

2) Instructions relevant to installation, configuration and settings, deployment, and maintenance for specified application;

3) Instructions for operational monitoring, maintenance, and contingency actions during specified application;

4) Information required for risk control during specified application;

5) Information for handling and controlling data, including management of privacy and security, during specified application; and

6) Information for providing feedback, including incident notifications.

14 Interoperability Performance Monitoring and Control of Changes

14.1 Performance evaluation and monitoring

14.1.1 The interoperability performance of the interoperable medical product shall be monitored and evaluated for continued interoperability, including, as appropriate, monitoring of emerging risks to safety and security when the interoperable medical product is used in an interoperable environment.

14.1.2 The following shall be determined for monitoring:

a) The interoperability performance aspects to be monitored and measured;

b) The methods for monitoring, measurement, analysis and evaluation needed to ensure valid results;

c) The operational points when the monitoring and measuring shall be performed; and

d) The frequency of analyses and response to the results from monitoring and measurement.

14.2 Information from monitoring

14.2.1 Monitoring activities shall ensure the following, as applicable:

a) The identity and status of the elements of the interoperable environment are logged as determined in 12.1.2;

b) Actions taken and any modification of those actions by the interoperable medical product or any element or operator in the interoperable environment are unambiguously traceable to their origin;

c) Modifications by an element/operator to data/objects within the system are unambiguously traceable to that element/operator. These modifications shall be logged;

d) Performance issues of the elements in the interoperable environment are logged as determined in 12.1.2, including:

1) Connectivity issues;

2) Security vulnerabilities;

3) Operational performance such as speed;

4) Data management issues;

5) Information about other incorporated components; and

6) Information about similar interoperable medical systems.

e) Failures of interoperable medical product interoperability in an interoperable environment are logged and communicated to the operator, either explicitly or implicitly.

14.2.2 If information from monitoring indicates significant imminent risk to safety and security, an incident response (see 12.3) shall be initiated.

NOTE: Relevant aspects may be included in responsibility agreements (see 10.4.2).

14.2.3 The information gathered from monitoring shall serve as potential input into risk management during design and development of interoperability (see Section 9, Design, Development and Implementation of Interoperability) and improvement (see Section 15, Improvement of Processes).

14.2.4 Appropriate information shall be communicated to the stakeholders in the interoperable environment through appropriate disclosures.

14.3 Incident response

14.3.1 Monitoring information shall be investigated for indications of actual or potential occurrence of an incident or condition representing current or imminent significant risk to safety and security.

14.3.2 Identified incidents or conditions shall be responded to, including:

a) Evaluating the role of products or services in contributing to the incident or condition, including:

1) Interoperable medical products provided by the organization; and

2) External products in the interoperable environment.

b) Determining and taking immediate actions as appropriate;

c) Determining and communicating relevant information within the organization;

d) Determining and communicating relevant information within the interoperable environment, through appropriate disclosures;

e) Determining and implementing appropriate actions required by regulations; and

f) Determining the need for and initiating improvements (see Section 15, Improvement of Processes).

14.3.3 If it is determined that no response is required, controlled information shall be maintained on the justification.

14.3.4 Incident response records shall be maintained (see 6.2).

15 Improvement of Processes

15.1 Any changes necessary to ensure and maintain the continued suitability, adequacy and effectiveness of the processes for assuring safe and secure interoperability shall be identified and implemented.

15.2 Opportunities for improvement in the Interoperability ecosystem shall be determined, as appropriate, and necessary actions shall be implemented, including:

a) Improving disclosures to better communicate aspects required for safe and effective interoperability;

b) Improving interoperable medical products to better meet interoperability objectives as well as to address future needs and expectations;

c) Correcting, preventing or reducing undesired performance, including mitigation of safety and security risks;

d) Improving the performance and effectiveness of the interoperability management and realization processes.

NOTE: Examples of improvement can include correction of the interoperable medical product, corrective and preventive action to improve the ability of the interoperable medical product to meet objectives, continual improvement, breakthrough change, and innovation of the interoperable medical product and re-organization or processes.

Annex A
(Informative)
Stakeholder Activities

A1 Development Context Activities

A1.1 Interoperable item development

A1.1.1 Interoperable item development is the activity of developing and assuring an interoperable item that may contribute to the behavior of one or more interoperable medical systems. This includes:

a) Specifying the boundary of the interoperable item in terms of interaction points and interfaces;

b) Developing interoperable item SSOs as appropriate and that provide the goals for the risk controls to be implemented by the interoperable item (See AAMI/UL 2800-1-1 for Candidate SSOs);

c) Developing interoperability-related requirements that refine the interoperable item SSOs and reflect the interoperable item's medical and technical context of use as specified in its use specification.

d) Developing an item interoperability specification that:

1) Includes interface specifications and contracts on those interfaces that refine the interoperable item requirements down to interface interaction constraints and that capture the external measures that the interoperable item needs in the usage context to adhere to ensure that the interoperable item SSOs are satisfied;

2) Specifies information oriented around the interoperable item interfaces including error propagation and risk control specifications sufficient for supporting risk analysis and risk control information by any item integration activities (see Annex D);

3) Is exchanged with other stakeholders to reflect the disclosed characteristics of the interoperable item that can be relied on when using the interoperable item (See the Annex for Guidance on Interoperability File of AAMI/UL 2800-1-2 and the Annex for Guidance on Disclosure of AAMI/UL 2800-1-2); and

4) Provides the interoperable item characteristics that will be used to determine compliance with this Standard;

e) Developing a realization of the interoperable item;

f) Collecting evidence of conformance of the interoperable item realization to the item interoperability specification via testing, artifact inspection, and process audits;

g) Developing instructions for integrating the interoperable item in its development context of use and deploying and operating the interoperable item in its deployment context of use; and

h) Providing arguments and evidence satisfying release criteria (see the Annex for Guidance on release criteria of AAMI/UL 2800-1-2) that the interoperable item realization conforms to its item interoperability specification. This last activity represents the primary objective of the interoperable item development.

A1.1.2 To support an arbitrarily deep architectural hierarchy, an interoperable item may have constituent interoperable items or may be an interoperable item that is not further decomposed for the purposes of interoperability and compliance to this Standard. Common examples of interoperable items that are units include:

a) Medical equipment with capabilities supporting interoperability;

b) Equipment including infrastructure components supporting communication (networking), hosting of application logic, and reusable safety service products, e.g., data loggers; and

c) Application logic, including "software only" products, that utilize infrastructure and medical equipment components to realize medical functions not achieved by the individual components.

See the Annex for Architecture Definition Guidance of AAMI/UL 2800-1-3 for additional examples and guidance for applying the topological vocabulary of this Standard.

A1.1.3 Interoperable medical systems are special cases of interoperable items that are composed of constituent interoperable items and that have a medical intended use. The recursive nature of the definition of interoperable item enables an interoperable medical system to be a constituents of other interoperable items or interoperable medical systems. This allows flexibility in the possible architecture and reuse of products addressed by this Standard, and supports the notion of "system of systems".

A1.1.4 It is understood that interoperable items are designed for reuse in multiple system contexts where assurance is required, and therefore a primary goal of the interoperable item development activity is to follow an approach that supports not only the reuse of the product's implementation but the reuse of risk management and assurance work products as well.

NOTE: The details of activities associated with Interoperable Item Development can be found in AAMI/UL 2800-1-2. Work products associated the activity are described in the Annex for Guidance on Interoperability File of AAMI/UL 2800-1-2. Release criteria that capture the important traceability relationships between the interoperable item Development Activity work products are found in the Annex for Guidance on release criteria of AAMI/UL 2800-1-2.

A1.2 Interoperable item integration

A1.2.1 interoperable item integration is the activity of engineering the exchange of data and control information between two or more interoperable items using the designed interoperability interfaces of the items. This includes the activities of:

a) Assessing the use specifications and item interoperability specifications (especially, the interface contracts) of the interoperable items to be integrated to determine their compatibility;

b) Realizing the appropriate architecture and engineering contexts required by the interoperable items, including designing and implementing needed connectivity medium between interoperability interfaces;

c) Configuring the interoperable items and constraining the interactions between interoperable items to ensure that interface contracts, including external measures specified by each interoperable item as captured in disclosures, are satisfied;

d) Carrying out hazard analysis and risk assessment of the engineered connectivity solution and use of interoperable item interfaces, using the risk-related information captured in item interoperability specifications;

e) Establishing integration verification plans to provide evidence of correct integration of the interoperable items;

f) Establishing instructions for assembly of the interoperable items in the deployment context of use and procedures for field testing to establish that an installed integration conforms to the integration claims; and

g) Constructing arguments and objective evidence that satisfy Release Criteria (see the Annex for Guidance on Release Criteria of AAMI/UL 2800-1-2) for the correctness of the integration of the items and the appropriate identification of risk controls that are the responsibility of the users in the context that the integration supports.

A1.2.2 The interoperable item-level integration activity does not speak to the top-level safety and security objectives associated with the context into which the integration is place. Instead, it focuses on the engineering objectives associated with the appropriate use of the interoperability interfaces of the

components. The task of arguing that the integration assurance appropriately supports top-level safety and security objectives falls to interoperable medical system development activity (as a special case of the interoperable item development activity).

A1.2.3 Interoperable item integration is distinct from interoperable item assembly according to the objectives and activities outlined above: the interoperable item integration activity leads to products subject to compliance with this Standard and should be carried out by engineers with appropriate competencies in interfacing technology, system risk management, and verification; interoperable item assembly addresses connecting items in the field whose integration has been previously assured, and carrying out confirmation measures designed during item integration to confirm that items have been deployed and are performing according to the integration plan.

NOTE: The details of activities associated with interoperable item integration can be found in AAMI/UL 2800-1-3. Work products associated the activity are described in the Annex for Guidance on Interoperability File, AAMI/UL 2800-1-2. Release criteria that capture the important traceability relationships between the interoperable item development activity work products are found in the Annex for Guidance on Release Criteria of AAMI/UL 2800-1-2).

A1.3 Interoperable medical system development

A1.3.1 Interoperable medical system development is the activity of engineering a system constructed from at least two interoperable items that comply with this Standard, to achieve one or more medical functions. An interoperable medical system provides a cohesive set of functions whose safety and security will be addressed as an aggregate.

A1.3.2 In the architectural topology (see the Annex for Architecture Definition Guidance of AAMI/UL 2800-1-3), an interoperable medical system is a special case of an interoperable item, thus the activities associated with interoperable item development apply to interoperable medical system development.

A1.3.3 Since an interoperable medical system includes two or more interoperable items, interoperable medical system development will typically include activities associated with interoperable item integration.

A1.3.4 An interoperable medical system will typically include one or more interoperable items (often implemented in software) that provide the application logic defining the behavior of the medical functions of the system. The interoperable item development activities associated with application logic items may or may not be carried out by the same entity that carries out the interoperable medical system development activities. The partitioning of activities described here aligns with the conventional approach of distinguishing software development from system development. interoperable medical system development activities will typically include interoperable item integration activities integrating application software Items in a system context that provides an execution environment for the software as well as other Items that provide services necessary for the overall system functionality to be achieved. In this activity, representative realizations of the constituents of the interoperable medical system may be used in verification of a specific constituent interoperable item with appropriate notions of coverage.

It may be the case that some of the constituents in the interoperable medical system were integrated in a previous activity distinct from the current system development effort. In such cases, the interoperable medical system activities are expected to provide the work products associated with that previous effort including integration assurance and arguments that the previous integration assurance is suitable for the current system context.

A1.3.5 In addition to the interoperable item development and interoperable item Integration activities above, interoperable medical system development includes the activities of:

a) Delimiting the specific set of medical functions that will be the subject of evaluation as part of determining compliance to this Standard.

b) Identifying the set of interoperable medical system interoperability architecture instances resulting from possible exchange of constituent interoperable items (e.g., replacing one interoperable medical device with another that provides like functionality) that are to be addressed in the evaluations associated with determining compliance to this Standard.

c) Identifying the top-level hazard situations associated with the interoperable medical system functions and using those as the risk concerns that drive the risk management process associated with interoperable item development (where the interoperable medical system is the product being addressed as a special case of the interoperable item development activity).

A1.4 Interoperability framework management

A1.4.1 Development and reuse of interoperable items may be supported by an organizational infrastructure, engineering and technology asset base, and assurance measures leading to trustworthiness of item reuse and a product-line development approach. interoperability framework activities include defining these elements in a manner that allows review for compliance to this Standard and reuse of the elements in subsequent evaluations. The notion of interoperability framework is specifically designed to address platform-based approaches and interoperability architectures, e.g., as reflected in ASTM F2761 Integrated Clinical Environment.

An interoperability framework may be supported by one or more organizations. In the case of a multi-organization framework, the interoperability framework enables trustworthy-interoperable item interoperability specifications, implementations, and assurance to be reused across organizations in a coordinated approach to development, risk management, and assurance. Interoperable item declarations of development context of use (See AAMI/UL 2800-1-2) enable interoperable item manufacturers to declare alignment with one or more Interoperability Frameworks which enables them to reuse interoperability framework assets with a corresponding commitment to align with development and assurance constraints specified by the interoperability framework.

A1.4.2 Interoperability framework management includes the activities of:

a) Defining the scope of interoperable medical products to be supported by the framework;

b) Defining the reference architecture associated with the framework following guidance in the Annex for Architecture Definition Guidance of AAMI/UL 2800-1-3 and the Interoperability Architecture Specification of AAMI/UL 2800-1-3;

c) Identifying the categories of interoperable items that will be supported by the reference architecture and providing reusable artifacts that speed the development and assurance of items aligned with the framework;

d) Developing and communicating to framework participants the activities necessary to coordinate quality management and risk management across organizations;

e) Providing technology and engineering assets for interoperability platforms including interface specification mechanisms, reusable infrastructure component implementations that comply with this Standard;

f) Declaring a mapping of development activities to interoperable items associated with the framework reference architecture;

g) Developing guidance (possibly in the form of release criteria) that clarifies the assurance objectives and corresponding assumed external measures for each interoperable item in the framework reference architecture;

h) Developing acceptance criteria including testing for determining if item interoperability specifications and realizations are aligned with the interoperability framework.

A2 Deployment Context Activities

A2.1 Interoperable item acquisition/business management

A2.1.1 Interoperable product technical administration focuses on defining the user needs and technical requirements of the customer organization. This includes the activities of:

a) Documenting the clinical objectives and workflows to be supported by the interoperable medical product (e.g., to determine the appropriateness of the interoperable medical product by assessing its use specification).

b) Documenting the technical needs of the customer organization including characteristics of the other systems and networks with which the interoperable medical product will be integrated.

c) Developing plans and objectives to be addressed by other deployment activities.

A2.2 Interoperable item technical administration

A2.2.1 Interoperable item technical administration focuses on the technical administration of interoperable items (possibly conforming to interoperability frameworks) in their deployment context of use. This includes the activities of:

a) Incorporating interoperable items into the deployment context of use inventory management and carrying out activities related to device identity management;

b) Configuring operator access policies, establishing an appropriate time base, etc. as indicated by the Item manufacturer's documentation of assumed external measures;

c) Performing manufacturer supplied confirmation tests to ensure that interoperable item interoperability functions are performing to specification this includes interoperable item assembly which is a sub-activity of interoperable item technical administration;

d) Integrating interoperable items with entities outside the scope of this Standard, including medical IT systems and the broader medical IT network;

e) Monitoring and tracking of technical anomalies of deployed items, including providing and receiving quality management information from interoperable items;

f) Performing maintenance on interoperable items including apply software updates; and

g) Decommissioning of interoperable items.

A2.2.2 Some activities such as initial deployment and configuration may occur in partnership with interoperable item manufacturers and organizations providing interoperability frameworks.

A2.3 Interoperable item assembly

A2.3.1 Interoperable item assembly, a sub-activity of technical administration, is the activity of (a) connecting interoperable items in the field whose integration has been previously assured and (b) confirming (in ways appropriate for personnel who competencies may not include system engineering or risk management) that behavior achieved by the connected interoperable items corresponds to claims made in the assurance of the corresponding integration.

A2.3.2 Interoperable item assembly may involve one or more of the following activities:

a) Physically connecting previously integrated interoperable items following assembly instructions provided with an interoperable item or interoperability framework;

b) Performing field tests designed by interoperable item Integrators and confirming that results align with expected results; and

c) Exchanging Interoperable Items as allowed by the architecture variability description documented by an interoperable medical system and/or interoperability framework and ensuring that appropriate confirmation tests are performed on the resulting variations.

A2.4 Interoperable item clinical administration

A2.4.1 Interoperable Item clinical administration focuses on the configuration and validation of clinical functions of interoperable items in their deployment context of use.

A2.4.2 interoperable item clinical administration may involve one or more of the following activities:

a) Assessing and configuring interoperable item clinical functionality to align with care-giving guidelines of the Health Delivery Organization (HDO),

b) Identifying "go live" criteria (building on suggested criteria provided by the interoperable item manufacturer) for the interoperable item clinical functionality,

c) Performing acceptance tests of the interoperable item clinical functionality on representative scenarios to ensure that "go live" criteria is satisfied,

d) Coordinating with interoperable item technical administration activities to ensure that instances of the Item are appropriately deployed at distinct points-of-care.

A2.5 Interoperable item operation

A2.5.1 Interoperable item operation focuses on the association of the interoperable item to a patient during a patient episode and operating the interoperable item to provide care for the patient.

A2.5.2 interoperable item operation may involve one or more of the following activities carried out by the operator (these activities may be carried out directly through interactions with the interoperable item or their effect may be achieved indirectly as a result of interacting with an interoperable medical system of which the interoperable item is a constituent):

a) Authenticating the operator for the use of the interoperable item;

b) Initiating and managing a patient episode for the interoperable item including associating and disassociating the patient under care to the interoperable item;

c) Confirming the appropriateness of input data and care-giving instructions to be entered into the interoperable item;

d) Configuring the interoperable item's settings for a particular care-giving procedure for the patient under care;

e) Confirming that the operational context state meets the go-live conditions of the interoperable item and initiating the medical function of the interoperable item;

f) Monitoring the interoperable item's technical alarms and other behavior to recognize failures of the interoperability mechanisms that may impact the interoperable item's safety and security;

g) Providing care to the patient under care utilizing output of the interoperable item; and

h) Realizing risk controls corresponding to the interoperable item's external measures allocated to the interoperable item operation activity.

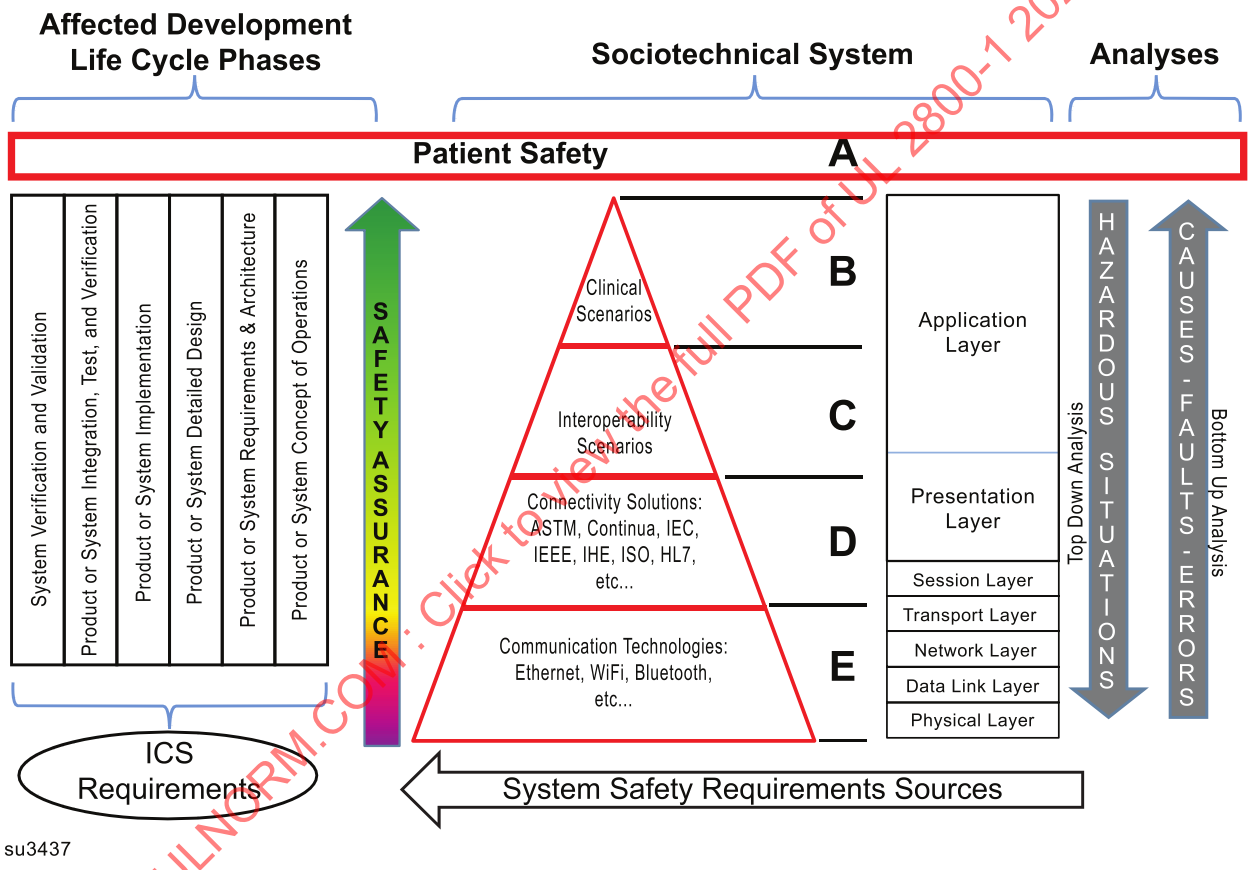
Annex B
(Informative)
Guidance on Declaration of Products and Services

B1 Interoperability Ecosystem

Figure B1.1 shows various layers of products within an integrated clinical system (ICS). For any specific clinical and technical context of use, risks need to be adequately managed as these products, and services associated with them, work together in an interoperable manner.

Figure B1.1

Elements of interoperability ecosystem and key processes



B2 Entities Subject to Compliance Claims

B2.1 This Standard provides for the following categories of products to be subject to evaluation:

a) Interoperable items; and

b) Interoperable medical systems (special case of interoperable item).

The Annex for Architecture Definition Guidance of AAMI/UL 2800-1-3 gives detailed guidance on how different categories of products with interoperability functionality can be presented in terms of the topological structures of interoperable item and interoperable medical system.

B2.2 This Standard provides for evaluation of the following categories of products and services for the purpose of supporting compliance:

a) Interoperability frameworks (including reference architecture and platform infrastructure) for building interoperable medical systems and interoperable items; and

b) Interoperability scenarios specifications.

B2.3 This Standard provides flexibility for claiming compliance for subsets of related work products that represent useful collections of specification or implementation artifacts that support development, assurance, or use of the product categories above.

B2.4 Figure B1.2 illustrates that interoperable items and interoperable medical systems (a system is a special case of a interoperable item in the product topology vocabulary of this Standard – see the Annex for Architecture Definition Guidance of AAMI/UL 2800-1-3) are presented for compliance in terms of a specification, and implementation (realization), and assurance that an implementation satisfies its specification. Artifacts supporting these relationships are recognized as work products (see Annex C) produced by the life cycle processes for this Standard (see the Annex for Guidance on Interoperability File of AAMI/UL 2800-1-2) produced by the life cycle processes for this Standard.