UL 2800-1-3

STANDARD FOR SAFETY

Interoperable Item Integration Life Cycle

UL Standard for Safety for Interoperable Item Integration Life Cycle, UL 2800-1-3

First Edition, Dated June 10, 2022

Summary of Topics

This is the First Edition of ANSI/AAMI/UL 2800-1-3, the Standard for Interoperable Item Integration Life Cycle.

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

No Text on This Page

AAMI
AAMI 2800-1-3
First Edition

Underwriters Laboratories Inc
UL 2800-1-3
First Edition

Standard for Interoperable Item Integration Life Cycle

June 10, 2022

Approved American National Standard

ANSI/AAMI/UL 2800-1-3-2022

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 First Edition. The most recent designation of ANSI/AAMI/UL 2800-1-3 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

No Text on This Page

Preface

This is the joint AAMI/UL Standard for Interoperable Item Integration Life Cycle, AAMI/UL 2800-1-3. It is the first edition of AAMI 2800-1-3 and the first edition of UL 2800-1-3.

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 and security 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 integration lifecycle requirements for assuring safe and secure interoperability of interoperable items assembled or otherwise integrated into interoperable medical systems.

3 Referenced Publications

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/UL 2800-1, *Medical Device Interoperability*

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

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

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

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

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

4 Terms and Definitions

4.1 Defined terms are located in AAMI/UL 2800-1.

5 Interoperable Item Integration Life-Cycle Activities

5.1 Architecture and interoperable item integration concept development

5.1.1 Item interoperability architecture and domain asset instantiation

5.1.1.1 Figure 5.1 provides a schematic representation of the interoperable environment.

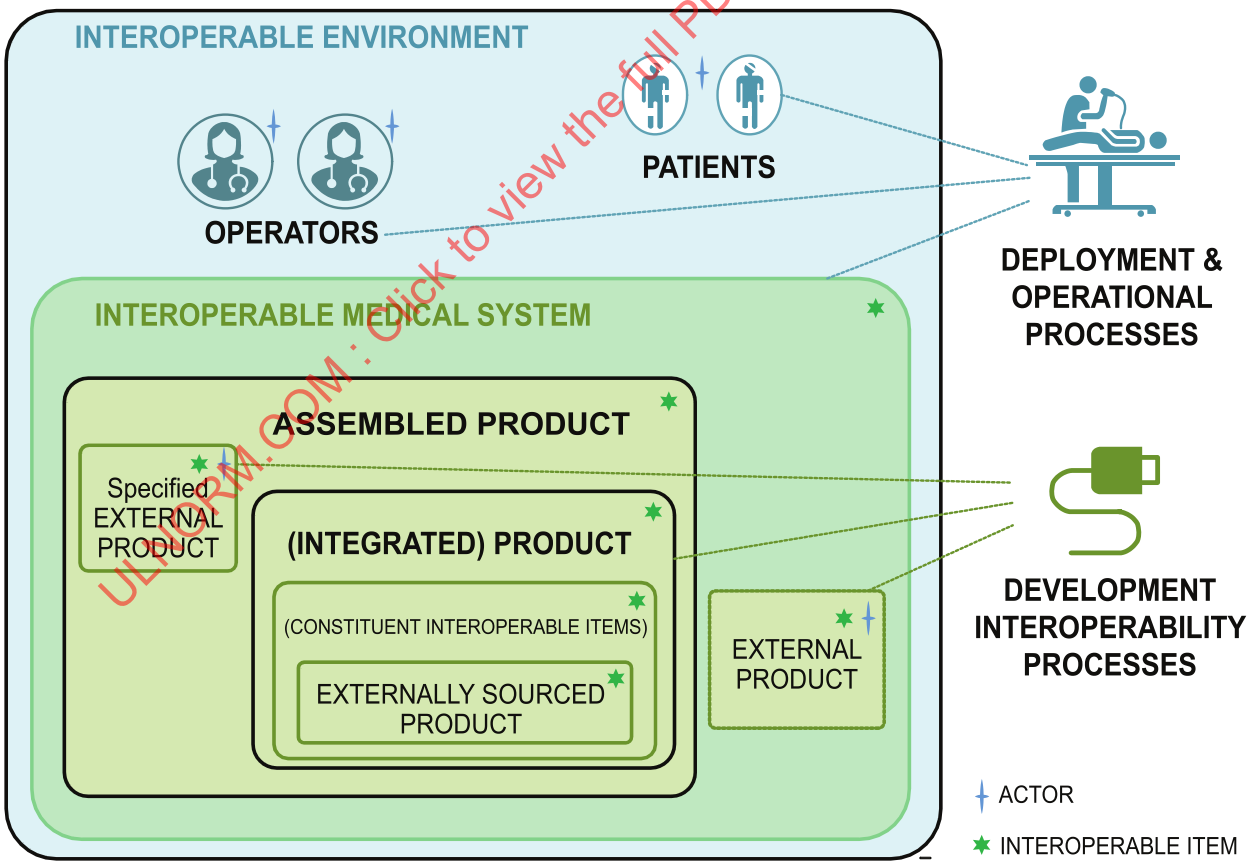
5.1.1.2 The interoperable item boundary definition shall be extended to document the preliminary interoperability architecture (including both external and internal interoperability) of the interoperable item.

5.1.1.3 The preliminary interoperability architecture shall be demonstrated to properly instantiate the reference architecture of the interoperability frameworks with which the interoperable item is to be aligned.

5.1.1.4 The range of interoperability architecture instances to be addressed in the interoperable item assurance arguments, including planned commonalities and variabilities within the architecture, shall be specified in an architecture variability report associated with the interoperability architecture.

Figure 5.1

Interoperable Environment Ontology



su3403a

5.1.2 Interoperable item internal interoperability management

5.1.2.1 The interoperability management plan shall properly instantiate the interoperability management plans of the aligned interoperability framework(s).

5.1.2.2 The interoperability management plan shall be extended to address the internal interoperability of the interoperable item. For each constituent interoperable item in the preliminary interoperability architecture (interoperability view), it shall be indicated if the interoperable item will be internally sourced or externally sourced.

5.1.2.3 For each internally sourced constituent interoperable item implementation, the following shall be specified in the interoperability management plan:

a) An indication if the constituent implementation is a new implementation to be developed, or a previous implementation to be reused; and

b) The interoperability frameworks to which the constituent implementation will claim conformance.

5.1.2.4 For each externally sourced constituent implementation, the following shall be specified in the interoperability management plan:

a) An indication if the constituent interoperable item implementation is a new implementation to be developed, or a previous implementation to be reused; and

b) An indication if the constituent interoperable item implementation shall be conformant with one or more interoperability frameworks.

5.1.2.5 The interoperability management plan shall include criteria for selecting suppliers for externally sourced interoperable items. The selection criteria shall provide a basis for determine a supplier's ability to deliver a compliant item implementation at appropriate levels of quality. development of the criteria shall consider the following:

a) Evidence of the supplier's quality management system and its ability to support products conforming to SSOs;

b) The supplier's past performance and quality;

c) Results of previous compliance to and supplier's participation in interoperability frameworks to which the item manufacturer has declared alignment.

5.1.3 Internal item interoperable interactions (use cases)

5.1.3.1 The interoperable item-context interactions of 5.1.5 shall be extended to show how achieving the interactions with an interoperable item exercises the interaction points of each of the constituent interoperable items.

5.1.3.2 The coverage of the internal interoperability interaction points and internal interoperability bindings shall be assessed.

5.1.3.3 The use cases reflected by the interactions assessed in 5.1.3.2 shall be extended as necessary to obtain complete coverage of the internal interoperability interaction points and internal interoperability bindings declared for use in the specification of interoperable item-context interactions.

5.1.4 Interoperable item preliminary hazard analysis – interoperability-related hazard analysis

5.1.4.1 A preliminary specification shall be developed of the primary failure modes and immediate effects of all constituent implementations and engineering and technology approaches that are used to achieve the internal interoperability bindings in the interoperable item-context interactions.

5.1.4.2 In situations where constituent implementations are externally sourced and information about the failure modes and effects of a constituent interoperable item are unknown:

a) Worst-case assumptions about the item shall be used in the analysis; and

b) Assumptions about the component's risk-related behavior that may be relied on to mitigate worst-case scenario shall be documented.

5.1.4.3 The specification activities in 5.1.4.1 and 5.1.4.2 shall consider the failure modes and effects identified in the preliminary hazard analysis – interoperability related hazard analysis of the interoperability framework reference architectures in aligned interoperability frameworks.

5.1.4.4 Mitigation measures and associated SSOs for each mitigation measure shall be specified.

5.1.4.5 A preliminary hazard analysis shall be performed to determine how component failures and internal interoperability mechanism failures may lead to violations of the interoperable item's SSOs and may contribute to hazardous control actions and data identified in AAMI/UL 2800-1-2.

5.1.4.6 The specification activities in 5.1.4.1 and 5.1.4.2 shall consider the failure modes and effects identified in the preliminary hazard analysis – interoperability related hazard analysis of the interoperability framework reference architectures in aligned interoperability frameworks.

5.1.4.7 The interoperable item's SSOs specified in AAMI/UL 2800-1-2 shall be refined to include any risk controls necessary to address causes of violations uncovered in the preliminary hazard analysis.

5.1.5 Refinement of interoperable item SSOs and development of functional safety concept

5.1.5.1 The SSOs of the interoperable item developed in AAMI/UL 2800-1-2 shall be refined to address failures and errors that may potentially arise from the interoperable item's internal interoperability communication or constituent interoperable item implementations.

5.1.5.2 A functional safety concept shall be developed for the interoperable item that documents how risk controls necessary to achieve the SSOs will be realized within the interoperable item. for each hazardous situation, the functional safety concept shall indicate how the following aspects of risk controls are allocated within the interoperable item:

a) Detection of faults and failures;

b) Decisions about whether or not to act or notify concerning the fault/failure, and associated response times;

c) Notification functions to operators that are expected to take action to achieve a safe state; and

d) Actions performed within the interoperable item to ensure it is in a safe state.

5.2 Internal architecture and integration specification

5.2.1 Development of internal interoperability architecture and interface specification

5.2.1.1 The internal interoperability architecture of the interoperable item shall be consistent with the preliminary architecture specification of the interoperable item boundary. The internal interoperability architecture shall be specified at a level of detail sufficient for supporting all system-level risk management and assurance activities. See Annex B for guidance.

5.2.1.2 Traceability shall be established between the interoperability architecture of the interoperable item and the internal interoperability architecture specification including variants.

5.2.1.3 Reasonably foreseeable misuses of the internal interoperability architecture shall:

a) Be identified; and

b) Have appropriate controls implemented.

5.2.1.4 Where appropriate, the design reflected in the internal interoperability architecture shall make use of:

a) Components with high-integrity characteristics;

b) Fail-safe functions;

c) Redundancy;

d) Partitioning of functionality; and

e) Defensive design.

5.2.1.5 The conformance of the internal interoperability architecture to the reference architectures from all interoperability frameworks with which the interoperable item is aligned shall be documented and appropriate traceability established.

5.2.1.6 The architecture variability description shall document all architecture variabilities to be addressed in item assurance.

5.2.1.7 For each constituent interoperable item in the interoperability architecture, architectural constraints that constrain the reuse of previous implementations of a constituent interoperable item or the development of a new interoperable item shall be documented.

5.2.1.8 For each externally sourced constituent interoperable item in the interoperability architecture, architectural constraints shall be included in requests for development / responsibility agreements communicated to potential suppliers of the constituent interoperable item.

5.2.2 Development of internal interoperability requirements

5.2.2.1 The interoperability requirements in the item interoperability specification shall be decomposed into integration requirements on the constituent interoperable items within the internal interoperability architecture. The resulting requirements shall be phrased as constraints on the anticipated specifications and interoperability interfaces of the constituent interoperable items as appropriate.

NOTE: For constituent interoperable item integration requirements, see:

1) Guidance from the Annex for Clinical Properties of Interoperable Medical Systems of AAMI/UL 2800-1-1 and 2) Technical and functional safety guidance in the Annex for Engineering Properties of Interoperable Medical Systems of AAMI/UL 2800-1-1.

5.2.2.2 The integration requirements for constituent interoperable items shall include integration requirements from any interoperability frameworks with which the interoperable item is aligned and be traceable to the internal interoperability requirements of the interoperable item that are necessary for the appropriate use of framework assets, safety/security controls, and assurance arguments and evidence.

5.2.2.3 The integration requirements for constituent interoperable items shall include constraints on constituent interoperable item interactions necessary to satisfy the properties of the technical safety concept specified in the development life cycle.

5.2.2.4 The integration requirements for a constituent interoperable item shall be traceable to the allocation of the functional safety concept in the technical safety concept as identified in the risk management activities.

5.2.2.5 The integration requirements for constituent interoperable items shall account for all variabilities in the architecture variability description including:

a) Requirements that may vary for different instances of a constituent interoperable item interface capabilities or a constituent interoperable item implementation capabilities;

b) Mechanisms used to judge if a particular instance of a constituent interoperable item is suitable for integration; and

c) Requirements on when “go live” status is achieved by the integrated components.

5.2.2.6 The integration requirements for a constituent interoperable item shall include constraints on constituent interoperable item interactions and interoperable item-derived context requirements necessary to ensure that failures of the constituent interoperable item or its interoperability mechanism are addressed to the degree justified by the risk management process.

5.2.2.7 The integration requirements for a constituent interoperable item shall clearly identify integration obligations that are addressed at different stages in the item life-cycle including:

a) Obligations to be met during interoperable item integration activity;

b) Obligations to be met during different stages of acceptability testing and deployment in the deployment context of use; and

c) Obligations to be met during monitoring phase of the interoperable item life cycle.

5.2.3 Item architecture analysis and risk management activities

5.2.3.1 Data/control flow analysis

5.2.3.1.1 Data/control flows specified in the item data flow analysis between interoperable item inputs and outputs shall be allocated to the constituent interoperable items as end-to-end flows that indicate pathways of the data/control through the constituent interoperable items. The end-to-end flows shall be documented in terms of:

a) Data/controls flows specified for the constituent interoperable item data/control flow analysis, including the specific interfaces supporting the in/out flows for each constituent interoperable item; and

b) Interoperability bindings between constituents.

5.2.3.1.2 The data/control flows documented as originating within the interoperable item as source information flows shall have the sources allocated to relevant constituent interoperable items.

5.2.3.1.3 The data/control flows documented as terminating within the interoperable item as synced information shall have their sync points allocated to relevant constituent interoperable items.

5.2.3.2 Fault and error propagation specification

5.2.3.2.1 Normalization of fault/error categorization

5.2.3.2.1.1 The item fault/error categorizations of all constituent interoperable items in the interoperable item's interoperability architecture and interoperability management plan shall be aligned with fault/error categorizations provided by the interoperable item.

The resulting integration fault/error categorization may have the same properties (e.g. error nomenclature, human readable semantics, etc.) as that for the interoperable item.

5.2.3.2.2 Analysis and reconciliation of interface error behavior at binding points

5.2.3.2.2.1 For each binding point in the interoperability architecture, the error propagation specifications of the bound interoperable items shall be analyzed to determine:

a) The completeness of fault/error propagation/specifications with respect to the operational behavior of interactions occurring at the binding.

b) The compatibility of the fault/error propagation/specifications, including analyses to determine if outward propagating faults/errors of a constituent interoperable item are accounted for in the error propagation specifications in destination constituent interoperable items.

c) The consistency of semantic interpretation of faults/errors across the constituent interoperable items participating in the bindings. Analysis for consistency shall consider the interpretation of out-of-range or corrupted values, violations of timing constraints captured in quality of service contracts, out-of-sequence messages.

d) The compatibility of declarations and assumptions about the likelihood of error occurrences in source and destination sub-items.

5.2.3.2.3 Mapping of interoperable item error propagation specification to constituent interoperable items in the internal interoperability architecture

5.2.3.2.3.1 Error/fault flows, sources, and sinks specified in the interoperable item error propagation specification shall be mapped to the error propagation specifications of the interoperable item in the interoperable item internal interoperability architecture.

5.2.3.2.3.2 An analysis shall be formed to determine the end-to-end error/fault propagations through the interoperable item internal interoperability architecture using the information reflected in the error propagation specifications of the constituent interoperable items. The interoperable item error propagation specification shall be revised to reflect the following outcomes of the analysis:

a) Each end-to-end flow reflected in the error propagation specification through the interoperable item internal interoperability architecture (originating at the boundary of the architecture and terminating at the boundary of the architecture) shall be appropriately abstracted in the interoperable item error propagation specification.

b) Each error source in a constituent interoperable item whose propagation reaches the boundary of the architecture shall be abstracted in the interoperable item error propagation specification as an error source.

c) Each error sink in a constituent interoperable item that terminates an error propagation originating at the boundary of the interoperable item shall be abstracted in the interoperable item error propagation specification as an error sink.

5.2.3.2.3.3 The failure modes declared in the interoperable item error propagation specification shall be mapped to the failure modes of constituent interoperable items in the internal interoperability architecture.

5.2.3.2.3.4 The failure modes and causal events declared in the interoperable item error propagation specification shall be revised as necessary to account for individual failure modes and combinations of failure modes of the constituent interoperable items of the internal interoperability architecture.

5.2.3.3 Control loop analysis

5.2.3.3.1 The control loop structures of the interoperable item shall be allocated to the constituent interoperable item of the internal interoperability architecture and aligned with the internal control loops. The specific interfaces, operations, and data associated with each point at which a path in the control loop crosses a constituent interoperable item's boundary shall be specified.

5.2.3.3.2 For each control loop in the interoperable item control loop analysis, the system theoretic notions of sensing, actuating, controlling, and controlled process shall be allocated to the constituent interoperable items or to actors in the context of the interoperable item.

5.2.3.3.3 The sensing, detecting/analyzing, response determination, and response actions of each mitigation in the technical safety concept shall be accounted for in the control loop structures, and control loop analysis shall determine the impact of interoperability failures and component failures to achieve the risk control goals of the technical safety concept.

5.2.3.3.4 The allocation of system theoretic notions to the constituent interoperable items internal interoperability architecture shall be mapped to the generic control loop analysis provided by all interoperability frameworks with which the interoperable item is aligned.

5.2.3.3.5 An analysis shall be performed to determine the potential impacts of the error behavior of the constituent interoperable items (as reflected in its disclosed error specification) on the ability of the interoperable item or its context towards safety/security objectives related to the control goals of each control loop.

5.2.3.4 Realization of the functional safety concept within architecture

5.2.3.4.1 The allocation of the functional safety concept for the interoperable item shall be allocated to the internal interoperability architecture to achieve the technical safety concept.

5.2.3.4.2 The contributions of each constituent interoperable item to achieving the technical safety concept shall be in a form that enables each constituent interoperable item to be assessed against its assumed contributions and reflected in the form of context-derived requirements for the constituent interoperable item.

5.2.3.4.3 The internal interoperability architecture of the interoperable item shall be analyzed for appropriateness to determine if the reliability of each instance of the architecture in the interoperability management plan is sufficient for the criticality of the technical safety concept.

5.2.3.4.4 The impacts of both interoperability failures and failures of constituent interoperable items on the technical safety concept of the interoperable item as reflected in the data/control flow and control loop analysis shall be analyzed and the technical safety concept shall be revised as necessary to achieve appropriate levels of reliability.

5.3 Constituent interoperable item development

5.3.1 Development of each internally sourced constituent interoperable item shall be carried out in accordance with the organization's requirements for interoperable item development life-cycle activities. See also AAMI/UL 2800-1-2.

5.3.2 The following information shall be communicated from the interoperable item integration activity to inform the development of the constituent interoperable item:

a) Aspects of interoperable use specification, development context of use, deployment context of use, and context interactions (see 5.1.3) necessary for the constituent interoperable item;

b) Elements of the interoperable item functional safety concept and technical safety concept relevant to the constituent interoperable item, including the allocation of the functional safety concept to the constituent interoperable item;

c) Elements of the interoperability architecture relevant to the constituent interoperable item;

d) Requirements for the constituent interoperable item derived from the interoperable item integration requirements;

e) Interoperable item error categorization;

f) Aspects of the interoperable item error propagation specification relevant to constituent interoperable item; and

g) Allocation of release criteria and assurance responsibilities.

5.3.3 Engineering activities shall ensure traceability of constituent interoperable item implementation to the information in 5.3.2.

5.4 Interoperable item integration

5.4.1 Planning of release criteria for interoperable item integration

5.4.1.1 The release criteria for the interoperable item integration shall be shall be planned and detailed. See the Guidance on Release Criteria Annex of AAMI/UL 2800-1-2.

5.4.1.2 The release criteria for the interoperable item integration shall be aligned with those provided by all aligned interoperability frameworks.

5.4.1.3 The release criteria for the interoperable item integration shall indicate how the responsibilities for generating assurance are assigned to development and operating stakeholders and how planning for generating required evidence is accounted for in the planning for the Interoperable Item integration verification, deployment, and development of operating instructions.

5.4.2 Initiation of interoperable item integration verification planning

5.4.2.1 Interoperable item integration verification planning shall be initiated for demonstrating that interoperable item contracts are compatible at each interoperability binding point and that conditions for use of integrated interoperable items are satisfied.

5.4.2.2 The integration verification planning shall be aligned with the integration testing requirements provided by aligned interoperability frameworks.

5.4.2.3 The integration verification planning shall incorporate testing of variants.

5.5 Interoperability file information

5.5.1 Information resulting from the activities in the preceding sections shall be maintained in the relevant interoperability file.

NOTE: Information may include the following without limitation and detailed to the extent that it informs the release criteria for the constituent interoperable item:

a) Constituent Interoperable Item concept / interoperability concept

1) Interoperability architecture (preliminary, focusing on interoperability view / preliminary);

2) Architecture variability descriptions that allow exchange of constituent interoperable items to achieve different architecture configurations;

3) Item interactions; and

4) SSOs of the constituent interoperable item.

b) Preliminary hazard analysis – internal interoperability-related hazard analysis;

c) Functional safety concept for the constituent interoperable item;

d) Interoperability management plan for the constituent interoperable item;

e) Constituent interoperable item verification report;

f) Constituent interoperable item validation report;

g) Updated description of risk management file;

h) Constituent interoperable item release criteria report; and

i) Information from constituent interoperable item integration relevant to interoperable item disclosures.

Annex A
(Informative)

Architecture Definition Guidance

A1 Overview

A1.1 Many of the life-cycle activities recognized in the standard, management aspects in particular, depend on abstract topological aspects of the product including an abstract description of the product's boundary, a high-level characterization of its constituent interoperable items and their interactions, as well as the interactions between the product and its context. Such activities can proceed without a detailed specification of the product's architecture, which is fully developed in later life-cycle activities. To support a description of the product's topology, this standard provides a collection of terms that address aspects of decomposition as supported by defined terms such as "software item" and "software system" as well as tasks related to defining product boundaries for the purpose of scoping safety engineering-related responsibilities.

A1.2 Given a characterization of the product topology, the following aspects can be addressed:

a) The functional boundary of the product including high-level descriptions of its inputs and outputs and dependences on external products,

b) A high-level characterization of the physiological interactions between the product and a patient, including sensing and actuation objectives,

c) A high-level characterization of interactions with operators and external systems,

d) Informing an initial characterization of harms and hazardous situations that may arise due to improper actuations of the patient's physiological state or improper information conveyed to operators or external systems,

e) Supply-chain management issues for constituent interoperable items,

f) Coordination of responsibility agreements between organizations producing constituent interoperable items as well as organizations using the constituent interoperable items, and

g) Planning for product development and tailoring of life-cycle activities oriented around the topological structure of the product.

A1.3 The recognized activities of this Standard as presented in the Annex for Stakeholder Activities of AAMI/UL 2800-1 are organized around and are inextricably linked to the topology-related terminology including interoperable item, interaction point, interoperable item boundary, constituent interoperable item, and interoperable medical system. For example, the Annex for Stakeholder Activities of AAMI/UL 2800-1 identifies activities related to the development, integration, deployment, and operation of the primary topological units of interoperable item and interoperable medical system.

A1.4 To provide a basis for safety and security engineering, risk management, and assurance tasks, the life-cycle activities of AAMI/UL 2800-1-2 guide the refinement of the topological characterization of a product into a detailed interoperability architecture description, which is a key element of the interoperable item specification. The Annex for Interoperability Architecture Specification Guidance on Declaration of Products and Services of AAMI/UL 2800-1 (referenced by AAMI/UL 2800-1-2) gives requirements on the specification of the interoperability architecture.

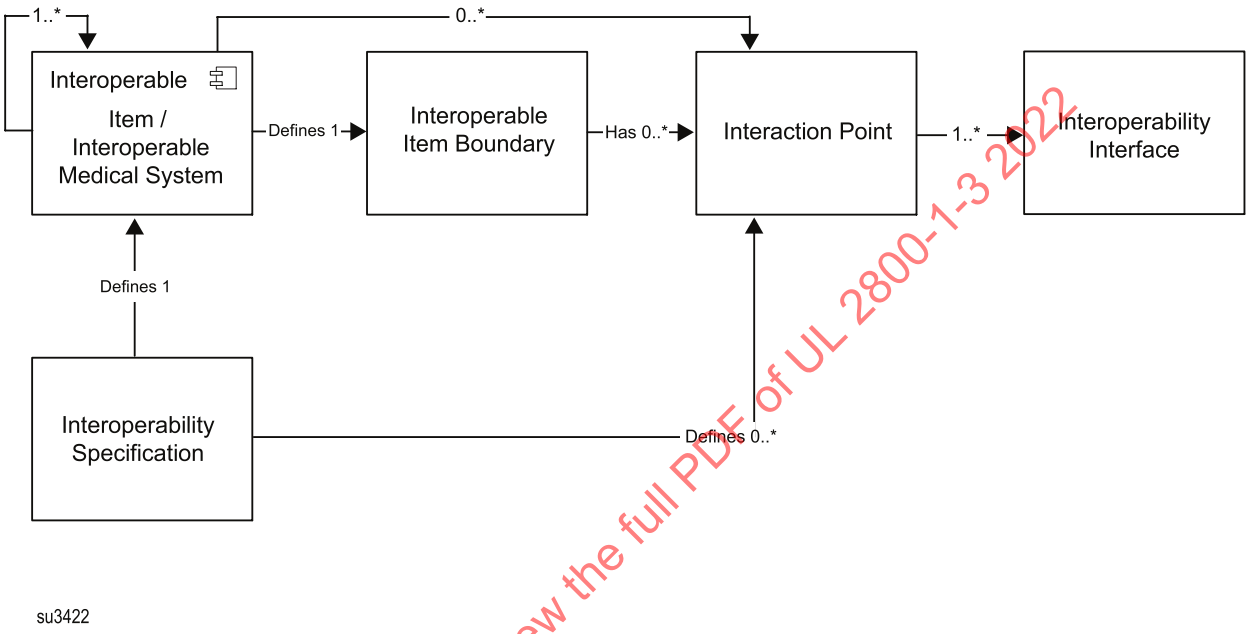
A2 Topological Vocabulary Overview

A2.1 The interoperable item is the basic unit of interoperability addressed in this standard. Examples of interoperable items include medical devices with network interfaces, infrastructure components such as communication hubs, computers that host application logic, as well as data loggers and other components designed to support safety and security. A software application providing medical functionality that runs on

a host computer associated with a platform can also be considered an interoperable item (for additional examples and discussion, See Section A3). Figure A1 captures the relationships between interoperable item, interoperable medical system, item interoperability specification, interaction point, interoperable item boundary, and interoperability interface.

Figure A1

Entity/Relation Diagram



A2.2 The definitions for interoperable item and interoperable medical system allow for an arbitrarily deep architectural hierarchy of nested system elements. This enables this standard to apply to products that are monolithic with respect to interoperable (i.e., they have no interoperable subcomponents) as well as integrations of products where the integration itself may be an aggregate product whose compliance to this standard may be evaluated. To support these notions, the definition of interoperable item encompasses either (a) a product that is monolithic with respect to interoperability (i.e., it lies at the bottom of the interoperability architecture hierarchy with no constituent interoperable items) or (b) an integration of interoperable items. It is important to note that a “leaf” interoperable item may be further decomposable, with an internal architecture that is of interest to the originating organization, but that decomposition is not exposed for considering compliance to this standard. Typical examples of leaf interoperable items include conventional medical devices with interoperability interfaces and infrastructure components such as network hubs and data loggers. Typical examples of integrations of interoperable items include systems consisting one or more interoperable medical devices, communication infrastructure, and some notion of system control logic.

A2.3 The definition of interoperable medical system is meant as a special case of an interoperable item that (a) is built from an integration of constituent interoperable items and (b) can be executed to provide care to a patient. Not all interoperable items composed of constituent interoperable items are interoperable medical systems. For example, one might have a collection of infrastructure interoperable items that provide functionality to support a system but cannot be executed direction themselves to provide caregiving functionality without the addition of other components.

A2.4 Each interoperable item – whether it is a leaf node in the architectural hierarchy or an integration of constituent interoperable items – has an interoperable item boundary consisting of interaction points that realize the interoperable item's interactions with its context. The notion of an interaction point is introduced to provide a convenient initial abstraction of topological features that can be used to begin management, planning, and architectural design activities. Each interaction point can be classified as one of three types:

a) An operator interaction point (supporting interactions between the interoperable item and operators),

b) A physiological interaction point (supporting sensing and actuation interactions with a patient), or

c) An interoperability interaction point (supporting interactions with other interoperable items or external systems not claiming compliance to this Standard).

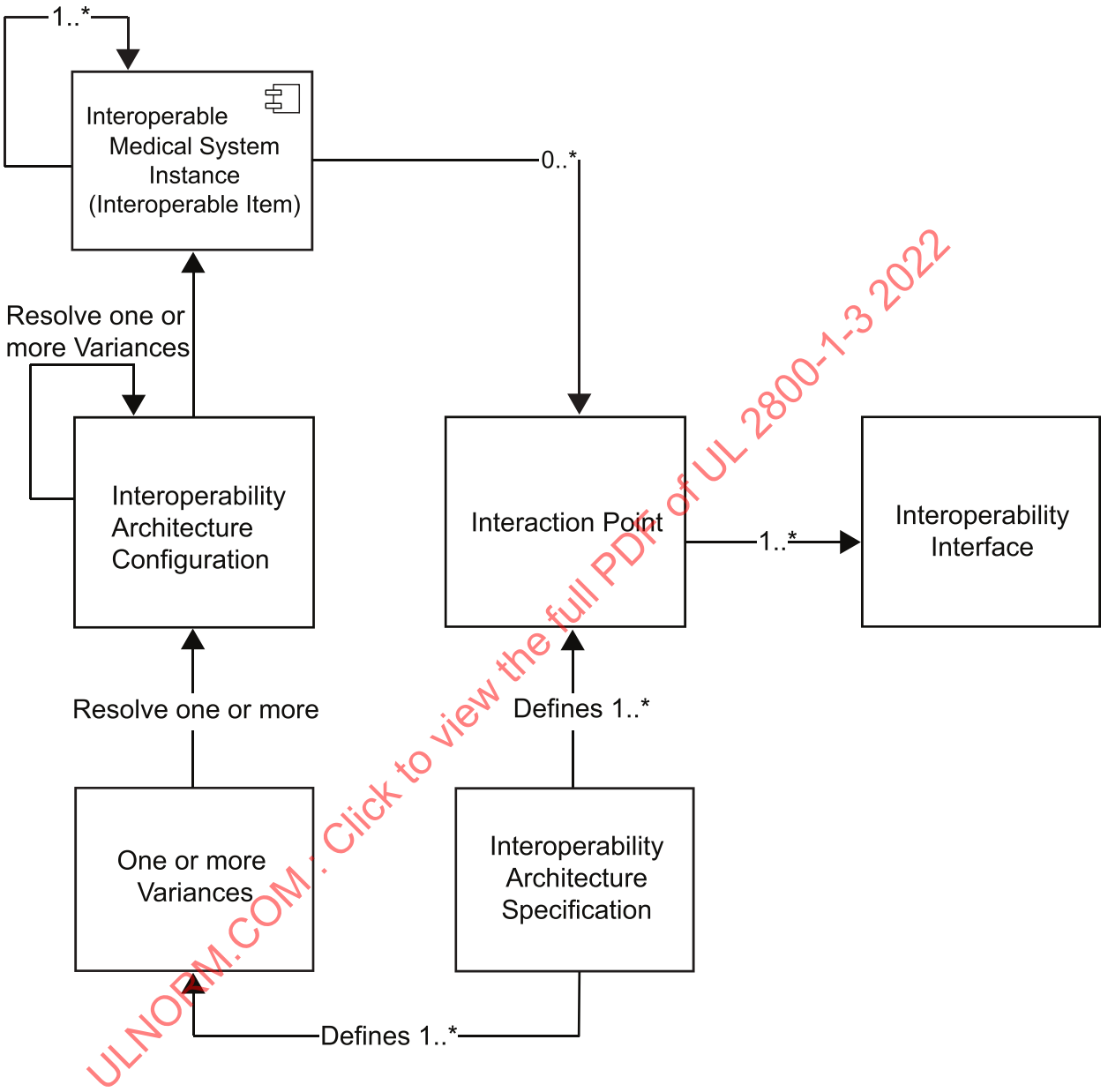
An interoperability interaction point is subsequently refined to describe the details of its realization as part of the interoperability architecture, which is included in the interoperability specification. in particular, an interoperable interaction point may be realized in terms of one or more logical or physical interoperability interfaces.

A2.5 The activities in the Annex for Stakeholder Activities of AAMI/UL 2800-1 are organized around the primary topological structures of interoperable item and interoperable medical system. In particular, the activity of interoperable item development address the development, realization and assurance of an interoperable item. interoperable item integration address engineering activities associated composing interoperable items to form functioning composite entity. When the interoperable item is a leaf node, development activities focus on the interoperable item boundary definition, realization of interoperability interfaces, etc. When an interoperable item has constituent interoperable items, the originating organization would also follow the interoperable item integration activities to integrate the constituent interoperable items to form the realize of the product.

A2.6 Figure A2 captures the relationships between interoperability architecture, variability, interoperability architecture configuration, and interoperability architecture instance. interoperable medical products with constituents are often designed to enable one or more constituents to be "swapped" with alternatives which provide analogous functionality (see examples in Section A3.2). In such cases, the planning, architecture specification, engineering, risk management, and assurance activities need to explicitly identify these possible variations of the product's topology in the Architecture Variability Description work product (see the Annex for Guidance on Interoperability File of AAMI/UL 2800-1-2). Given an interoperability architecture with variability, it may be useful to restrict the variability to obtain specific topological arrangements that support classes of care-giving activities. For example, the variability of an interoperability architecture of a platform presented as an interoperability framework might be restricted to a set of medical devices focused on respiratory health, and an accompanying collection of software applications. The term interoperability architecture configuration is used to capture such situations in which the interoperability architecture's variability is restricted, but some variability still exists (e.g., enabling one pulse oximetry device to be swapped for another as in the previous example). The term interoperability architecture instance is used to refer to an instantiation of the interoperability architecture where no variability remains. This captures the notion of a specific executable entity whose behaviors are assessed for safety and security. An important concept of this standard is that assessing the safety and security of an interoperable medical product whose interoperability architecture has variability requires demonstrating that all possible interoperable architecture instances (as accounted for in the Architecture Variability Description) achieve the SSOs stated for the interoperable medical product.

Figure A2

Concepts Related to Variability Within an Interoperable Architecture



A3 Examples

A3.1 Interoperable item

Example 1: Interoperable Medical Device

This example considers a medical device with a manufacturer-defined interoperability interface. Specifications of the interface may be derived from technologies identified in interoperable ecosystem, but things to which the item connects are not assumed to be in compliance with this Standard. In this example, the device is presented as a single entity for compliance to this standard, however a device can be decomposed to further expose interoperability to be considered for compliance to this standard (see Example 3, where a device+dongle combination is treated as an Interoperable Medical Device but can be decomposed into a legacy device and the attached dongle as two distinct constituent interoperable items).

Primary Topological Vocabulary Elements:

Interoperable Item

Discussion:

The originating organization follows the Stakeholder Activities Annex of AAMI/UL 2800-1 of item development and the associated life-cycle process steps of item development described in AAMI/UL 2800-1-2.

Example 2: Interoperable Medical Device designed to work with a particular interoperability platform.

This example considers a medical device with a manufacturer-defined interoperability interface as in Example 1, but with the additional compliance goal of alignment with a specified interoperability framework corresponding to the interoperability platform.

Primary Topological Vocabulary Elements:

Interoperable Item, Interoperability Framework

Discussion:

Activities are as stated in Example 1, with the addition that requirements associated with alignment with an interoperability framework are addressed. See also AAMI/UL 2800-1-2 for examples of such requirements.

Example 3: Legacy medical device using a dongle to achieve interoperability capability.

This example considers the addition of a dongle (or other form of adapter) to establish a particular interoperability protocol for a medical device with a network interface (e.g., one not designed for interoperability or designed for a different interoperability platform).

Primary Topological Vocabulary Elements:

Interoperable Item

Discussion:

In this case, the interoperable item consists of the original medical device in conjunction with its adapter/dongle. Decoupling and switching the dongle/device does not result in compliance with this Standard unless separate evaluations are made for such configurations.

The organization adding the interoperability dongle follows the activity of item development in the Annex for Stakeholder Activity of AAMI/UL 2800-1 and associated life-cycle activities in this Standard. The organization will likely acquire detailed design and implementation information about the medical device from the original equipment manufacturer. If the original device was compliant to this standard, this material may be readily available. The organization provides a specification addressing the combined device/dongle functionality, and an architecture and realization description that accounts for the conjoining of the device with the dongle. The device+dongle combination presented as an interoperable item is assured comply with its item interoperability specification.

Example 4: Data Logger.

This example considers an interoperable infrastructure component such as a Data Logger that does not have a traditional medical intended use but supports safety and security goals of interoperable medical systems in which it participates.

Primary Topological Vocabulary Elements:

Interoperable Item

Discussion:

The Data Logger would be treated as an interoperable item similar to Examples 1 – 3 above. However, the technical function of the interoperable item would be emphasized as their driver for identification of SSOs rather than a medical function. The development context of use for the interoperable item should address possible approaches for integrating the interoperable item into the context of an interoperable medical system. Other infrastructure items, such as a network hub or a platform-connected computer for hosting software applications that provide medical functionality, would be treated similarly.

Example 5: Platform-based Software Application (App) providing a medical function.

This example considers a software application designed to be run on a host computer attached via networking infrastructure to a collection of medical devices and Health IT systems. The host computer, networking infrastructure, and suite of medical devices may be realized using platform engineering approaches.

Primary Topological Vocabulary Elements:

Interoperable Item, Interoperable Medical System, Interoperability Framework

Discussion:

The software application (app) can be presented as an interoperable item designed to be integrated with the host computer, networking infrastructure, and collection of devices. Since the app needs to be composed with the rest of the integration context to obtain an executable entity with behavior whose safety is assessed, the safety of the app cannot be fully assessed without consideration of its context. However, the app can be assessed against SSOs, declaration of external measures, and description of the context of development and context of use. The most common approach would be to present the host computer, networking infrastructure, and devices from the device suite as interoperable items compliant with this standard. If the host computer, networking infrastructure, and device suite is designed as a platform that would support multiple apps, the platform would likely be presented as an interoperability framework with a reference architecture the specifies constraints for integrating the app with the platform context. The app and other components of the platform would be presented as interoperable items aligned with the interoperability framework.

A3.2 Interoperable medical system

Example 6: System with fixed integration of interoperable components for a fixed clinical function.

This example considers the integration of a fixed (non-swappable) collection of interoperable medical devices (e.g., a pulse oximeter of a specific manufacturer model, a capnograph of a specific manufacturer model, and an infusion pump of a specific manufacturer model) with a computing hub to provide a specific medical function (e.g., implementation of a smart alarm for PCA infusion).

Primary Topological Vocabulary Elements:

Interoperable Medical System, Interoperable Item

Discussion:

The interoperable medical system consists of the fixed collection of devices, the computing hub that includes network infrastructure required to connect to the devices, and the smart alarm functionality realized in software running on the computing hub. The organization originating interoperable medical system follows the activity of item development in the Annex for Stakeholder Activity of AAMI/UL 2800-1. Since the system is considered “fixed”. It may not be necessary to present the system elements as interoperable items. In this case, the product may be presented as a single interoperable item that is monolithic with respect to interoperability. However, it is more likely that some of the elements such as the medical devices and computing hub will also be presented as interoperable items for compliance to this standard. In this case, the system would be presented as an interoperable medical system with the components presented as constituent interoperable items.

Example 7: System with varying integration of interoperable components for a fixed clinical function

As with the example above, this example considers integration of a collection of medical devices with a computing hub to provide a specific medical function. In contrast with the previous example, the devices in this case are explicitly designed for interoperability and a designated subset of the interoperable medical devices are exchangeable as justified by compatibilities in their interoperability interfaces. For example, one might have a common interface defined for pulse oximetry functionality, and the designated exchangeable devices include three different pulse oximeters that support that interface.

Primary Topological Vocabulary Elements:

Interoperable Medical System, Interoperable Item

Discussion:

In this type of situation, the medical devices and computing hub would be presented as interoperable items for compliance to this standard. The system would be presented as an interoperable medical system with the components presented as constituent interoperable items. The architecture variability specification (one of the identified work products of the Annex for Guidance on Interoperability File of AAMI/UL 2800-1-2) has a variability specification that indicates that the pulse oximetry functionality may be achieved by three different pulse oximeters (i.e., there are three different interoperability architecture instances of the system). In contrast to the previous example in which the medical function of the system interfaces with an interface for a specific pulse oximeter, in this case the medical function, e.g., as realized by software on the computing hub, interfaces with an interface specified in terms of pulse oximetry capabilities that provides an abstraction (may be referred to as “device model” or “domain information model configuration”) of multiple devices. Assurance for the system must show that it will satisfy its specification no matter which architecture instance is used to provide care to the patient.

Example 8: Product with varying integration of Interoperable Components for varying (but completely enumerated) medical functions.

This example extends the previous one by considering – not just a single medical application – but a collection of applications designated at the time of evaluation of compliance to this standard. For example, a suite of medical devices, including exchangeable pulse oximeters, might be used to support a collection of five applications, designed for different care-giving scenarios (the applications with have distinct medical intended uses), that support monitoring and smart alarms for respiratory health.

Primary Topological Vocabulary Elements:

Interoperable Item, Interoperable Medical System, Interoperability Framework

Discussion:

Differing topology arrangements of this example may be submitted at the discretion of those concerned. If the five applications have sufficiently different intended uses (e.g., have substantially notions of patient harm and hazardous situations), a typical approach would be to address the situation with five different interoperable medical system submissions. In such a situation, each application+host+device-set combination would be assessed separately. In this case, the interoperable architecture and the Architecture Variability Specification would document a single application with variability associated with the swappable devices. If the applications have similar notions of harm, and also if some of the applications are designed to be executed simultaneously with each other, a single compliance submission for an interoperable medical system might be used with the interoperable architecture and Architecture Variability Description documenting the variations in the application functionality, including the different combinations of applications that may be running simultaneously. In either case, assurance must show that each will satisfy its specification no matter which architecture instance is used to provide care to the patient. In the case where a single system is presented with simultaneously executing applications, this will include arguments about the non-interference of the applications and the ability of the applications to achieve SSOs even when they may be sharing resources of the hosting computer.

A3.3 Interoperability framework

Example 9: Platform with a fixed device suite but open-ended set of applications.

This example extends examples from the previous section (e.g., Example 10), but supporting an unspecified (open-ended) set of applications. This situation is best addressed as an interoperability framework. In such situations, because the specific medical function and associated patient harms are not known at the time of compliance evaluation, a specific interoperable medical system is not considered (however, it would be wise to provide an accompanying compliance evaluation for one or more example systems). The interoperability framework supports future compliance evaluations for interoperable medical systems as instances of the interoperability framework, with substantial reuse of the work products associated with the interoperability framework.

Primary Topological Vocabulary Elements:

Interoperability Framework

Discussion:

Some of the distinguishing topological features of an interoperability framework are significant architecture variability, desire to provide an assurance foundation for an unbounded set of instances (i.e., all possible interoperability architecture instances are not known at the time of submission, and thus compliance cannot assessed by an enumeration of all possible combinations of constituent interoperable items), or the intent to achieve significant reuse of work products and assurance across a broad set of system instances.

Important aspects of compliance evaluation include the specification of the specification of reference architecture that constrains the topology of interoperability architecture instances of systems built with the platform, development processes that are expected to be followed when building systems from the platform, and assurance responsibilities including typical SSOs and External Measures for constituent interoperable items for interoperable medical systems built from the platform. Since the variability of the reference architecture centers around the ability to run different applications on the platform, review of processes for developing, assuring, and qualifying applications for use on the platform are especially important.

Example 10: Platform with an open-ended device suit and open-ended set of applications.