INTERNATIONAL STANDARD

ISO/IEEE 11073-20701

First edition
2020-03

Health informatics — Device interoperability —

Part 20701: Point-of-care medical device communication — Service oriented medical device exchange architecture and protocol binding

Informatique de santé — Interopérabilité des dispositifs —

Partie 20701: Communication entre dispositifs médicaux sur le site des soins — Architecture d'échange orientée services entre dispositifs médicaux et liaison par protocole

Reference number
ISO/IEEE 11073-20701:2020(E)

Institute of Electrical and Electronics Engineers, Inc
3 Park Avenue, New York
NY 10016-5997, USA

Email: stds.ipr@ieee.org
Website: www.ieee.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted (see www.iso.org/directives).

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

ISO/IEEE 11073-20701 was prepared by the IEEE 11073 Standards Committee of the IEEE Engineering in Medicine and Biology Society (as IEEE Std 11073-20701-2018) and drafted in accordance with its editorial rules. It was adopted, under the “fast-track procedure” defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE, by Technical Committee ISO/TC 215, *Health informatics*.

A list of all parts in the ISO/IEEE 11073 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Health informatics—Point-of-care medical device communication

Part 20701: Service-Oriented Medical Device Exchange Architecture and Protocol Binding

Sponsor

IEEE 11073™ Standards Committee
of the
IEEE Engineering in Medicine and Biology Society

Approved 27 September 2018

IEEE-SA Standards Board

Abstract: Within the context of the ISO/IEEE 11073 family of standards for point-of-care (PoC) medical device communication, an architecture for service-oriented distributed PoC medical devices and medical IT systems is defined. This standard defines a binding of the Participant, Discovery, and Communication Model defined in IEEE Std 11073-10207™ to the profile for transport over Web Services defined in IEEE Std 11073-20702™. Moreover, a binding to Network Time Protocol (NTP) and Differentiated Services (DiffServ) is defined for time synchronization and transport Quality of Service requirements.

Keywords: alert systems, BICEPS, DiffServ, IEEE 11073-20701™, ISO/IEEE 11073, MDPWS, medical device communication, NTP, patient, point-of-care, remote control, service-oriented architecture

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-1-5044-5264-9 STD23381
Print: ISBN 978-1-5044-5265-6 STDPD23381

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE-SA") Standards Board. IEEE ("the Institute") develops its standards through a consensus development process, approved by the American National Standards Institute ("ANSI"), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An existing IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore at http://ieeexplore.ieee.org/ or contact IEEE at the address listed previously. For more information about the IEEE-SA or IEEE's standards development process, visit the IEEE-SA Website at http://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this IEEE standard was completed, the Point of Care Devices Working Group had the following membership:

Jan Wittenber, *Chair*
Stefan Schlichting, *Subgroup Chair*

Bjoern Anderson
Malcolm Clarke
Todd Cooper
Chris Courville
Michael Faughn
Kenneth Fuchs
John Garguilo
Frank Golatowski
David Gregorczyk
Kai Hassing
John Hatcliff
Stefan Karl
Martin Kasparick
Koichiro Matsumoto
Joerg-Uwe Meyer
Stephan Poehlsen
Tracy Rausch
John Rhoads
Paul Schluter
Masato Tanaka
Eugene Vasserman
Stan Wiley

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Bjoern Andersen
Lyle Bullock
Carole Carey
Keith Chow
Sourav Dutta
Kenneth Fuchs
David Fuschi
David Gregorczyk
Randall Groves
Werner Hoelzl
Noriyuki Ikeuchi
Atsushi Ito
Raj Jain
Stefan Karl
Piotr Karocki
Martin Kasparick
Thomas Kurihara
Joerg-Uwe Meyer
Beth Pumo
Stefan Schlichting
Janek Schumann
Sarah Shafqat
Walter Struppler
J. Wiley
Jan Wittenber
Oren Yuen
Janusz Zalewski
Daidi Zhong

When the IEEE-SA Standards Board approved this standard on 27 September 2018, it had the following membership:

Jean-Philippe Faure, *Chair*
Gary Hoffman, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse
Guido R. Hiertz
Christel Hunter
Joseph L. Koepfinger*
Thomas Koshy
Hung Ling
Dong Liu
Xiaohui Liu
Kevin Lu
Daleep Mohla
Andrew Myles
Paul Nikolich
Ronald C. Petersen
Annette D. Reilly
Robby Robson
Dorothy Stanley
Mehmet Ulema
Phil Wennblom
Philip Winston
Howard Wolfman
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 11073-20701-2018, Health Informatics—Point-of-care medical device communication—Part 20701: Service-Oriented Medical Device Exchange Architecture and Protocol Binding.

ISO/IEEE 11073 standards enable communication between medical devices and external computer systems. They provide automatic and detailed electronic data capture of patient vital signs information and device operational data. The primary goals are to:

— Provide real-time plug-and-play interoperability for medical devices

— Facilitate the efficient exchange of vital signs and medical device data, acquired at the Point-of-Care (PoC), in all health care environments

"Real-time" means that data from multiple devices can be retrieved, time correlated, and displayed or processed in fractions of a second. "Plug-and-play" means that all the clinician has to do is to make the connection—the Participants automatically detect, configure, and communicate without any other human interaction.

"Efficient exchange of medical device data" means that information that is captured at the PoC (e.g., patient vital signs data) can be received, parsed, and interpreted by many different types of applications without unnecessary loss of information. The standards are especially targeted at acute, surgical, and continuing care devices, such as patient monitors, ventilators, infusion pumps, ECG devices, endoscopic camera system, insufflators, endoscopic light sources, dissectors, etc. They comprise a family of standards that can be bound to one another to provide optimized connectivity for devices at the Point-of-Care.

Within the context of the ISO/IEEE 11073 family of standards for PoC medical device communication, this standard defines an architecture for service-oriented distributed PoC medical devices and medical IT systems. It defines a binding of the Participant, Discovery, and Communication Model defined in IEEE Std 11073-10207 to the profile for transport over Web Services defined in IEEE Std 11073-20702. Moreover, a binding to Network Time Protocol (NTP) and Differentiated Services (DiffServ) is defined to satisfy time synchronization and transport Quality of Service requirements.

Contents

1. Overview 10
1.1 Scope 10
1.2 Purpose 10

2. Normative references 10

3. Definitions 11

4. Notational conventions 15
4.1 XML schema namespaces 15

5. Introduction 16

6. Service-oriented medical device exchange architecture 17

7. Service-oriented device connectivity (SDC) participant model binding 18
7.1 Coded values 18
7.2 Remote-control capabilities 18
7.3 Retrievability of containment tree entries 20
7.4 Dynamic containment tree changes 21
7.5 MDIB versioning 22
7.6 Types 22

8. Communication model binding 23
8.1 Service 23
8.2 Message 25

9. Discovery binding 27
9.1 Discovery mechanism 27
9.2 Complex device component based discovery 27
9.3 SDC PARTICIPANT KEY PURPOSE based discovery 28
9.4 Context-based discovery 29
9.5 Announcing absence 31

10. Non-functional quality attributes 31
10.1 Cybersecurity 31
10.2 Patient safety 33
10.3 Clinical effectiveness 34

11. Conformance 36
11.1 General format 36
11.2 ICS tables 37

Annex A (normative) Constants 39

Annex B (normative) SDC service provider WSDL service descriptions 40
B.1 Get Service 40
B.2 Set Service 40
B.3 Description Event Service 40
B.4 State Event Service 41
B.5 Context Service 41
B.6 Waveform Service 41

B.7 Containment Tree Service 42
B.8 Archive Service 42
B.9 Localization Service 42

Annex C (informative) Bibliography 43

Health informatics—Point-of-care medical device communication

Part 20701: Service-Oriented Medical Device Exchange Architecture and Protocol Binding

1. Overview

1.1 Scope

The scope of this standard is a service-oriented medical device architecture and communication protocol specification for distributed system of Point-of-Care (PoC) medical devices and medical IT systems that need to exchange data or safely control networked PoC medical devices. It identifies the functional components, their communication relationships as well as the binding of the components and communication relationships to protocol specifications.

1.2 Purpose

This standard defines an architecture for service-oriented distributed PoC medical devices and medical IT systems. It describes a binding of the Participant and Communication model as defined in IEEE Std 11073-10207™ to Medical Devices Communication Profile for Web Services (MDPWS) as defined in IEEE Std 11073-20702™ for transport over Web Services.[1] Moreover, a binding to the Network Time Protocol (NTP) and Differentiated Services (DiffServ) is specified for time synchronization and transport Quality of Service requirements.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 11073-10207-2017, IEEE Health informatics—Point-of-care medical device communication—Part 10207: Domain Information and Service Model for Service-Oriented Point-of-Care Medical Device Communication. [2, 3]

[1] Information on references can be found in Clause 2.
[2] IEEE publications are available from the Institute of Electrical and Electronics Engineers (http://standards.ieee.org/).

IEEE Std 11073-20702-2016, IEEE Health informatics—Point-of-care medical device communication—Part 20702: Medical Devices Communication Profile for Web Services.

IETF RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, D. Mills, March 1992. Available at https://tools.ietf.org/html/rfc1305.

IETF RFC 1769, Simple Network Time Protocol (SNTP), D. Mills, March 1995. Available at https://tools.ietf.org/html/rfc1769.

IETF RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, K. Nichols et al., December 1998. Available at https://tools.ietf.org/html/rfc2474.

IETF RFC 2475, An Architecture for Differentiated Services, S. Blake et al., December 1998. Available at https://tools.ietf.org/html/rfc2475.

IETF RFC 4330, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, D. Mills, January 2006. Available at https://tools.ietf.org/html/rfc4330.

IETF RFC 5227, IPv4 Address Conflict Detection, S. Cheshire, July 2008. Available at https://tools.ietf.org/html/rfc5227.

IETF RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, T. Dierks et al., August 2008. Available at https://tools.ietf.org/html/rfc5246.txt.

IETF RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification, D. Mills et al., June 2010. Available at https://tools.ietf.org/html/rfc5905.

ISO/IEEE Std 11073-10101:2004, Health informatics—Point-of-care medical device communication—Part 10101: Nomenclature.[4]

3. Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause. [5]

ALERT: Synonym for the combination of patient-related physiological alarms, technical alarms and equipment user advisory signals.

NOTE 1—Patient-related physiological alarms as well as technical alarms are ALARM SIGNALs indicating the presence of ALARM CONDITIONs. An ALERT CONDITION is an ALARM CONDITION if the priority is LOW PRIORITY, MEDIUM PRIORITY, or HIGH PRIORITY and where the origin is a Physiological or Technical. See IEC 60601-1-8:2006+AMD1:2012 [B3].[6, 7]

NOTE 2—Equipment user advisory signals are INFORMATION SIGNALs indicating the presence of conditions that are not ALARM CONDITIONs. An ALERT CONDITION is not an ALARM CONDITION if the priority is neither LOW PRIORITY nor MEDIUM PRIORITY nor HIGH PRIORITY. See IEC 60601-1-8:2006+AMD1:2012 [B3].

[3] The IEEE standards or products referred to in Clause 2 are trademarks owned by the Institute of Electrical and Electronics Engineers, Incorporated.
[4] ISO/IEEE publications are available from the International Organization for Standardization (http://www.iso.org/) and the Institute of Electrical and Electronics Engineers (http://standards.ieee.org/).
[5] *IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org.
[6] The numbers in brackets correspond to those of the bibliography in Annex C.
[7] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

CLINICAL WORKPLACE: Set of medical devices that interacts with, monitors, or provides treatment to a single patient, or is setup to interact with, monitor, or provide treatment to a single patient by some other means.

NOTE—Besides direct announcement of being associated to the same patient a CLINICAL WORKPLACE can also be indicated by the same spatial location or treatment session.

CLINICAL WORKPLACE SOMDS: Subset of PARTICIPANTs of a service-oriented medical device system (SOMDS) that is assigned to one CLINICAL WORKPLACE.

CLINICAL WORKPLACE SOMDS PROXY SERVICE: Proxy service in a CLINICAL WORKPLACE that is an external interface to other systems.

NOTE—Examples for external systems are network gateways, electronic health records (EHRs), central stations, wireless sensor networks, or other CLINICAL WORKPLACE service-oriented medical device system (SOMDSs).

CODE: Identifier used to semantically describe an entity within a CODING SYSTEM.

CODED VALUE: Value that utilizes a CODING SYSTEM and a CODE to semantically describe a certain object within the MEDICAL DATA INFORMATION BASE (MDIB).

NOTE—In general, CODED VALUEs are based on standardized terminologies to increase interoperability.

CODING SYSTEM: Set of CODEs.

CONTAINMENT TREE ENTRY: Node of a CONTAINMENT TREE that encloses descriptive and state information.

CONTAINMENT TREE: Device configuration and capability description of a medical device system that represents a POINT-OF-CARE (PoC) MEDICAL DEVICE.

NOTE—It is modeled as a tree with a depth of four.

CONTEXT: Abstraction of a component of a POINT-OF-CARE (PoC) MEDICAL DEVICE that defines the relationship of a PoC MEDICAL DEVICE with its usage environment. Technically, a context can be understood as a token that is shared between two or more PoC MEDICAL DEVICEs to let them know they are “talking about the same things.”

DIFFERENTIATED SERVICE (DiffServ): Coarse-grained, class-based mechanism for traffic management as defined in the DiffServ specification, IETF RFC 2474.

DIFFERENTIATED SERVICES (DiffServ) CODE POINT: 6-bit code for classification of network packets as defined in the DiffServ specification, IETF RFC 2474.

DIFFERENTIATED SERVICE (DiffServ) DOMAIN: Group of NETWORK NODEs that implement common, administratively defined DiffServ policies as defined in the DiffServ specification, IETF RFC 2475.

DIFFERENTIATED SERVICE (DiffServ) FIELD: Eight-bit field in the IP header for network packet classification purposes as defined in the DiffServ specification, IETF RFC 2474.

ELEMENT: XML element as defined in Extensible Markup Language (XML) 1.0.

NOTE—See W3C® XML 1.0 [B12]. [8]

[8] W3C is a trademark (registered in numerous countries) of the World Wide Web Consortium; marks of W3C are registered and held by its host institutions MIT, ERCIM, Keio, and Beihang.

INTEGRATED CLINICAL ENVIRONMENT (ICE): Environment that combines interoperable heterogeneous POINT-OF-CARE (PoC) MEDICAL DEVICEs and other equipment integrated to create a medical device system for the care of a single high acuity patient (ASTM F2761-09 [B1]).

MDIB VERSIONING ATTRIBUTE: An attribute of an ELEMENT that allows detection of outdated data and provisioning of a CONTAINMENT TREE history. MEDICAL DATA INFORMATION BASE (MDIB) VERSIONING ATTRIBUTEs are any pm:@DescriptorVersion, pm:@StateVersion, pm:@MdibVersion, pm:@SequenceId, pm:@InstanceId, pm:AbstractContextState/@BindingMdibVersion, and pm:AbstractContextState/@UnbindingMdibVersion.

MEDICAL DATA INFORMATION BASE (MDIB): Structured collection of any data objects that are provided by a particular POINT-OF-CARE (PoC) MEDICAL DEVICE and include descriptive and state information.

MEDICAL SAFETY CLASSIFICATION: Classification of the quality of data and criticality of operations from a risk management perspective in accordance with the pm:SafetyClassification of a CONTAINMENT TREE ENTRY that evaluates to either “MedA,” “MedB,” or “MedC” as defined in IEEE Std 11073-10207-2017.

MEP: MESSAGE exchange pattern.

MESSAGE: Set of data in a specific format that is exchanged between PARTICIPANTs.

METRIC: Abstraction of a component of a POINT-OF-CARE (PoC) MEDICAL DEVICE that is able to generate or store direct and derived, quantitative and qualitative biosignal measurements, settings, and status values.

NETWORK NODE: Node in a network that exchanges MESSAGEs either by sending, receiving, or forwarding.

NOTIFICATION: MESSAGE exchange pattern (MEP) where a SERVICE PROVIDER uses a SERVICE OPERATION to transmit a MESSAGE to one or more SERVICE CONSUMERs periodically or triggered by an event. The SERVICE PROVIDER sends a notification MESSAGE, which encloses event-related data, to the SERVICE CONSUMER(s).

OPERATOR: Person handling a POINT-OF-CARE (PoC) MEDICAL DEVICE or any other equipment that is part of PoC ENVIRONMENT or SERVICE-ORIENTED MEDICAL DEVICE SYSTEM (SOMDS).

PARTICIPANT: Any NETWORK NODE that is part of a SERVICE-ORIENTED MEDICAL DEVICE SYSTEM (SOMDS) and exchanges information by means of a service-oriented architecture and can be either a SERVICE PROVIDER or a SERVICE CONSUMER.

PER-HOP BEHAVIOR (PHB): Defines the packet forwarding properties of a NETWORK NODE associated with a class of network traffic as defined in the DiffServ specification, IETF RFC 2475.

POINT-OF-CARE (PoC) ENVIRONMENT: Environment encompassing a particular diagnostic, bed, or treatment area which is specific to one patient.

NOTE—It usually includes those systems and personnel that are involved in the acute monitoring and treatment of the patient.

POINT-OF-CARE (PoC) MEDICAL DEVICE: Medical device providing support for electronic communication that directly interacts with, monitors, provides treatment to, or is in some way associated with a single patient.

NOTE—For this specification the scope of PoC MEDICAL DEVICEs is further limited to medical devices that provide support for electronic communication.

PRIMARY UDI: First entry in the list of pm:MdsDescriptor/pm:MetaData/pm:Udi if multiple entries are available for a POINT-OF-CARE (PoC) MEDICAL DEVICE.

PROTOCOL BINDING: Specification that defines how to connect two separated protocol layers with each other.

REQUEST-RESPONSE: MESSAGE exchange pattern (MEP) where a SERVICE CONSUMER invokes a SERVICE OPERATION on a SERVICE PROVIDER by sending a request MESSAGE, which encloses input payload, to the SERVICE PROVIDER, and receiving a response MESSAGE, which encloses output payload, from the SERVICE PROVIDER.

RISK: Combination of the probability of occurrence of harm and the severity of that harm.

NOTE—See ISO 14971:2007 [B7].

SDC (Service-oriented Device Connectivity): Describes the non-normative title of this standard, IEEE Std 11073-20701.

SDC (Service-oriented Device Connectivity) PARTICIPANT: PARTICIPANT that adheres to the requirements of this specification, IEEE Std 11073-20701.

SDC PARTICIPANT KEY PURPOSE: A set of requirements a Service-oriented Device Connectivity (SDC) PARTICIPANT is complying and that allows it to act in a SERVICE-ORIENTED MEDICAL DEVICE SYSTEM (SOMDS) accordingly.

NOTE 1—An SDC PARTICIPANT KEY PURPOSE might be for example a set of requirements that guarantees safe and effective communication with for SDC PARTICIPANTs that participate in a SOMDS function, e.g., closed-loop remote control between devices.

NOTE 2—An SDC PARTICIPANT KEY PURPOSE might be for example a set of requirements that guarantees safe and effective communication with SDC SERVICE PROVIDERs that represent specialized clinical POINT-OF-CARE (PoC) MEDICAL DEVICE specializations contributing to functions in a SOMDS.

NOTE 3—If an SDC SERVICE PROVIDER has more than one SDC PARTICIPANT KEY PURPOSE, then those SDC PARTICIPANT KEY PURPOSEs cannot contradict as per definition the SDC PARTICIPANT has to comply with the superset of the set of requirements defined for each SDC PARTICIPANT KEY PURPOSE.

SDC (Service-oriented Device Connectivity) SERVICE CONSUMER: SERVICE CONSUMER that adheres to the requirements of this specification, IEEE Std 11073-20701.

SDC (Service-oriented Device Connectivity) SERVICE PROVIDER: SERVICE PROVIDER that adheres to the requirements of this specification, IEEE Std 11073-20701.

SERVICE CONSUMER: A NETWORK NODE that utilizes at least one SERVICE.

SERVICE CONTRACT: SERVICE INTERFACE with constraints and policies.

SERVICE INTERFACE: Set of SERVICE OPERATIONs that is provided by a SERVICE to describe its capabilities.

SERVICE OPERATION: Single operation that can be executed remotely at a SERVICE PROVIDER.

SERVICE PROVIDER: NETWORK NODE that provides at least one SERVICE.

SERVICE REGISTRY: SERVICE PROVIDER that provides SERVICE CONTRACTs to a SERVICE CONSUMER and thus facilitates discovery of SERVICEs.

NOTE—A SERVICE REGISTRY can be implemented either as centralized SERVICE PROVIDER or as a distributed SERVICE PROVIDER.

SERVICE: Part of a software system that exposes functional capabilities on a communication backbone.

SERVICE-ORIENTED MEDICAL DEVICE SYSTEM (SOMDS): Instance of a distributed system that implements a service-oriented architecture composed of SERVICE PROVIDERs and SERVICE CONSUMERs as defined in IEEE Std 11073-20702.

STREAMING: A special NOTIFICATION MESSAGE exchange pattern (MEP) where a SERVICE PROVIDER uses a SERVICE OPERATION to transmit MESSAGEs to 0 or more SERVICE CONSUMERs continuously in short time periods without a specified beginning and end.

TYPE: Complex or simple type definition as defined in W3C XML Schema 1.1 [B15].

4. Notational conventions

4.1 XML schema namespaces

This standard references WSDL files that include XML Schema 1.1 [B15] to describe SERVICE INTERFACEs. The WSDL files and included XML Schemas utilize the XML namespaces (W3C Namespaces in XML 1.0 [B13]) as defined in Table 1.[9]

Table 1—Namespace mappings

Namespace prefix	URI	Specification
ext	http://standards.ieee.org/downloads/11073/11073-10207-2017/extension	IEEE 11073-10207 Extension Model
pm	http://standards.ieee.org/downloads/11073/11073-10207-2017/participant	IEEE 11073-10207 Participant Model
msg	http://standards.ieee.org/downloads/11073/11073-10207-2017/message	IEEE 11073-10207 Message Model
sdc	http://standards.ieee.org/downloads/11073/11073-20701-2018	This specification
mdpws	http://standards.ieee.org/downloads/11073/11073-20702-2016	IEEE 11073-20702
wse	http://schemas.xmlsoap.org/ws/2004/08/eventing	WS-Eventing

[9] The xml schema files necessary to ease the understanding of this standard are available at the following URL: http://standards.ieee.org/downloads/11073/.

4.1.1 XML schema referencing

References to TYPE or ELEMENT definitions of the XML Schema are made by using the corresponding QName (W3C Namespaces in XML 1.0 [B13]). To reference a nested TYPE definition, the QName is enhanced with a chain of QNames and unqualified ATTRIBUTE names, each separated by XPath delimiters (W3C XPath 1.0 [B14]). Examples include the following:

- pm:Handle points to the *Handle* TYPE defined in the Participant Model.
- msg:OperationInvokedReport/msg:ReportPart/@OperationTarget points to the ATTRIBUTE *OperationTarget* that is defined as part of the *ReportPart*, which is included in the *OperationInvokedReport*. Since the QName prefix is msg, the referenced TYPE refers to the Message Model.
- ./@ActivationDuration refers to an ATTRIBUTE within an arbitrary TYPE definition.

Throughout the XML Schema, a camel case notation is used for the following:

- Every artifact begins with a capital letter (e.g., “Handle”)
- Names are separated by a capital letter (e.g., “ActivationState”)
- Abbreviations are denoted in camel case (e.g., “VmdDescriptor”)

5. Introduction

This specification comprises two major parts as follows:

- The definition of a service-oriented medical device exchange architecture.
- A PROTOCOL BINDING of IEEE Std 11073-10207 [BICEPS] and IEEE Std 11073-20702 [MDPWS] to implement the service-oriented medical device exchange architecture.

The PROTOCOL BINDING consists of four parts as follows:

- A binding to describe the capabilities and state of a PoC MEDICAL DEVICE by using SERVICEs.
- A binding to describe the MESSAGEs that are conveyed between SERVICE CONSUMERs and SERVICEs to exchange the capabilities and state of the PoC MEDICAL DEVICE with the SERVICE CONSUMERs.
- A binding to describe how SERVICE CONSUMERs are enabled to discover suitable SERVICEs.
- A binding to describe non-functional quality attributes that are needed for a safe and effective operation of the service-oriented medical device exchange architecture.

6. Service-oriented medical device exchange architecture

The architecture for a distributed system of PoC MEDICAL DEVICEs in an INTEGRATED CLINICAL ENVIRONMENT (ICE) that is defined in this specification is following the concept of a CLINICAL WORKPLACE service-oriented medical device system (SOMDS).

A CLINICAL WORKPLACE SOMDS is based on the main principles of a service-oriented architecture (SOA). The relationships between these two are explained subsequently and in compliance with the Reference Model for Service Oriented Architecture 1.0 [B9].

There exist three major roles that a NETWORK NODE in a SOA may act in (see Figure 1).

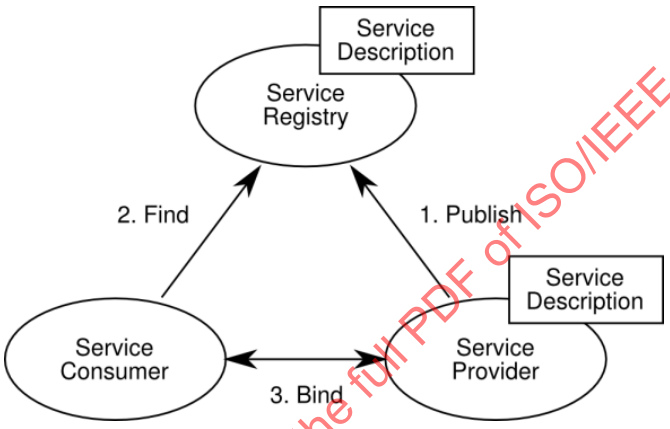

Figure 1—Major roles in a SOA

A SERVICE PROVIDER offers its capabilities by means of a SERVICE.

In a SOA, a SERVICE is a mechanism to enable access to one or more capabilities of a NETWORK NODE, where the access is provided by using a prescribed SERVICE INTERFACE and is exercised consistently with constraints and policies that are specified in conjunction with the SERVICE INTERFACE. The SERVICE INTERFACE with its constraints and policies is also called SERVICE CONTRACT. A SERVICE can send or receive MESSAGEs over at least one network endpoint.

NOTE 1—Typical network endpoints are network addresses like IP addresses.

NOTE 2—A SOA is commonly implemented with the Web Services technology. In the Web Services technology, MESSAGEs can be understood as SOAP messages (W3C SOAP 1.1 [B10]) that are transmitted, e.g., over HTTP.

A SERVICE PROVIDER announces itself with a SERVICE CONTRACT to a SERVICE REGISTRY. Hence, the SERVICE REGISTRY is a SERVICE PROVIDER that provides SERVICE CONTRACTs to a SERVICE CONSUMER and thus facilitates the discovery of SERVICEs.

A SERVICE CONSUMER needs a SERVICE in order to fulfill its purpose. After discovering a suitable SERVICE PROVIDER, the SERVICE CONSUMER establishes communication with the SERVICE PROVIDER by exchanging MESSAGEs.

The application of SOA principles to a distributed system of medical devices is called SERVICE-ORIENTED MEDICAL DEVICE SYSTEM (SOMDS). In addition to REQUEST-RESPONSE, NOTIFICATIONs, STREAMING, and discovery are used in a SOMDS to send MESSAGEs to SERVICE CONSUMERs.

7. Service-oriented device connectivity (SDC) participant model binding

All of the requirements in the following specifications are included by reference except where superseded by normative statements herein:

— IEEE Std 11073-10207, Clause 5 (Participant Model)

— IEEE Std 11073-10207, Clause 6 (Alert Signal Delegation)

— IEEE Std 11073-10207, Clause 8 (Extension Model)

— IEEE Std 11073-10207, Annex A (Extension Model)

— IEEE Std 11073-10207, Annex B (Participant Model)

7.1 Coded values

7.1.1 Coding system

R0001: An SDC PARTICIPANT SHALL use the ISO/IEEE 11073-1010X nomenclature and amendments whenever there exist an appropriate CODE.

NOTE 1—R0001 restricts the optionality from biceps:R0128 so that 11073 nomenclature becomes mandatory.

NOTE 2—Additional CODEs from other nomenclatures can be utilized by using pm:CodedValue/pm:Translation.

R0024: An SDC PARTICIPANT SHALL use a context-free numerical CODE representation if the CODING SYSTEM supports it.

NOTE 3—R0024 allows to directly locate the code in the nomenclature as no additional information like a partition is needed to find the concept that the code is representing. For ISO/IEEE 11073-1010X nomenclatures this translates to use the context-free nomenclature codes as defined in 7.2.1 in ISO/IEEE 11073-10101:2004.

7.2 Remote-control capabilities

7.2.1 Remote-control capabilities description

R0002: An SDC SERVICE PROVIDER SHALL describe all offered remote invocation capabilities to be transported via MDPWS using the pm:ScoDescriptor structure in pm: AbstractComplexDeviceComponentDescriptor/pm:Sco.

NOTE 1—R0002 clarifies biceps:R0011 so that all remote-control capabilities that use MPDWS as a transport protocol have to be described as CONTAINMENT TREE ENTRIES.

R0025: An SDC SERVICE PROVIDER SHALL ensure that the meaning of any remote invocation operation is specified by the combination of pm:AbstractOperationDescriptor/pm:Type and pm:AbstractOperationDesriptor/pm:OperationTarget.

NOTE 2— In order to allow an easier implementation that does not demand the parsing of pm:AbstractSetStateOperationDescriptor/pm:ModifiableData this specification requires the SDC SERVICE PROVIDER to provide pm:AbstractOperationDescriptor/pm:Type.

R0026: If pm:AbstractOperationDescriptor/@Type contains a CODED VALUE from a private CODING SYSTEM or a private part of a CODING SYSTEM, then an SDC SERVICE PROVIDER MAY specify the meaning by pm:AbstractSetOperationDescriptor/@ModifiableData.

NOTE 3—In order to allow a limited interpretation of the effect of an operation an SDC SERVICE PROVIDER is requested to include pm:AbstractSetOperationDescriptor/@ModifiableData.

R0027: An SDC SERVICE PROVIDER SHALL embed a mdpws:SafetyReq ELEMENT in the ext:Extension of a pm:AbstractOperationDescriptor if it requires safety information to be transmitted from an SDC SERVICE CONSUMER during a MESSAGE exchange that invokes a remote-control command.

NOTE 4—MDPWS requires the mdpws:SafetyReqAssertion to be inserted only at WSDL policy attachment points which imposes the need for an SDC SERVICE CONSUMER to parse the WSDL. Embedding the mdpws:SafetyReq directly into the MEDICAL DATA INFORMATION BASE (MDIB) allows easier implementation, better encapsulation, and allows the SDC SERVICE CONSUMER to not parse the WSDL. The SDC SERVICE PROVIDER can still include the WSDL policy attachments in the WSDL though.

R0057: If an SDC SERVICE PROVIDER requires safety information to be transmitted from an SDC SERVICE CONSUMER for a MESSAGE exchange, then the SDC SERVICE PROVIDER SHALL define XPath expressions for mdpws:SafetyContextDef/mdpws:Selector with an XPath root node that is equal to the pm:Mdib ELEMENT of that SDC SERVICE PROVIDER in the current MDIB version.

NOTE 5—R0057 defines the XPath root node as IEEE Std 11073-20702 does not define the root.

NOTE 6—Setting the XPath root node to pm:Mdib for the mdpws:SafetyContextDef/mdpws:Selector "./Your-XPath-Here" is equal to applying the following XPath expression to any XML Infoset that contains the type pm:Mdib: "//Mdib[1]/Your-XPath-Here", where Mdib[1] is referencing the first pm:Mdib element to be the root for the given XPath expression.

R0028: An SDC SERVICE PROVIDER SHALL provide a pm:AbstractOperationDescriptor/@SafetyClassification item for all pm:AbstractOperationDescriptor for all SCOs if erroneous or inadvertent invocation of the operation results in an unacceptable RISK.

NOTE 7—The implied safety classification for remote-control operations leads to a classification of "Inf" for all pm:AbstractOperationDescriptor which might not be the safe state for a remote-control operation and therefore it has to be considered if this is the value determined by the risk management.

R0060: The pm:AbstractOperationDescriptor/@SafetyClassification of each pm:AbstractOperationDescriptor SHALL correspond to the RISK related to erroneous or inadvertent invocation of the operation.

R0065: An SDC SERVICE PROVIDER SHALL send any modification that is a result of a remote-control command within the same MDIB version as the msg:OperationInvokedReport that indicate the finalization of the execution.

R0066: If an mdpws:SafetyContextDef does not reference one of the MDIB VERSIONING ATTRIBUTEs then an SDC SERVICE CONSUMER SHALL ensure that OPERATOR awareness of the content of each defined mdpws:SafetyContextDef ELEMENT of a pm:AbstractOperationDescriptor is achieved before remote-control command invocation of that operation.

NOTE 8—OPERATOR awareness can be achieved by displaying the information, labelling at the physical instance of the SDC SERVICE CONSUMER, labelling in the Instruction for Use of the SDC SERVICE CONSUMER, or other adequate means determined by the risk management of the SDC SERVICE CONSUMER. Labelling can comprise the content itself or the algorithm that is used to determine the content that will be transmitted as mdpws:SafetyContext .

NOTE 9—If for an MDIB VERSIONING ATTRIBUTE OPERATOR awareness is needed then surrogates may be utilized. Surrogates can be clinically relevant information entities that are derived from the descriptors or states in that version, e.g., "the current value" in combination with "the current unit" or other attributes of the descriptor and state.

7.2.2 Remote-control capability behavior

R0003: An SDC SERVICE PROVIDER MAY reject an incoming REQUEST-RESPONSE SERVICE OPERATION call on the SET SERVICE if the SERVICE CONSUMER has not subscribed to msg:OperationInvokedReport MESSAGEs in advance with

- **msg:InvocationInfo/msg:InvocationState set to "Fail"**
- **msg:InvocationInfo/msg:InvocationError set to "Oth"**

NOTE 1—R0003 relaxes biceps:R0057 so that a missing subscription now can lead to a failure.

NOTE 2—The identifying information from the X.509 certificate can be used to correlate REQUEST-RESPONSE SERVICE OPERATION calls on the SET SERVICE with previous subscriptions.

R0029: An SDC SERVICE CONSUMER SHALL not invoke a REQUEST-RESPONSE SERVICE OPERATION associated with a pm:AbstractOperationDescriptor that does not contain a specific pm:AbstractOperationDescriptor/@SafetyClassification.

NOTE 3—In R0029 "specific" means that the SafetyClassification ATTRIBUTE has not been empty during any MESSAGE transmission that includes the ATTRIBUTE from the SDC SERVICE PROVIDER to the SDC SERVICE CONSUMER.

R0077: An SDC SERVICE PROVIDER SHALL use the following pm:InstanceIdentifier for identifying an unknown SDC PARTICIPANT that invoked a SERVICE OPERATION:

- **@Root = "http://standards.ieee.org/downloads/11073/11073-20701-2018"**
- **@Extension = "AnonymousSdcParticipant".**

R0078: An SDC SERVICE PROVIDER SHALL use the following pm:InstanceIdentifier for identifying a known SDC PARTICIPANT that invoked a SERVICE OPERATION:

- **@Root = "http://standards.ieee.org/downloads/11073/11073-20701-2018/DistinguishedName"**
- **@Extension = the Common Name of the Distinguished Name of the x.509 Certificate of the SDC PARTICIPANT.**

7.3 Retrievability of containment tree entries

R0005: An SDC SERVICE PROVIDER SHALL include an msg:Retrievability ELEMENT as a descriptor extExtension for all CONTAINMENT TREE ENTRIEs that are retrievable via BICEPS SERVICEs other than the GET SERVICE.

R0030: An SDC SERVICE CONSUMER MAY assume that every CONTAINMENT TREE ITEM is retrievable via the BICEPS GET SERVICE even if no msg:Retrievability ELEMENT is included in the descriptor extension.

NOTE—Since CONTAINMENT TREE ENTRIEs might be retrievable by several methods, msg:Retrievability comprises a list of msg:RetrievabilityInfo ELEMENTs that describe the methods so that a SERVICE CONSUMER is able to determine which SERVICE OPERATIONs can be invoked or subscribed in order to get up-to-date information on the CONTAINMENT TREE ENTRIEs.

7.4 Dynamic containment tree changes

R0031: An SDC SERVICE PROVIDER SHALL utilize msg:DescriptionModificationReport with @ModificationType="Upt" to indicate modifications where the SDC SERVICE PROVIDER has determined that the change can negatively influence the utilization of the CONTAINMENT TREE ENTRY by an SDC SERVICE CONSUMER.

NOTE 1—R0031 addresses "breaking changes" such as updating the pm:AbstractMetricDescriptor/@SafetyClassification. Modifications are considered "breaking changes" if they can negatively influence the utilization of the CONTAINMENT TREE entry, i.e., if an SDC SERVICE CONSUMER can misinterpret old states by applying the updated descriptor to previously captured values. For example, if the safety classification changes to a MEDICAL SAFETY CLASSIFICATION and the SDC SERVICE CONSUMER applies this change to previous state versions that have not had a MEDICAL SAFETY CLASSIFICATION, it could falsely display these as suited for medical purposes, e.g., in trend views.

NOTE 2—In case an SDC SERVICE PROVIDER cannot determine if a modification can negatively influence the utilization of the CONTAINMENT TREE entry, it is reasonable to assume that it is a breaking change and therefore R0031 applies to these modifications.

R0073: An SDC SERVICE PROVIDER SHALL utilize a msg:DescriptionModificationReport having a msgDescriptionModificationReport/msg:ReportPart/@ModificationType="Del" or msg:DescriptionModificationReport/msg:ReportPart/@ModificationType="Crt" to indicate modifications where the SDC SERVICE PROVIDER has determined that the change cannot negatively influence the utilization of the CONTAINMENT TREE ENTRY by an SDC SERVICE CONSUMER.

NOTE 3—R0073 addresses "non-breaking changes" like adding a new channel to a VMD or changing the clinical relevance of metrics within a channel by resorting the list of pm:VmdDescriptor/pm:Channel.

R0059: If a PoC **MEDICAL DEVICE is capable to determine the value of a METRIC with more than one unit, then the SDC SERVICE PROVIDER SHALL provide for each METRIC a separate CONTAINMENT TREE ENTRY.**

NOTE 4—The SDC SERVICE PROVIDER sets pm:AbstractMetricState/@ActivationState to "StndBy" for all METRICs of a type that have just a different unit and are currently not activated but could be activated without requiring a reboot.

7.4.1 Modular PoC Medical Devices

If a PoC MEDICAL DEVICE changes its capabilities due to a physical removing of a subsystem, then the CONTAINMENT TREE history SHALL contain the following sequence:

— The pm:AbstractDeviceComponentState/@ActivationState of the removed subsystem is set to "Off" according to biceps:R0025.

— The CONTAINMENT TREE ENTRIEs of the removed subsystem as well as CONTAINMENT TREE ENTRIEs referencing a CONTAINMENT TREE ENTRY of the removed subsystem are removed from the CONTAINMENT TREE.

NOTE 1—A subsystem is represented by a VMD or channel.

NOTE 2—CONTAINMENT TREE ENTRIEs that might reference a CONTAINMENT TREE ENTRY of a removed subsystem are, e.g.,

— pm:AlertConditionDescriptor of a pm:AlertSystemDescriptor where the pm:AlertSystemDescriptor is located on a parent level relatively to the CONTAINMENT TREE ENTRIEs of the removed subsystem, or

— pm:AbstractOperationDescriptors of a pm:ScoDescriptor where the pm:ScoDescriptor is located on a parent level relatively to the CONTAINMENT TREE ENTRIEs of the removed subsystem.

7.5 MDIB versioning

An SDC SERVICE PROVIDER SHOULD determine the pm:MdibVersionGroup/@SequenceId using the UUIDv5 algorithm when the PoC MEDICAL DEVICE possesses at least one UDI where

— The namespace is the PRIMARY UDI of the PoC MEDICAL DEVICE in UUIDv5 form, where the PRIMARY UDI is calculated based on the entries in Table 2 for the UUIDv5 namespace and the pm:MdsDescriptor/pm:MetaData/pm:Udi/pm:HumanReadableForm for the UUIDv5 name.

— The name is a unique identifier of the InstanceId if available.

NOTE 1—In order to allow a data collector to store the messages received from a SDC SERVICE PROVIDER, it is beneficial if the MdibVersionGroup/@SequenceId is unique. In IEEE Std 11073-20701 the MdibVersionGroup/@SequenceId is just unique within one MdibVersionGroup/@InstanceId if provided, but not between different SDC SERVICE PROVIDERs.

NOTE 2—The unique identifier can either be pm:MdibVersionGroup/@InstanceId, if used or any other type of UUID, e.g., UUIDv4.

NOTE 3—The SDC Base Namespace for UUIDv5 Generation is defined in Annex A.

NOTE 4—Example for a namespace for PRIMARY UDI of PoC MEDICAL DEVICE for an FDA UDI where the pm:MdsDescriptor/pm:MetaData/pm:Udi/pm:HumanReadableForm is equal “(01)00884838038752(21)DE35115712” is 845754B1-8934-51D7-9EA1-203FB7A8B1B9 = uuidv5(“6F8C705D-3A57-5736-A501-972E826947E8”, “(01)00884838038752(21)DE35115712”).

Table 2—Calculated PRIMARY UDI to PRIMARY UDI UUDIv5 namespace mapping

PRIMARY UDI	SDC Base Namespace for UUIDv5 Generation	Name	Calculated PRIMARY UDI namespace
FDA UDI	72772F61-0266-49F9-9552-393C1857B269	fda-udi	6F8C705D-3A57-5736-A501-972E826947E8
EU UDI	72772F61-0266-49F9-9552-393C1857B269	eu-udi	99A295DD-8C45-52B2-8AF8-1C584FC4CDEE

7.6 Types

R0080: An SDC SERVICE PROVIDER shall define pm:AbstractDescriptor/pm:Type for ELEMENTs of the following TYPEs or any TYPE derived from the listed TYPEs:

— **pm:AbstractComplexDeviceComponentDescriptor**

— **pm:ChannelDescriptor**

— **pm:AbstractOperationDescriptor**

— **pm:AlertConditionDescriptor**

— **pm:AbstractMetricDescriptor.**

NOTE—R0080 defines that certain optional pm:AbstractDescriptor/pm:Type are mandatory to ease semantic interpretation of the ELEMENTs.

8. Communication model binding

All of the requirements in the following specifications are included by reference except where superseded by normative statements herein:

— IEEE Std 11073-10207, 7.1 (Communication Model—General)

— IEEE Std 11073-10207, Clause 8 (Extension Model)

— IEEE Std 11073-10207, Annex A (Extension Model)

8.1 Service

All of the requirements in the following specifications are included by reference except where superseded by normative statements herein:

— IEEE Std 11073-10207, 7.2 (Service Model)

— IEEE Std 11073-20702, Clause 6 (Service Description)

R0058: An SDC PARTICIPANT MAY utilize the TCP port 6464 for any MDPWS HOSTED SERVICE.

NOTE 1—The TCP port 6464 has been reserved with the IANA for medical device communication in accordance with this specification.

NOTE 2—The SDC SERVICE PROVIDER can utilize the port 6464 for an MDPWS Hosting Service and/or MDPWS Hosted Services.

NOTE 3—An SDC SERVICE COSUMER can utilize the port 6464 for an MDPWS Event Sink.

8.1.1 Subscription handling

R0034: An SDC SERVICE PROVIDER SHALL implement at least the following BICEPS SERVICEs as one MDPWS HOSTED SERVICE if the SDC SERVICE PROVIDER exhibits the capabilities that require the BICEPS SERVICE:

— **Description Event Service**

— **State Event Service**

— **Context Service**

— **Waveform Service**

R0035: An SDC SERVICE CONSUMER SHALL subscribe to NOTIFICATION and STREAMING MESSAGEs from the following BICEPS SERVICEs, if the SDC SERVICE CONSUMER needs the data transmitted with those MESSAGEs, with one wse:Subscribe MESSAGE if these BICEPS SERVICEs are transported using mechanisms defined in IEEE Std 11073-20702, Clause 7 (Eventing):

— **Description Event Service**

— **State Event Service**

— **Context Service**

— **Waveform Service**

R0056: An SDC SERVICE PROVIDER SHALL send an msg:DescriptionModificationReport MESSAGE before any MESSAGE from the BICEPS STATE EVENT SERVICE, WAVEFORM SERVICE, or CONTEXT SERVICE that contain the changed pm:AbstractState that is also comprised in the msg:DescriptionModificationReport.

NOTE 1—R0035 and R0056 guarantee that changes to the MDIB are transmitted in the correct MESSAGE order. The only exception is the msg:OperationInvokedReport as this does not convey the state of the MDIB directly.

R0036: An SDC SERVICE PROVIDER SHALL stop sending any NOTIFICATION or STREAMING MESSAGEs to a subscribed SDC SERVICE CONSUMER if the delivery of one MESSAGE related to a subscription of that SDC SERVICE CONSUMER failed and if these MESSAGEs are transported using mechanisms defined in IEEE Std 11073-20702, Clause 7 (Eventing).

NOTE 2—If an SDC SERVICE PROVIDER has stopped sending MESSAGEs to an SDC SERVICE CONSUMER due to a delivery failure and if the SDC SERVICE CONSUMER provides a wse:EndTo with its wse:Subscribe MESSAGE, then the SDC SERVICE PROVIDER sends a wse:SubscriptionEnd MESSAGE with wse:Status indicating a delivery failure.

8.1.2 Large payloads

R0067: An SDC SERVICE PROVIDER SHALL utilize the HTTP status code 413 (payload too large) to indicate if the response to a request MESSAGE could be satisfied but the content length would exceed the maximal MESSAGE length defined in MDPWS:R0006.

NOTE 1—R0067 most likely will occur for response MESSAGEs received from the BICEPS GET SERVICE, ARCHIVE SERVICE, and LOCALIZATION SERVICE.

NOTE 2—R0067 allows an SDC SERVICE CONSUMER to invoke the BICEPS operation where it received an HTTP status code 413 with a filter that limits the expected response, e.g., split the requested range of handles.

8.1.3 Description event service

If a PoC MEDICAL DEVICE is capable of being extended by removable subsystems, then the SDC SERVICE PROVIDER for that PoC MEDICAL DEVICE SHALL provide a BICEPS DESCRIPTION EVENT SERVICE.

8.1.4 Localization service

R0068: If a PoC MEDICAL DEVICE supports more than one language while being discoverable, then the SDC SERVICE PROVIDER SHALL provide these languages.

R0069: If an SDC SERVICE PROVIDER provides more than one language, it SHALL provide a BICEPS LOCALIZATION SERVICE.

NOTE 1—The BICEPS LOCALIZATION SERVICE is intended to be used if an MDIB contains many human-readable texts that would inflate SERVICE response and NOTIFICATION MESSAGE sizes.

NOTE 2—A PoC MEDICAL DEVICE is discoverable as an SDC SERVICE PROVIDER if it responds to explicit discovery MESSAGEs and sends out implicit discovery messages as defined in 9.1.

NOTE 3—A PoC MEDICAL DEVICE might not support multiple language while being discoverable if during operation that device can load only one language and the user would need to reboot to change languages.

8.1.5 Prioritization of connection establishment

R0076: An SDC SERVICE CONSUMER SHALL delay to send the first HTTP(S) MESSAGE regardless of the type to an endpoint after an implicit discovery MESSAGE has been received by a delay time Td where

- **there exists 10 priority groups with the identifiers 0-9 with 0 the highest priority and 9 the lowest priority, and the SDC SERVICE CONSUMER is configured to one of the priority groups, and**
- **the delay time Td is a random number that has the following properties: prio_group_id*5[s]<Td<(prio_group_id*5[s])+15 [s].**

NOTE 1—R0076 allows different configurations of priority groups for SDC SERVICE CONSUMER for different SDC SERVICE PROVIDER.

NOTE 2—R0076 allows an SDC SERVICE PROVIDER to limit the number based on a configured priority because they now establish connection in a timed sequence.

NOTE 3—R0076 reduces peak CPU and network loads for an SDC SERVICE PROVIDER when it is joining the network and announces itself, e.g., in case of a lost network connection or startup.

8.2 Message

All of the requirements in the following specifications are included by reference except where superseded by normative statements herein:

- IEEE Std 11073-10207, 7.3 (Message Model)
- IEEE Std 11073-10207, Annex C (Message Model)

8.2.1 Transmission

All of the requirements in the following specifications are included by reference except where superseded by normative statements herein:

- IEEE Std 11073-20702, Clause 4 (General Messaging)
- IEEE Std 11073-20702, Clause 11 (Message Serialization)
- IETF RFC 5227, IPv4 Address Conflict Detection

NOTE 1—Including IEEE Std 11073-20702 Clause 4 (General Messaging) satisfies biceps:R0093: A BICEPS BINDING SHALL provide means that allow to distinguish unique MESSAGEs in a sequence of MESSAGEs with potential duplicates.

NOTE 2—IEEE Std 11073-20702 Clause 11 (Message Serialization) allows the usage of compact transmission (W3C EXI 1.0 [B11]).

8.2.2 Request-response

All of the requirements in the following specifications are included by reference except where superseded by normative statements herein:

- IEEE Std 11073-20702, Clause 9 (Safe Data Transmission)

8.2.3 Publish-subscribe

All of the requirements in the following specifications are included by reference except where superseded by normative statements herein:

— IEEE Std 11073-20702, Clause 7 (Eventing)

8.2.4 Parameterized filtering for subscriptions

R0038: The Handle-based Filter Dialect is designated as 'sdc.filter://Handle' and comprises the following characteristics:

— **A Filter in this Dialect contains a white space delimited list of type pm:HandleRef as well as the pm:MdibVersionGroup/@SequenceId and pm:MdibVersionGroup/@InstanceId attached to the wse:Filter that indicate the fullqualified handles of the desired CONTAINMENT TREE ENTRIES.**

— **If a Filter in this Dialect references a CONTAINMENT TREE ENTRY and this CONTAINMENT TREE ENTRY is an instance of a pm:AbstractDeviceComponentDescriptor then the CONTAINMENT TREE ENTRY as well as any child CONTAINMENT TREE ENTRY are transmitted as NOTIFICATIONs for this subscription.**

NOTE 1—A Filter in this Dialect with no pm:HandleRef or pm:MdibVersionGroup specified defines a subscription to an empty set and therefore no NOTIFICATIONs will be transmitted for this subscription.

A fullqualified handle means the combination of the attributes @SequenceId and @InstanceId of pm:MdibVersionGroup together with the pm:HandleRef.

R0070: A given pm:HandleRef in a Handle-based Filter implies the subscription to all NOTIFICATIONs of this particular CONTAINMENT TREE ENTRY.

NOTE 2—R0070 does not include related objects to that CONTAINMENT TREE ENTRY that are referenced by a pm:HandleRef or reference the CONTAINMENT TREE ENTRY, e.g., ALERTs or OPERATIONs or the entries of a pm:AbstractMetricDescriptor/pm:Relation.

NOTE 3—This also implies that in case of a pm:AbstractDescriptor/@Handle where a multi state for that pm:AbstractDescriptor exists, the NOTIFICATIONs of all states of the multi state are subscribed to.

R0037: An SDC SERVICE CONSUMER SHOULD subscribe to EVENT SOURCEs using the Handle-based Filter Dialect in a wse:Subscribe MESSAGE if it is interested only in certain CONTAINMENT TREE ENTRY changes with a defined set of pm:Handle.

NOTE 4—"Interested" in R0037 means that the SDC SERVICE CONSUMER needs only certain CONTAINMENT TREE ENTRIEs to fulfill its intended purpose.

R0039: An SDC SERVICE PROVIDER SHOULD support filtering by the Handle-based Filter Dialect.

NOTE 5—If an SDC SERVICE PROVIDER does not support the Handle-based Filter Dialect, it has to respond to a wse:Subscribe MESSAGE that includes such a wse:Filter with a fault MESSAGE of type wse:FilteringRequestedUnavailable. No subscription is created.

8.2.5 Streaming

All of the requirements in the following specifications are included by reference except where superseded by normative statements herein:

— IEEE Std 11073-20702, Clause 8 (Streaming)

R0040: An SDC SERVICE PROVIDER SHALL include the endpoint reference as defined in OASIS DPWS [B8] in every STREAMING MESSAGE in the wsa:From ELEMENT.

NOTE 1—IEEE Std 11073-20702 defines the wsa:From header field as optional. To ensure resolving its origin of a STREAMING packet the wsa:From header as the source IP address might not suffice to do that, especially in cases where multiple SDC SERVICE PROVIDERs operate on a single NETWORK NODE.

R0041: An SDC SERVICE PROVIDER MAY utilize the mechanism of WS-Eventing as defined in Clause 7 of IEEE Std 11073-20702 for STREAMING purposes.

NOTE 2—Clarification of the requirements in IEEE Std 11073-20702 Clause 8 (Streaming) that even if STREAMING indicated the actual used transport may be not the one defined in IEEE Std 11073-20702 Clause 8 (Streaming) but those defined in IEEE Std 11073-20702 Clause 7 (Eventing).

9. Discovery binding

R0042: An SDC SERVICE PROVIDER SHALL include the dpws:DiscoveryType attribute in its portType WSDL description with the value "http://standards.ieee.org/downloads/11073/11073-10207-2017/ServiceProvider".

NOTE—R0042 satisfies biceps:R0123: A BICEPS BINDING SHALL define a discovery type to state compliance with IEEE Std 11073-20702.

9.1 Discovery mechanism

All of the requirements in the following specifications are included by reference except where superseded by normative statements herein:

— IEEE Std 11073-10207, Clause 9 (Discovery)

— IEEE Std 11073-20702, Clause 5 (Dynamic Discovery)

NOTE 1—Including Clause 5 of IEEE Std 11073-20702 satisfies biceps:R0078: A BICEPS BINDING SHALL provide means for implicit discovery.

NOTE 2—Including Clause 5 of IEEE Std 11073-20702 satisfies biceps:R0080: A BICEPS BINDING SHALL provide means for explicit discovery.

9.2 Complex device component based discovery

For every instance derived from pm:AbstractComplexDeviceComponentDescriptor in the MDIB an SDC SERVICE PROVIDER SHOULD include a URI-encoded pm:AbstractComplexDeviceComponentDescriptor/pm:Type as dpws:Scope of the MDPWS discovery messages. The URI encoding conforms to the following Extended Backus-Naur Form:

```
Scheme ::= 'sdc.cdc.type'
CodingSystem ::= Segment
CodingSystemVersion ::= Segment
Code ::= SegmentNz
CdcType ::= '/' CodingSystem '/' CodingSystemVersion '/' Code
CdcTypeUri ::= Scheme ':' CdcType
```

where

— `Scheme` is the Complex Device Component type URI scheme.

— The content of `CodingSystem` is the pm:CodedValue/@CodingSystem of pm:AbstractComplexDeviceComponentDescriptor/pm:Type. An empty `CodingSystem` expresses the use of the default CODING SYSTEM as defined in pm:CodedValue.

— The content of `CodingSystemVersion` is the pm:CodedValue/@CodingSystemVersion of the pm:AbstractComplexDeviceComponentDescriptor/pm:Type or the empty string if not specified.

— The content of `Code` is the pm:CodedValue/@Code of pm:AbstractComplexDeviceComponentDescriptor/pm:Type.

— `CdcTypeUri` is the encoded URI.

NOTE 1—`Segment` conforms to segment as defined in 3.3 in IETF RFC 3986.

NOTE 2—`SegmentNz` conforms to segment-nz, which is a non-zero-length segment, as defined in 3.3 in IETF RFC 3986.

NOTE 3—The requirement in this subclause satisfies biceps:R0134: A BICEPS BINDING SHALL make MDS types available for discovery.

NOTE 4—An example for a ventilator MDS is sdc.cdc.type:///70001. 70001 is the context-free code from 1::4465 from ISO/IEEE Std 11073-10101, which is the default CODING SYSTEM. Thus, CODING SYSTEM and CODING SYSTEM version are empty.

NOTE 5—Translations of the pm:CodedValue ELEMENTs can be added as separate dpws:Scope entries.

9.3 SDC PARTICIPANT KEY PURPOSE based discovery

For every SDC PARTICIPANT KEY PURPOSE that is also defined using the mechanisms for Trust Establishment (see 10.2.3), an SDC SERVICE PROVIDER SHOULD include a URI-encoded SDC PARTICIPANT KEY PURPOSE as dpws:Scope of the MDPWS discovery messages. The URI encoding conforms to the following Extended Backus-Naur Form:

```
Scheme ::= 'sdc.mds.pkp'
CodingSystem ::= Segment
CodingSystemVersion ::= Segment
Code ::= SegmentNz
Pkp ::= KeyPurposeOid
PkpTypeUri ::= Scheme ':' Pkp
```

where

— `Scheme` is the SDC PARTICIPANT KEY PURPOSE type URI scheme.

— The content of `KeyPurposeOid` is the textual representation of the OID of the SDC PARTICIPANT KEY PURPOSE.

— `PkpTypeUri` is the encoded URI.

NOTE 1—`Segment` conforms to segment as defined in 3.3 in IETF RFC 3986.

NOTE 2—`SegmentNz` conforms to segment-nz, which is a non-zero-length segment, as defined in 3.3 in IETF RFC 3986.

R0079: An SDC PARTICIPANT SHALL include the URI-encoded SDC PARTICIPANT KEY PURPOSE as defined in 9.3 for declaring its certified capabilities as defined in Table 3 in the dpws:Scope of the MDPWS discovery MESSAGEs.

9.4 Context-based discovery

For every associated context in the MDIB an SDC SERVICE PROVIDER SHOULD include a URI-encoded pm:AbstractContextState/pm:Identification as dpws:Scope of the MDPWS discovery messages. The URI encoding conforms to the following Extended Backus-Naur Form:

```
Scheme ::= 'sdc.ctxt.' ('loc' | 'pat' | 'ens' | 'wfl' | 'opr' | 'mns')
NullFlavorRoot ::= 'biceps.uri.unk'
Root ::= NullFlavorRoot | SegmentNz
Extension ::= Segment
InstanceIdentifier ::= '/' Root '/' Extension
ContextUri ::= Scheme ':' InstanceIdentifier ('?' Query)?
```

where

- `Scheme` designates the URI scheme that also encodes the location context type, i.e., `loc` is a location context, `pat` is a patient context, `ens` is a ensemble context, `wfl` is a workflow context, `opr` is an operator context, and `mns` is a means context.
- `NullFlavorRoot` encodes a null flavor root as defined by biceps:R0135.
- `Root` conforms either to the null flavor encoding or pm:AbstractContextState/pm:Identification/@Root if not null.
- `Extension` conforms to pm:AbstractContextState/pm:Identification/@Extension and is omitted if pm:AbstractContextState/pm:Identification/@Root is set only.
- `ContextUri` is the encoded URI.

NOTE 1—`Segment` conforms to segment as defined in 3.3 in IETF RFC 3986.

NOTE 2—`Query` conforms to query and contains non-hierarchical identification data as defined in 3.4 in IETF RFC 3986. `LocCtxtQuery` is a special instance of `Query`. It is defined in 9.4.1.2.

9.4.1 Location context

As location contexts are especially relevant for forming a CLINICAL WORKPLACE SOMDS this specification defines an algorithm to calculate an instance identifier if no instance identifier assigning authority is available in the SOMDS.

R0006: An SDC SERVICE PROVIDER SHALL determine the instance identifier for a location context using the Fallback Instance Identifier Algorithm as defined in 9.4.1.1 if no instance identifier assigning authority is available in the SOMDS.

9.4.1.1 Fallback instance identifier algorithm

An SDC SERVICE PROVIDER SHALL support the following algorithm specified in Extended Backus-Naur Form to determine an instance identifier for a location context from pm:LocationContextState\pm:LocationDetail:

```
Facility ::= SegmentNz
Building ::= SegmentNz
PointOfCare ::= SegmentNz
Floor ::= SegmentNz
Room ::= SegmentNz
Bed ::= SegmentNz
Delim ::= '/'
LocRootSegment ::= 'sdc.ctxt.loc.detail'
LocExtensionSegment ::= ((Facility)? Delim (Building)? Delim (Floor)?
Delim (PointOfCare)? Delim (Room)? Delim (Bed)?) - (Delim Delim Delim
Delim Delim) // at least 1 entry with 1 character
```

where

- `Facility` is taken from pm:LocationContextState\pm:LocationDetail/@Facility if available.
- `Building` is taken from pm:LocationContextState\pm:LocationDetail/@Building if available.
- `PointOfCare` is taken from pm:LocationContextState\pm:LocationDetail/@PointOfCare if available.
- `Floor` is taken from pm:LocationContextState\pm:LocationDetail/@Floor if available.
- `Room` is taken from pm:LocationContextState\pm:LocationDetail/@Room if available.
- `Bed` is taken from pm:LocationContextState\pm:LocationDetail/@Bed if available.
- `LocRootSegment` is the root of the instance identifier to identify a certain location.
- `LocExtensionSegment` is the extension of the instance identfier to identify a certain location.

NOTE—`SegmentNz` conforms to segment-nz, which is a non-zero-length segment, as defined in 3.3 in IETF RFC 3986.

9.4.1.2 Location context query transformation

An SDC SERVICE PROVIDER SHALL transform the pm:LocationDetail of an associated context to a scope URI where the query conforms to the following Extended Backus-Naur Form:

```
QueryItem ::= ('fac=' Facility) | ('bldng=' Building) | ('poc='
PointOfCare) | ('flr=' Floor) | ('rm=' Room) | ('bed=' Bed)
LocCtxtQuery ::= (QueryItem ('&' QueryItem)*)?
```

where

- `Facility` is taken from pm:LocationContextState\pm:LocationDetail/@Facility if available.
- `Building` is taken from pm:LocationContextState\pm:LocationDetail/@Building if available.
- `PointOfCare` is taken from pm:LocationContextState\pm:LocationDetail/@PointOfCare if available.
- `Floor` is taken from pm:LocationContextState\pm:LocationDetail/@Floor if available.

— `Room` is taken from pm:LocationContextState\pm:LocationDetail/@Room if available.

— `Bed` is taken from pm:LocationContextState\pm:LocationDetail/@Bed if available.

— `LocCtxtQuery` is put as a `Query` to the location context scope URI.

9.4.1.3 Location context details

An SDC SERVICE PROVIDER SHOULD provide the following ATTRIBUTEs in pm:LocationContextState\pm:LocationDetail if the SDC SERVICE PROVIDER is providing pm:LocationContextState\pm:LocationDetail.

— LocationDetail/@Facility

— LocationDetail/@PoC

— LocationDetail/@Bed

9.5 Announcing absence

NOTE—SERVICE CONSUMERs are encouraged to detect the absence of devices even if the SDC SERVICE PROVIDER has to send the announcement in case of communication failures, e.g., the message got lost.

10. Non-functional quality attributes

All of the requirements in the following specifications are included by reference except where superseded by normative statements herein:

— IEEE Std 11073-10207, Clause 10 (Non-functional Requirements)

NOTE—All requirements of this subclause are related to this specification only and are not implying any requirements that are beyond of the scope of this specification.

10.1 Cybersecurity

All of the requirements in the following specifications are included by reference except where superseded by normative statements herein:

— IEEE Std 11073-20702, Clause 10 (Security Considerations)

— IETF RFC 5246

NOTE 1—The BINDING to the requirements defined in Clause 10 of IEEE Std 11073-20702, especially TLS, satisfies biceps:R0087: An IEEE 11073-20702 compliant BINDING SHALL provide means that allows confidential transport of a MESSAGE between two PARTICIPANTS.

NOTE 2—The BINDING to the requirements defined in Clause 10 of IEEE Std 11073-20702, especially TLS, satisfies biceps:R0088: An IEEE 11073-20702 compliant BINDING SHALL provide means that ensures integrity of a MESSAGE during transport between two PARTICIPANTS.

NOTE 3—The BINDING to the requirements defined in Clause 10 of IEEE Std 11073-20702, especially TLS mutual authentication, satisfies biceps:R0089: An IEEE 11073-20702 compliant BINDING SHALL provide means that allows determining the originator of a MESSAGE .

NOTE 4—The BINDING to the requirements defined in Clause 10 of IEEE Std 11073-20702, especially TLS mutual authentication, biceps:R0084: A BICEPS BINDING SHALL provide means to allow the detection of corrupted data in a MESSAGE.

R0063: An SDC PARTICIPANT SHALL NOT use SSL2.0 (Hickman [B2]), SSL3.0 (IETF RFC 6101 [B6], TLS 1.0 (IETF RFC 2246 [B4]), or TLS1.1 (IETF RFC 4346 [B5]).

R0064: An SDC PARTICIPANT SHOULD utilize the highest TLS version.

NOTE 5—R0063 and R0064 restrict the use of secure channel mechanisms to versions that are considered to be secure at the time of release of this specification, but still allow interoperability of SDC PARTICIPANTs if a newer version of TLS is released after this specification.

R0074: An SDC PARTICIPANT SHALL establish an MDPWS SECURE CHANNEL only with other SDC PARTICIPANTs if an exchange of MESSAGEs with that SDC PARTICIPANT cannot result in an unacceptable RISK.

NOTE 6—R0074 restricts the use of a secure channel to trusted SDC PARTICIPANTs based on certificate information and certification chain.

R0043: An SDC PARTICIPANT SHALL transmit any MESSAGE that contains context information only via an MDPWS SECURE CHANNEL.

NOTE 7—R0043 satisfies biceps:R0120 as IEEE Std 11073-20702 defines a secure channel for all MESSAGESs to be TLS with mutual authentication.

NOTE 8—R0043 includes not only provisioning as a response to a request but also the provisioning as NOTIFICATION and as remote-control commands.

R0044: AN SDC PARTICIPANT SHALL transmit any MESSAGE that contains context information only to SDC PARTICIPANTs.

NOTE 9—R0044 restricts the transmission from any PARTICIPANT to only SDC PARTICIPANTs.

R0045: As Common Name of the Distinguished Name in X.509 certificates an SDC PARTICIPANT SHOULD use the PRIMARY UDI of the PoC MEDICAL DEVICE in UUIDv5 form as described in 7.5.

NOTE 10—R0045 makes the definition of white and black lists for access control manageable easily because you can calculate the white or black list entry without retrieving data from the SDC PARTICIPANT.

R0046: An SDC PARTICIPANT SHOULD NOT send a SOAP ENVELOPE without protecting the integrity of any Message Information Header blocks matching the following XPath expressions:

(a) /soap:Envelope/soap:Header/wsa:Action,

(b) /soap:Envelope/soap:Header/wsa:MessageID,

(c) /soap:Envelope/soap:Header/wsa:To,

(d) /soap:Envelope/soap:Header/wsa:ReplyTo,

(e) /soap:Envelope/soap:Header/wsa:RelatesTo,

(f) /soap:Envelope/soap:Header/wsa:FaultTo, and

(g) /soap:Envelope/soap:Header/*[@isReferenceParameter='true'].

NOTE 11—R0046 relaxes mdpws:R0018.

10.2 Patient safety

10.2.1 Information utilization

R0047: An SDC PARTICIPANT SHALL mitigate RISKs related to delayed or lost MESSAGEs if they result in an unacceptable RISK.

NOTE 1—An SDC PARTICIPANT does not need to consider delayed sending of MESSAGEs or loss of its sent MESSAGEs in its risk management as this is in the responsibility of the receiving SDC PARTICIPANT.

R0061: If an SDC PARTICIPANT uses information received from another SDC PARTICIPANT in a way that is not covered by the pm:AbstractDescriptor/@SafetyClassification, it SHALL mitigate RISKs related to erroneous information.

NOTE 2—The device manufacturer of an SDC SERVICE CONSUMER may consider that RISKs related to use according to the pm:AbstractDescriptor/@SafetyClassification does not lead to unacceptable RISKs due to erroneous information.

NOTE 3—Information that could be falsified is each CONTAINMENT TREE ENTRY in the MDIB. This includes METRICs, ALERTs, or CONTEXTs.

R0048: An SDC SERVICE CONSUMER SHALL utilize only METRICs where pm:MetricQuality/@Validity is either valid or validated if erroneous information results in an unacceptable RISK.

10.2.2 Operation utilization

R0062: An SDC SERVICE CONSUMER SHALL mitigate RISKs related to the erroneous or inadvertent invocation of an operation in correspondence to the pm:AbstractOperationDescriptor/@SafetyClassification.

NOTE—The device manufacturer of an SDC SERVICE CONSUMER has to consider that erroneous or inadvertent invocation of a pm:ScoDescriptor/pm:Operation could lead to a hazardous situations.

10.2.3 Trust establishment

As defined in 10.1, TLS is used for securing the communication between PARTICIPANTs.

R0051: An SDC PARTICIPANT SHALL utilize the Extended Key Usage (EKU) extension of the x.509 Certificate of a SERVICE CONSUMER to restrict modifications that modify performance characteristics if necessary to achieve freedom from unacceptable RISK.

NOTE 1—Examples are execution of remote-control commands or changing its alert signal generation behavior.

NOTE 2—R0051 satisfies biceps:R0083: A BICEPS BINDING SHOULD provide means to enable authorization capabilities between PARTICIPANTs.

NOTE 3—**R0052: An SDC PARTICIPANT SHALL include the SDC PARTICIPANT KEY PURPOSE for declaring its certified capabilities as defined in Table 3 in the Extended Key Usage (EKU) extension of the x.509 Certificate.**

NOTE 4—This specification defines two SDC PARTICIPANT KEY PURPOSEs that are exchanged during the communication between SDC PARTICIPANTs using the described means of R0051.

Table 3—Key purposes for declaring capabilities

SDC PARTICIPANT KEY PURPOSE	OID	Description
SDC SERVICE PROVIDER	1.2.840.10004.20701.1.1	Complies with all mandatory requirements for an SDC SERVICE PROVIDER as defined in the specification.
SDC SERVICE CONSUMER	1.2.840.10004.20701.1.2	Complies with all mandatory requirements for an SDC SERVICE CONSUMER as defined in the specification.

R0053: An SDC PARTICIPANT MAY include other SDC PARTICIPANT KEY PURPOSEs as defined in Table 3 if no standardized key purpose for declaring its certified capabilities is available.

NOTE 5—SDC PARTICIPANT KEY PURPOSEs **defined** in other specifications, e.g., in ISO/IEEE 11073-103XX, ISO/IEEE 11073-104XX, or proprietary specifications, can also be exchanged during the communication between SDC PARTICIPANTs using the described means of R0051.

R0075: An SDC PARTICIPANT MAY restrict modifications that modify performance characteristics based on information from x.509 Certificate or the certificate chain if necessary to achieve freedom from unacceptable RISK.

NOTE 6—R0051 defines that an SDC PARTICIPANT can utilize the SDC PARTICIPANT KEY PURPOSE of another SDC PARTICIPANT to restrict access to function based on the granularity of an SDC PARTICIPANT KEY PURPOSE. R0075 optionally extends R0051 as it allows an SDC PARTICIPANT to combine the information from SDC PARTICIPANT KEY PURPOSE with other certificate information or certificate chain information if the granularity of the SDC PARTICIPANT KEY PURPOSE is not fine-grained enough for an appropriate risk management.

R0054: An SDC SERVICE PROVIDER MAY detect lost connections to an SDC SERVICE CONSUMER by defining a short expiration time for subscriptions.

R0055: An SDC SERVICE CONSUMER MAY detect lost connections to an SDC SERVICE PROVIDER by requesting the subscription state or trying to renew a subscription in case it did not receive any MESSAGE from the SDC SERVICE PROVIDER for a defined amount of time.

NOTE 7—R0054 and R0055 satisfy biceps:R0127: A BICEPS BINDING SHALL provide means to allow the detection of the loss of connection from one PARTICIPANT to another PARTICIPANT.

10.3 Clinical effectiveness

10.3.1 Time synchronization

Time is inherently important to the function of a SOMDS. It provides a frame of reference between all PARTICIPANTs on the network and therefore allows correlating information between PARTICIPANTs with the given synchronization accuracy.

Moreover, time is also important for security as accurate clocks are needed to effectively validate certificates for TLS connections.

R0007: An SDC PARTICIPANT SHALL support time synchronization using the NTP version 3, IETF RFC 1305, or any compatible version previously mentioned.