Technical report „Medical device approval based on the SDC Participant Key Purpose standards for safe interoperability “

Björn Andersen, Paulinka Bandel, Jens Bartlog, Anna Feiler, Simon Gisch, Armin Janß, Martin Kasparick, Anton Keller, Gerd Matzke, Lorenz Rosenau, Stefan Schlichting

1 Table of Contents

2 Introduction – Benefits of interoperable medical device systems

Historically, medical device interoperability had been focussed on data transfer from medical devices to hospital information systems. In most solutions, this was achieved using gateways or protocol converters that translated different proprietary communication protocols into Health Level Seven (HL7) version 2 messages. To that end, the Integrating the Healthcare Enterprise (IHE) initiative provides integration profiles for consistent mapping of device data to HL7 v2 messages. Whereas this addresses the need for medical device data to be available in hospital IT systems, it does not facilitate clinical applications that require data exchange or external control between two or more medical devices. Therefore, current acute care medical devices such as ventilators, patient monitors, or infusion pumps are rarely capable of connecting to one another, much less of exerting external control [1]. Moreover, according to the National Institute of Standards and Technology (U.S.), “The lack of interoperability between medical devices can lead to preventable medical errors and potentially serious inefficiencies that would otherwise be avoided.” [2]

Clinical workplaces in high-acuity environments like the operating room (OR) or the intensive care unit (ICU) typically comprise medical devices and IT infrastructure from more than one manufacturer. Clinicians therefore need a solution that facilitates the integration of medical devices, IT systems, and software provided by multiple vendors. This solution must allow for independent innovation and product life cycles through loose coupling of the individual components and provide increased flexibility over proprietary integration solutions with predefined clinical functionality.

Therefore, medical device manufacturers, research organisations, and clinicians have joined forces to develop the interoperability architecture that was standardised as the ISO/IEEE 11073 Service-oriented Device Connectivity (SDC) series. SDC enables safe, effective, and secure data exchange and external control in an open connected system of medical devices. The original triad of SDC standards, which has come to be known as the SDC core standards, was published in 2018 and is being expanded since. They benefit patients and healthcare providers by facilitating the safe provision of System Functions, i.e. clinical functions that two or more devices from multiple manufacturers contribute to.

Systems of medical devices that communicate via SDC increase the availability of medical-grade clinical data from multiple sources at the point-of-care, thereby informing clinicians’ treatment decisions to improve patient outcome, reduce treatment errors, and streamline clinical workflows. In addition, they can integrate reliable administrative information from an Electronic Health Record (EHR) and report clinical observations, reducing demands on the staff and the cost of care. External control of medical devices and automation of clinical procedures can furthermore mitigate the risk of exposure to pathogens in the treatment of infectious or immunocompromised patients as well as support care provision in austere environments.

Offering sensitive personal data and critical services in a network of SDC participants entails exposing the medical devices to the risk of deliberate threats to information security. SDC therefore recommends established assessment and mitigation methods, such as mutual authentication of communication partners and asymmetric cryptography using digital certificates, to ensure confidentiality.

In addition to cybersecurity, the SDC standards also address the process of assessing and mitigating application risks. A more detailed description can be found in the SDC Conformance Principles [3].

The following sections explain how the most recent SDC standardisation efforts – the Participant Key Purpose specifications – support manufacturers and regulatory authorities in conducting the device approval and certification process for interoperable medical devices. Wherever this report refers to medical devices, the contents hold true for other participants in an SDC system.

3 ISO/IEEE 11073 SDC standards

The ISO/IEEE 11073 series of standards facilitates manufacturer-independent medical device interoperability. Whereas the Personal Health Device (PHD) standards in this series focus on the reporting of measurement data from patient-operated devices, the Point-of-Care Device (PoCD) standards focus on device-to-device communication in high-acuity environments. Both sub-series rely on a common nomenclature to ensure that recorded data is semantically interoperable throughout the entire process of care delivery.

Service-oriented Device Connectivity (SDC) constitutes the latest addition to the IEEE 11073 PoCD series focussing on networked interoperable medical device systems. ISO/IEEE 11073-10207 provides a Domain Information and Service Model that evolved from the previous ISO/IEEE 11073-10201 Domain Information Model. It is complemented by the ISO/IEEE 11073-20702 Medical Devices Communication Profile for Web Services (MDPWS), which serves as its transport technology. This modular standardisation allows for independence of the domain model from the underlying technical foundation. Only the ISO/IEEE 11073-20701 Architecture and Protocol Binding combines domain model and transport into a standard for a Service-Oriented Medical Device System (SOMDS).

The IEEE 11073 SDC standards integrate well with Health Level Seven (HL7) and DICOM: Whereas SDC provides unique capabilities such as bidirectional device communication, alert management, and external control, gateways may leverage HL7 version 2 and HL7 Fast Healthcare Interoperability Resources (FHIR) for retrieving administrative data and for reporting to clinical information systems as well as DICOM for medical imaging. Prototypes that connect IEEE 11073 SDC to clinical IT infrastructure as well as DICOM configuration management over SDC have been demonstrated in industry showcases (MEDICA 2019, DMEA 2019).

SDC now challenges proprietary systems of connected medical devices by providing a manufacturer-independent ecosystem for interoperable participants based on layered sets of requirements to support a wide range of use cases and deployment scenarios.

3.1 Medical Device Interoperability with SDC Standards

This section including Figure 1 is a modified excerpt from the dissertation draft of Björn Andersen. Copyright remains with the author.

The SDC standards form an integral part of the Medical Device Interoperability (MDI) standards landscape. *Figure 1*. shows how the SDC Standards can be leveraged to achieve different levels of interoperability as defined in the Levels of Conceptual Interoperability Model (LCIM) introduced by Tolk et al. [4].

The individual layers and their benefits are described below. From the bottom up, every layer requires the previous ones. Therefore, the standards normatively reference those below, transitively including those referenced therein. Protection against deliberate threats is not specific to any level of interoperability. Security must thus be considered at every layer.

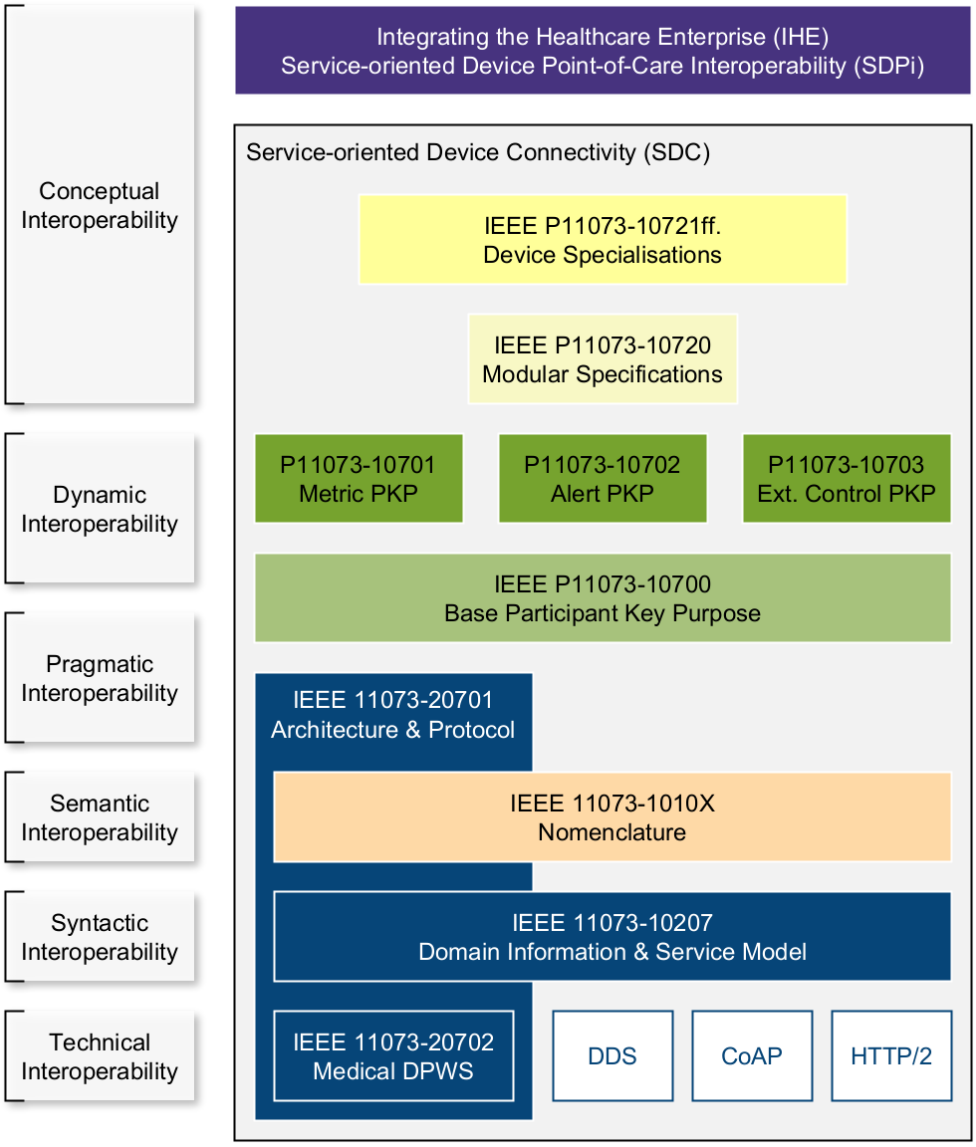

Figure 1 Medical device interoperability with SDC standards

IEEE 11073-20702 MDPWS ensures *technical interoperability* by providing a transport mechanism for all kinds of payload that needs to be exchanged between medical devices. Based on OASIS DPWS, it includes safety measures for use in medical devices. Whereas MDPWS is currently the only normatively defined transport for IEEE 11073 SDC, alternative technologies have been prototyped and could be used interchangeably in the mid-term future.

The Domain Information and Service Model defined in IEEE 11073-10207 provides the building blocks for modelling the network representation of real-world medical devices. It is structured as a tree, in which higher-level nodes denote components of a participant and leaf nodes represent Metrics, i.e. parameters such as measurements and settings. Alert systems and external control capabilities are also expressed in the model. The compulsory use of these data structures ensures *syntactic interoperability* in a SOMDS.

In order for this data to be interpreted consistently by devices and systems from all manufacturers, the same terminology codes from the IEEE 11073-1010X Nomenclature standards series must be used to describe every element of the participant description and current state. Applying these coding rules down to the level of every setting or parameter ensures *semantic interoperability*.

Many scientific publications on interoperability in healthcare do not consider the upper three layers of the LCIM, mostly because the context, interactions, and purpose of the participants

in question are often defined implicitly by the specific interoperability challenges they address. But for medical devices whose manufacturers are unable to foresee all the possible use cases that their System Function Contributions may facilitate, more stringent requirements need to be standardised.

The IEEE 11073-20701 Service-Oriented Medical Device Exchange Architecture and Protocol Binding lays the foundations for *pragmatic interoperability*. It maps the -10207 Service Model to the -20702 Web Services as well as including Quality-of-Service (QoS) and time synchronisation capabilities.

Building upon this foundation, the IEEE 11073-1070X Participant Key Purpose (PKP) standards, which are in focus of this technical report, offer the means to ascend to the level of *dynamic interoperability*. They introduce the decomposition of System Functions that are performed by two or more participants into System Function Contributions that can be allocated to the individual participants. These contributions entail responsibilities for the participants, which work like a contract: The other participants are safe to assume that these responsibilities are fulfilled, enabling manufacturers to perform risk management solely for their own System Function Contributions. IEEE 11073-10701 to -10703 address the different requirements for exchanging metric information, remotely managing alerts, and performing external control – all of which refer to IEEE 11073-10700 as a common base. Compliance to the PKP standards results in predictable interactions, thereby ensuring reliability and safety.

The highest level of *conceptual interoperability* cannot be achieved by technical means alone. It requires a common goal between medical devices as well as responsible organisations and the humans involved in the process of delivering care. Nevertheless, the effectiveness of System Functions can be supported through compliance to further standards and other specifications. Within the SDC series, IEEE 11073-1072X Device Specialisations provide modelling guidance and application-specific requirements for particular kinds of medical devices, such as high-frequency surgical equipment or endoscopic devices. By specifying the required and optional elements of the participants' network representations, they facilitate exchangeability of devices from different manufacturers. They may also define application-specific System Function Contributions, e.g. automatic illumination control provider/consumer that include by reference the more generic roles defined in the PKP standards as well as requirements towards the behaviour at runtime. Furthermore, responsibilities of the responsible organisation can be specified, including e.g. the presence of certain System Functions in the SOMDS or QoS requirements towards the clinical IT network infrastructure.

Specifications on the level of conceptual interoperability are also defined outside of standards, most notably by the Integrating the Healthcare Enterprise (IHE) initiative that publishes integration profiles leveraging existing standards. Regarding medical devices, the IHE Devices domain develops the Services-oriented Device Point-of-care Interoperability (SDPi) profiles that describe how to address specific use cases employing IEEE 11073 SDC standards as well as HL7 FHIR.

The connection from SDC to FHIR is important for the communication needs between medical devices and clinical IT systems, the latter of which would typically not feature an SDC interface. The link between both worlds is established by the Point-of-Care Device Implementation Guide [5] that is developed by the HL7 Devices-on-FHIR work group. It includes resource profiles as well as extensive mappings from the IEEE 11073-10207 participant model to FHIR.

3.2 The Participant Key Purpose standards – assuring the safety of open medical device systems

The SDC Conformance Principles [3] describe that each SDC system is a combination of medical devices and IT systems tailored to the individual clinical needs of the responsible organisation that operates the system. Hence, a manufacturer of an SDC participant must assure that the participant can provide its System Function Contribution in a safe way, even if the other participants in the system are not known at the time of development. Each manufacturer must consider the risks related to the SDC System Function Contribution in their

risk management. For example, the manufacturer of an SDC Service Consumer must consider whether the technical specifications of an SDC Service Provider are sufficient to safely implement a System Function together (see detailed description in the SDC Conformance Principles).

A clear allocation of responsibilities that is publicly available and known to the manufacturers of participants of an SDC system is required to make sure that all parts of the overall System Function are being taken care of. As described above, the SDC PKP standards will therefore define the allocation of responsibilities to the different components of a system and their respective manufacturers.

The SDC core standards define three basic mechanisms of interaction in a medical device system that System Functions with medical purposes build on: the exchange of metric data, alert data, and external control commands. The SDC PKP standards are thus divided into four parts representing these key interoperability purposes with the addition of common base requirements that apply to all participants.

It is important to note that the scope of the SDC PKP standards is not limited to allocating the responsibilities for the technical design of a System Function Contribution but includes consideration of all relevant tasks of medical device development by:

- ensuring a consistent risk management and human factors engineering for all SDC participants in the SDC system,
- requiring that the design process considers the safety and security of the component as well as of the overall system,
- defining the methods and steps necessary to verify and validate correct functionality of an SDC participant without knowing the other participants in an SDC system, and
- introducing documentation and labelling requirements for the participants.

The latter are especially relevant if the manufacturer needs to assign tasks or requirements to the responsible organisation, e.g. QoS requirements (such as bandwidth and packet loss rate) towards the medical IT network. Details on the concepts behind those requirements can be found in the SDC Conformance Principles [3].

In order to make use of these concepts in an interoperable medical device system, the SDC Participants need to be able to check whether they can rely on other SDC Participants to have fulfilled their part of the responsibilities for an overall System Function. This is solved through trust establishment introduced by the SDC protocol standard utilising information contained in the digital cryptographic certificates.

The FDA guidance document “Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices” [6] identifies design considerations for electronic interfaces. These have been regarded as requirements for the development of the SDC PKP standards. The qualification concept for the PKP standards has been laid out to demonstrate appropriate testing to provide evidence for safety, especially when SDC Participants are intended to communicate with other SDC Participants that are yet unknown at the time of technical design.

3.3 Outlook – Upcoming MDI standards and transition phase

Whereas the PKP standards are the decisive step forward to achieve safety for open medical device interoperability, conformance to them alone cannot ensure the availability and effectiveness of use of any given System Function. To increase the amount of safe assumptions that can be made about the capabilities of other SDC participants, additional standardisation efforts are underway.

The Device Specialisations introduced above will link SDC to the particular standards of the IEC 60601-2 series and require functionally similar devices to also have similar network representations by providing precise modelling instructions and further restrictions. Thereby they ease the exchangeability of devices from different manufacturers by reducing complexity inherent to different device capability representations.

Developed in parallel, the IHE SDPi profiles will specify the coordinated use of the SDC and FHIR medical device interoperability standards to develop solutions for the use cases and user narratives that require device interaction in the first place. And finally, architectures and frameworks that are developed by third parties, such as the Medical Device Interoperability Reference Architecture (MDIRA) Specification Document [7], may refer to and include the standards and profiles for the purpose of solving interoperability challenges in particular environments.

It is the responsibility of every medical device manufacturer to carry out a systematic and comprehensive risk management and human factors engineering process in order to integrate a product into an SDC system. While Device Specialisations and IHE Profiles are still under development, these processes are only supported by the interoperability specifications up to and including the PKP standards. Conceptual interoperability must be achieved by other means. Whereas not compromising safety, this can lead to temporary limitations in the availability of distributed System Functions or increased effort required to provide them effectively in early SDC deployments. Furthermore, the execution of very critical System Functions can be limited to known device type combinations whereas less critical functions can already be provided together with previously unknown SDC participants. With the availability of additional Device Specialisations and IHE Profiles, however, these limitations will gradually dissipate.

4 Conformity Assessment Goals

With the intended use of an SDC participant to include System Function Contributions in addition to standalone functionality, it needs to demonstrate safety, effectiveness, and security of these contributions. A major part thereof is conformance to the SDC standards. Therefore, conformity assessment programs are to be established (see SDC Conformance Principles [3], Sect. 7).

4.1 Establish trust between participants

In order to establish trust between SDC participants, products need to provide evidence that their conformance to the SDC standards has been demonstrated. Therefore, the consistent and appropriate implementation of the SDC protocol and the provision of appropriate information to other SDC participants and users need to be verified in a globally accepted way. To that end, conformity assessment programs should be developed as early as possible.

4.2 Consistent, modular system conformity assessment based on verification and validation of the individual SDC standards

Section 3.1 describes how the SDC standards follow a modular approach with several layers to enable different levels of interoperability. The set of standards a manufacturer chooses to comply with depends on the functionality to be implemented and the related risks. This modular approach extends to requirements towards the development process, such as risk management, verification, or documentation considerations, affecting the provision of appropriate information to network integrators.

The completeness of each standard layer with respect to its specific contribution to interoperability allows for separate testing of the individual layers from the bottom up. SDC conformance assessment thereby follows a similarly modular approach with different levels of conformance testing results specific to the individual SDC standards.

The benefit of this approach lies in its flexibility. It allows for future extension of capabilities of SDC participants, (backward compatible) protocol updates, etc. with an acceptable number of tests focused on the modified or added capabilities whereas enabling reuse of certifications for layers that are not affected by the changes.

These tasks require a careful segmentation of conformity tests and assessments with modular conformity statements, on which a summary conformity assessment of an SDC participant is performed with focus on additionally necessary integration testing.

Backward compatibility is required for SDC participants in order to integrate new SDC devices into networks with existing SDC devices. Backward compatibility is therefore also needed – as far as possible – for SDC conformity assessment procedures and assessment results.

Like in medical device standardisation, it is also advisable to separate process-related requirements (i.e. risk management, software development life cycle, etc.) from specific design-related requirements (i.e. implemented protocols, contents of information to the user, etc.) in a specific conformance test protocol.

4.3 Conformity assessment based on globally accepted public test methods

For each applicable SDC standard, the manufacturer must provide objective evidence for compliance. For the technical layers (IEEE 11073 SDC standards family), that evidence will likely be a technical standard compliance report for the applicable requirements based mainly on verification of the device SDC interface. Typically, a new or modified design of a certain layer requires testing of that layer and a functional integration test on the next higher layer level. For the use case-centred layers (e.g. SDPi profiles) different validation approaches, such as an IHE Connectathon, are more appropriate. This enables, e.g., to add or update a device specialisation purpose to an SDC participant, based on already tested and assessed unchanged implementation of key purpose standards and core standards.

To achieve global acceptance, test specifications and test protocol templates should be developed and made publicly available, thus also strengthening globally comparable performance and reproducibility of conformity assessments.

As SDC capability is – in many cases – an added-value feature for devices that also need type approval, e.g. as a medical device, independent of SDC, the intent is to include SDC conformity assessments into the technical documentation for SDC independent approval as a supplement (e.g. extended intended use, risk management, human factors engineering), which addresses especially safety and security aspects of its System Function Contributions. If an SDC participant is not a medical device (e.g. a data logger used in a medical application), the SDC conformity assessment should be included into the documentation that is required for the market release of this product.

4.4 Digital certificates for communicating standard compliance to SDC participants in an interoperable system

Compliance of a product to certain standards is communicated to other products via digital certificates (see section 3.2). Thus, participants in an SDC system can understand which SDC standards are supported by the connected device(s) and decide which related System Functions can be enabled in that system. Users may be notified of supported functionalities.

For establishing trust in the SDC capabilities, these digital certificates must be digitally signed by a designated authority. Initially, it will be sufficient for manufacturers to sign their own certificates. With the availability of a conformity assessment program, however, a governance body will define how compliance to the SDC standard requirements shall be demonstrated, including which organisations are qualified to certify compliance. As part of that responsibility, these organisations (e.g. test laboratories) are also going to inspect and sign the manufacturers' digital certificates.

In the meantime, it is in the responsibility of the manufactures' internal risk management to decide, based on the provided information, if they accept digital certificates from other manufacturers and therefore allow the execution of specific System Functions. This may lead to an intermediate state where low risk functionality, e.g. providing measurements, is provided to many participants, but critical functions, e.g. external control, is limited to a small number of qualifying consumers.

Every SDC participant is required to specify the supported certified System Function(s) in its digital certificate and to ensure that only certified System Functions can be executed. With this

approach, it is possible to determine the safe system functionality when integrating SDC participants and to avoid misuse of safety-critical functions.

5 References

[1] P. Provonost, M. M. E. Johns, S. Palmer, R. C. Bono, D. B. Fridsma, A. Gettinger, J. Goldman, W. Johnson, M. Karney, C. Samitt, R. D. Sriram, A. Zenooz and Y. C. Wang, Procuring Interoperability: Achieving High-Quality, Connected, and Person-Centered Care, Washington, DC: National Academy of Medicine, 2018.

[2] National Institute of Standards and Technology, “Medical Device Interoperability Fact Sheet,” Gaithersburg, MD, 2011.

[3] OR.NET e.V., “SDC Conformance Principles,” Herzogenrath, 2019.

[4] A. Tolk and J. A. Muguira, “The levels of conceptual interoperability model,” in *Proceedings of the 2003 fall simulation interoperability workshop*, 2003.

[5] HL7 Devices Work Group, “Point-of-Care Device Implementation Guide,” HL7 International, 1 September 2020. [Online]. Available: https://build.fhir.org/ig/HL7/uv-pocd/index.html.

[6] United States Food and Drug Administration, “Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices,” White Oak, MD, 2017.

[7] The Johns Hopkins University Applied Physics Laboratory, “Medical Device Interoperability Reference Architecture (MDIRA) Specification Document,” Laurel, MD, 2019.