JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Enclosure to AOS-L-21-1925

AOS Report No. (AOS-20-1754)

Publication Date: June 2021

Medical Device Interoperability Reference Architecture (MDIRA)

Version 2.1

Prepared for: U.S. Army Medical Research and Development Command

Prepared by:
The Johns Hopkins University
Applied Physics Laboratory
11100 Johns Hopkins Rd.
Laurel, MD 20723-6099

The Johns Hopkins Armstrong Institute for Patient Safety and Quality

Massachusetts General Hospital, Medical Device Interoperability and Cybersecurity Program

DocBox, Inc.

Trusted Solutions Foundry, Inc.

Task No.:	NH029
Contract No.:	N00024-13-D-6400
Distribution Statement A:	APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

ACKNOWLEDGMENTS

The authors thank the many content contributors and reviewers of this document and the prior draft releases. Pertinent to MDIRA Version 2.0, we extend special thanks to the following individuals for their in-depth technical reviews and commentary: Mr. Hinrich Althoff (Dräger, Inc.), Mr. Ken Fuchs (Dräger, Inc.), Dr. David Gregorczyk (Dräger, Inc.), Dr. Stefan Schlichting (Unity Consulting & Innovation, Inc.), and Dr. Steven Dain, MD (consultant for DocBox, Inc.). The contributions of these individuals does not necessarily imply their agreement to all the material herein. We also thank Ms. Barbara Johnson and Mr. Mark Mercready of JHU/APL's Editorial and Publications Section for their ongoing editorial support.

CONTENTS

FIGURES

TABLES

REVISION LOG

Rev.	Date	Description	By
–	14 October 2019	Release of Draft 1 of MDIRA Version 1.0	S. A. Gearhart
1	24 November 2019	Changes included in Draft 1.1: • Editorial corrections throughout • Update of Section 5 requirements • Content added in Sections 6.1.5 and 6.1.6 • Update of sequence diagrams in Appendix A	S. A. Gearhart
		Content planned for future drafts: • Elaboration of data nomenclature and data model requirements (Sections 5.1.19, 5.1.20, 6.1, and 6.2) • MDIRA requirements compliance criteria and descriptions of corresponding verification and validation activities • Standards gaps	S. A. Gearhart
2	Draft released for review December 2020; final release June 2021	Changes in Version 2.0: • Better clarified what is and is not within the MDIRA scope. • Removed some detail from Sections 2 and 3 because it seemed like a digression that broke the flow of the document. Some content moved to new Appendix C. • Added about 25 requirements to Section 5. • Removed about 13 requirements from Section 5. Added Appendix D, which lists those removed requirements. • Opted not to include standards gaps in this document. Team documented these elsewhere. • Added new Section 7 to introduce the topic of MDIRA conformance assessment.	MDIRA team
2.1	11 June 2021	Changes in Version 2.1 • Updated acknowledgement • Add missing requirement (102.0) to table 7-1.	J. M. Rizzuto

EXECUTIVE SUMMARY

Need and Operational Vision

In recent military conflicts, air superiority and relatively few casualties allowed medical treatment and evacuation within 60 minutes—the so-called Golden Hour. Today, Joint military planners cannot rely on these assumptions. In future military conflicts, and in civilian disaster events, limited air access and high numbers of casualties can result in overwhelming available medical and evacuation resources. Military and disaster relief first responders need autonomous medical care capabilities to sustain patients for up to several days until evacuation is possible.

In a notional scenario, a first responder connects critically injured casualties to autonomous care systems assembled from kits delivered to the site of care. Each system continuously monitors a patient's condition and provides autonomous medical interventions such as fluid resuscitation, ventilation management, and medication infusions. The autonomous care system allows a care-giver to leave a patient's side to attend to other casualties, perhaps even in other physical locations. A single caregiver can monitor the status of multiple patients via a mobile device. In the future, medical robots can be part of those systems, thereby further reducing the workload of medical personnel.

Broader Benefits

Realizing such systems to meet the immediate needs will require leveraging the concepts and technologies emerging in other industries. Doing so can transform how medical treatment is delivered in other care settings as well.

Autonomous medical care systems, whether in austere environments or in well-equipped hospitals, have the potential to provide:

- Skilled medical treatments delivered with fewer personnel, and reduced medical training required for those personnel
- Improved care outcomes through tighter control and reduced variability of medical treatments
- Improved patient safety by reducing actions involving personnel where errors and communication breakdowns can occur, particularly in repetitive tasks
- Reduced costs, as has been achieved in other industries

To develop these systems, medical devices and medical device systems must be interoperable and have interfaces that comply with commonly accepted standards.

Medical Device Interoperability Challenge

Today, diverse technological systems across the globe can seamlessly interface and share data in seconds, allowing once labor-intensive processes to occur now automatically in the background with little supervision. The increase in productivity and convenience for the average person has increased in ways unimaginable just a few decades ago. The same is true for financial, information technology, cable, manufacturing, aerospace, defense, and other industries. However, there are challenges such as increased risk of compromising sensitive information and cyber-attacks that are devastating for people and organizations. Nevertheless, there is common drive to expand the benefits while working to manage the risks.

Unfortunately, the healthcare industry lags behind other industries in achieving interoperable and secure systems and components. It is only in the last few years that the industry began to adopt health interoperability standards related to Electronic Health Record systems. Interoperability and security of medical devices lags even further. This, coupled with the increasing number and sophistication of medical devices in medical care settings, has increased risk to patients, increased workload for caregivers, increased potential for compromise of sensitive information, and limited opportunities for technological and medical advancement. Although several medical device interoperability standards are and have been available for more than a decade, the industry has been slow to adopt those standards.

It is expected that increasing needs for autonomous medical care systems will increase customer demand for interoperable and secure medical devices. A reference architecture that draws upon and extends the current interoperability standards is needed that enables the development of these capabilities.

Medical Device Interoperability Reference Architecture (MDIRA)

The Defense Health Agency funded the U.S. Army Medical Research and Development Command to research technical architectures to support autonomous medical systems for prolonged care in austere environments and hospitals of the future. The result is MDIRA, a technical framework intended to guide stakeholder organizations and industry in developing interoperable, safe, and secure medical device systems that will deliver advanced and autonomous medical care. The MDIRA research team is engaging stakeholders from Government, industry, academia, and civilian healthcare who are on the cutting edge of integrated clinical environments, closed-loop care systems, medical device and cybersecurity standards, and regulatory clearance and approvals for patient safety.

MDIRA will evolve incrementally. MDIRA Version 2.0 provides requirements and implementation guidance for MDIRA-conformant systems focused on trauma and critical care in austere environments.

Points of Contact

Please refer questions regarding this document to Ms. Catherine Carneal (240-228-5737) or Mr. Steven Griffiths (240-228-9472) of the Johns Hopkins University Applied Physics Laboratory (Main telephone 240-228-5000).

1. INTRODUCTION

1.1 Motivation and Project Overview

In recent military conflicts, air superiority and relatively few casualties allowed medical treatment and evacuation within 60 minutes—the so-called Golden Hour. Today, Joint military planners cannot rely on these assumptions. In future military conflicts, and in civilian disaster events, limited air access and high numbers of casualties can result in overwhelming available medical and evacuation resources. Military and disaster relief first responders need autonomous medical care capabilities to sustain patients for up to several days until evacuation is possible.

Autonomous medical care systems, whether in austere environments or in hospitals, have potential to provide the following:

- Skilled medical treatments delivered with fewer personnel, and reduced medical training required for those personnel
- Improved care outcomes through tighter control and reduced variability of medical treatments
- Improved patient safety by reducing actions involving personnel where errors and communication breakdowns can occur, particularly in repetitive tasks
- Reduced cost of care through autonomy, as has been achieved in other industries

To develop these systems, medical devices and medical device systems (MDSs) must be interoperable and have interfaces that comply with commonly accepted standards.

Unfortunately, the healthcare industry lags behind other industries in achieving interoperable and secure systems and components. It is only in the last few years that the industry began to adopt health interoperability standards related to Electronic Health Record (EHR) systems. Interoperability and security of medical devices lags even further despite work in the area since the early 1980's. This, coupled with the increasing number and sophistication of medical devices in medical care settings, has increased risk to patients, increased workload for caregivers, increased potential for compromise of sensitive information, and limited opportunities for technological and medical advancement. Although several burgeoning medical device interoperability standards have been available for over two decades, the industry has been slow to adopt those standards.

It is expected that increasing needs for autonomous medical care systems will increase customer demand for interoperable and secure medical devices. A reference architecture that draws upon and extends the current interoperability standards is needed to enable the development of these capabilities.

The charter of the Medical Device Interoperability Reference Architecture (MDIRA) project is to specify and prototype a technical framework that guides stakeholder organizations and industry in developing interoperable, safe, and secure MDSs that will deliver advanced and autonomous medical care for patients in austere environments and hospitals of the future. Through open-architecture modular design principles that draw upon industry-consensus standards and best practices, MDIRA supports the development of MDSs with operational flexibility that enables the flow of patient data and the ability to perform medical interventions at the device level. MDIRA also allows developmental extensibility for insertion of emerging technologies such as autonomous medical care protocols, devices, and systems; medical robots; and artificial intelligence (AI). The Defense Health Agency (DHA) funded the MDIRA project, and the U.S. Army Medical Research and Development Command (MRDC) is the executing organization.

1.2 MDIRA Users and Stakeholders

While the military has significantly advanced MDIRA as described within this document to address operational battlefield needs, the specification has received input from and is relevant to the broader medical care and first responder communities. The intended users and stakeholders of MDIRA include, but are not limited to, the following:

- Civilian and Joint military medical treatment organizations that use and procure MDSs
- Disaster response organizations that use and procure MDSs
- Vendors, developers, and researchers of the following:
  - Medical devices (e.g., infusion pumps and vitals monitors)
  - Patient care software applications (e.g., diagnostics and clinical decision support applications)
  - Autonomous medical care systems (e.g., autonomous hypotension management)
  - Medical robots (e.g., autonomous or semi-autonomous intubation)
  - Medical evacuation vehicles and on-board support systems
- Researchers of advanced prescriptive and predictive analytics for medical care applications [e.g., AI- and machine learning (ML)-based decision support]
- Standards development organizations (SDOs)

1.3 MDIRA Version 2.0 Scope

1.3.1 Operational Scope

Interoperable, autonomous, safe, and secure MDSs are relevant to a wide range of medical uses in a wide range of medical settings. Ideally, the process of developing MDIRA would involve rigorous consideration of all possible uses. In practice, however, some bounding of the scope is necessary to achieve meaningful incremental process. By focusing on several challenging, high-priority needs, it is expected that a MDIRA that meets these needs would also support a range of other needs. Maturation of MDIRA over time will include expanding to other medical needs and operational settings.

MDIRA Version 2.0 focuses on MDSs for critical care in austere joint combat operations and in civilian and military disaster relief settings including telemedicine support. Restricted physical access in these austere settings can hinder the evacuation of injured personnel and the delivery of medical resources (personnel and supplies) to the site. Therefore, a key operational objective of MDIRA is guiding the development of advanced medical systems to support patient care for up to 3 days prior to evacuation. The need for prolonged critical care, combined with potentially high casualties with limited medical personnel, requires these advanced systems to support autonomous medical care technologies.

The types of medical care resources pertinent to MDIRA Version 2.0 support general trauma and critical care in the field with consideration of the following specific conditions:

- Severe burns
- Pulmonary insufficiency and respiratory depression
- Acute renal failure
- Multi-system organ failure
- Cranio-cerebral trauma
- Hemorrhage and coagulopathy
- Infectious disease and progression to septic shock

1.3.2 Scope of MDIRA

MDIRA establishes requirements and implementation guidance for the functional and information architectures, as well as non-functional characteristics, of MDIRA-conformant medical care systems and their components. Key MDIRA topics include the following:

- System health and status monitoring
- Technical enablers for system reliability and patient safety
- Data integrity, confidentiality, and validity
- Discovery of components that connect to the system
- Authentication of components and system users
- Trusted authorization for a component to change the settings of another component (i.e., trusted control)

- Time synchronization of data streams
- Data logging
- Use of standard information models, controlled vocabularies, and semantics.

To provide industry as much design flexibility as possible, an objective for MDIRA was not to be overly prescriptive. For example, requirements for component authentication and system health and status monitoring do not prescribe the details of how those functions will be implemented. In addition, the emphasis here are the technical enablers for advanced patient care systems, not clinical particulars of the devices and software applications operating within the system.

The scope of MDIRA does not include requirements that would derive from a system's unique operational requirements or from industry-specific standards [e.g., Military Specifications (MIL-SPECs)] that dictate design particulars and qualification requirements for applications, customers, and deployment settings. For example, MDIRA does not consider the following:

- Specifics on user interface implementations (i.e., data entry and displays)
- Physical characteristics such as form factor, and mechanical and electrical interfaces
- Operating and non-operating environments
- External power supply and battery requirements
- Performance requirements that flow from specific operational requirements in particular operational contexts (e.g., communications availability and reliability requirements tied to a remote austere environment)
- Particulars of how a MDIRA-conformant system is deployed to a specific operational domain (e.g., hospital, austere military setting)
- Methods of supply and preservation (e.g., refrigeration) of medical consumables (e.g., fluids, blood, medication) used in the patient's medical care, although a MDIRA-conformant system can have an application that tracks the usage of these medical consumables thus supporting the re-supply process

Practical deployment of MDIRA-conformant systems will require rigorous assessment of these types of operational considerations.

1.4 Overview of this MDIRA Document

This remainder of this document is organized as follows:

- Section 2 provides background on the conceptual underpinnings of MDIRA and how it is to be used.
- Section 3 describes the MDIRA operational objectives.

- Section 4 describes the scope of MDIRA with regard to the external entities with which a MDIRA-conformant system may interact. It also describes the functional components.

- Section 5 presents MDIRA requirements for these components.

- Section 6 provides implementation guidance to system and component developers.

- Section 7 introduces the subject of MDIRA conformance assessment. This section will mature in subsequent MDIRA updates.

- Section 8 lists the references cited in this document.

- Appendix A provides sequence diagrams that elaborate selected functional behavior and data flow.

- Appendix B provides a glossary of terms used in this document.

- Appendix C provides one of the operational scenarios used as foundation for MDIRA requirements analysis.

- Appendix D lists requirements from the previous MDIRA version (Version 1.0) that are removed from this version (Version 2.0).

- Appendix E provides consideration for alarm management.

- Appendix F defines the acronyms used in this document.

1.5 Maturation and Management of MDIRA

Under the auspices of the U.S. Army MRDC, the Johns Hopkins University Applied Physics Laboratory (JHU/APL) will release approved updates of MDIRA to military, civilian, industry, health standards, and research stakeholders for community review and comment. JHU/APL will receive and adjudicate these comments for subsequent releases.

2. BACKGROUND

2.1 Medical Device Interoperability Standards

Perhaps the earliest concerted effort in developing medical device interoperability standards was the Institute of Electrical and Electronics Engineers (IEEE) 1073 project dating to the mid-1980s, which resulted from industry discussions in prior years. This work culminated in several interoperability demonstrations using highly specified data transport protocols and implementations in the late 1980s and early 1990s. Industry was not very receptive, however, because of concerns about cost of adoption coupled with poor market incentive.

Much of the momentum of IEEE 1073 shifted to Europe in the 1990s, including the engagement with the European Committee for Standardization (CEN) Technical Committee 251 (TC251), which resulted in two CEN standards that eventually became the IEEE 1073 Nomenclature and Domain Information Model for transport and application profile specifications. Note that briefings from the 1990s explicitly called out plug-and-play (PnP) interoperability as the key scope for the IEEE 1073 standards family.

In the early 2000s, a process was established to advance the jointly developed and branded IEEE, International Standards Organization (ISO), and CEN 11073 family of medical device interoperability standards building on the IEEE 1073 foundation (see https://standards.ieee.org/ for access to IEEE 11073 standards). In about this same timeframe, work began on standardizing Health Level 7 (HL7), an interoperability standard for EHR systems, for capturing data from medical devices. To this end, the HL7 International and Integrating the Healthcare Enterprise (IHE) organizations established device working groups to develop profiles prescribing how HL7 Version 2 and IEEE 11073 standards should be used to implement transfer of data to EHRs and hospital billing systems (see https://www.ihe.net/).

Parallel to this work, efforts continued on the ISO/IEEE 11073 standards with a focus on personal health devices (PHDs) (e.g., weight scale, blood pressure monitor). In 2006, the Continua Health Alliance was founded (now the Personal Connected Health Alliance) to begin work on the Continua Design Guidelines that leveraged ISO/IEEE 11073 PHD standards and other standards to guide implementation of integrated PHD and health information system solutions.

The previous efforts did achieve some important interoperability objectives. For example, major EHR developers and medical device manufacturers implemented common solutions to bring selected medical device data into EHR systems. In addition, a few medical device manufacturers used parts of the IEEE 11073-10101 Nomenclature standard (Reference [1]) and a few adapted parts of the IEEE 11073-10201 Domain Information Model (DIM) standard (Reference [2]). Even given these efforts, however, manufacturer adoption of IEEE 11073 standards for their individual medical devices has been slow and much work remains for the medical community to achieve ubiquitous medical device interoperability. Much of the reluctance in adoption of IEEE 11073 is related to manufacturers not wanting to open up their systems to other vendors, limited hospital system resources to invest in capital information technology assets, and the regulatory frameworks that existed in the past.

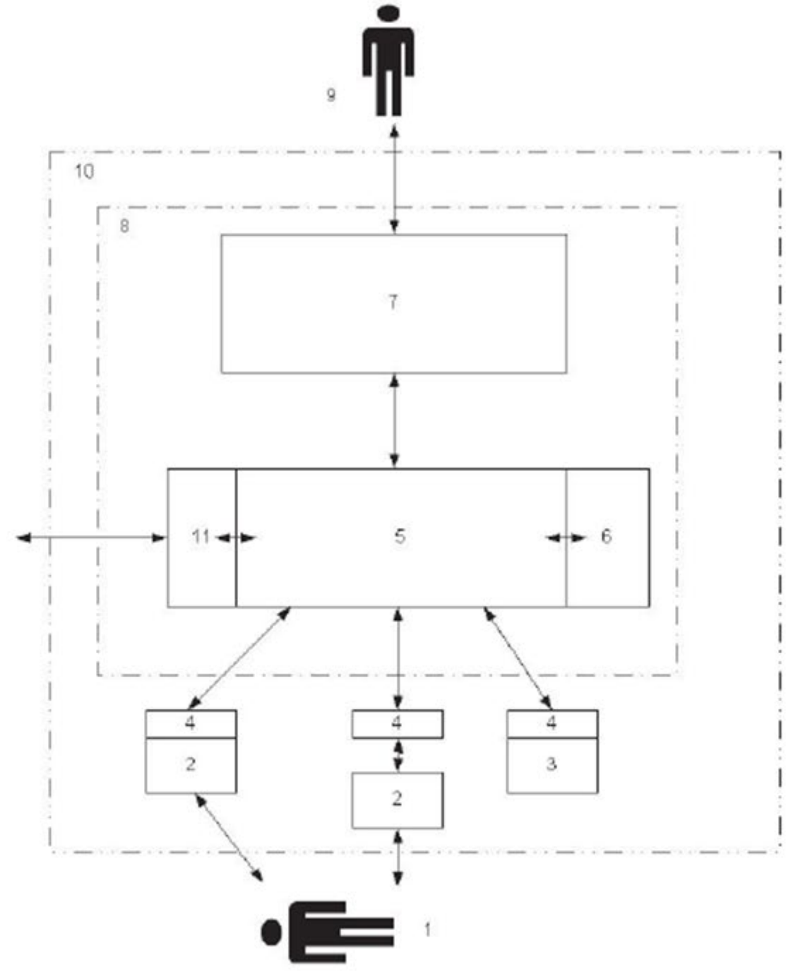
Leveraging the work over the preceding 20 to 25 years, initial development of the ISO/IEEE/CEN 11073 Service-oriented Device Connectivity (SDC) family of standards (see https://standards.ieee.org/) began around 2010, with the first published standards in 2014. Built on the foundation of legacy efforts, this recent family of 11073 standards reflects advances in technology and lessons learned from prior standard adoption challenges.

2.2 Integrated Clinical Environment (ICE)

ICE is a standardized architecture for interoperable medical systems. It was first proposed and developed by a group convened under auspices of the Medical Device Interoperability and Cybersecurity Program (MD PnP) circa 2004 and then formally defined in American Society for Testing and Materials (ASTM) F2761-09 (the "ICE standard") in 2009 (Reference [3]).

Because of its general applicability to interoperable medical devices, the ICE architecture was recognized by the U.S. Food and Drug Administration (FDA) in 2014 and since then has informed FDA's regulatory policies on medical device interoperability (Reference [4]). In 2019, the ICE architecture was accepted by the American National Standards Institute (ANSI) and the Association for the Advancement of Medical Instrumentation (AAMI) (as standard number ANSI/AAMI 2700-1) as a national standard (Reference [5]). Since its inception, the ICE architecture has been widely adopted as a conceptual functional framework for enabling, promoting, and assessing interoperability solutions. Example ICE instantiations include openICE (Reference [6]), DocBox (Reference [7]), and Dräger's openSDC (open Smart Device Connect) (Reference [8]). Notably, the ICE architecture also lays the foundation for basic safety, cybersecurity, and essential performance standards for interoperable medical systems [e.g., AAMI 2700-2 (Reference [9]) and ANSI/AAMI/UL 2800-1:2019 (Reference [10])]. ICE inspired the IEEE 11073 SDC standards, the most recent additions to IEEE 11073 family of standards.

Rather than prescribing technical solutions for realizing interoperability, the ICE architecture defines a set of capabilities essential for interoperable medical systems—each as a generic functional component—and how such capabilities should interact with each other. As illustrated in Figure 2-1, the core of the ICE architecture is the notion of the ICE Supervisor, which provides a platform for functional integration of medical devices and equipment connected to the system. The architecture also provides a platform to host intelligent (software) applications that implement clinical functions (e.g., clinical decision support) or instruct the system to achieve its intended medical use. Data exchange among the ICE Supervisor, other ICE components, and connected devices and equipment is managed and facilitated through the ICE Network Controller, a concept independent of specific networking technologies. ICE-compliant medical devices and equipment communicate with the ICE Network Controller through ICE equipment interfaces, developed as part of device development or afterward, that translate standardized health and technical data to the devices' own communication protocols. (ICE equipment interfaces would not be necessary for fully compliant ICE devices.) External systems, such as EHR systems, communicate with an ICE system through the ICE Network Controller (via ICE external interfaces). A standard ICE architecture also requires methods for logging clinical and technical data to enable analysis of patient-related events, ICE system performance, and continuous system improvement.



Key

1 PATIENT
2 MEDICAL DEVICE
3 equipment
4 ICE EQUIPMENT INTERFACE
5 ICE NETWORK CONTROLLER
6 data logger
7 ICE SUPERVISOR
8 ICE manager
9 OPERATOR
10 ICE
11 external interface

NOTE 1 Figure 1 is not intended to represent a specific physical configuration of ICE components, but to represent the functional relationships between the major elements of an ICE.

NOTE 2 A MEDICAL DEVICE or equipment can or need not have OPERATOR-accessible interfaces.

Figure 2-1 Conceptual Functional Model of ICE

2.3 Reference Architecture

A Reference Architecture is a template that guides the development of a particular system type so that systems built using this template possess attributes deemed important by the stakeholder community associated with those systems. Reference Architectures exist in many industries, for many types of systems, including submarine systems, ship combat systems, autonomous air vehicles (Reference [11]), autonomous ground vehicles (Reference [12]), and robotic systems (Reference [13]). A Reference Architecture typically provides or consists of the following:

- Nomenclature standards (i.e., standards that specify numeric codes for each data item communicated between systems, as well as the corresponding definition)
- Common system and data security requirements
- Common function and component taxonomies
- Identification of industry interoperability standards and guidance relating to data definition, representation, and transport
- Core capabilities and functions allocated to architectural components
- Functional handshaking between connected components
- Guidelines for implementing systems that comply with the reference architecture

As shown in Figure 2-2, a Reference Architecture supplements the system requirements and developmental specifications for a system that performs specific operational functions. MDIRA focuses on the development of advanced medical care systems that include autonomous capabilities.

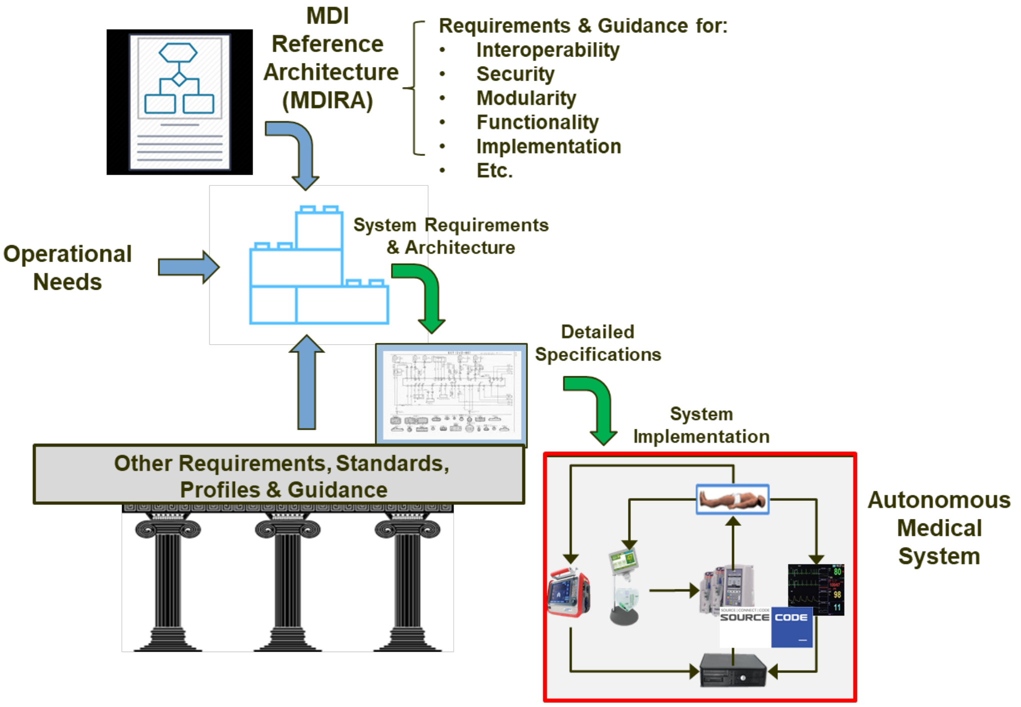

MDI Reference Architecture (MDIRA)
Requirements & Guidance for:
• Interoperability
• Security
• Modularity
• Functionality
• Implementation
• Etc.
Operational Needs
System Requirements & Architecture
Detailed Specifications
System Implementation
Other Requirements, Standards, Profiles & Guidance
Autonomous Medical System
SOURCE CODE

Figure 2-2 Role of MDIRA in Development of Autonomous Medical Systems

2.4 Key Definitions

The following definitions lay the foundation for subsequent sections. Appendix B provides a comprehensive glossary of terms.

- **Authentication**: The process of verifying the identity of users, devices, and processes within a system. Correctly identifying these entities is a key part of implementing robust access control, a security measure. In context of MDIRA, the term *authentication* is used in reference to validating the credentials of a component that is connected into the communications architecture of a MDIRA-conformant medical care system.

- **Authorization**: Authorization provides the access rights to resources for users, devices, and processes by defining access policies imposed throughout the system. In MDIRA, the term *authorization* is used extensively in reference to granting permission for a component in a MDIRA-conformant system to interact in a particular manner with another component. For example, MDIRA prescribes that a supervisory function must authorize a component before it can control the operations of another component.

- **Autonomy**: (1) Capacity to monitor, select, and execute a clinical function with no or limited operation intervention (Reference [14]). (2) An unmanned system's own ability of sensing, perceiving, analyzing, communicating, planning, decision-making, and acting or executing to achieve its goals as assigned by its human operator(s) through designed human-computer interaction or assigned by another system with which the unmanned systems interact (Reference [11]).

- **Device model**:An abstract representation of capabilities and characteristics of a device that can be accessed and operated externally in a particular context of use, typically including data types, relationships, and nomenclature used for input and output of observations and controls (Reference [15]). AAMI 2700-1 (Reference [5]) provides insightful elaboration.

- **Information model**: A representation of concepts and the relationships, constraints, rules, and *operations* to specify *data semantics* for a chosen domain. An information model provides a sharable, stable, and organized structure of information requirements for the domain context. A Device Model (see previous definition) is a specific type of information model representing attributes and capabilities of a medical device.

- **Integrated clinical environment**: An environment that combines heterogeneous medical devices and other equipment to create a medical system for the care of a single patient (adapted from Reference [5]).

- **MDIRA-conformant system**: An ICE that complies with the MDIRA. Unless otherwise evident from the context, the term *system* in this document generally refers to a MDIRA-conformant system.

- **MDIRA-conformant component**: Parts of a MDIRA-conformant system that may include medical devices, medical and non-medical software applications, system management components, and other support equipment. Section 4.4 describes the functional components of a MDIRA-conformant system.

- **Medical device**: Appendix B provides the FDA definition of a medical device that ranges in scope from tongue depressors to complex medical equipment. Within this spectrum, MDIRA's emphasis is on the following:

  – **Medical electrical equipment (MEE)**: Electrical equipment having an applied part or transferring energy to or from the patient or detecting such energy transfer to or from the patient for the purpose of diagnosis, treatment, or monitoring of the patient (adapted from Reference [14]).

  – **Medical electrical systems (MES)**: Combination, as specified by its manufacturer, of items of equipment, at least one of which is MEE to be interconnected by functional connection or by use of a multiple-socket outlet (e.g., multi-parameter patient vital signs monitor) (Reference [14]).

  – **Software-as-a-medical device (SaMD)**: Software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device (Reference [16]). Note that a MDIRA-conformant system may also include medical software applications that do not meet the formal SaMD definition in the references.

  – **Medical robot**: Robot intended to be used as MEE or MES (Reference [14]).

- **Nomenclature**: A data item's numeric code communicated between systems as well as the corresponding definition.

- **Plug-and-play (PnP)**: (1) Ability of medical devices, clinical systems, or their components to communicate to safely fulfill a manufacturer's intended purpose without custom integration or development (Reference [15]). (2) Seamless connection and disconnection ("hot swapping") of medical devices without having to shut down and reboot the medical devices or the system to which the devices are connected (Reference [5]).

- **Profile**: Specification showing in detail how to apply existing standards by restricting or constraining requirements in the referenced standards (Reference [15]).

- **Registration**: The process of making authenticated components in a MDIRA-conformant system available to support the system's medical operations. For example, MDIRA requires a component to perform a successful power-on self-test (POST) as prerequisite to it being registered.

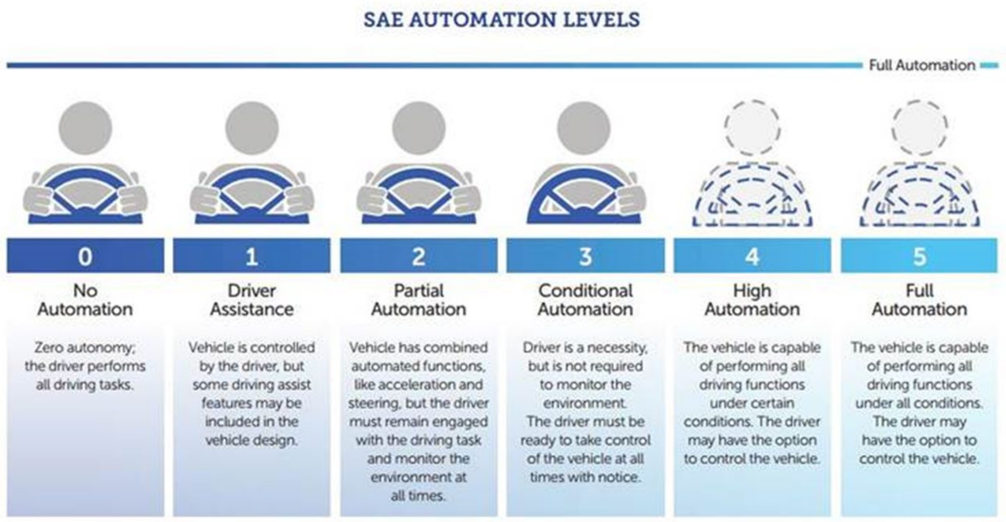
- **Standard**: Document established by consensus and approved by a recognized body that provides for common and repeated use, rules, guidelines, or characteristics for activities or their results. A standard aims to achieve the optimum degree of order in a given context. Standards are (Reference [15]):

- Shaped by consensus
- Typically developed in an open and transparent process, with representation of all interested and engaged parties
- Primarily market-driven (industry-sponsored)

A standard also aims to facilitate trade and commerce.

2.5 MDIRA Role in Advancing Autonomy in Medical Care

Progress in advancing autonomy in certain industry domains has typically been incremental. For example, Figure 2-3 shows the degrees of autonomy implemented in self-driving cars, which ranges from no autonomy through higher levels of automation to full autonomy. Figure 2-4 shows a notional analog for advancing autonomy in medical care. Medical care, in general, involves a sequence of workflow tasks that, respectively, can have different degrees of autonomy. An accurate assessment of the current state would therefore require an aggregation of the autonomy assessments of the individual tasks. The lower half of Figure 2-4 illustrates this stepwise workflow decomposition and autonomy assessment for using an Automatic External Defibrillator (AED). Although the AED performs its function autonomously, there are several manual tasks such as initially detecting that a person is in trouble, retrieving the AED, applying electrodes on the person, and activating the unit.



Zero autonomy; the driver performs all driving tasks.

Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.

Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.

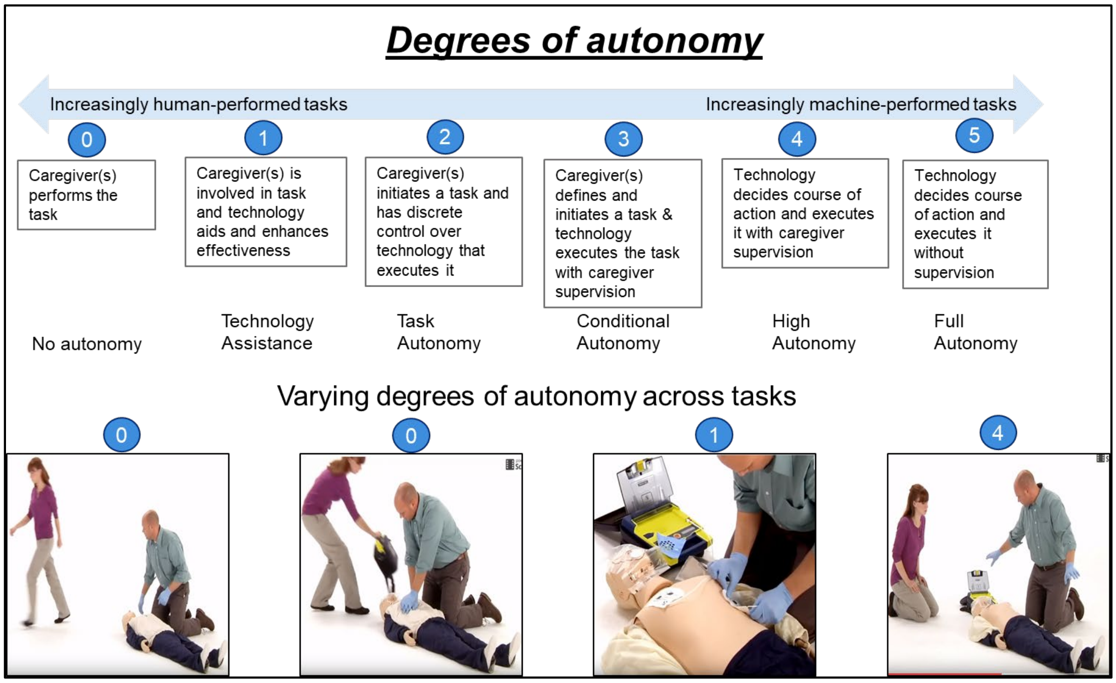
Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.

The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.

The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

https://www.nhtsa.gov/technology-innovation/automated-vehicles

Figure 2-3 Degrees of Autonomy for Driving a Car



Degrees of autonomy

Increasingly human-performed tasks

Increasingly machine-performed tasks

0 Caregiver(s) performs the task — No autonomy

1 Caregiver(s) is involved in task and technology aids and enhances effectiveness — Technology Assistance

2 Caregiver(s) initiates a task and has discrete control over technology that executes it — Task Autonomy

3 Caregiver(s) defines and initiates a task & technology executes the task with caregiver supervision — Conditional Autonomy

4 Technology decides course of action and executes it with caregiver supervision — High Autonomy

5 Technology decides course of action and executes it without supervision — Full Autonomy

Varying degrees of autonomy across tasks

Figure 2-4 Notional Autonomy Degrees for Medical Care and AED Example

MDIRA-conformant systems that execute semi-autonomous or autonomous medical tasks must operate within the broader spectrum of tasks involved in patient care. As technology advances, it may be possible for autonomous systems to perform some medical tasks, thereby reducing the workload and requirements for medical personnel. MDIRA-conformant systems will need to interact with these future autonomous systems in increasingly sophisticated ways. Although many of these types of systems are in the research and development phase, the need for provisions enabling interfaces to these future systems is a key MDIRA consideration.

3. MDIRA OPERATIONAL OBJECTIVES AND ANALYSIS

3.1 Operational Objectives

The MDIRA team drew upon prior work that provided operational and conceptual foundation for the project, for example:

- Materials from the Autonomous Medical Evacuation Workshop led by the U.S. Army MRDC Telemedicine and Advanced Technology Research Center (TATRC)
- Autonomous Medical Care and Evacuation Validated Joint Capability Gaps
- A MRDC Joint Program Committee (JPC-1) briefing titled "Medical Device Interoperability for Patient Safety and Autonomous Closed-Loop Control in Healthcare Delivery" (circa 2017)
- Thought leadership of MD PnP program (http://www.mdpnp.org/) and DocBox, Inc. (http://www.docboxinc.com)
- Inputs from regular service and special operations force medics

Based on these and other stakeholder engagements, the following operational objectives were identified that guided development of the MDIRA requirements of Section 5.

Access to Data
Enable exchange and use of data between medical devices, software applications, and information input to the system

Information Security, Cybersecurity, and Access Control
Protect sensitive information and provide safeguards for cybersecurity including preventing access by unauthorized system users.

Extensibility
Support the development of care delivery systems whose individual components, both devices and software applications, can evolve in sophistication and capability. Also support the development of systems that can scale in size regarding the number of components and medical treatments delivered. Provide for the aggregation of data from care delivery systems serving individual patients to support a multi-patient monitoring and care capability.

Ease of Set Up and Use
Enable operational flexibility for quick-assembly care delivery systems in a form-factor appropriate for the environment of use and tailored to the needs of individual patients in rapid response situations.

PnP of Components from Various Manufacturers

Enable the removal or addition of medical devices in response to emerging events (e.g., the patient stops breathing and requires a ventilator) without the need for system reconfiguration or other user intervention (sometimes called a hot-swap). The stipulation of PnP of components from various developers is one driver for mutual compliance to a set of prescribed interoperability standards. The desire for PnP includes software applications.

Virtual Care Consults

Provide access to remote medical personnel or resources enabling care by less skilled caregivers collocated with the patients. The sophistication of virtual care consultations is highly dependent on the communications resources available.

Data Logging

Provide a data logging capability for capturing a detailed record of system (i.e., technical) and patient events, data collected, and data generated during use of the platform. The data log should support root-cause analysis of component and system failures, patient safety incidents, care quality and best practice improvements, and advanced medical research.

Report Generation and Export

Support software applications that collect and package information in various forms for users, including continuity-of-care reports during care transitions. Provide external interface(s) to export these reports to various external entities.

Patient Documentation

Support various types of user interfaces (e.g., a keyboard or a voice recognition and transcription device) that allow a caregiver to enter patient documentation that can eventually be included in reports exported to the patient's electronic medical record (EMR). The scope of documentation can range from a single identification number to more extensive information such as demographics, medical history, and clinical observations.

Support of Advanced Medical Technologies

Examples include autonomous delivery of medical treatments such as fluid resuscitation and drug administration, medical device-assisted robotics, flight profiles for unmanned evacuation vehicles that adapt to a patient's medical condition, and AI-based clinical decision support.

Safety Assurance

Support timely detection and responses to system fault conditions, including those associated with medical devices, software applications, non-medical equipment, and the network infrastructure, to ensure safe and reliable system operation. Information on system faults and executed mitigation protocols can inform applications for intelligent clinical decision-making that reduces risk of patient harm.

3.2 Operational Analysis

An operational analysis was performed to aid in developing the requirements for MDIRA-conformant systems in Section 5. Because MDIRA is a high-level specification intended to apply across various manufacturer implementations, an analysis based on postulated system operational activities was adequate for purposes here. The major steps in the process were as follows:

1. Define operational scenarios. Narratives that describe how caregivers use MDIRA-conformant systems to treat critically injured individuals

2. Postulate system operational activities. Widely-relevant system operation activities distilled from the operational scenarios. These are essentially system-level use cases that classify caregiver-system interactions necessary to accomplish various objectives. (Note that the interpretation of the term *use case* varies widely; hence, the use of alternative terminology here.)

3. Analyze system operational activities. Describe the state of affairs before and after completion of the activity (i.e., pre-condition and post-condition states), identify the actors involved in the activity, and break down the steps in execution of the activity (i.e., primary and secondary flows).

4. Identify MDIRA requirements topics. In team brainstorming exercises, assess the results of step 3 and postulate candidate system requirements topics for further development.

Figure 3-1 shows that two operational scenarios were adequate for identifying system operational activities for supporting development of the MDIRA requirements. Intuitively, this may seem a small number; however, for identifying system operational activities, these scenarios are highly relevant and provide details at the appropriate level. Appendix C provides the two-patient scenario—a Humvee damaged by an improvised explosive device involving two critically injured personnel. After a detailed assessment of this scenario, only a cursory analysis of the second scenario involving five patients in a bombed building was needed to identify system operational activities not covered in the first scenario. Note also that within these two operational scenarios, excursion cases can be considered involving, for example, additional patients with different conditions, more sophisticated telemedicine encounters, and support from a medical robot. In the future, these excursions can reveal additional system operational activities for consideration in future MDIRA versions.

Figure 3-1 also illustrates that although the two operational scenarios identified correspond to a combat operations domain, these could also apply to a disaster relief domain. Furthermore, although efforts on MDIRA focused on prolonged care in austere environments, the operational scenarios considered here can also inform subsequent MDIRA requirements for systems used in hospitals.

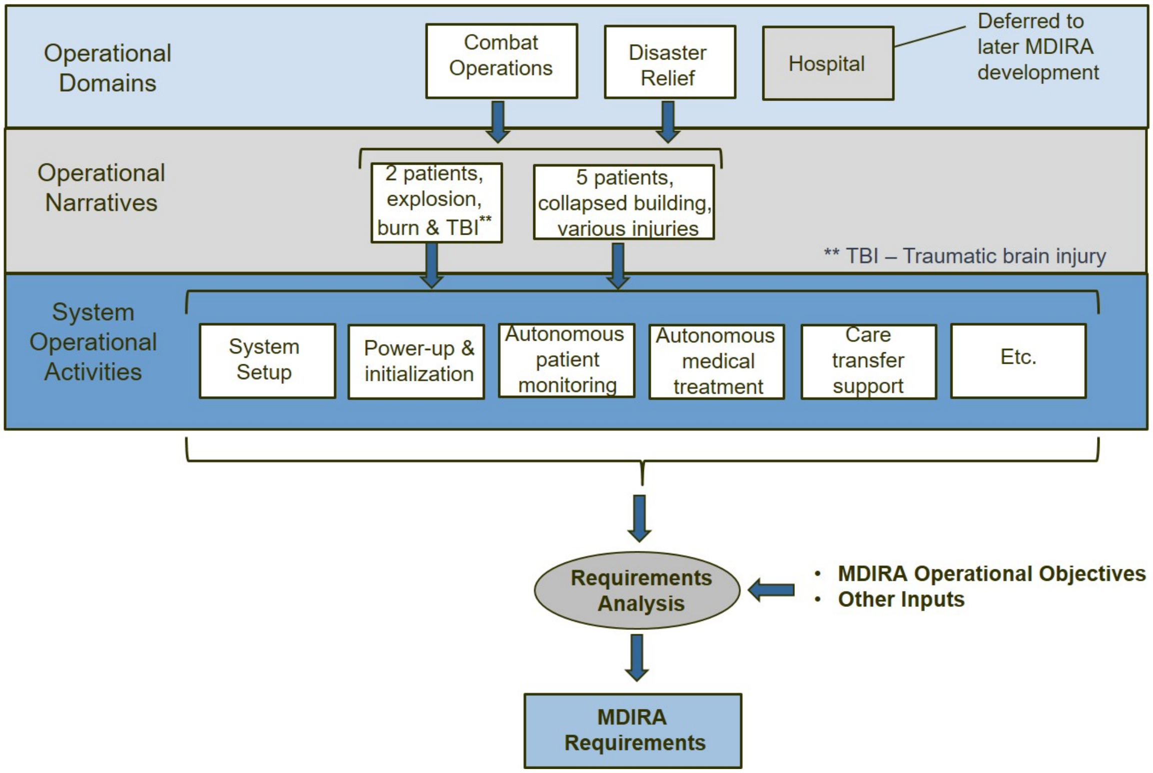

Operational Domains
Combat Operations
Disaster Relief
Hospital
Deferred to later MDIRA development
Operational Narratives
2 patients, explosion, burn & TBI**
5 patients, collapsed building, various injuries
** TBI – Traumatic brain injury
System Operational Activities
System Setup
Power-up & initialization
Autonomous patient monitoring
Autonomous medical treatment
Care transfer support
Etc.
Requirements Analysis
• MDIRA Operational Objectives
• Other Inputs
MDIRA Requirements

Figure 3-1 High-level Operational Hierarchy

4. CHARACTERISTICS OF A MDIRA-CONFORMANT SYSTEM

4.1 General Assumptions and Observations

Although MDIRA-conformant systems may be developed in many different forms serving many different purposes, a number of general assumptions and observations are appropriate. These provide helpful context for interpreting the requirements in Section 5, and convey to acquisition and medical operations planners that MDIRA-conformant systems may need to be supported within a broader resource infrastructure (e.g., communications, logistics). For brevity, the term *system* used in the following observations and throughout this document refers to a MDIRA-conformant system.

- A manufacturer may deliver a system as a fully assembled unit or in a kit of compatible parts that can be assembled in various approved configurations determined by the medical needs of a patient.

- A system will be capable of operating from an external power source (i.e., a generator) as well as from battery power. The requirements of the power subsystems will depend on the operational requirements. The system will be capable of transitioning from one power source to another without impacting patient medical care operations.

- A system deployed to support medical care of patients in an austere environment will need to operate at times with no or limited access to external communications.

- Medical device manufacturers may need to make function and interface modifications to their products to make them MDIRA-conformant. For an existing product, it may be possible to meet some or all of the MDIRA requirements through use of an equipment adaptor delivered with the product [see the ICE equipment adaptor concept described in AAMI 2700-1 (Reference [5])].

- A system can have a dedicated data network and computing infrastructure. Alternatively, an implementation can use a shared network and computing infrastructure to support multiple systems each serving a different patient.

- Autonomous medical care capabilities can be implemented in a system in different ways subject to risk control measures. Section 6.15 describes several bounding concepts. The method a system manufacturer selects should depend on the performance requirements of a particular autonomous capability. For example, the data latency requirements for a medical robot that inserts a catheter in a patient is significantly more demanding than autonomous control of an infusion pump to maintain patient hydration. The medical robot would most plausibly interface into the system as a self-contained subsystem (see Section 6.15).

4.2 System Users

The following types of users are associated with a MDIRA-conformant system:

- **Caregiver**: A user who employs a system to provide medical care to a patient. A caregiver can include personnel such as a military medic, a civilian paramedic, or a physician.

- **System administrator**: A user who performs IT-related functions for a system such as assisting in setting up user accounts, auditing user logs, installing routine software updates, loading authentication certificates, maintaining the system log, and ensuing compliance to security and other regulatory requirements.

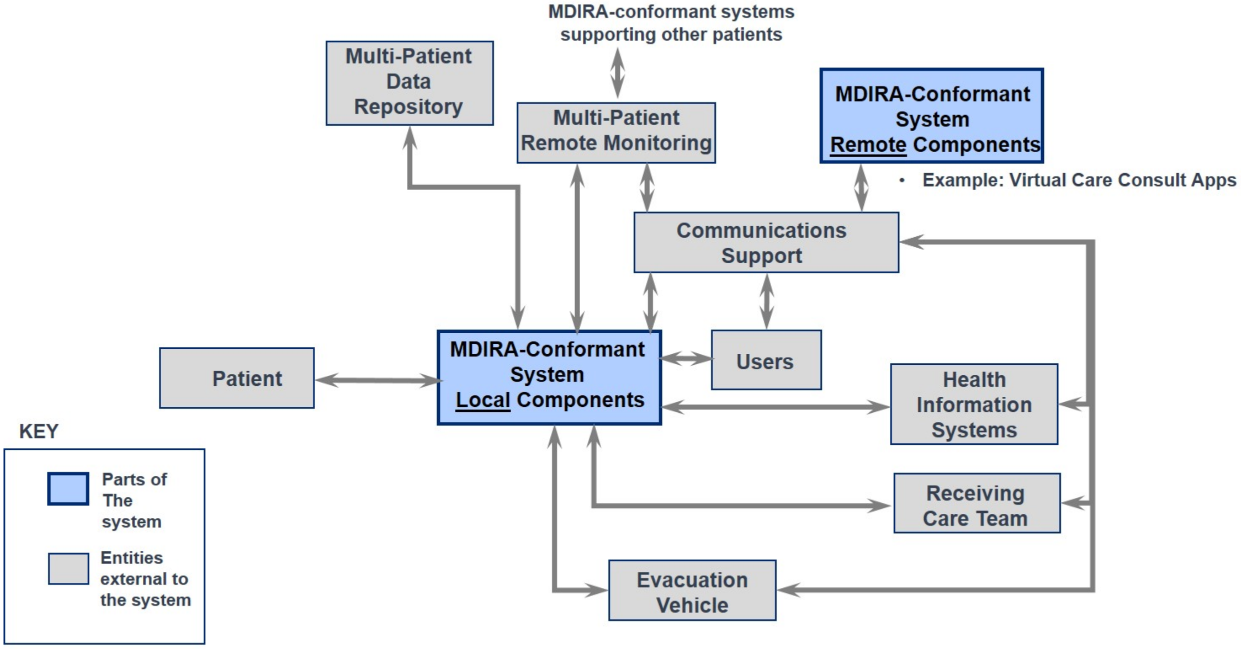
- **Maintainer**: A user who maintains and sustains a system. Maintainers would be responsible for activities such as periodic maintenance of biomedical systems, calibration of system components, test and check-out of system upgrades, help support and troubleshooting, system diagnostics and repairs, inventory management, and user training.

In MDIRA, the term *user* (lowercase u) is employed where there is no need or intention of delineating particular types of users. The term *User* (uppercase U) refers collectively to the three specific types just described. References to specific user types will cite caregiver, system administrator, or maintainer. Lastly, Users may be physically collocated with the system or interacting with the system from a remote location.

4.3 Potential System Interfaces

Figure 4-1 shows a context diagram for a MDIRA-conformant system. A context diagram is a system engineering tool to show external entities that may influence or interact with a system. A system is represented by two blue rectangles that, respectively, indicate components that are physically collocated with the patient (i.e., local) and components that can be remote. For example, an infusion pump delivering medication to the patient would be local, whereas a software application enabling a Virtual Care Consultation (VCC) operates remotely. Note also that some external entities, like system Users, can be local or remote.

Whether an entity is considered part of a MDIRA-conformant system (regardless of local or remote) or external largely follows from the definition of an ICE given in Section 2. Specifically, if an entity is exclusively supporting the medical care of a single patient, it is considered part of the system. For example, the remote VCC application that serves the needs of a particular patient is considered part of the system, whereas a health information system (e.g., EHR system) that serves multiple patients is not. Likewise, an evacuation vehicle is not typically considered part of the system. Granted, the vehicle can be dedicated to a single patient, but its primary purpose is patient transport, not the patient’s medical care (a MDIRA-conformant system evacuating with the patient can serve this purpose). Note that this criterion is a rule-of-thumb, not a rigid rule without possibility of exceptions.


MDIRA-conformant systems supporting other patients
Multi-Patient Data Repository
Multi-Patient Remote Monitoring
MDIRA-Conformant System Remote Components
• Example: Virtual Care Consult Apps
Communications Support
Patient
MDIRA-Conformant System Local Components
Users
Health Information Systems
Receiving Care Team
Evacuation Vehicle
KEY
Parts of The system
Entities external to the system

- A system may not require all interfaces depicted
- Local: Components co-located with the patient
- Remote: Components **NOT** co-located with the patient

Figure 4-1 Potential External System Interactions

In addition, in systems engineering practice, one may or may not consider human users as part of the system. For example, the definition of a ship combat system can include the crew. Here, the boundaries of a system do not include the users because the latter are subject to practices and procedures that are outside the scope of MDIRA.

Lastly, if an entity is deemed part of the system (regardless of local or remote), it is subject to MDIRA. In the case where an entity is NOT considered part of the system, it may or may not be subject to parts of MDIRA. This would depend on the operational requirements of a particular system, the components and external entities involved, and the context of care.

Observations regarding the potential interactions with entities shown in Figure 4-1 are:

- **Evacuation Vehicle**: A system can evacuate with the patient and exchange data with the evacuation vehicle through a notional standard interface.
  - The system can provide patient status information for display to a manned evacuation crew. Also, a manned or unmanned vehicle may be able to forward this information via a communications link (e.g., radio, satellite communications) to a receiving care team at the vehicle's destination.
  - The system may include an application that determines and provides flight dynamics and altitude recommendations to the evacuation vehicle to minimize medical risk to the patient (e.g., maintain a minimum safe cabin pressure).

- **Receiving Care Team**: Upon arrival at the medical care facility, the system can provide information on the patient's care and status directly to the local care team to support the continuity of care. (As described previously, the receiving care team may also have the ability to receive patient status updates in transit during evacuation as well.)

- **Health Information Systems**: The system may have interfaces to health information systems containing patient health-related information (e.g., an EHR system). To the extent possible, these interfaces should comply with an industry standard [e.g., a web services interface compliant with the Fast Healthcare Interoperability Resource (FHIR) standard (see https://www.hl7.org/fhir/index.html)].

  – The system may connect to a remote health information system via the external communications infrastructure.

  – The system can have the ability to connect locally to a hospital data network.

- **System Users**: Although there are efforts to increase the autonomy of care near the point of a patient's injury, in general, the system will require appropriately designed human-machine interfaces for local caregivers. Other direct users that may access the system either locally or remotely include personnel responsible for maintaining the system (e.g., load certificates, update software, perform troubleshooting).

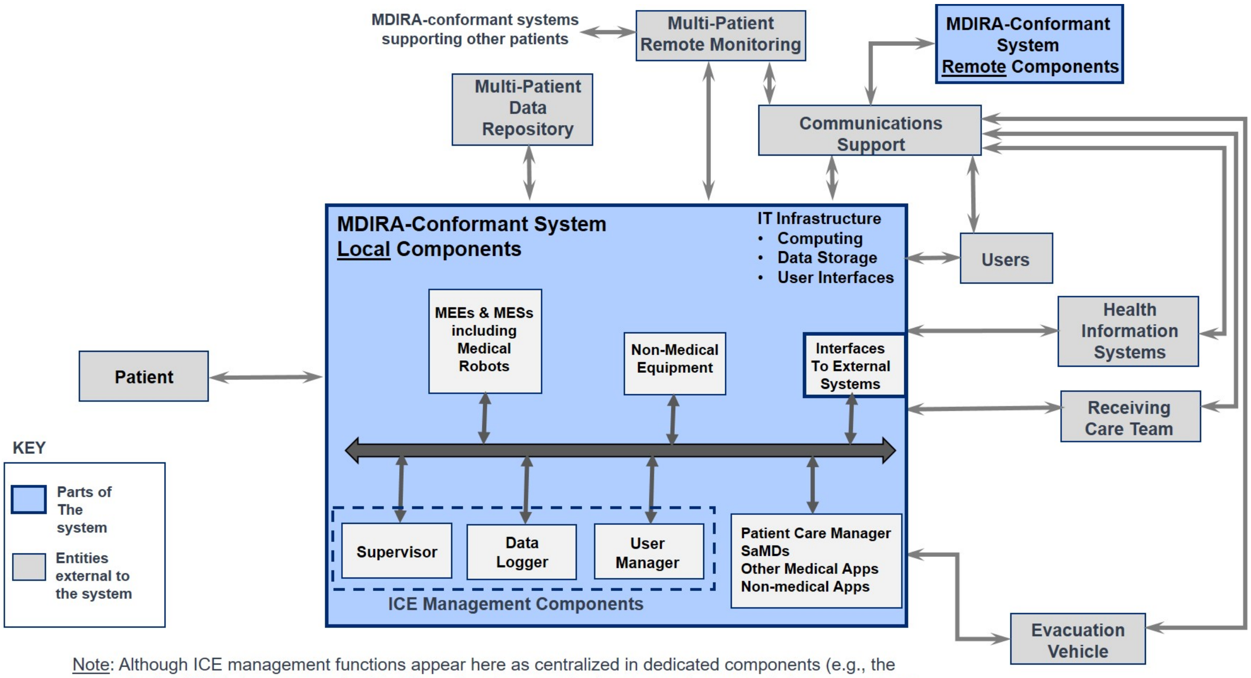
- **Virtual Care Consultation**: The system may connect to remote medical staff including specialists who team with on-site caregivers in supporting the patient's medical needs. Patient status data, audio and video information may be exchanged over this interface. Note also that a VCC may enable coordinated interactions between the system and a health information system (discussed previously).

- **Multi-Patient Monitoring**: There may be a number of MDIRA-conformant systems that support the needs of many patients in a multiple casualty scenario. Notionally, each individual system would connect to a mobile device that displays a status dashboard for all the patients, thereby allowing a caregiver to navigate among those patients who require most attention.

- **Multi-Patient Data Repository**: Section 5 includes requirements for the system to perform detailed data logging. Typically, such detailed information would not be suitable for current EHR systems. Notionally there may be future health information systems to capture data log information for patient care encounters with MDIRA-conformant systems. Such a data repository could aid in investigation of patient safety issues and provide high-quality, time-correlated data to support research in advanced medical care applications that may leverage AI methods.

4.4 General Components of a MDIRA-conformant System

Figure 4-2 illustrates the general components for MDIRA-conformant systems that derive from the conceptual function model of an ICE shown in Figure 2-1; see AAMI 2700-1 (Reference [5]). Accordingly, systems require supervisory, data logging, and user management functions. Certain aspects of these functions may be distributed across the components of the system. Note that supervisory, data logging, and user management functionality could range from rudimentary to complex, depending on a system's specific operational requirements.


MDIRA-conformant systems supporting other patients
Multi-Patient Remote Monitoring
MDIRA-Conformant System Remote Components
Multi-Patient Data Repository
Communications Support
MDIRA-Conformant System Local Components
IT Infrastructure
• Computing
• Data Storage
• User Interfaces
Users
MEEs & MESs including Medical Robots
Non-Medical Equipment
Interfaces To External Systems
Health Information Systems
Patient
Receiving Care Team
KEY
Parts of The system
Entities external to the system
Supervisor
Data Logger
User Manager
Patient Care Manager
SaMDs
Other Medical Apps
Non-medical Apps
ICE Management Components
Evacuation Vehicle

Note: Although ICE management functions appear here as centralized in dedicated components (e.g., the Supervisor), MDIRA does not require this. These functions may be incorporated as part of other components contingent on MDIRA requirements for these functions being met.

Figure 4-2 General Components of a MDIRA-conformant System

Note that the legacy ICE layout in Figure 2-1 identifies a network controller component. MDIRA does not explicitly require this because some ICE communications architectures may not need it (e.g., in modern web services communications, there is no centralized controller; network control functions are distributed within the components on the network). If a particular system does require a network controller, a manufacturer has latitude to include one as part of the IT Infrastructure and Other Apps elements in Figure 4-2. In addition to those components described in Reference [5], MDIRA adds a user management component as part of the MDIRA security provisions; specifically for access control.

For convenience here, the supervisory, data logging, and user management functions are referred to here as the Supervisor, Data Logger, and User Manager, respectively. Use of these specific terms are not required as long as there are functions within a particular system implementation that satisfy the requirements of Section 5. Also, for convenience, MDIRA denotes the combination of the supervisory, data logging, and user manager functions as the *ICE Management Components*, adapting the *ICE Manager* terminology used in Reference [5].

Figure 4-2 depicts the general components of a MDIRA-conformant system. Brief descriptions follow:

- **Supervisor** – Functions that determine and manage system health and status (i.e., whether the system is operating correctly), manage the registry of authenticated components in the system, execute system fault protocols, and manage and authorize requests of components to control other components that are externally controllable. Conceptually, system supervisory functions may be consolidated in a dedicated Supervisor component or implemented as part of a multi-purpose component. (For illustration purposes, Figure 4-2 implies the former implementation.)

- **Data Logger** – Functions that store detailed and comprehensive system and patient data during a care encounter for later download to an information system. System data logging functions may be distributed across multiple components.

- **User Manager** – Functions that facilitate the setup of user accounts and privileges, control access to the system according to those privileges, and maintain a user audit log.

- **MEEs and MESs** – Equipment involved in monitoring the patient's medical state and administering medical treatments. Per the definitions provided in Section 2.4, a medical robot is a sub-class of MEE/MES and hence is considered a component in a MDIRA-conformant system.

- **Patient Care Manager (Optional)** – Functions that manage the overall care of the patient such as monitoring patient medical status, managing alarms, tracking workflows, and managing therapies.

- **Software Applications** – Includes SaMDs and medical applications that may not fall within the SaMD definition (i.e., non-SaMD medical apps) as well as other (non-medical) applications. Note that Section 5.1.6 recommends that a system include a SaMD that performs patient care management functions. This is noted on Figure 4-2.

- **Non-Medical Equipment** – Equipment not intended for a specific medical purpose, although it may support medical operations (e.g., sensors that monitor environmental conditions like temperature, humidity, and air pressure).

5. REQUIREMENTS FOR MDIRA-CONFORMANT SYSTEMS

Sections 5.1 and 5.2 provide MDIRA requirements at the system level and for supervisory functions, respectively. Section 5.3 provides requirements for the other components shown in Figure 4-2. Sections 5.4 and 5.5 provide requirements supplementary to those in Section 5.3 that are unique to user management and data logging functions, respectively.

The requirements described for the ICE Management components (i.e.. Supervisor, User Manager, and Data Logger) in Sections 5.2, 5.4, and 5.5, respectively, do not imply a specific physical architecture. Conceptually, the ICE Management components may be consolidated in dedicated components (as depicted in Figure 4-2) or implemented as part of other components. Regardless of whether the implementation is centralized or distributed, the functional requirements specified herein apply.

Requirement statements use the following conventions:

- The MR numbering prefix (e.g., MR-001) denotes a *mandatory requirement* that all MDIRA-conformant systems must meet. In this case, ***SHALL*** appears in the requirements statement.
- The RR prefix (e.g., RR-004) denotes a *recommended requirement* that a developer or customer of a MDIRA-conformant system should consider. These statements use ***SHOULD*** rather than ***SHALL***.
- The use of the term *system* refers to a MDIRA-conformant system.

Note there has been an attempt to keep requirement numbers consistent between MDIRA releases; however, some caveats are appropriate. First, numbers may not be in consecutive order, indicating that either requirements have been moved to new locations compared to prior releases or new requirements have been inserted. Also, there can be discontinuities where requirements from a previous release are removed from an update. In addition, a number may be qualified by a decimal digit that can have several meanings. For example, a number MR-028.1 reflects a revision of MR-028. Also, a compound requirement statement may be split into separate constituents; for example, MR-001.1 and MR-001.2 are a decomposition of what was previously MR-001. Requirements numbered 79 and above have been added since the prior MDIRA version. Appendix D includes a table showing the requirements that were removed from this release.

5.1 System Requirements

A requirement at the system-level specifies two things:

- A high level functional capability that MDIRA-conformant systems are required or recommended to have
- A property that MDIRA-conformant systems are required or recommended to possess (sometimes called non-functional requirements)

In general, the component-level requirements in the subsections that follow derive from functional requirements expressed at the system level. It is not a firm rule here, however, that a system functional requirement always has associated supervisory or component requirements. Some system requirements may have a number of design options that satisfy the requirement. For example, there are several requirements related to context data in Subsection 5.1.12.3. This requirement could be allocated to the Supervisor or to another component such as a Patient Care Manager. In these cases, it is left to the system developer to flow down requirements to the supervisor or component level. MDIRA strives to avoid being overly prescriptive regarding design choices. Another reason is that the choice of the design solution may largely be dictated by the broader operational requirements for a system as well as standards, practices, and regulations specific to the manufacturer, customer, or the operational context. Table 7-1 and Table 7-2 in Section 7.3 identify system requirements where the manufacturer has discretion in functional allocation to components.

5.1.1 Interoperability

(MR-001.1) A system ***SHALL*** enable the communication of data between components.

These data may include medical device data, data entered by the Caregiver, data received from an EHR system, etc. Specifics of the data would depend on the operational requirements of the system.

(MR-001.2) For all data exchanges, a system ***SHALL*** provide the reliability, throughput, latency, and essential performance necessary to support the system's intended medical uses including required autonomous medical capabilities.

Examples of autonomous care delivery capabilities include closed-loop control of medication and fluid infusions. Another example is providing patient vital signs data to influence the operations of a medical robot. Because quantitative performance requirements are coupled to a particular system's operational requirements, MDIRA conformance verification for MR-001.2 will involve review of system verification and validation (V&V) data from analyses and tests conducted by the system manufacturer.

5.1.2 Openness

(MR-002) A system ***SHALL*** have an architecture that allows the connection and disconnection of compatible components without shutting down or rebooting the system, or the components, regardless of the suppliers of those components.

AAMI 2700-1 (Reference [5]) describes PnP as the seamless connection and disconnection of medical devices without having to shut down and reboot the medical devices or the system. Ideally, other than plugging the device in, PnP involves no additional user actions. The stipulation of PnP irrespective of the supplier implies that the design of a system, including the medical devices, complies with the industry-consensus interoperability standards and the implementation guidance described herein.

5.1.3 Minimize Risk of Patient Harm

(MR-028.1) A system risk analysis SHALL be performed that systematically identifies and assesses residual risk levels in accordance with ISO 14971 (Reference [17]) and is the basis for system safety provisions and fault protocols.

Depending on the operational requirements, the system risk analysis will consider factors such as critical points of failure, patient vulnerabilities, and potential for and impacts of degraded system performance. For example, the risk in the event of malfunction of ICE management components (i.e., supervisory, user management, and data logging functions) will vary depending on the system capabilities. In a system that is providing treatment to a patient (not just monitoring), the system could mitigate risk through implementation of a redundant Supervisor component that takes over operations if the primary Supervisor fails, thereby avoiding a single point of failure.

5.1.4 User Management Capabilities

(RR-080) A system ***SHOULD*** have provisions for managing user privileges according to defined roles in system operations.

Note that although this requirement is recommended, there is a mandatory requirement for user access control (see MR-027).

5.1.5 Data Logging Capabilities

(MR-081) During a patient care episode, a system ***SHALL*** comprehensively log data pertinent to the system's health and operations as well the patient's condition and medical care received to support later reconstruction of events and care quality improvement initiatives.

5.1.6 Patient Care Manager

(RR-82) A system ***SHOULD*** have a patient care management capability that includes monitoring the patient's medical status, managing alarm conditions, tracking execution of medical workflows, and supporting patient risk management.

Some form of patient care management may be essential for systems that include autonomous medical treatments that operate unattended by a caregiver. The need and sophistication of patient management functions would depend on the system's operational requirements.

5.1.7 Standardized External Interfaces

(MR-003) An interface between a system and an external system ***SHALL*** conform to existing interoperability standards and profiles associated with that external system.

This requirement stipulates that if an external system has an established interface compliant to one or more interoperability standards, the manufacturer of a system must leverage these to the greatest extent possible. For example, the FHIR standard is a candidate for interfacing a system to an EHR system. If an EHR system supports an interface based on a standard implementation of FHIR for that purpose, and that interface supports the needed data exchanges, the system shall use that interface rather than a custom interface. In the case where a new interface needs to be developed because there is no existing interface that supports the needed data exchanges, a system manufacturer should work with their external system counterpart to design the interface using existing standards.

5.1.8 External Interfaces

Requirements related to external interfaces for systems follow. See Section 6.13 for additional guidance.

(RR-004) A system ***SHOULD*** include an interface to support an external system's monitoring of multiple systems supporting the needs of multiple patients.

Such an interface is particularly relevant in a mass casualty scenario where the caregiver-to-patient ratio is small. The ability to monitor the operations of multiple systems would allow a small number of caregivers to track the status of multiple patients, perhaps via a mobile device (see Figure 4-1).

(RR-005.1) A system ***SHOULD*** include an interface to an EHR system.

Specifics regarding EHR type and manufacturer depends on the system's operational requirements.

(RR-005.2) A system ***SHOULD*** include an interface to electronically export the system's data log (see MR-081.0) to an information system suitable for receiving it.

(RR-006.1) If a system is required to transport with a patient, and the transport vehicle is capable of exchanging relevant data with the system via an electronic interface, the system ***SHOULD*** support exchange of the data over that interface.

(RR-018.1) A system ***SHOULD*** be capable of exporting patient status reports and transfer notes to external entities.

An example is exporting a status report to a receiving care team at a medical facility to facilitate the patient's continuity of care.

(RR-007.1) A system ***SHOULD*** include an interface to the external communications architectures pertinent to the operational setting to enable communications with remote external systems and Users.

Examples of potential external communication architectures are a tactical radio link, secure Internet connection, or hospital network. This requirement can enable virtual care consultations as well as remote access for System Administrators and Maintainers of a system. The need for remote access capabilities would depend on the system's operational requirements. Note that MR-003 stipulates that a system use existing interface standards.

5.1.9 Initialization

(MR-008.1) A system ***SHALL*** initialize to a stable ready state prescribed to meet its operational requirements prior to execution of system operations.

In general, after initialization the system would be ready to discover and register medical devices as they become available to the system (e.g., a caregiver connects a vital sign monitor to the system), and be ready to use these resources for the medical care of the patient. Note that the baseline state at initialization for a system maintenance operation may differ from the baseline state prerequisite to initiating care support operations for a patient.

5.1.10 Health and Operating Status

(MR-101) A system ***SHALL*** include provisions for monitoring and managing the health and operating status of the system.

5.1.11 Fault Response Protocols

(MR-009.1) A system ***SHALL*** execute fault response protocols as determined by the system's operational requirements and risk analysis (see MR-028.1).

5.1.12 Data Management

5.1.12.1 Patient Identification

(MR-011) A system ***SHALL*** include a capability to manage patient care episodes.

(MR-012.1) A system ***SHALL*** be capable of assigning patient identity and other patient information to a unique patient identifier.

MR-040.1 stipulates that the Supervisor assign a unique identifier to each patient.

(MR-012.2) A system ***SHALL*** be capable of assigning patient identity and other patient information when a unique patient identifier is created or at any time thereafter.

Trauma care occurs with urgency and may require the caregiver to provide care prior to entering patient identity or other more detailed patient information into the system.

(MR-013.1) A system ***SHALL*** enable the Caregiver to associate a patient's unique identifier with other identifiers assigned to the patient throughout the course of the patient's care.

The Supervisor will automatically assign a unique identifier to a patient at the initiation of a care episode (see MR-040.1). Because the system notionally transports with the patient from a remote care site to a hospital, it may be necessary, for example, to associate the patient's unique identifier with the hospital's patient episode numbering system.

5.1.12.2 Entry of Patient Medical Information

(RR-015.1) A system ***SHOULD*** provide a means for receiving patient medical information such as patient history and clinical observations, as well as a means for reviewing these data.

Such information can be received in a number of ways including manual data entry at the system user interface, the Caregiver applying a scanning device to a "smart" identification tag possessed by the patient that contains medical information, or electronic data transfer from an EHR system. A component of the system (e.g., an application) may have the role of consolidating patient medical information from various sources and distributing these as appropriate to other components.

5.1.12.3 Entry of Care Context Information

(MR-083) A system ***SHALL*** provide the means for entering and receiving care context information including the patient's name and other identifying information, location of care, identification of caregivers, and medical workflows planned or in-process.

Such information can be entered or received in a number of ways including manual data entry in one component that distributes the information to all the components via the system's data network, entry at the user interfaces of the individual components, or electronic data transfer from an EHR system. The specifics on the type and detail of the context information depends on the operational requirements for the system.

(MR-084) A system ***SHALL*** provide a means to ensure all components that use context data, including the types listed in MR-083, have consistent and current knowledge of that information.

One notional approach for a component to be authorized to control another component (see Section 5.2.5) is based in part on the Supervisor's comparison of context information stored in the respective components. For this reason, accurate and timely context information updates to components is essential.

(MR-085) A system ***SHALL*** include provisions for reporting contextual data including the types listed in MR-083 to the Data Logger.

5.1.12.4 Data Provenance

(MR-016) A system ***SHALL*** provide the ability to identify the source or origin of each piece of data entered into the system including traceable identification of the source component (manufacture, make model, serial number, unique identifier if available from the component data interface), identification of a user that manually entered the data if applicable, and a timestamp of when the data originated.

5.1.13 Time Synchronization

(MR-019) A system ***SHALL*** include provisions to time synchronize system- and component-level operations, events, and data streams.

Many distributed functions require synchronized time to coordinate operations. Additionally, many security mechanisms, such as certificate-based encryption, require an accurate representation of the current time. To provide a robust infrastructure that supports functionality ranging from authentication to autonomous care protocols, a system requires an accurate and precise synchronization of time between all components.

The resolution of the time synchronization and the accuracy of the reference clock will depend on the operational requirements of a particular system implementation. Section 6.9 provides guidance regarding time synchronization.

(MR-019.1) The representation of time in a system ***SHALL*** conform to ISO 8601 including date and time [Coordinated Universal Time (UTC)] and time zone offsets.

Example: 2021-02-11T15:54:43-05:00 for February 11, 2021 at 10:00 am Eastern Standard Time

5.1.14 Component Authentication

(MR-020) A system ***SHALL*** provide a means to ensure that all components participating in the system are authenticated.

Depending on a specific system's design, the authentication mechanism may be based wholly within the system or through distributed services. In either case, all components will provide credentials to authenticate themselves for access to other components of the system. If all means of authenticating the credentials fail, the requesting entity is not permitted access to the system's components.

5.1.15 Trusted Control

(MR-021) If a system includes components that can control (i.e., change the operational settings of other components), the system ***SHALL*** include provisions for safe control operations accounting for suitability for end use and mitigation of control conflicts.

Control examples include an alarm management application that changes alert condition thresholds in a patient's vital sign monitor and a therapy control application that regulates medication flow rate from an infusion pump.

5.1.16 Component and Resource Usage

(MR-100) A system ***SHALL*** determine the safe use of system components and their associated data resources for the patient's medical care.

5.1.17 Security

The following subsections identify security requirements for MDIRA-conformant systems. Refer to Sections 6.4, 6.5, and 6.7 for additional guidance.

5.1.17.1 Information Security

(MR-025) A system ***SHALL*** apply information security measures and processes as required by the information security governing body having authority over the operations of the system.

5.1.17.2 Cyber Security

(MR-026) A system ***SHALL*** apply cybersecurity measures and processes as required by the cybersecurity governing body having jurisdiction over the operations of the system.

Security mitigations should be based on a systematic threat analysis as well as consensus standards and industrial best practices. Such an analysis should encompass the possible range of components that may be included in a particular system commensurate with its intended uses.

5.1.17.3 Access Controls

(MR-027) A system ***SHALL*** include user access control measures and processes to prevent unauthorized access.

Note that MR-027 applies to both local and remote users. As described in Section 4.3, a local user is physically collocated with the patient, whereas a remote user is not.

5.1.18 Detect, and Minimize Impacts of, Data Degradation

(**MR-030.1**) A system ***SHALL*** include provisions for detecting degradations in the availability and fidelity of data being used for the care of a patient.

(**RR-030.2**) A system ***SHOULD*** include provisions for minimizing the impacts of detected degradations in the availability and fidelity of data being used for the care of a patient.

For example, suppose heart rate data from a particular MEE or MES component in a system are being used by a SaMD to monitor a patient's condition, and for some reason these data become noisy. The SaMD may detect this and seek an alternative MEE or MES in the system that can provide heart rate data. MR-061.1 in Section 5.3.7 stipulates that MEEs, MESs, and software applications (including SaMDs) test the validity and integrity of their respective input data streams (also see Sections 6.4 and 6.6). Note that MR-030.1 and MR-030.2 are expressed here at the system level because the Supervisor may also have a role in detecting data anomalies and minimizing the impacts. Specific implementations would depend on the operational requirements for a particular system.

5.1.19 Data Nomenclature and Semantics

(MR-031.1) Systems ***SHALL*** conform with IEEE 11073-10101 (Reference [1], 2019 revision) and the Rosetta Terminology Mapping Management System (RTMMS) for medical device data.

MR-086 addresses the situation when neither of these resources includes terms required for a particular system implementation.

(MR-031.2) For medical data that are not associated with medical devices, systems ***SHALL*** use nomenclature terms in accordance with commonly used standards including Logical Observation Identifiers, Names, and Codes (LOINC) and Systematized Nomenclature of Medicine – Clinical Terms (SNOMED CT).

Note that there may be cases where some data items are represented in multiple coding systems. If there is no broad consensus as to which coding system to use, a system should choose one, then provide the system a mapping of the data item to the alternative coding systems. This would allow an external system receiving the data to translate the data item in terms that it can interpret. Consensus on which nomenclature systems to employ in MDIRA-conformant systems might be addressed in IHE initiatives to profile common system implementation for specific use cases.

(MR-086) If some data pertinent to a system cannot be represented using industry-accepted nomenclature and semantics resources, a custom data dictionary can be used, but this ***SHALL*** be non-proprietary and readily available.

It is recommended that manufacturers who require a custom data dictionary engage with the pertinent SDO regarding the possibility of having custom terminology included in an update of a nomenclature standard.

5.1.20 Information Models

(MR-087) A system ***SHALL*** use either the Basic Integrated Clinical Environment Protocol Specification (BICEPS) Participant Model described in IEEE 11073-10207 (Reference [18]) or the ISO/IEEE 11073-10201 DIM (Reference [2]) as the baseline information model for representing the capabilities and data associated with point-of-care (POC) medical devices.

Given limited industry adoption of parts of the DIM, and increasing interest in the BICEPS Participant Model (both a streamlining and enhancement of the DIM) particularly in Europe, MDIRA supports, for now, the use of either. However, achieving ubiquitous interoperability of medical devices that may use different information models is problematic. One potential solution is the development of a standardized tool that reliably maps medical device information represented using one model into the form of the other model. With such a mapping tool, standard adaptors might be developed that allow a medical device to effectively support either information model standard. Development of a reliable mapper would be a worthy investment of medical device interoperability research funds.

Note that neither the DIM nor the BICEPS Participant Model are adequate for meeting the requirements for MDIRA-conformant systems.

(MR-032.1) For representing information for which the DIM or the BICEPS Participant Model are unsuitable, a system ***SHALL*** employ other industry-accepted information model standards including, but not limited to, the resource definitions of FHIR.

Such information may include clinical observations, medications, patient history, and data received from a medical robot.

(MR-088) If some information pertinent to a system cannot be represented using an industry-accepted information model, a standard information model could be adapted or as last resort a custom model used, but these ***SHALL*** be non-proprietary and readily available.

5.2 Supervisor Requirements

As discussed in Section 4.4, a MDIRA-conformant system requires supervisory functions to provide system-level situational awareness, manage system resources, and, if necessary, execute fault protocols (e.g., "safe" shutdown) minimizing risk to the patient. Although for illustration purposes Figure 4-2 depicts the Supervisor as a separate component, it should be recognized that the Supervisor functionality could be included as part of another component. Also, to reiterate, a particular Supervisor implementation can vary in sophistication depending on the operational requirements of a particular system. Supervisor requirements follow.

5.2.1 Power-on Self-Test

(MR-089) The Supervisor ***SHALL*** perform a POST immediately after start-up and initialize to a state ready to support system operations.

5.2.2 Supervisor Time Synchronization

(MR-033) The Supervisor ***SHALL*** synchronize its clock to a common system reference clock.

(MR-033.1) The Supervisor ***SHALL*** timestamp all its operations, events, and communications to support the system's functions.

Section 6.9 provides guidance regarding time synchronization.

5.2.3 Shutdown

(MR-034) When a User initiates shutdown of the system, the Supervisor ***SHALL*** prepare the system for safe shutdown, and prompt the user in the appropriate sequence of shutdown actions according to risk management (see Section 5.1.3).

There may be several options for nominal shutdown. For example, one shutdown sequence might correspond to the case when the patient is removed from the system just prior to being evacuated. Because the system is not transported with the patient, this sequence ends with all system components powered down. Alternatively, another shutdown sequence might discontinue system autonomous medical operations, but allow the option for some equipment (like a vital signs) to remain powered on and connected to the patient during transport.

5.2.4 Discovery and Registration

Figure A-1 in Appendix A provides a high-level sequence diagram illustrating Supervisor discovery and registration of components in a MDIRA-conformant system. Note that the purpose of this diagram is to illustrate the concept, not specify a particular design approach.

5.2.4.1 Discovery of Components

(MR-035.1) The Supervisor ***SHALL*** have a means for discovering the existence of system components.

5.2.4.2 Registration of Components

(MR-035.2) The Supervisor ***SHALL*** execute a registration process for discovered components that makes the components available to support the medical care of a patient.

(MR-035.3) The Supervisor ***SHALL*** perform an authentication process that validates a component's identity prerequisite to registration.

(MR-036.1) The Supervisor ***SHALL*** verify the successful result of a component's POST prerequisite to registration.

5.2.5 Authorization

Figure A-3 in Appendix A shows a sequence diagram notionally illustrating the Supervisor's authorization function. Note that the purpose of this diagram is to illustrate the concept, not specify a particular design approach.

5.2.5.1 Safe Device Combinations and Interactions

(MR-037) The Supervisor ***SHALL*** authorize the use of a component or the combined use of one or more components based on compatibility for the intended purpose in accordance with risk management (see Section 5.1.3).

(RR-039.1) The Supervisor ***SHOULD*** prioritize data resource allocations as necessary in accordance with risk management (see Section 5.1.3).

For example, during periods of high utilization, a medically critical SaMD must have priority in accessing the information resources it requires from another component. In this case, the Supervisor may dedicate this component to exclusively support the SaMD.

5.2.5.2 Authorize Control Requests

(MR-038.1) The Supervisor ***SHALL*** verify that the combination of controller and controlled components are safe and compatible for the intended purpose according to protocols established through the risk management process (see Section 5.1.3).

Control examples include an alarm management application that changes alert condition thresholds in a patient's vital sign monitor and a therapy control application that regulates medication flow rate from an infusion pump.

(MR-038.2) The Supervisor ***SHALL*** prevent control conflicts (i.e., two or more components inappropriately attempting to concurrently change the same operational setting) in the same component, according to protocols established through the risk management process (see Section 5.1.3).

(MR-038.3) The Supervisor ***SHALL*** authorize, subject to MR-038.1 and MR-038.2, component requests to control other components (i.e., change their operational settings).

An example is the Supervisor authorizing a software application to change the infusion rate setting of an infusion pump. The criteria for the Supervisor's authorization decision depends on the system operational requirements and the application of risk management (see Section 5.1.3). For example, the Supervisor can stipulate that once a component is authorized to control an infusion pump, subsequent authorization requests for control of the pump from other components are ignored, thus eliminating the potential for control conflicts.

5.2.6 Unique Patient Identification

(MR-040.1) The Supervisor ***SHALL*** create a unique identifier for each patient within the system.

(MR-040.2) The Supervisor ***SHALL*** provide a mechanism to associate component data with a patient unique identifier.

5.2.7 Episode Initiation and Termination

(MR-014.1) The Supervisor ***SHALL*** include a capability to initiate and terminate a patient episode.

An episode is a continuous period of time over which a system is supporting the care of a patient. When the Caregiver initiates the episode, the system creates the patient's unique identifier. Later, the Caregiver terminates the episode, thereby ending the system's support of the patient's medical care. Note that during an episode, there may be multiple caregivers and multiple caregiver-patient visits.

(MR-014.2) The Supervisor ***SHALL*** include a capability to restart a previously terminated patient episode.

This is needed to correct an error of termination.

5.2.8 System Monitoring and Fault Handling

Figure A-2 in Appendix A depicts component status reporting and Supervisor monitoring and fault handling. Note that the purpose of this diagram is to illustrate the concept, not specify a particular design approach.

5.2.8.1 Receive Component Operating Status Data

(MR-041) The Supervisor ***SHALL*** receive operating status data (including technical alerts) from the system components.

5.2.8.2 Assess System Operating Status

(MR-042) The Supervisor ***SHALL*** routinely assess the operating status of the overall system to verify nominal operation and identify faults.

5.2.8.3 Notification of System Operating Status

(MR-043) The Supervisor ***SHALL*** provide notifications of the system's overall operating status to the User according to a notification protocol.

5.2.8.4 Execute System Fault Protocol

(MR-044.1) The Supervisor ***SHALL*** provide system fault response protocols determined through risk analysis (see MR-028.1) when faults are detected.

Specifics on fault response protocols depend on the system's operational requirements. The simplest response protocol would be to notify the system's User.

(RR-044.2) The Supervisor ***SHOULD*** execute fault response protocols when it receives an unsuitable data alert (see MR-061.1) as determined through risk analysis (see MR-028.1).

5.2.8.5 Record System Status and Fault Recovery Information

(MR-046) The Supervisor ***SHALL*** record system operating status data, as well as data regarding any fault protocols executed, for generating system operating status reports during an episode of care.

The Supervisor must be capable of providing data to feed dashboards, time-series history, and/or other software and/or hardware to analyze or process system status information during a patient care episode. Specifics implementations would depend on the operational requirements of the system. The Data Logger (see Section 5.5) will log similar data for detailed reconstruction of system operating status changes after a patient care episode is completed.

5.2.8.6 Logging of Supervisor Data

(MR-090) The Supervisor ***SHALL*** report system operating status data, as well as data regarding fault protocols executed, to the Data Logger.

(RR-099) The Supervisor ***SHOULD*** report to the Data Logger the information that it sends to and receives from other MDIRA-conformant components during a patient care episode.

5.2.9 Provide Patient Care Management Support

Section 5.1.6 recommends that a MDIRA-conformant system include a patient care management component. The requirements in this section address the Supervisor's support of patient care management functions.

(MR-091) If a patient care management component is part of the system, the Supervisor ***SHALL*** provide it information regarding technical alerts.

A decline in the patient's condition could be caused by a perturbation in treatment caused by a component fault; hence, a patient care manager (PCM) may use this information to determine the appropriate safety protocol to execute.

(RR-050.1) If a patient care management component is part of the system, the Supervisor ***SHOULD*** include provisions to receive and execute recommendations from it that may alter the system's operations.

For example, if the PCM determines the medical operations being used are unsafe, it could recommend that the Supervisor execute a predetermined safe shutdown sequence. The definition of faults and predetermined safe state protocols are determined through risk management (see MR-028.1).

5.3 Component Requirements

In general, the requirements in this section apply to all system components identified in Section 4.4 except the Supervisor, which was addressed in Section 5.2. The one exception is that the requirements in Section 5.3.10 do not apply to the Data Logger. Functionality-specific requirements for the User Manager and Data Logger components, which extend beyond those of this section, are addressed in Sections 5.4 and 5.5.

5.3.1 Component POST and Initialization

(MR-053) A component ***SHALL*** perform a POST immediately after start-up and initialize to a state ready to support system operations.

5.3.2 Component Discovery and Authentication

(MR-054.1) A component ***SHALL*** be discoverable by other components once in its initial ready state.

Although each component must be discoverable, the specifics regarding which components are capable of discovering other components depends on the system's operational requirements.

(MR-055.1) Components ***SHALL*** make their authentication credentials available prior to establishing communications beyond discovery.

(MR-092) Other than for discovery, a component ***SHALL*** only communicate with components whose credentials have been authenticated.

The specifics regarding which components validate credentials depends on the system's operational requirements.

Figure A-1 in Appendix A notionally illustrates component discovery and authentication.

5.3.3 Component Capability Advertisement

(MR-056.1) A component ***SHALL*** have the means to provide to other components descriptive information about its identity, purpose, capabilities, and the data that it can produce.

Capability advertisement is a key enabler to connecting and disconnecting components into a MDIRA-conformant system without powering the system down and having User intervention. Subsection 5.1.20 stipulates the use of standard information models to convey component descriptive information. The specifics of the information and associated Information Models depends on the component type (i.e., a MEE versus a SaMD) and the system's operational requirements. See Sections 2.4, 5.1.20, and 6.2 for further discussion regarding Information Models.

5.3.4 Changes to Component Settings

(MR-093) A component ***SHALL*** only change its operational settings in response to requests from an authorized component.

See Section 5.2.5 regarding the Supervisor's role in authorizing one component to change the operational settings of another.

5.3.5 Synchronize Component Clock

(MR-057) A component ***SHALL*** synchronize its clock to a common system reference clock.

There are a number of options a system manufacturer might employ to meet this requirement. For example, if the system is using Network Time Protocol (NTP) as the reference clock, a component may synchronize directly to the NTP reference. Alternatively, the component might synchronize its clock to the clock of another component (like the Supervisor), which is synchronized to the NTP reference. Section 6.9 provides additional guidance on time synchronization.

5.3.6 Component Time Synchronization

(MR-058) A component ***SHALL*** timestamp all its operations, events, and communications to support the system's functions.

5.3.7 Data Integrity and Validity Monitoring

(MR-061.1) A component ***SHALL*** generate an alert when its input data are no longer available or suitable to support it operations, with the alert condition priority determined by risk management (see Section 5.1.3).

The specifics of the information conveyed in the alert as well as the component and system's response to it depends on the operational requirements of the system. See Sections 6.4 and 6.6 for further discussion of data integrity and validity.

5.3.8 Component Operational Assessment

(MR-062) A component of the system ***SHALL*** periodically assess its health and operating status (including technical alerts) and make this assessment available to other components that have requested this status.

At a minimum, the Supervisor would use this information as part its assessment of system-level operations. The information may also support the operations of other components. Specifics regarding the use of component operational status information depends of the operational requirements of a system.

Figure A-2 in Appendix A depicts component operational status reporting and Supervisor monitoring and fault handling.

5.3.9 Component Data

(MR-066) Component data ***SHALL*** be made available to other components that have requested that data (e.g., descriptive information, metrics, alarm settings, signal averaging time, and computation constants).

5.3.10 Logging of Component Data

As noted in Section 5.3, the requirements in this section do not apply to the Data Logger. However, these requirements apply to all other components.

(MR-094) Each component of the system ***SHALL*** report available descriptive information about itself to the Data Logger.

Examples may include component type, approved intended use, manufacturer, model name, serial number, software version, and settings. The type and volume of data, as well as when and how frequently the data are reported, will depend on the component and system operational requirements.

(MR-095) Each component ***SHALL*** report to the Data Logger the control commands, including parameters associated with those commands, it intends to send to other MDIRA components.

(MR-096) Each component ***SHALL*** report to the Data Logger the control commands, including parameters associated with those commands, it received from other MDIRA components.

During post-operation investigation of system and patient incidents, MR-095 and MR-096 allows verification that control commands generated by one component are correct, and are correctly sent and received by another component.

(RR-097) Each component ***SHOULD*** report to the Data Logger the information that it sends to and receives from other MDIRA-conformant components during a patient care episode.

(RR-098) Each component ***SHOULD*** report to the Data Logger user-initiated changes to the component's settings.

Although it is desirable to record a comprehensive set of data for analysis, there may be practical limitations such as storage capacity and availability that prevent capturing and recording data. As a result, RR-097 and RR-098 are recommended rather than mandatory requirements. However, they should be considered for implementation, if feasible.

5.3.11 Component Shutdown

(MR-067.1) When a User directly deactivates a component (e.g., through its user interface) during a nominal shutdown procedure, or puts it in a standby mode, the component ***SHALL*** immediately notify other components that are receiving data from the component.

5.4 User Manager Requirements

The User Manager can facilitate the setup of User accounts and privileges, controls access to the system according to those privileges, and maintains a User audit log. In accordance with Section 5.1.4, the User Manager is a recommended functional component of a MDIRA-conformant system. The need and sophistication for a User Manager depends on the operational requirements of a system. As a system component, the requirements of Section 5.3 apply to the User Manager. Supplementary requirements are provided next.

5.4.1 Manage User Accounts

(RR-068) The User Manager ***SHOULD*** provide the means to add, remove, and maintain User accounts for a system.

(**RR-069**) While a system is treating a patient, the User Manager ***SHOULD*** prohibit the execution of any user management functions that could increase risk to the patient (e.g., deleting the current Caregiver’s user account).

5.4.2 Assign User Roles and Privileges

(RR-070) The User Manager ***SHOULD*** allow System Administrators to manage (i.e., assign, change, and revoke) system access privileges and User roles as attributes to a User account.

5.4.3 Authenticate Users

(MR-071) The User Manager ***SHALL*** verify the identity of Users requesting access to the system.

5.4.4 Authorize Users

(MR-072) The User Manager ***SHALL*** grant only approved Users access to the system.

5.4.5 Remote Login

(RR-073) The User Manager ***SHOULD*** allow login of remote Users.

5.4.6 Record User Login

(RR-074) The User Manager ***SHOULD*** record User login and logout activity.

The intent of this requirement is to capture sufficient data to allow system administrators to audit user login and logout activities.

5.4.7 Logging of User Manager Data

(MR-102) The User Manager SHALL report to the Data Logger user account changes and user login/logout activity.

5.5 Data Logger Requirements

The Data Logger stores system and patient data during a care encounter for later download to an information system. The Data Logger is a MDIRA component and follows the requirements of Section 5.3 in addition to the functional requirements provided next. The data log will allow a User to review prior system and clinical events associated with the care of a patient and support the post-care, root-cause analysis of system, treatment protocol, or patient safety issues. Data logs downloaded and aggregated from multiple patient encounters will provide an extensive database for analytics to improve care practices and improve patient safety.

Note that AAMI-2700-2-1, "Basic Safety and Essential Performance of a Forensic Data Logger," is currently under development. In lieu of writing requirements that conform to a draft standard, MDIRA Version 2.0 identifies a minimum set of data logging requirements. Data logging requirements will be reconsidered once AAMI-2700-2-1 is completed and approved.

(MR-075.1) The Data Logger ***SHALL*** record the information reported by MDIRA-conformant components during a patient care episode.

Note that this includes all information logged by MDIRA-conformant component and could include commands, interactions between components, and user actions.

(MR-076) Logged data items ***SHALL*** include time tags and provenance metadata.

6. IMPLEMENTATION GUIDANCE

This section provides implementation considerations and guidance on selected topics pertinent to the requirements of Section 5.

6.1 Nomenclature

An important consideration for achieving medical device interoperability is agreement of the nomenclature of data that may flow within a MDIRA-conformant system. Nomenclature is a data item's coded identifier communicated between systems as well as the corresponding definition. Just as communication between people is only made possible by the agreement of definitions for words and phrases, communication between devices and other systems also is only made possible with the agreement of definitions for pieces of information.

The following subsections provide background regarding relevant controlled vocabularies in the medical device and healthcare domains, followed by guidance for MDIRA-conformant systems.

6.1.1 Medical Device Communications (MDC)

The ISO/IEEE 11073-10101 nomenclature standard and amendments (Reference [1]) defines MDC codes, the detailed system of codes used in POC medical devices and PHDs for identification of physiological measurements and settings as well as for alerts, alarm systems, and numerous equipment-related parameters such as calibration state and battery state. The abstract of the source standard ISO/IEEE 11073-10101-2019 (Reference [1]) states:

> *"The nomenclature is specialized for patient vital signs information representation and medical device informatics, with major areas including concepts for electrocardiograph (ECG), haemodynamics, respiration, blood gas, urine, fluid-related metrics, and neurology, as well as specialized units of measurement, general device events, alarms, and body sites. The standard defines both the architecture and major components of the nomenclature, along with extensive definitions for each conceptual area."*

MDC codes were first defined in ISO/IEEE 11073-10101, published in 2004, with an amendment, ISO/IEEE 11073-10101a, published in 2015. Reference [1] cites the 2019 update of the document. Although originally designed for POC medical devices, the nomenclature was also extended in ISO/IEEE 11073-20601 (Reference [19]), published in 2016, for PHDs.

Codes are defined as two 16-bit integers (2-tuple), the first defined as the *code block number* and the second defined as the *term code*. The code block number is represented in the high-order bits, and the term code is represented in the low-order bits (see Figure 6-1, from Reference [1]). Each code has an associated definition as well as a reference identifier to provide semantic interoperability between medical devices. For example, code 149514 [code block (or partition) number 2, term code 18442] has the reference identifier MDC_PULS_RATE, which translates to the "rate of blood pulse in an artery."

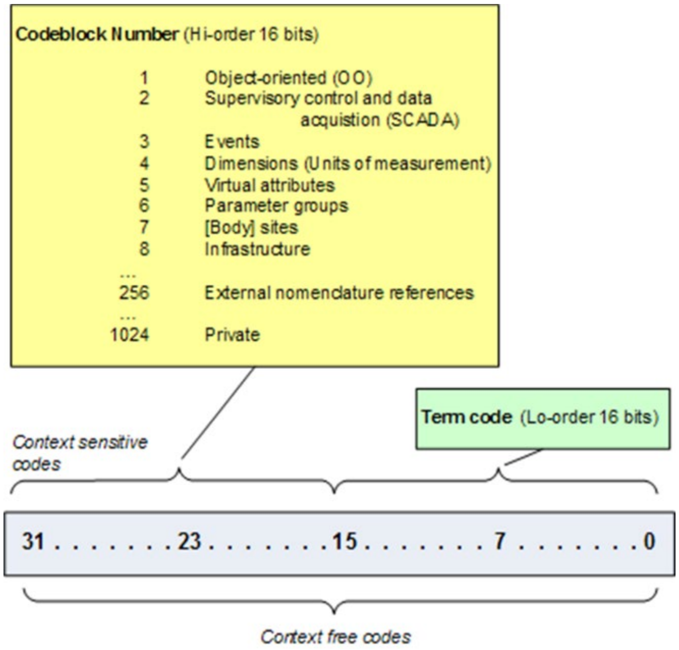


Figure 6-1 Elements of an MDC Code

In addition to definitions found in the ISO/IEEE 11073 series of standards, the National Institute of Standards and Technology (NIST) also created a web application called the Rosetta Terminology Mapping Management System (https://rtmms.nist.gov/rtmms/index.htm) to provide a publicly available database based on the MDC nomenclature to support ongoing conformance and interoperability test efforts. The intent of the tool is to allow medical device manufacturers the ability to map vendor-specific terminology to MDC codes and suggest future MDC codes, thereby reducing the time required to add newly vetted terminology.

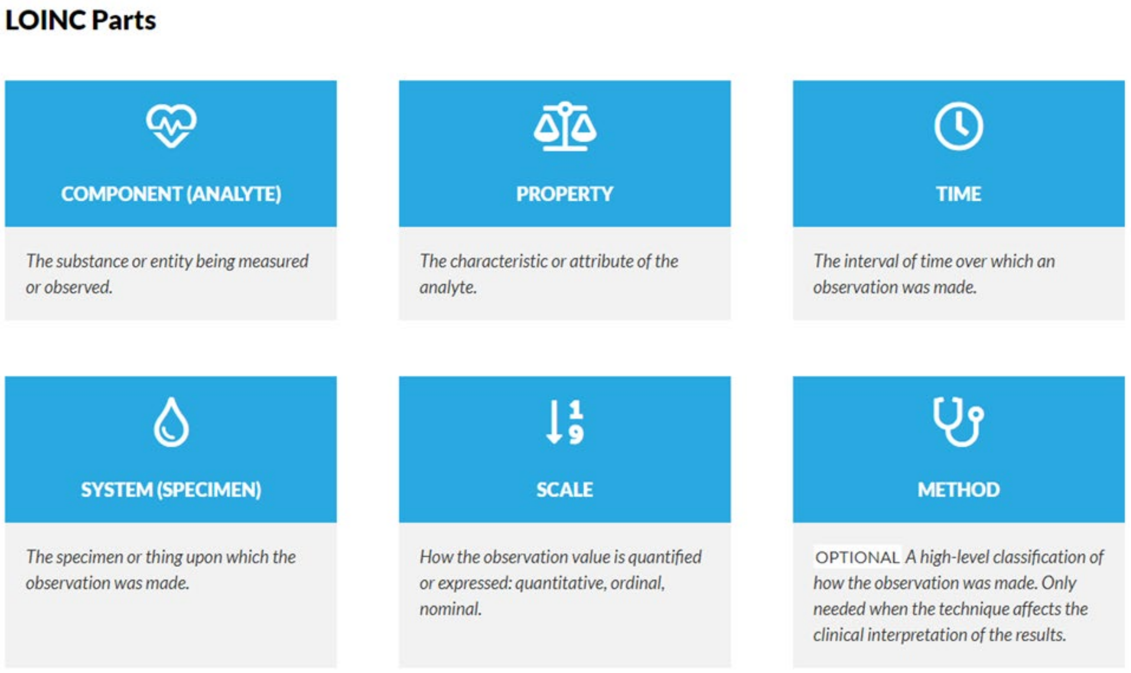
6.1.2 Logical Observation Identifiers, Names, and Codes

As defined on the LOINC website (https://loinc.org/get-started/what-loinc-is/ from Regenstrief Institute, Inc.), "LOINC is a common language (set of identifiers, names, and codes) for identifying health measurements, observations, and documents." LOINC currently has nearly 100,000 terms split into two major divisions of content: Laboratory and Clinical. The LOINC database of codes is updated regularly, with new versions released twice a year in June and December.

Each LOINC code is assigned a number, currently up to five digits (soon to be up to six digits when LOINC reaches 100,000 terms) followed by a hyphen or dash and a single-digit number, which is known as the check digit and is mandatory to include. Each term also comes with six fields known as LOINC Parts, as shown in Figure 6-2, so that similar code definitions are more easily distinguishable. As an example, the code 806-0, which represents "manual count of white blood cells in cerebral spinal fluid specimen," has the following assignment of parts:

- Component (Analyte): Leukocytes (white blood cells)
- Property: NCnc (number concentration)

- Time: Pt (point in time)
- System (Specimen): CSF (cerebral spinal fluid)
- Scale: Qn (quantitative)
- Method: Manual Count



LOINC Parts

COMPONENT (ANALYTE)

The substance or entity being measured or observed.

PROPERTY

The characteristic or attribute of the analyte.

TIME

The interval of time over which an observation was made.

SYSTEM (SPECIMEN)

The specimen or thing upon which the observation was made.

SCALE

How the observation value is quantified or expressed: quantitative, ordinal, nominal.

METHOD

OPTIONAL A high-level classification of how the observation was made. Only needed when the technique affects the clinical interpretation of the results.

Source: https://loinc.org/get-started/loinc-term-basics/

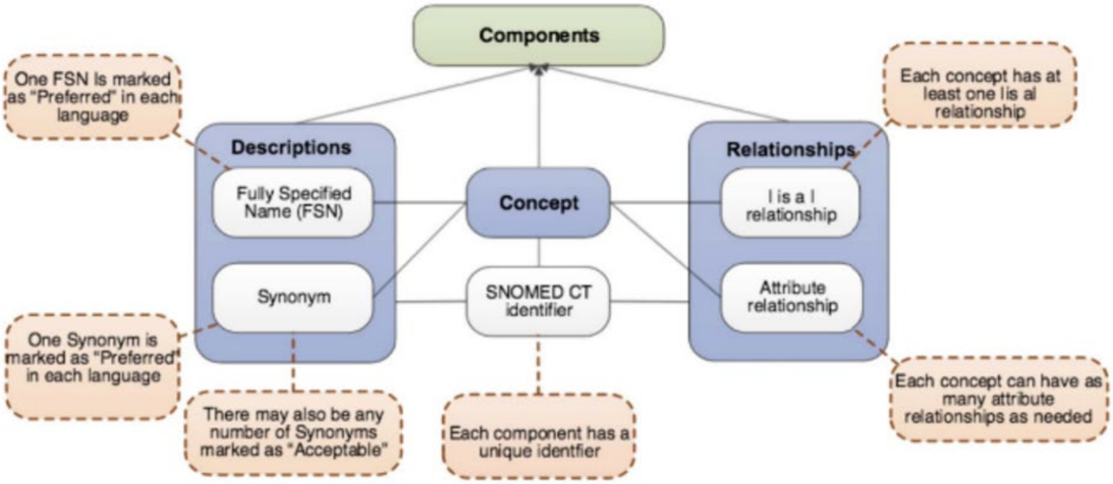
Figure 6-2 Elements of LOINC

LOINC also has many resources to help a user implement the code system. In addition to downloadable files that include the full database, there is also a browser-based application of LOINC at https://search.loinc.org/. Similar to RTMMS for MDC, LOINC also has software known as the Regenstrief LOINC Mapping Assistant (RELMA) that assists a user in mapping local codes to LOINC codes. Lastly, LOINC also supplies a Top 2000+ list of the most common LOINC codes to help users map large sets of local laboratory test codes.

6.1.3 Systematized Nomenclature of Medicine – Clinical Terms

As defined on the SNOMED website (https://www.snomed.org/snomed-ct/five-step-briefing), SNOMED CT is a coding system for the clinical practice, diagnosis, and other types of clinical findings such as signs and symptoms. It includes tens of thousands of surgical, therapeutic, and diagnostic procedures. It includes observables (e.g., heart rate) as well as concepts representing body structures, organisms, substances, pharmaceutical products, physical objects, physical forces, specimens, and many other types of information that may need to be recorded in or around the health record.

There are three components to SNOMED CT: concepts, descriptions, and relationships (see Figure 6-3). Every concept has a unique clinical meaning and is referenced by a unique 64-bit numeric SNOMED CT identifier or code. Concepts are linked to two types of descriptions: (1) the Fully Specified Name (FSN), which represents a unique, unambiguous description of a concept's meaning, and (2) a Synonym that allows the use of other terms to represent the same concept. Lastly, SNOMED CT concepts may be linked to other concepts through the relationship component. For example, the SNOMED CT concept "diabetes mellitus type 2 (disorder)" with identifier 44054006 is linked to the concept "diabetes mellitus (disorder)" with identifier 73211009 by a third relationship type concept called "is a" with identifier 116680003.


Components
One FSN is marked as "Preferred" in each language
Each concept has at least one |is a| relationship
Descriptions
Fully Specified Name (FSN)
Synonym
Concept
SNOMED CT identifier
Relationships
| is a | relationship
Attribute relationship
One Synonym is marked as "Preferred" in each language
There may also be any number of Synonyms marked as "Acceptable"
Each component has a unique identifier
Each concept can have as many attribute relationships as needed

Source: https://www.snomed.org/snomed-ct/five-step-briefing

Figure 6-3 SNOMED CT Components

The SNOMED CT database can be searched through the SNOMED CT browser found at http://browser.ihtsdotools.org/.

6.1.4 Requirement for Medical Device Data Nomenclature

Section 5.1.19 stipulates that a MDIRA-conformant system shall conform with industry-accepted medical data nomenclature and semantics resources to the greatest extent possible including IEEE 11073-10101-2019 for medical device data. Table 6-1 presents examples of MDC codes for selected medical devices. Section 6.1.5 provides guidance in the event an MDC code does not exist for a required parameter. Ongoing MDIRA development includes assessing the adequacy of the scope of the data items addressed in the ISO/IEEE 11073-10101 series, as well as adequacy of the data item definitions.

Table 6-1 Example of MDC Codes for Selected Medical Devices

Device	Parameter	MDC Reference Identifier	MDC Code
Multi-parameter Patient Monitor	Heart rate	MDC_ECG_CARD_BEAT_RATE	147842
	Cardiac beat-to-beat rate	MDC_ECG_CARD_BEAT_RATE_BTB	147850
	Premature ventricular contractions	MDC_ECG_V_P_C_CNT	148065
	ST generic label	MDC_ECG_AMPL_ST	131840
	QTc	MDC_ECG_TIME_PD_QTc	147236
	QT	MDC_ECG_TIME_PD_QT_GL	147232
	Pulse rate	MDC_PULS_RATE	149514
	Arterial O_2 saturation	MDC_PULS_OXIM_SAT_O2	150456
	Pulse rate from plethysmogram	MDC_PULS_OXIM_PULS_RATE	149530
	Perfusion indicator	MDC_PULS_OXIM_PERF_REL	150448
	Noninvasive blood pressure (NBP)	MDC_PRESS_BLD_NONINV	150020
	Pulse from NBP	MDC_PULS_RATE_NON_INV	149546
	Respiration rate	MDC_RESP_RATE	151562
	Skin temperature	MDC_TEMP_SKIN	150388
Ventilator	Peak inspiratory pressure	MDC_PRESS_AWAY_INSP_MAX	151817
	Mean airway pressure	MDC_PRESS_AWAY_MEAN	151795
	Positive end expiratory pressure	MDC_PRESS_AWAY_END_EXP_POS	151804
	Total breath rate	MDC_RESP_RATE	151562
	Exhaled tidal volume	MDC_VOL_AWAY_TIDAL	151868
	Minute volume	MDC_VOL_MINUTE_AWAY	151880
	I:E ratio	MDC_RATIO_IE	151832
Infusion Pump	Rate mL/hr	MDC_FLOW_FLUID_PUMP	157784
	Dose rate	MDC_RATE_DOSE	157924
	mL VTBI	MDC_VOL_FLUID_TBI_REMAIN	157872
	Time (hr:min)	MDC_TIME_PD_REMAIN	157916
Urimeter	Urine flow	MDC_FLOW_URINE_INSTANT	157708

6.1.5 Guidance for Non-Medical-Device Data Nomenclature

Other types of data are pertinent to MDIRA-conformant systems, for example, patient demographics, medications administered, clinical observations, and diagnostic data. In such situations, and when an MDC code does not exist for a required medical-device–related parameter, other nomenclature standards may be drawn upon. Table 6-2 provides recommendations on nomenclatures to use for various categories of data. Also, several nomenclature standards may represent the same types of data. For example, some blood analyte parameters have LOINC as well as MDC codes (there are now POC blood analysis devices). In this case, the recommendation is to use LOINC since there is long precedent for using LOINC codes to represent blood analyte data collected in laboratory testing.

Table 6-2 Standards for MDIRA Terminology (Preliminary – Not All-Inclusive)

Data Elements	Standard for Nomenclature
Vital signs name (observation label)	ISO/IEEE11073-10101
Vital signs name (observation value)	ISO/IEEE11073-10101
Units of measure for medical devices covered by ISO/IEEE 11073	ISO/IEEE11073-10101
Laboratory and diagnostic imaging orders	LOINC
Laboratory test results name	LOINC
Laboratory test results quantitative (value)	LOINC
Laboratory test results units of measure	UCUM (although this is often embedded in the LOINC laboratory test results name) (see http://unitsofmeasure.org)
Laboratory test results qualitative (value)	SNOMED CT (positive or negative)
Laboratory test results infectious disease	SNOMED CT
Specimens (e.g., specimen types, specimen source types)	SNOMED CT
Procedures (laboratory methods)	SNOMED CT (although this is often embedded in the LOINC laboratory test results name)

In the case where neither ISO/IEEE11073-10101, LOINC, nor SNOMED CT define codes a particular parameter, a private MDC code may be used for medical-device–related parameters, as indicated in Section A.2 of IEEE 11073-10101 (Reference [1]).

However, it is also recommended to contact the pertinent SDO to consider including missing terms in future standard releases, specifically:

- IEEE for medical device data that should be in MDC
- Regenstrief Institute, Inc., for laboratory observations that should be in LOINC
- National representatives for SNOMED International for all other healthcare terms that are absent from SNOMED CT

6.2 Information Model

Another consideration in achieving medical device interoperability is the information model. The information model is a data hierarchy that specifies elements, attributes, and services that may be used to communicate data and to control and configure the reporting of information. In other words, the model describes the relationships between data elements and how to communicate those elements so that every component in a MDIRA-conformant system can find relevant pieces of data.

Analysis of the MDIRA information model requirements is ongoing. There is no single existing information model sufficient to represent all the types of information pertinent to MDIRA-conformant systems. It is expected that MDIRA pertinent information model will built upon extensions of several standards, including those of the ISO/IEEE 11073 series as well as the FHIR standard (for clinical data). Standard information models for robotic systems may also be pertinent.

6.2.1 IEEE 11073 DIM

ISO/IEEE 11073-10201 describes the IEEE 11073 DIM standard originally published in 2004 and revised in 2018 by IEEE and adopted by ISO in 2020 (see Reference [2] for the latter). As shown in Figure 6-4 (reproduced from the standard, Reference [2]), the DIM consists of a number of packages of data objects. The medical package (green box), which is expanded in Figure 6-5 (reproduced from the standard, Reference [2]), contains the metric object that represents observed measurement values from medical devices. For example, a multi-parameter monitor (i.e., an MDS) may have a blood pressure module along with several other plug-in sensors, each represented as a virtual medical device (VMD). A blood pressure VMD may then have one Channel object that groups all blood pressure metrics together and a second Channel object that groups all heart rate metrics together. Lastly, a blood pressure value (Numeric) and a blood pressure oscillometric waveform (SampleArray) as well as other parameters in the blood pressure Channel are represented as Metric objects. This section provides a brief intro to the DIM, and represents a very small set of the DIM content. Further detail on the objects shown in Figures 6-4 and 6-5 and the DIM can be found in ISO/IEEE 11073-10201.

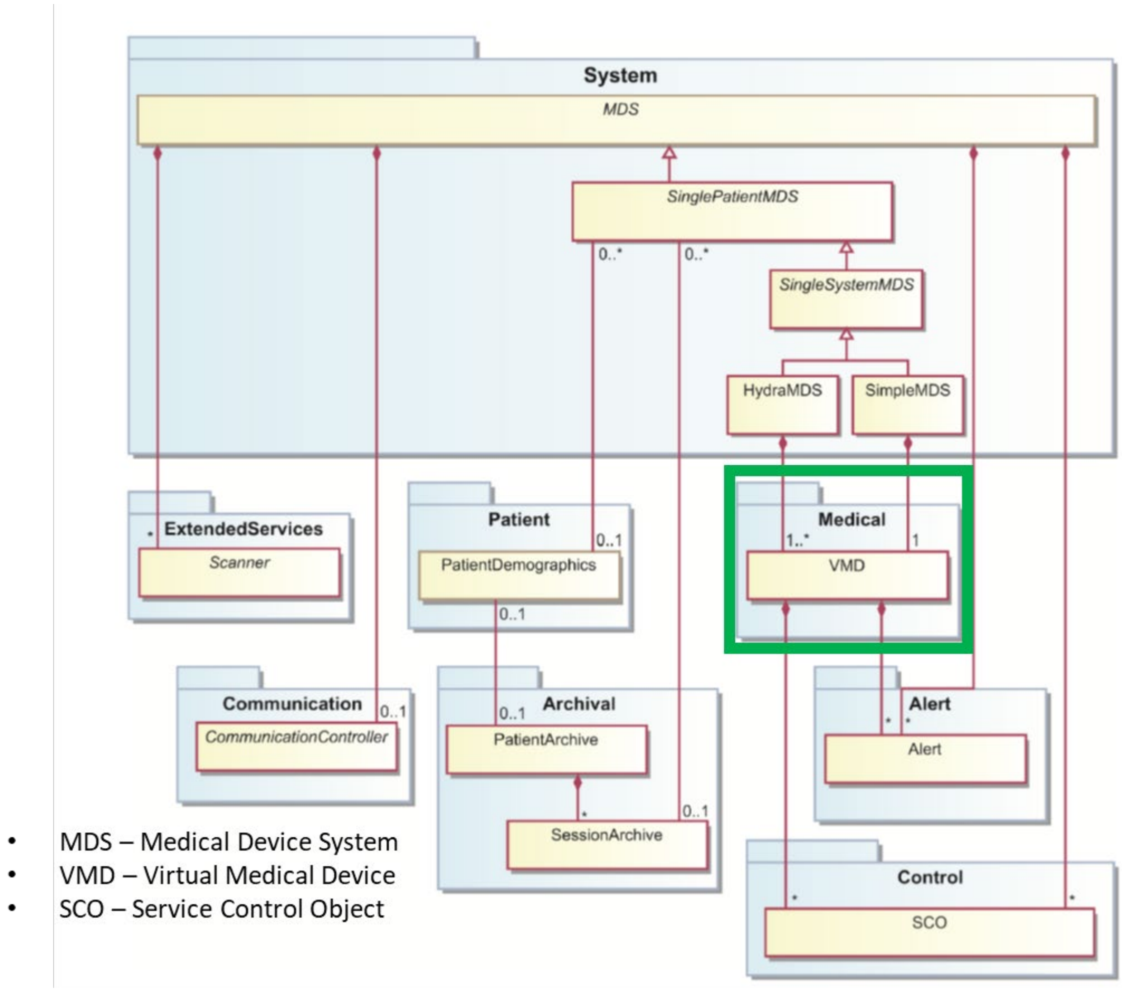


Figure 6-4 IEEE 11073 DIM Structure

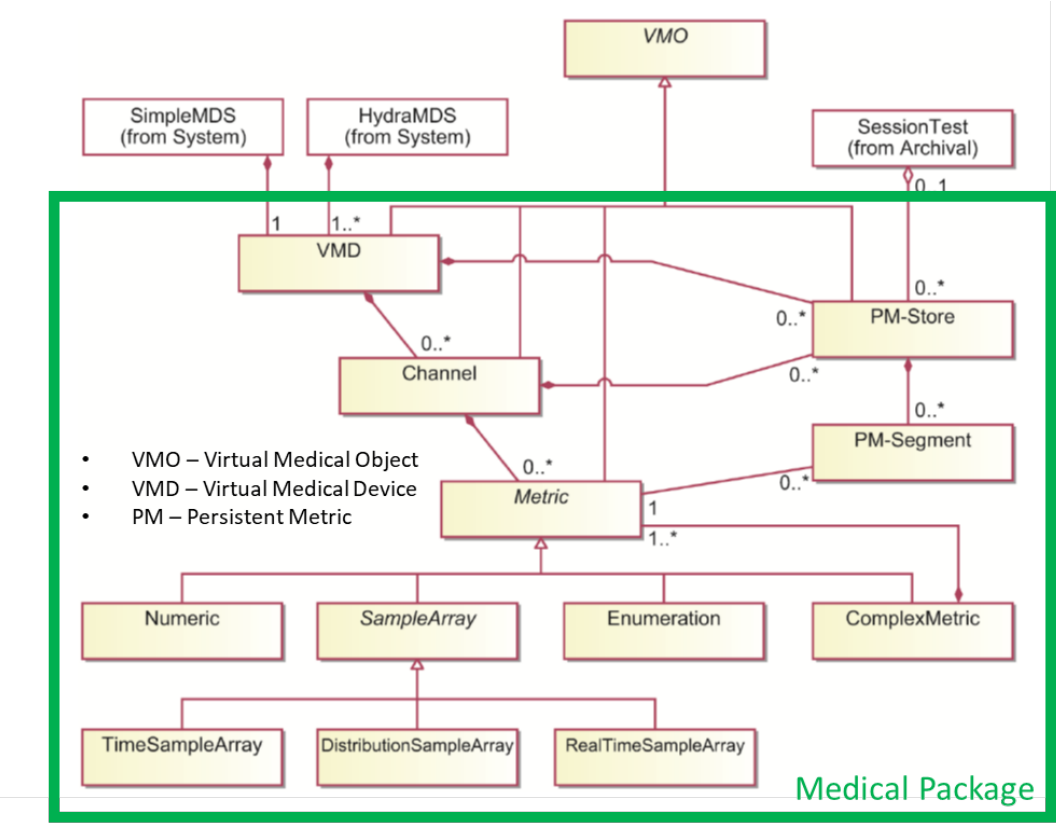


Figure 6-5 Objects of the IEEE 11073 DIM Medical Package

6.2.2 IEEE 11073 Basic Integrated Clinical Environment Protocol Specification

BICEPS is the non-normative name for ISO/IEEE 11073-10207 (Reference [18]) published in 2017 and is one of a family of standards named as IEEE 11073 SDC. BICEPS is composed of three major parts: Participant Model, Communication Model, and Discovery Model. The Communication and Discovery Models, which provide specifics on one communication architecture implementation for a MDIRA-conformant system (i.e., web services based), are outside the scope of this subsection. The Participant Model, which describes the information model within BICEPS, is this focus here, and it has applicability regardless of communication architecture implementation. Figure 6-6 (taken from Reference [18]) gives an overview of the containment tree in the Participant Model, which is closely related but not equivalent to the IEEE 11073 DIM from ISO/IEEE 11073-10201 (Reference [2]).

BICEPS also includes multiple open-source code repositories to aid in the implementation of the information model as well as other parts of the IEEE 11073 SDC family of standards. These include the following:

- openSDC (https://sourceforge.net/projects/opensdc/)
- sdc11073 (https://github.com/Draegerwerk/sdc11073)

- SDCLib/ (https://github.com/surgitaix/sdclib)
- SDCLib/J (https://bitbucket.org/surgitaix/sdclib)

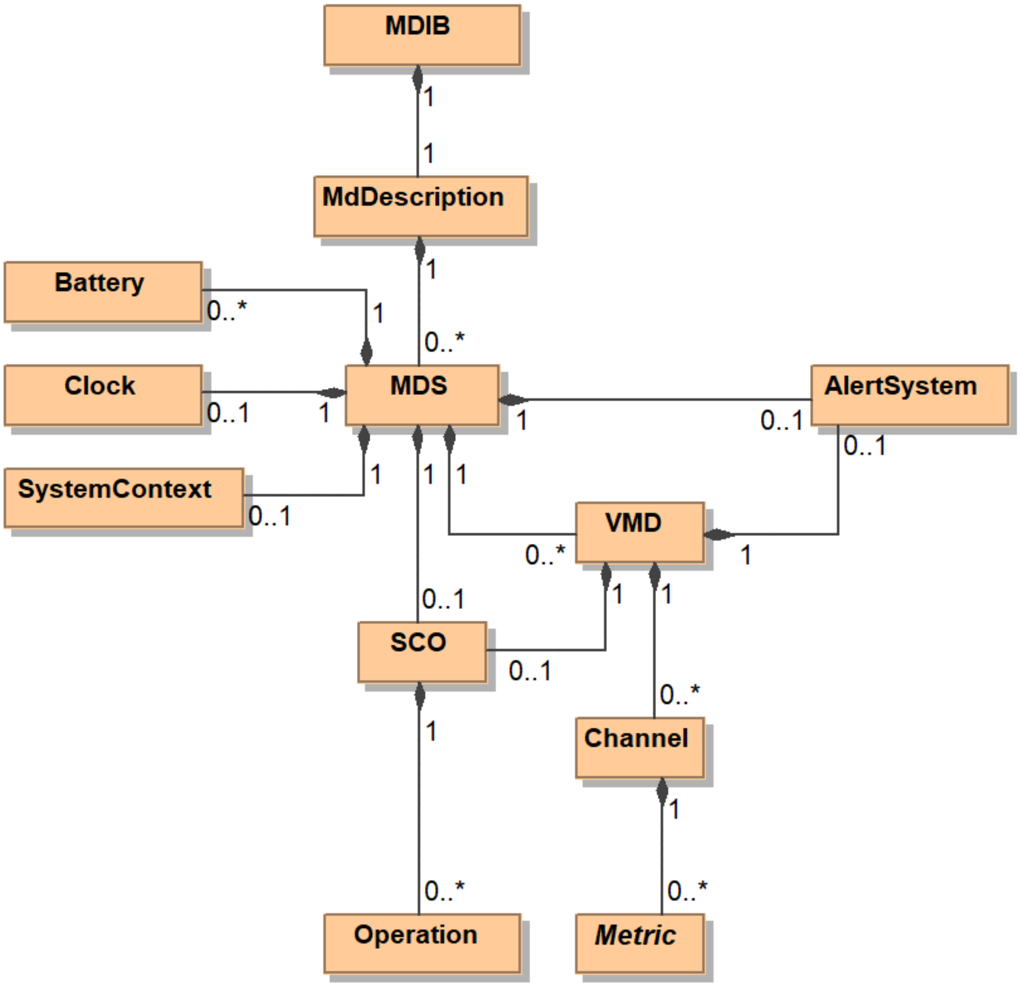


Figure 6-6 IEEE 11073 BICEPS Structure

6.2.3 Fast Healthcare Interoperability Resources

FHIR is a framework created by HL7 International and is currently in v4.0 (Reference [20]). Although many components of FHIR are still incomplete, the FHIR community is actively filling the gaps. FHIR consists of a set of modular components called resources. These resources can be easily assembled into data components. Resources use a set of nomenclatures that is suitable to that resource (SNOMED CT or LOINC or others where appropriate).

Figure 6-7 (taken from Reference [20]) shows the components of FHIR that address the information model, constraints, terminology, and usage. The information model has two base classes: Element and Resources.

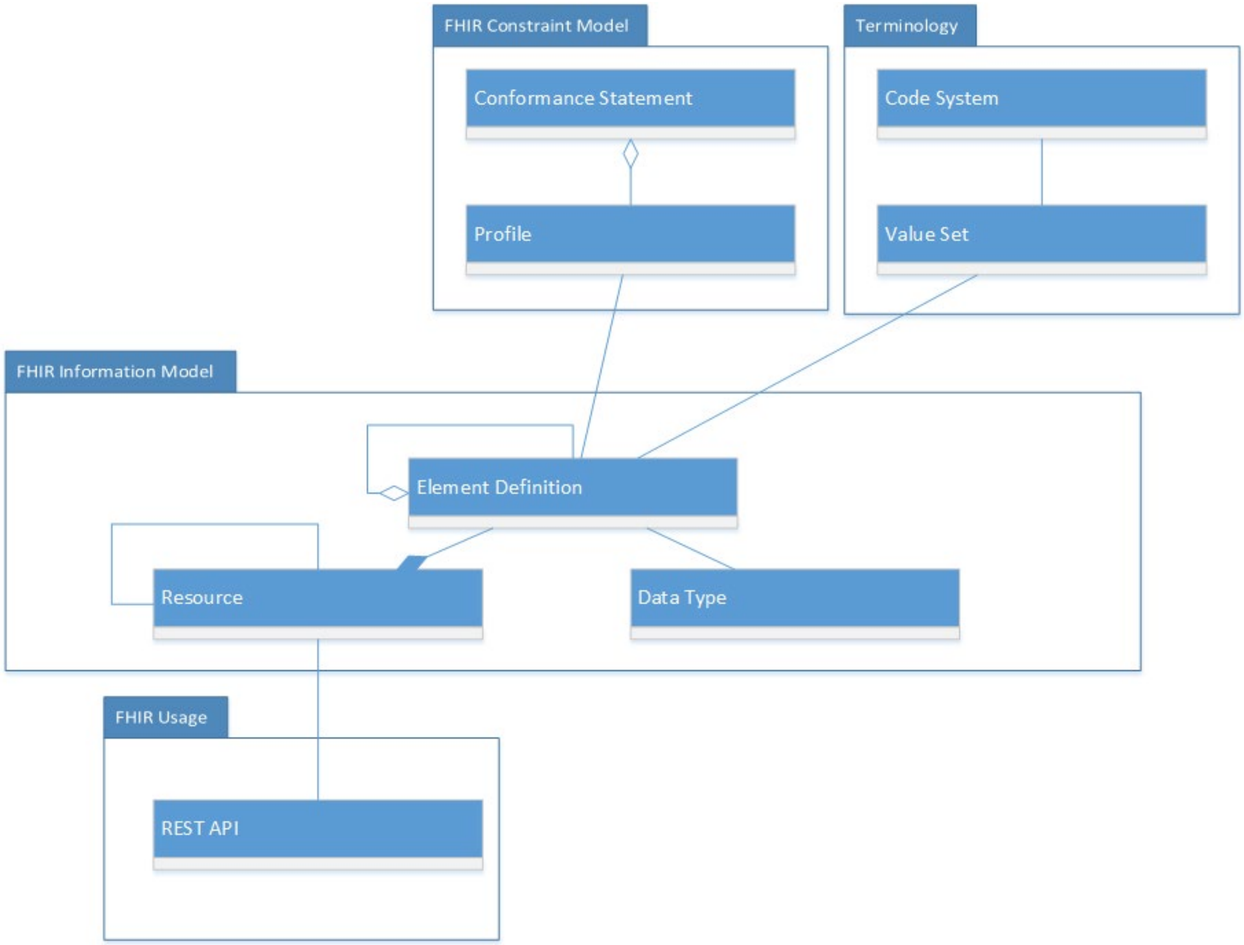


Figure 6-7 Components of FHIR

6.3 Data Transport

Data transport refers to the delivery of data from a component producing the data to the component consuming the data. In MDIRA-conformant systems, a uniform data transport solution provides ubiquitous connectivity among all components within the system. Uniformity is necessary (although not sufficient) to facilitate PnP solutions with components from multiple sources. There are a variety of data transport functional requirements necessary to have a robust, safety-critical solution for systems. The specifics of these requirements depend on the operational requirements for a particular system. Even so, some general observations are appropriate.

Reliable delivery of data is a critical component for a data transport solution. While it is reasonable for applications to develop their own reliability mechanisms, most applications rely on standardized, reliable transport protocols such as the Transmission Control Protocol (TCP) as part of its data transport service. The data transport service detects and handles the loss of data while the data are in transit for all components, thereby facilitating retransmission of the lost data, as needed.

Depending on the operational requirements of a system, the scope of the data sharing between components will determine the data transport selected. Situations where all components are collocated within a small network or within a single hardware chassis allow for relatively simple data transport solutions given the proximity of components. If components are distributed and connected over high-latency network paths (i.e., long roundtrip times), a potentially more complex data transport protocol will be required to manage the data delivery among components and to react to changing network conditions.

In many data transport solutions, other features are incorporated into the transport mechanism. For example, TCP within the Internet Protocol (IP) family provides reliable, in-order delivery of data between two communicating devices. If TCP is protected using the Transport Layer Security (TLS) protocol, the data transport channel also provides data integrity, confidentiality, and sender authentication (via X.509 certificates).

The data transport approach should be based on open commercial standards to facilitate inter-operability, system openness, and security. Proprietary solutions restrict the sources of components for a MDIRA-conformant solution. By leveraging standards, a compliant architecture reduces the cost and complexity of developing, testing, and deploying components. A variety of data transport solutions is available. The following subsections describe two of the more predominant solutions proposed for use in medical environments.

6.3.1 Web Services

The World Wide Web Consortium (W3C) defines a web service as a software system designed to support interoperable machine-to-machine interaction over a network (Reference [21]). A web service typically relies on the Hypertext Transfer Protocol (HTTP) to transfer data encoded in a machine-readable format [e.g., eXtensible Markup Language (XML) and JavaScript Object Notation (JSON)]. HTTP is designed to operate atop both TCP and the User Datagram Protocol (UDP) within an IP-based network.

The IEEE 11073 SDC family of standards defines a Medical Device Profile for Web Services (MDPWS) (Reference [22]) for sharing medical device data across networks. By leveraging an existing standard for data exchange, the MDPWS satisfies functional requirements for reliable data delivery (TCP), integrity and confidentiality (TLS), and discovery (Web Services Dynamic Discovery).

6.3.2 Publish/Subscribe

Publish/subscribe (pub/sub) refers to a method of data exchange where the data producer (the publisher) shares data without explicitly knowing the data consumers (the subscriber) or vice versa. Publishers categorize their data into topics and make them available via middleware. Consumers register for and receive topics from the middleware when they become available. The paradigm can be thought of as being data (or message) oriented.

The Open Management Group (OMG) Data Distribution Service (DDS) standard defines a machine-to-machine middleware that enables reliable and scalable data exchanges using the pub/sub model. The DDS specification provides for reliable data delivery, discovery, and prioritization of data topics. Recent OMG standards have added authentication, access control, and data-in-transit confidentiality (Reference [23]). DDS middleware is available as open source or supported with extensions from several vendors. Versions are available free of charge for teaching and academic research.

6.4 Data Integrity

Data integrity refers to the consistency and accuracy of data. Examples (non-exhaustive) include the following:

- Leveraging a data model to describe each data element within an application
- Using error correcting codes on data at rest
- Applying message authentication codes on data in transit

In MDIRA-conformant systems, data integrity capabilities are necessary for managing data at rest, sharing data between system components, and protecting the software and processes that comprise the system. The development of a system must include a focus on data integrity. The overall data integrity approach needs to account for identifying altered data, restoring data to its last known good state, correlating events that coincide with data alteration events, and determining any impact of the data alteration.

Each system component must be concerned with the integrity of data stored on that component and the integrity of the software and processes that comprise that component. The requirements for each component will vary based on its functionality and storage capabilities. In-depth recommendations and guidance on data integrity are available in NIST Special Publication (SP) 1800-11 (Reference [24]).

Given the data sharing inherent within the system, integrity for data shared between components is critical. A component that is receiving data must be able to verify the integrity of that data to ensure correct operation of the system. To that end, network data integrity must be incorporated into the system. Typically, network data integrity is provided as a function of the overall network security solution (e.g., hash-based message authentication code within the TLS solution).

6.5 Data Confidentiality

Data confidentiality refers to protecting information from unauthorized access. Only authorized parties should be allowed to view sensitive data. Given the nature of MDIRA-conformant systems, such sensitive data include personally identifiable information (PII) as well as protected health information (PHI). As with data integrity, confidentiality functions are needed for data at rest and in transit.

Protecting data at rest from unauthorized access requires several capabilities. First, each component must support authorized access for all data stored on that component. Only users, applications, and processes with authorization should be allowed to access an element of the data. The granularity of the access rules depends on the operational and regulatory requirements imposed on the MDIRA-conformant system. In addition to access control, data at rest must be protected from data breaches caused by, for example, hacking, software corruption, and physical intrusion. To provide such protection, sensitive data should be encrypted while stored on stable medium within each component. Recommendations and guidelines for protecting data at rest are available in NIST SP 800-111 (Reference [25]).

As with integrity, confidentiality for data in transit is typically provided by the overall network security solution associated with the data transport protocol(s). It is essential that any MDIRA-conformant system comply with legal and regulatory.

6.6 Data Validity

Data validity refers to collected data being correct, accurate, and reasonable. The *validity* of data should not be confused with the *integrity* of data. Typical data validation steps may include validating the following:

- Data types – Data provided are of the expected primitive data types
- Ranges – Data provided fall within an expected range
- Cross-references – Data provided meet defined rules, constraints, and requirements
- Structure – Complex data provided meet conditional constraints for the data structure

Data validity is tightly coupled with the capabilities of the data producer and the requirements of the data consumer.

A MDIRA-conformant system may produce, share, and consume a myriad of data elements. There will be no one unified set of data validation rules that can be imposed across all systems. To that end, each possible data element or stream will have its own set of validation rules. The point of implementation of those validation rules will depend on the system's design driven by requirements and regulations. In many instances, the data consumer should be performing the validation checks after verifying the integrity of the received data. Performing the data validation checks at the consumer level reduces the potential for secondary corruption of the data prior to its consumption. Implementing data validity checks at other points in the data exchange are possible, but requires more complexity to ensure corruption does not occur prior to the data being used.

6.7 Authentication

Adequate authentication is essential to implementing robust security policies. Each user and component, henceforth referred to as *subject*, shall be identified to a MDIRA-conformant system. Each subject maintains a *digital identity* within the system, and authentication is the process of validating that identity using *authenticators*. Systems define the authenticators being used by all subjects and the processes needed to validate those authenticators. Note that a system developer could implement multiple levels of assurance within a single system, if needed.

Varying levels of assurance allows a system to protect information and resources in different ways based on their sensitivities. The level of assurance will dictate the lifetime of the authenticator(s), complexity of the verification step(s), and duration of any session established based on successful authentication. In-depth recommendations and guidance on authentication are available in NIST SP 800-63B (Reference [26]).

There are numerous design considerations for MDIRA-conformant systems given the sensitivity of the information (PHI and PII) being shared across the system. A non-exhaustive list of such considerations includes the following:

- Mutual authentication versus one-way authentication
- Single Sign-On
- Standalone versus integrated authentication (e.g., Kerberos versus OAuth)
- Credential and Key management
- Single- or multi-factor authentication

6.8 Authorization

As with authentication, authorization is an essential function of a robust security framework. Authorization provides the access rights to resources for users, devices, and processes by defining access policies imposed throughout the system. After a subject is authenticated, any attempt by the subject to access resources should be controlled by the defined access policies.

A MDIRA-conformant system defines an authorization framework that satisfies all applicable legal and regulatory requirements. There are a myriad of authorization frameworks available that approach the access control function from a number of ways (e.g., role-based versus attribute-based). NIST Interagency Report 7316 (Reference [27]) provides an assessment of access control systems that contains clear descriptions of a variety of approaches as well as the advantages and disadvantages of each.

6.9 Time Synchronization

Reliable time synchronization is becoming a requirement for many distributed systems. Functions such as public-key cryptography, event correlation, data logging, and distributed decision-making all require involved components to have consensus on the current time. The lack of time coordination makes these functions either difficult or impossible to perform accurately. The requirements levied on the system regarding time synchronization focus on two key aspects: (1) providing a reliable reference clock and (2) having all components synchronize to the reference clock.

The need for absolute time accuracy drives the selection of a reference clock. If requirements exist for maintaining absolute time, implementers should focus on real reference clocks. Some examples include global positioning system (GPS) and radio-wave time signals (e.g., DCF77 and WWVB). The use of a reliable reference clock provides the ability to correlate activities within a system to outside actions (e.g., human actions). On the other hand, if requirements only dictate the need for synchronization of time between MDIRA-conformant components (i.e., relative), a local reference clock can be used. The local reference clock simply refers to the system time on the device providing the time synchronization signal. The components within the system will all be able to agree on the time, but it will not be accurate enough to correlate with activities outside the system.

The synchronization of time between all components is necessary for a variety of reasons. The exchange of public-key cryptography credentials involves exchanging certificates that have a fixed lifetime. Devices verifying a certificate need to know the current date and time to determine whether the certificate has expired. Algorithms coordinating distributed actions need to be able to synchronize those actions across multiple components, algorithms, or platforms. The method selected to synchronize all components within a system drives the granularity of the synchronization. There are several possibilities for time synchronization:

- Network Time Protocol (NTP) is the de facto time synchronization protocol within the Internet. It is natively supported by a wide variety of devices and has configurable options for selecting reference clocks and synchronization algorithms. NTP can generally provide time synchronization between a client and a reference clock within a ±50-millisecond window. NTP is specified in Request for Comment (RFC) 5905 (Reference [28]).

- Precision Time Protocol (PTP) performs clock synchronization within a local network and can provide clock accuracy in the sub-microsecond range. PTP has been deployed for clock synchronization to support applications such as financial transactions, acoustic arrays, and cellular transmissions. The PTP standard is published in IEEE 1588 (Reference [29]).

6.10 Device Health Status

A device health status infrastructure allows users to efficiently track the current state of all (or important) devices within a system. Many commercial systems provide rudimentary, but proprietary, methods for tracking a device’s status (e.g., Apple’s Device Health Check). Within distributed systems, the device health status approach needs to be consistent across all heterogeneous devices.

The most prevalent device health monitoring approaches leverage the standardized Simple Network Management Protocol (SNMP). SNMP supports a wide variety of device status indicators, arranged in Management Information Blocks (MIBs), for a range of networked devices. For example, the SNMP Interfaces MIB allows users to track the operational status of all network interfaces connected to a network.

Within the context of MDIRA, there is no defined device health status mechanism that is common across all possible components. Individual medical devices typically perform status assessments, display messages, and produce technical alarms; and the implementation and sophistication of these vary widely between device types and manufacturers. A key work item for this effort will be the definition of the indicators needed for device health and the transport mechanism for sharing that device health information with the relevant consumers.

6.11 Discovery

To support a true PnP paradigm, a MDIRA-conformant system needs a singular mechanism that allows for the dynamic insertion of a component or device into the system. Either the device needs to discover the system or the system needs to discover the device. Once discovery occurs, the device can advertise its capabilities and be registered for use within the system.

The discovery function can be accomplished in multiple ways. The first involves leveraging services integrated into the data transport solution. Many of the data transport solutions identified for use in medical devices enable a discovery feature. Many pub/sub solutions support participant discovery mechanisms, such as the Simple Participant Discovery Protocol (SPDP) within DDS. Web-services–based solutions leverage the Organization for the Advancement of Structured Information Standards (OASIS) standard for device discovery using IP multicast messaging on the local network. Another method is to use a standalone device discovery mechanism. A non-exhaustive list of examples includes:

- Device registration via link-specific protocols, such as IEEE 802.1x
- Standardized discovery solutions, such as the Simple Service Discovery Protocol (SSDP)
- Service registration via rendezvous protocols, such as multicast Domain Name Server (mDNS)

6.12 Logging

Data logging within a MDIRA-conformant system takes on two primary forms. The first is that of a data log. The second form is that of data stores to facilitate the functional operations of the system. These functions are distinct and should be kept isolated from one another.

6.12.1 Data Log

A data log provides a historical record for forensic analysis of system failures and adverse events, as well as for supporting system and process improvements. The data log should be considered a write-only capability, whereas the system is in an operational state. That is, components do not access the data log to retrieve data stored within it. Additionally, it is critical that the data log leverages the data integrity, data confidentiality, and time synchronization functions within the system.

The primary use of the data log is post-operational analysis. By storing relevant data produced by the system during patient care (e.g., patient data, device data, device status, commands), the data log provides a record of activities within the system. The data recorded can be analyzed to audit the function of the system, diagnose failures within the system, and track treatments invoked. A system should carefully identify which data elements within the system (including their syntax, semantics, and coding mechanisms) need to be logged to fully support analysis and possible continuous system improvement. The AAMI 2700-2-1 draft standard provides a useful list of data elements that should be considered for recording in the data log.

The engineering characteristics of the data logger, such as data velocity and throughput and data storage capacity, should also be carefully designed. For example, the storage capacity of the data logger should be specified to preserve the logged data for a period of time that is appropriate based the system's intended use and typical operation patterns. It is also preferable to design the data logger to operate independent of the rest of the system so that data logging can continue even during system failures. In addition, a system will provide a facility to access the data log when the system is not operational (e.g., diagnostic state).

6.12.2 Data Stores

Data stores provide localized storage accessible by some number of components, applications, or users. A data store can take a variety of forms, such as a database, flat file, or virtual disk. The primary function of a data store is to provide read/write data management to facilitate operations within a system. Access to such a data store is protected via the authentication and authorization frameworks employed by the system.

Information in a data store can take many forms. In some instances, the data are ephemeral and subject to the operations imposed by the associated component (e.g., results of an intermediate calculation for a clinical care protocol). In other instances, the data are maintained throughout the operational lifetime of the system (e.g., authentication credentials for the system).

Data store functions are separate from data logging operations to ensure the of the data log.

6.13 External Interfaces

MDIRA is designed to be flexible to satisfy a variety of medical-care delivery missions. In many instances, a MDIRA-conformant system will require information sharing with a variety of external systems, parties, or users. Some examples are as follows:

- Telemedicine – Two-way, audio/video conferencing to facilitate use of remote medical expertise
- Recordkeeping – Data exchange with EHR systems to maintain patient data
- Evacuation – Data sharing on patient status and treatment plans with evacuation vehicles and/or patient-receiving personnel
- Robotic assistants – High-level command and control and data exchange with robots participating in the medical care process

These functions, as well as others, can require radically different capabilities from an interface. In some instances (e.g., EHR systems), interfaces may already exist and simply need to be incorporated into the system. In other instances (e.g., evacuation), interfaces will need to be developed in concert with the programs responsible for the external system.

The form and functionality of new interfaces will depend on the functionality required. Some interfaces will simply be application programming interfaces that facilitate data exchange over existing network connections. Other interfaces may require the definition of hardware and software interfaces. Regardless of the form, these external interfaces will need to be developed, or agreed to, in concert with the other organizations and programs involved.

6.14 Component Configuration Arbitration

It is critical for the correct operation of the system that the configuration settings are known and available for each component in the system. If multiple entities can change the configuration of a specific component, or changing the configuration of that component can affect its output and in turn the operation of other components consuming its output, there should be a means to notify all relevant components and users of the specific individual component's configuration change. In some situations, configuration changes may need arbitration before they are allowed to occur so as to reduce the potential for configuration actions that adversely affect the operation of the system or increase risk to a patient. The system application may perform this arbitration as could a local or remote user.

As an example, consider a system that contains a sensing component capable of reporting its data in one of two formats controlled by a configuration setting and two applications wishing to receive the sensor data. If both applications have the ability to set the sensor's configuration, there will be a conflict if the applications want the data in different formats.

To minimize the effect of such configuration conflict or deadlock, MDIRA-complaint systems need to consider the mechanisms employed to control the configuration of each component. This is especially true for scenarios where multiple care protocols are being administered to a single patient and there is an overlap in the devices used to monitor the patient or deliver the treatment. Potential approaches for maintaining coherent device configurations include the following:

- Arbitrated configuration requests through a mediator (e.g., Supervisor)
- Configuration locks within the component
- Direct notification of configuration changes to all paired components

Regardless of the approach used, the end result should be the same. All interested components should have a consistent representation of the configuration of other components of interest.

6.15 Control Topology Considerations

Developers may implement autonomous care capabilities in a MDIRA-conformant system in a number of different ways. This section describes several bounding approaches and practical considerations for each.

6.15.1 Bounding Topologies

There are two bounding topologies:

- Topology A – Coordination of self-contained autonomous medical subsystems (SCSubs)
- Topology B – Federated components with centralized control

Many hybrids of Typology A and Typology B are possible. For purposes here, the discussion considers only these two bounding cases.

6.15.1.1 Topology A: Description

Figure 6-8 shows a notional MDIRA-conformant autonomous medical system assembled from three SCSubs. The figure identifies controllers with a "C" in a yellow box, a sensor with an "S" in a blue box, and an actuator with an "A" in a red box. An integrated controller/actuator, shown for example as the joined C_5 and A_2 boxes, indicates a medical device with a local controller (e.g., an infusion pump). Notionally, the SCSubs are products respectively developed and marketed by different medical system manufacturers. Each may be approved for several intended uses, including use in the configuration shown here. (Note that any reference to the approval process is notional. As regulatory organizations like the FDA provide updates to guidelines regarding approval requirements for autonomous medical systems, that information will be reflected in future updates of this implementation guidance.) In this topology, each SCSub has a MDIRA-conformant interface to the network that allows it to communicate with other components.

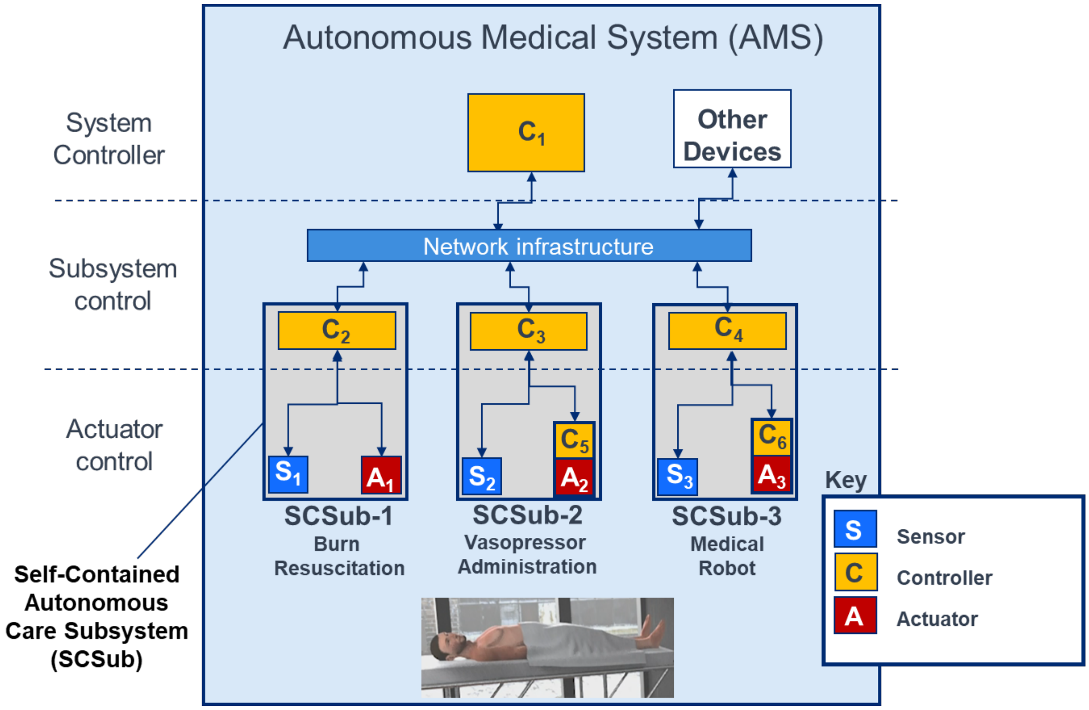


Figure 6-8 Coordination of Self-Contained Autonomous Medical Subsystems

6.15.1.2 Topology B: Description

Figure 6-9 shows an alternative architecture consisting of individual medical devices (sensors, actuators, etc.) and a central controller. The three autonomous care operations (ACOs) are functionality equivalent to the functions performed by the SCSubs in the approach depicted in Figure 6-8. Note the absence of S_1 in this figure. This architecture has the flexibility for a single sensor, S_2, to support both ACO-1 and ACO-2. Note also that actuator A_1 is controlled directly from the system controller rather than through an actuator controller.

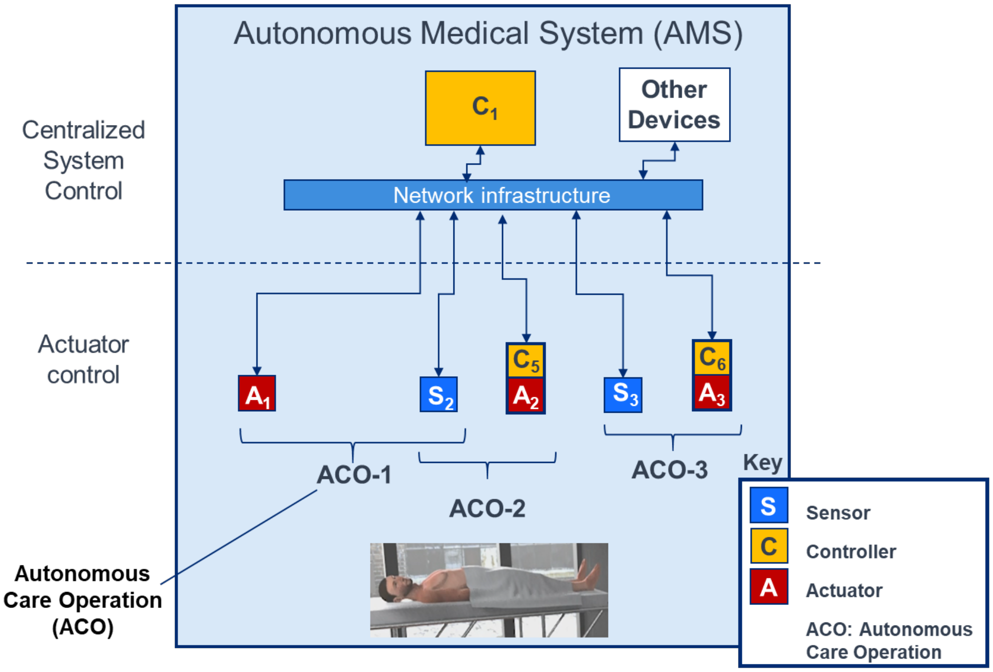

Autonomous Medical System (AMS)
C1
Other Devices
Centralized System Control
Network infrastructure
Actuator control
A1
S2
C5
A2
S3
C6
A3
ACO-1
ACO-2
ACO-3
Autonomous Care Operation (ACO)
Key
S Sensor
C Controller
A Actuator
ACO: Autonomous Care Operation

Figure 6-9 Federated Components with Centralized Control

6.15.2 Control Hierarchy

6.15.2.1 Topology A: Control Hierarchy

Figure 6-8 shows three levels of control: actuator control at the lowest level, SCSub control at the middle level, and system control at the highest level. The SCSub controllers, respectively, handle the control of the individual therapies. The form of the SCSub control may vary depending on whether the controller is directly commanding an actuator or commanding another controller at the actuator level. The former would involve relatively high-frequency servo commands sent to the actuator. The latter would be similar to actively adjusting an infusion pump by periodically changing the flow rate settings. Because each controller in a SCSub may not be aware of the other components in the system and how these may affect a patient, the system controller monitors everything that is happening in the system and with the patient, and it intervenes with the SCSubs when necessary based on predetermined protocols or a decision algorithm. Conceptually, system control, perhaps a function of the PCM described in Section 5.1.6, manifests as episodic actions as required.

6.15.2.2 Topology B: Control Hierarchy

The centralized system controller in this approach coherently controls the three ACOs. The design sophistication of the control algorithm could vary depending on the system requirements. For example, for tightly coupled (highly dependent) ACOs with stringent time response and performance requirements, the controller algorithm may have nested control loops. For less demanding applications, the design may be the virtual equivalent of the approach shown in Figure 6-8—separate control functions for each ACO with oversight from an episodic coordination function.

Conceptually, a fully integrated central controller would have performance advantages compared to the control architecture of Topology A, assuming there no other performance-limiting factors (such as latency in data communications). Even so, many autonomous care applications like closed-loop delivery of intravenous fluids and medications, where the required response times are on the order of seconds and minutes, do not have demanding control requirements. It is important that these design decisions be grounded with a thorough understanding of the system's clinical requirements, rigorous control system analysis and risk analysis.

6.15.3 Modularity

The topologies depicted in Figure 6-8 and Figure 6-9 are modular but at different levels of aggregation: Typology A is modular at the SCSub level, and Typology B is modular at the device component level. This presents the question: Which level of modularity is best?

Autonomous medical systems are only recently transitioning from research laboratories to early practical use. There is still much to learn regarding the development, marketing, procurement, end-use approval, and life-cycle support of these systems and the question regarding "appropriate" modularity factors into these considerations. No single decision regarding modularity applies universally to all applications, but one can make some broad observations.

6.15.3.1 Topology A: Modularity

Envision vendors who develop SCSubs commensurate with their expertise in a medical treatment or technology domain. An SCSub module can be marketed as a standalone medical system, or as illustrated in Figure 6-8, be procured and used by a system integrator as part of a larger system.

An advantage of this notional concept is that each SCSub module may undergo considerable V&V testing to obtain end-user regulatory approval. Furthermore, customer experience in using these modules in various ways potentially provides plentiful data supporting performance and reliability upgrades. When the required coordination (from a system-level controller) is not overly complex, or when the control requirements are not demanding from a performance perspective, V&V of the system as a whole (for regulatory approval) may be relatively efficient.

One potential disadvantage of this concept is that the system integrator may have limited insight to the design of the SCSub modules, and the modules may either lack features the integrator desires or have features that the integrator does not need. In addition, between the SCSub modules there may be redundant capabilities. Suppose SCSub-1 and SCSub-2 in Figure 6-8 both require monitoring of patient vitals, respectively represented by S_1 and S_2. Obviously, having two multi-parameter vital signs monitors, and redundant vital sign sensors on the patient, is an unacceptable complication. To avoid this, MDIRA-conformant SCSubs should be capable of exporting data from their internal sensors for other SCSubs to potentially use, and a SCSub should have the option to use sensor data from an external source.

6.15.3.2 Typology B: Modularity

Envision here system developers who procure and integrate individual components into multi-treatment MDIRA-conformant autonomous medical systems. In the furthest extreme, the sensors, actuators, and controller software components may be the basic building blocks. For example, rather than purchasing a standalone infusion pump packaged in a chassis with keypad controls and user displays, the system developer may purchase a pump, the servo electronics, an interface board, and a control software application.

The advantage here is flexibility. The system integrator can use only the components necessary to meet the operational requirements without procuring unwanted features. There are also potential advantages in system usability, size/form factor, and patient safety (e.g., multiple user displays consolidated to a well-designed few). As mentioned previously, this typology also provides flexibility for the developer to implement sophisticated control designs if needed for particular autonomous care applications.

There are potential challenges. System developers may need to acquire and maintain broad clinical and engineering expertise to build these systems. The need to test low-level basic functions may also make V&V testing more challenging and time-consuming. Notionally, in Topology A, the respective SCSub manufacturers may validate some of these lower-level functions, thereby alleviating burden from system integrators.

Lastly, a manufacturer may market the entire autonomous medical system depicted in Figure 6-9 as a MDIRA-conformant SCSub that could function standalone or be a building block for a larger system. As the system becomes larger and increasingly complex, however, the number of potential customers may decrease. Design decisions regarding modularity should factor into a manufacturers's long term business strategy.

7. MDIRA CONFORMANCE

7.1 Meaning of Conformance in a MDIRA Context

The term *conformant* used herein means that a system implementation satisfies requirements essential to its fundamental purpose as determined by the key stakeholders (e.g., customers, users, or industry and government entities). A system may have thousands of system engineering requirements and derived specifications, but typically the focus of conformance is requirements at the operational, system, and architectural (e.g., physical, functional, information exchange) levels. The customer of a system often requires the manufacturer to perform V&V activities to confirm that the system is implemented correctly (verification) and that the implementation is conformant to the operational and system requirements (validation).

For advanced POC medical systems, MDIRA defines high-level requirements that supplement the systems engineering described previously (see Figure 2-2). MDIRA-conformant in part means that an implemented system satisfies the MDIRA requirements. In addition, however, the system must also conform to the underlying interoperability standards (e.g., IEEE 11073-10101 Nomenclature) and profiles (see key definitions in Section 2.4) that enable manufacturers to build interoperable implementations. For example, profiles might eventually be available for MDIRA-conformant implementations based on the web-services communication architecture. There may also be different profiles for implementation based on the pub/sub communication paradigm.

Therefore, although the following subsections address conformance to groups of MDIRA requirements, this implies an implementation that also conforms to a prescribed set of standards and profiles that cannot be specified at this time. In subsequent MDIRA updates, this section may include more details as the standards and profiles underlying MDIRA advance and mature.

7.2 MDIRA Conformance Requirements

A MDIRA-conformant system or component implementation ***SHALL*** satisfy the mandatory requirements (i.e., SHALL statements) specified in Section 5. A system or component manufacturer ***SHALL*** prepare a high-level description of the various aspects of their implementation that satisfies each of the mandatory requirements, as well as describe the conformance verification activities already conducted (e.g., tests, analyses, inspections, demonstrations) and the data they can produce to substantiate their conformance assertions. It is recognized that given the operational requirements of a particular system or component implementation, some of the MDIRA requirements may not apply. For example, if a system has no interfaces to external entities, the mandatory requirements pertaining to external interfaces in Section 5.1.7 would not apply. As part of the conformance documentation just mentioned, the manufacturer ***SHALL*** identify and give rationale for all MDIRA requirements that do not apply to their system or component.

A manufacturer ***SHALL*** also prepare documentation for recommended (optional) requirements (i.e., SHOULD statements) from Section 5 that they have implemented in a system or component. The documentation requirement is the same as for the mandatory requirements described previously. Specifically, for each MDIRA-recommended requirement implemented, the manufacturer ***SHALL*** describe aspects of that implementation as well as the conformance verification activities they have performed. Note that a manufacturer's decision to implement or not implement recommended requirements will have no bearing on a MDIRA-conformance accreditation; however, the descriptive documentation just mentioned is required for accreditation. The intent is to have complete documentation regarding the MDIRA features and capabilities that the manufacturer has implemented.

Section 7.3 provides additional requirements regarding the organization of the manufacturer's submittal of mandatory documentation.

7.3 Organization of Conformance Data Submittals

Table 7-1 shows mandatory MDIRA system and component requirements grouped into 11 MDIRA-characteristic features. Accordingly, the manufacturer ***SHALL*** provide 11 documentation modules corresponding to each of these features. Each module ***SHALL*** describe implementation particulars and verification activities performed (see Section 7.2) for each requirement associated with a feature. Note that in Table 7-1, several system-level requirements do not decompose to requirements for specific components for the following reasons:

- Some are non-functional requirements (e.g., system attributes, stipulation for use of approved security design practices, etc.)
- Some will apply to all components (e.g., use of standard nomenclature)
- Some can be implemented using various methods; hence, the allocation to lower-level components is left to the manufacturer's discretion

Table 7-2 shows similar groupings of recommended (optional) MDIRA requirements to MDIRA-characteristic features. Note that some of the features in Table 7-1 are not included in Table 7-2 because those features do not include any optional requirements. The manufacturer ***SHALL*** provide a documentation module for each feature in Table 7-2 that includes a MDIRA-recommended requirement they have implemented. For example, if the only recommended requirement implemented is an external interface to an EHR system (RR-005.1 in Section 5.1.8), they would only need to provide one module corresponding to Feature 2 (standard external interface) that describes their implementation and conformance verification activities relating to the EHR interface. Note that Table 7-2 contains several system requirements that are mandatory (i.e. MR-100 and MR-81) but trace to component-level recommended requirements. These mandatory requirements are included here to preserve the association between the system- and component-level requirements.

Table 7-1 Mandatory MDIRA Requirements Mapped to MDIRA Characteristic Features

No.	MDIRA Characteristic Features	System	Supervisor	Component	Data Logger	User Manager
1	Information and system security	25.0	Non-functional system requirement			
		26.0	Non-functional system requirement			
		27.0	–	–	–	71.0, 72.0
2	Standard external interfaces	3.0	Allocation TBD by designer			
3	Standard nomenclature(s) and information model(s)	31.1	Applies to All			
		31.2	Applies to All			
		86.0	Applies to All			
		87.0	Applies to All			
		32.1	Applies to All			
		88.0	Applies to All			
4	Component authentication, registration, and PnP	2.0	35.1, 35.2, 36.1	54.1, 56.1		
		8.1	89.0	53.0		
		20.0	35.3	55.1, 92.0		
5	Component data exchange and time synchronization	1.1		66.0		
		1.2	Non-functional system requirement			
		16.0	Applies to All			
		19.0	33.0, 33.1	57.0, 58.0		
		19.1	Applies to All			
6	Manage patient care episodes	11.0	40.1, 40.2, 14.1, 14.2	–	–	–
7	Manage patient and context information	12.1	Allocation TBD by designer			
		12.2	Allocation TBD by designer			
		13.1	Allocation TBD by designer			
		83.0	Allocation TBD by designer			
		84.0	Allocation TBD by designer			
		85.0	Allocation TBD by designer			
8	System monitoring, fault handling, and patient safety support	101.0	34.0, 41.0, 42.0, 43.0, 46.0	62.0, 67.1		
		9.1	44.1	–	–	–
		28.1	Non-functional system requirement			
		100.0	37.0	–	–	–
		30.1		61.1		
9	Trusted control	21.0	38.1, 38.2, 38.3	93.0	–	–
10	Data logging	81.0	90.0	94.0, 95.0, 96.0	75.1, 76.0	94.0, 95.0, 96.0, 102.0
11	Patient care management – Optional	–	91.0	–	–	–

Table 7-2 Recommended MDIRA Requirements Mapped to MDIRA Characteristic Features

No.	MDIRA Characteristic Features	System	Supervisor	Component	Data Logger	User Manager
2	Standard external interfaces	4.0	Allocation TBD by designer			
		5.1	Allocation TBD by designer			
		5.2	Allocation TBD by designer			
		6.1	Allocation TBD by designer			
		18.1	Allocation TBD by designer			
		7.1	Allocation TBD by designer			
7	Manage patient and context information	15.1	Allocation TBD by designer			
8	System monitoring, fault handling, and patient safety support	100.0[1]	39.1	–	–	–
		30.2	44.2	–	–	–
10	Data logging	81.0[1]	99.0	97.0, 98.0		97.0, 98.0
11	Patient care management – Optional	82.0	50.1	–	–	–
12	User management	80.0	–	–	–	68.0, 69.0, 70.0, 73.0, 74.0

7.4 MDIRA Conformance Review and Certification

The conformance documentation described in Section 7.3 anticipates that customers of advance POC systems and components may include requirements for MDIRA conformance in their procurement contracts. Note that although Section 7.3 does not require the manufacturers to provide the evidence artifacts from MDIRA conformance verification activities, manufacturers should expect that customers may request (perhaps contractually) to receive, review, and verify them.

In the future, customers may have the option to require from a manufacturer a formal MDIRA-conformance certification. This may involve, for example, independent reviewers examining data from the manufacturer’s conformance verification activities and determining whether there is sufficient evidence that the system conforms to MDIRA and the relevant underlying standards and profiles. In addition, there may be integration exercises involving functional tests of manufacturer systems and components with industry-approved MDIRA Reference Implementations. Lastly, there may be openly available MDIRA Reference Implementations that manufacturers can acquire to support their in-house development and test activities.

[1] Indicates a mandatory system requirement that decomposes to recommended component requirements.

8. REFERENCES

[1] IEEE 11073-10101-2019, Standard for Health Informatics – Point-of-Care medical device communication – Part 10101: Nomenclature, 13 June 2019 (update to ISO/IEEE 11073-10101:2004)

[2] IEEE 11073-10201-2020, Standard for Health Informatics – Point-of-Care medical device communication – Part 10201: Domain Information Model, 10 June 2019

[3] ASTM F2761-09, Medical Devices and Medical Systems – Essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE), Part 1: General requirements and conceptual model, 2009 (https://www.astm.org/Standards/F2761.htm)

[4] Design Considerations and Pre-Market Submission Recommendations for Interoperable Medical Devices, Guidance for Industry and Food and Drug Administration (FDA) Staff, September 2017 (https://www.fda.gov/regulatory-information/search-fda-guidance-documents/design-considerations-and-pre-market-submission-recommendations-interoperable-medical-devices)

[5] ANSI/AAMI 2700-1:2019, Medical Devices and Medical Systems – Essential safety and performance requirements for equipment comprising the patient-centric integrated clinical environment (ICE), Part 1: General requirements and conceptual model, 2019

[6] Open Source Integrated Clinical Environment (OpenICE), Massachusetts General Hospital Medical Device Plug-and-Play Interoperability Program website, 2015 (https://www.openice.info/)

[7] DocBox website, 2021 (http://www.docboxmed.com/)

[8] W. Buschke, A. Loose, and S. Schlichting, "An Innovative Web Services-Based Architecture for Distributed Systems of Medical Devices, Dräger, 2015 (https://www.draeger.com/library/content/interoperability-whitepaper-wp-9069254-en-us.pdf)

[9] "Standards Spotlight: A Fresh Start for Medical Device Interoperability," *AAMI News*, October 2019 (https://www.aami.org/productspublications/articledetail.aspx?ItemNumber=10413)

[10] "AAMI and UL Publish Joint Safety Standard for Medical Device Interoperability, AAMI/UL 2800-1," AAMI and Underwriters Laboratories, Inc. (UL), 25 February 2019 (https://www.aami.org/productspublications/pressreleasedetail.aspx?ItemNumber=7436)

[11] "Architecture Framework for Unmanned Systems (AFUS)," Aerospace Standard AIR5665B, 23 August 2018 (https://saemobilus.sae.org/content/AIR5665B)

[12] "Autonomous Ground Vehicle Reference Architecture (AGVRA): Concept Definition, Appendix A," U.S. Army Tank-Automotive Research Development and Engineering Center (TARDEC) Report, 16 April 2018

[13] M. Kozlowski, M. Hinton, and M. Johannes, "Toward a Common Architecture for the Advanced Explosive Ordnance Disposal Robotic Systems (AEODRS) Family of Unmanned Ground Vehicles," NDIA Ground Vehicle Systems Engineering and Technology Symposium, Vehicle Electronics and Architecture (VEA) Mini-Symposium, Dearborn, MI, 17–19 August 2010

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

[15] FDA/AAMI Summit on "Medical Device Interoperability," AAMI, 30 March 2012 (https://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/Summits/Interoperability/MDI_1203.pdf)

[16] "Software as a Medical Device (SaMD), U.S. Food and Drug Administration (FDA) 31 August 2018 (https://www.fda.gov/medical-devices/digital-health/software-medical-device-samd)

[17] ISO 14971:2007, Medical devices – Application of risk management to medical devices; Edition 2, March 2007

[18] IEEE 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, 21 February 2018

[19] IEEE 11073-20601-2016, Standard-based communications protocol for personal health device, 2016

[20] "Architect's Introduction," HL7 FHIR Release 4, 1 November 2019 (https://www.hl7.org/fhir/overview-arch.html)

[21] "Web Services Glossary," W3C Working Group, 2004 (https://www.w3.org/TR/ws-gloss/)

[22] IEEE 11073-20702:2018, Standard for Health Informatics – Point-of-Care Medical Device Communication – Part 20702: Medical devices communications profile for web services, 19 September 2018

[23] "Data Distribution Service Version 1.4," Object Management Group (OMG), April 2015 (https://www.omg.org/spec/DDS/1.4/PDF)

[24] T. McBride, M. Ekstrom, L. Lusty, J. Sexton, and A. Townsend, "Data Integrity NIST SP 1800-11 Practice Guide," National Cybersecurity Center of Excellence (NCCoE), National Institute of Standards and Technology, U.S. Department of Commerce, 2017 (https://www.nccoe.nist.gov/library/data-integrity-nist-sp-1800-11-practice-guide)

[25] NIST SP 800-111, “Guide to Storage Encryption Technologies for End User Devices,” November 2007 (https://doi.org/10.6028/NIST.SP.800-111)

[26] NIST SP 800-63B, “Digital Identity Guidelines, Authentication and Lifecycle Management,” June 2017 (https://doi.org/10.6028/NIST.SP.800-63b)

[27] NIST Interagency Report 7316, “Assessment of Access Control Systems,” September 2006 (https://doi.org/10.6028/NIST.IR.7316)

[28] D. Mills, J. Martin, J. Burbank, and W. Kasch, “Network Time Protocol Version 4: Protocol and Algorithms Specification,” RFC 5905, Internet Engineering Task Force, June 2010 (https://www.rfc-editor.org/rfc/rfc5905.txt)

[29] IEEE 1588-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, 24 July 2008 (https://standards.ieee.org/standard/1588-2008.html)

[30] “Is The Product A Medical Device?”, U.S. FDA, 22 March 2018 (https://www.fda.gov/medical-devices/classify-your-medical-device/product-medical-device)

[31] IEEE 610-1990, “IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries,” 18 January 1991 (https://standards.ieee.org/findstds/standard/610-1990.html)

[32] “Medical Device Interoperability,” U.S. FDA, 27 September 2018 (https://www.fda.gov/medical-devices/digital-health/medical-device-interoperability)

[33] “Department of Defense Open Systems Architecture: Contract Guidebook for Program Managers V.1.1,” June 2013

[34] Definition of open system architecture, Business Directory website, 2019 (http://www.businessdictionary.com/definition/open-system-architecture.html)

[35] IEC 60601-1-18:2021, Medical electrical equipment – Part 1-8: General requirements for basic safety and essential performance – Collateral standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems, January 2021

[36] AAMI TIR 71:2017, “Guidance for logging of alarm system data,” 11 August 2017

[37] AAMI TIR 66:2017, “Guidance for the creation of physiologic data and waveform databases to demonstrate reasonable assurance of the safety and effectiveness of alarm system algorithms,” 28 February 2017

[38] “A Siren Call for Action: Priority Issues from the Medical Device Alarms Summit,” AAMI, 2011 (http://kami.camp9.org/Resources/Pictures/2011%20Alarms%20Summit%20Report.pdf)

[39] J. M. Goldman and F. A. Robertson, "Pulse-OX Tone Conveys Vital Information," *APSF Newsletter*, Vol. 19, No. 4, Summer 2004 (https://www.apsf.org/article/pulse-ox-tone-conveys-vital-information/)

[40] S. Weininger, M. B. Jaffe, T. Rausch, and J. M. Goldman, "Capturing Essential Information to Achieve Safe Interoperability," *Anesthesia & Analgesia*, Vol. 124, Issue 1, pp. 83–94, January 2017 (https://journals.lww.com/anesthesia-analgesia/pages/articleviewer.aspx?year=2017&issue=01000&article=00014&type=Fulltext)

[41] S. Weininger, M. B. Jaffe, M. Robkin, T. Rausch, D. Arney, and J. M. Goldman, "The Importance of State and Context in Safe Interoperable Medical Systems," *IEEE Journal of Translational Engineering in Health and Medicine*, Vol. 4, Article 2800110, 8 August 2016 (https://ieeexplore.ieee.org/document/7536138?arnumber=7536138)

[42] S. Dain, "Normal accidents: human error and medical equipment design," *The Heart Surgery Forum*, Vol. 5, No. 3, pp. 254–257, February 2002 (https://pubmed.ncbi.nlm.nih.gov/12538141/)

APPENDIX A. SysML DIAGRAMS

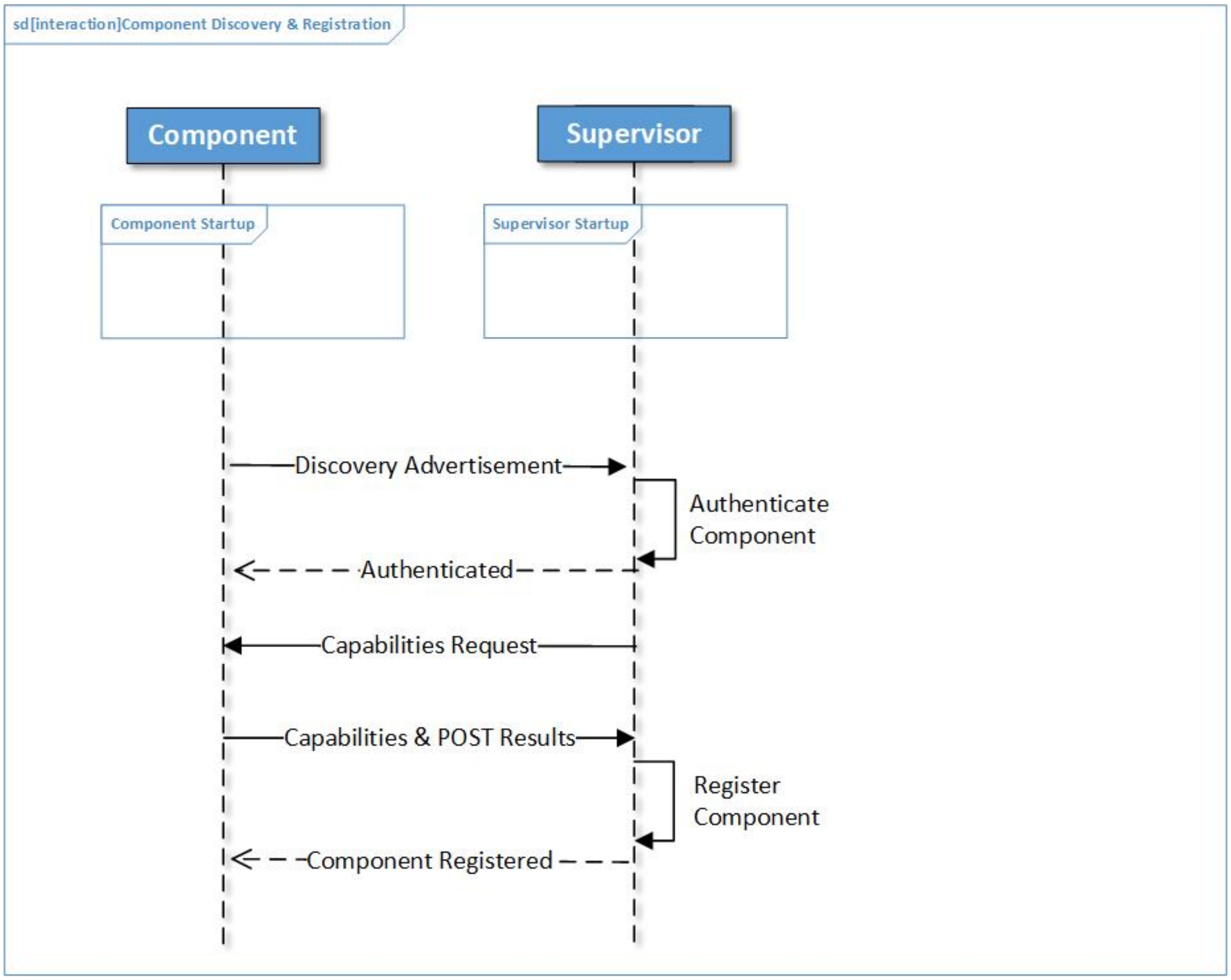


Figure A-1 Component Discovery, Authentication, and Registration

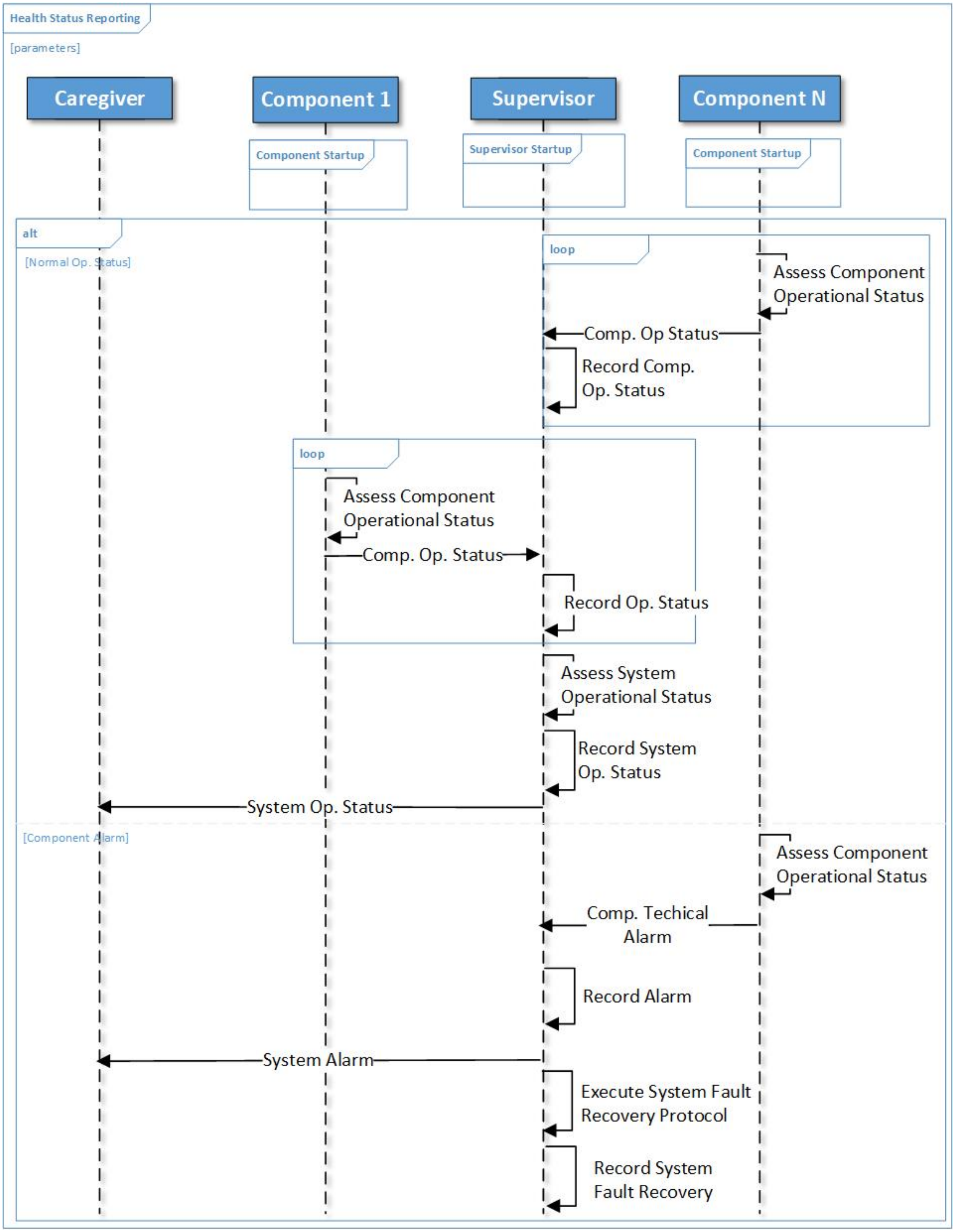


Figure A-2 System Health and Status Reporting

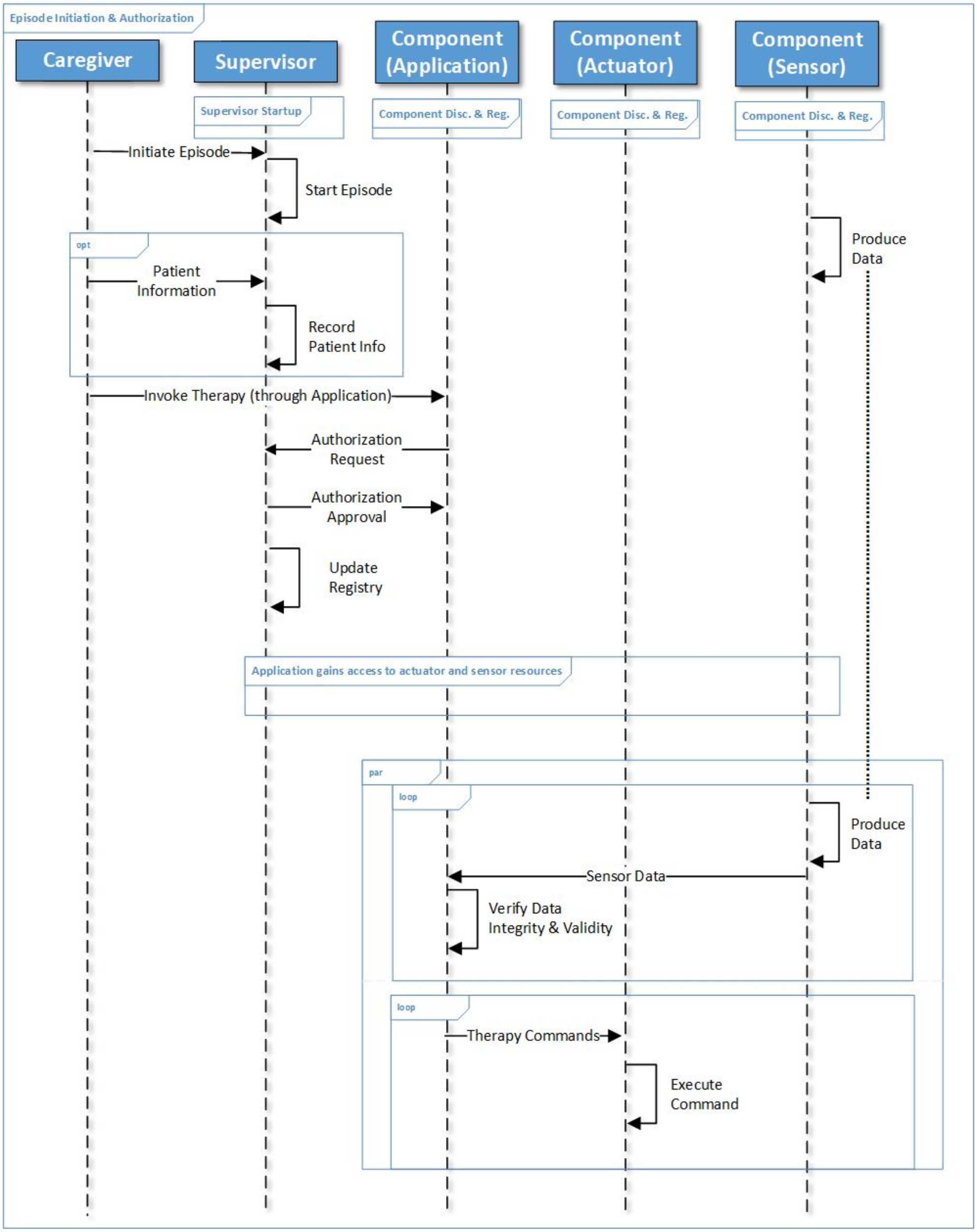


Figure A-3 Episode Initiation and Request Authorization

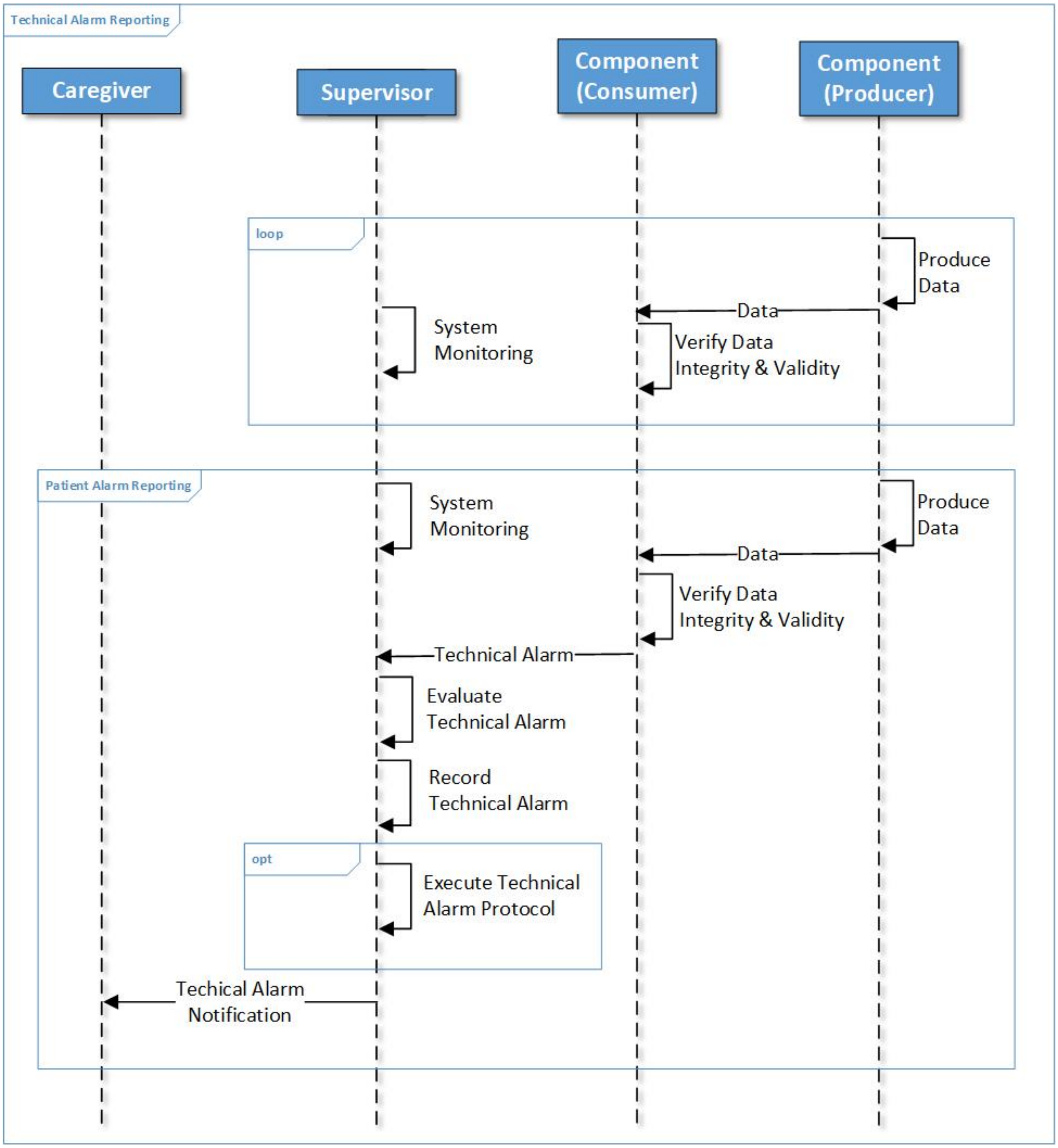


Figure A-4 Technical Alarm Reporting

APPENDIX B. GLOSSARY

Term	Definition
Applied Part	Part of a medical electrical device that in normal use necessarily comes into physical contact with the patient for the medical electrical device or a medical electrical system to perform its function (Reference [14]). Example: A blood pressure cuff
Authentication	The process of verifying the identity of users, devices, and processes within a system. Correctly identifying these entities is a key part of implementing robust access control, a security measure. In context of MDIRA, the term *authentication* is used in reference to validating the credentials of a component that is connected into the communications architecture of a MDIRA-conformant medical care system.
Authorization	Authorization provides the access rights to resources for users, components, and processes by defining access policies imposed throughout the system. In MDIRA, the term *authorization* is used extensively in reference to granting permissible for a component in a MDIRA-conformant system to interact in a particular manner with another component. For example, MDIRA prescribes that a supervisory function must authorize a component before it can control the operations of another component.
Autonomy	(1) Capacity to monitor, select, and execute a clinical function with no or limited operation intervention (Reference [14]). (2) An unmanned system's own ability of sensing, perceiving, analyzing, communicating, planning, decision-making, and acting or executing to achieve its goals as assigned by its human operator(s) through designed human-computer interaction or assigned by another system with which the unmanned systems interacts (Reference [11], Section 4.1.4). Autonomy in a system can vary in degrees or levels ranging from technology assistance to fully autonomous. (See Section 2.5 in this report.)
Degree of Autonomy	Taxonomy based on the properties and capabilities of the medical electrical device or a medical electrical system related to autonomy (Reference [14], Section 3.7). The following are assumed to apply: • Degree of autonomy can vary from low to high. • Degree of autonomy can be classified at different levels (e.g., task level, function level, MEE or MES level) depending on where and how it is implemented in the MEE or MED. (Reference [14], Section 4.1)
Device Model	An abstract model that represents those capabilities and characteristics of a device that can be accessed and operated externally in a particular context of use, typically including data types, relationships, and nomenclature used for input and output of observations and controls (Reference [15]). AAMI 2700-1 (Reference [5]) provides insightful elaboration.
Information Model	A representation of concepts and the relationships, constraints, rules, and *operations* to specify *data semantics* for a chosen domain. An information model provides a sharable, stable, and organized structure of information requirements for the domain context.
Integrated Clinical Environment (ICE)	Environment that combines heterogeneous medical devices and other equipment to create a medical system for the care of a single, high-acuity patient (Reference [5]).

Term	Definition
MDIRA-conformant system	An ICE that complies with MDIRA. MDIRA's use of the term 'system' refers to a MDIRA-conformant system.
MDIRA-conformant component	Parts of a MDIRA-conformant system that may include medical or non-medical devices, medical and non-medical software applications, system management components, and other support equipment. Section 4.4 describes the functional components of a system.
Medical Device	Any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material, or other similar or related article intended by the **manufacturer** to be used, alone or in combination, for human beings for one or more of the following specific purpose(s): • Diagnosis, prevention, monitoring, treatment or alleviation of disease • Diagnosis, monitoring, treatment, alleviation of or compensation for an injury • Investigation, replacement, modification, or support of the anatomy or of a physiological process, supporting or sustaining life • Control of conception • Disinfection of medical devices • Providing information for medical purposes by means of in vitro examination of specimens derived from the human body and which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which can be assisted in its function by such means (Reference [30]). Example: A medical device can be medical electrical equipment
Medical Device Interoperability	(1) The ability of two or more systems or components to exchange information and to use the information that has been exchanged (Reference [31]). (2) The ability of medical devices, clinical systems, or their components to communicate with each other in order to safely fulfill an intended purpose (Reference [15]). (3) The ability to safely, securely, and effectively exchange and use information among one or more devices, products, technologies, or systems. This exchanged information can be used in a variety of ways including display, store, interpret, analyze, and automatically act on or control another product (Reference [32]).
Medical Device Interoperability Reference Architecture (MDIRA)	Architectural requirements and implementation guidelines that direct developers in designing medical systems consisting of interoperable medical devices, clinical decision capabilities, and other supporting technologies (i.e., robotic systems) with particular emphasis on realizing autonomous operations, open architecture (OA) using industry accepted standards, and system and data security. MDIRA is an overarching specification that supplements the operational, system, and architectural requirements that system developers derive based on user needs. It establishes a basis for developing systems that possess essential industry-consensus characteristics.
Medical Electrical Equipment (MEE)	Electrical equipment having an applied part or transferring energy to or from the patient or detecting such energy transfer to or from the patient for the purpose of diagnosis, treatment, or monitoring of the patient (adapted from Reference [14]).

Term	Definition
Medical Electrical System (MES)	Combination, as specified by its manufacturer, of items of equipment, at least one of which is medical electrical equipment to be interconnected by functional connection or by use of a multiple-socket outlet (Reference [14]). Example: Multi-parameter patient vital signs monitor
Medical Robot	Robot intended to be used as medical electrical equipment or medical electrical system (Reference [14]).
Nomenclature	A data item's numeric code communicated between systems as well as the corresponding definition.
Open Architecture (OA) or Open System	(1) One subsystem can be replaced with minimal impact on the other as long as the replacement meets the OA specifications. In the most successful OA applications, exchanging one subsystem for another has no integration impact. The full or partial OA implementation has the potential to ease integration workload and costs associated with upgrading a system. Consequently, individual subsystems can be enhanced on a more frequent basis, enabling managed obsolescence and new capability insertion (Reference [33]). (2) A technical architecture that adopts open standards supporting a modular, loosely coupled, and highly cohesive system structure that includes publishing key interfaces within the system and full design disclosure (Reference [33]). (3) Vendor-independent, nonproprietary, computer system or device design based on official and/or popular standards. It allows all vendors (in competition with one another) to create add-on products that increase a system's (or device's) flexibility, functionality, interoperability, potential use, and useful life (Reference [34]).
Open-Source Code	Refers to computer source code that the developer makes publicly available. Open-source developers typically use Internet websites like GitHub to post their code for others to access. Note that use of publicly available source code can be challenging because many developers provide only minimal explanatory comments embedded in the code or other support documentation. The robustness of configuration management process for open source can be widely variable.
Open Source	In the public domain
Plug-and-Play (PnP)	(1) Ability of medical devices, clinical systems, or their components to communicate to safely fulfill a manufacturer's intended purpose without custom integration or development (Reference [15]). (2) Seamless connection and disconnection ("hot swapping") of medical devices without having to shut down and reboot the medical devices or the system the devices are connected to (Reference [5]). Note that definition (1) describes to an open system, whereas definition (2) achieves the furthest realization of OA similar to what has been achieved in the computer and telecommunications industries.
Profile	Specification showing in detail how to apply existing standards by restricting or constraining requirements in the referenced standards (Reference [15])
Robot	Programmed actuated mechanism with a degree of autonomy, operating within its environment, to perform intended tasks.
Reference Architecture	A template that guides the development of a particular system type so that systems built using this template possess attributes deemed important by the stakeholder community associated with those systems.

Term	Definition
Reference Implementation	An implementation of a specification that is to be used as a definitive interpretation for that specification.
Registration	The process of making authenticated components in a MDIRA-conformant system available to support the system's medical operations. For example, MDIRA requires a component to perform a successful POST as prerequisite to it being registered.
Software as a Medical Device (SaMD)	Software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device (Reference [16]). Note that a MDIRA-conformant system may also include medical software applications that do not meet the formal SaMD definition in the references.
Standard	Document established by consensus and approved by a recognized body that provides for common and repeated use, rules, guidelines, or characteristics for activities or their results. A standard aims to achieve the optimum degree of order in a given context. Standards are (Reference [15]): • Shaped by consensus • Typically developed in an open and transparent process, with representation of all interested and engaged parties • Primarily market-driven (industry-sponsored)

APPENDIX C. OPERATIONAL SCENARIO EXAMPLE

Operational Domain: Combat Operations

Summary:

- Caregivers: Single medic with several helpers
- Two patients: A severe burn victim and a traumatic brain injury (TBI) patient
- Equipment: MDIRA-conformant prolonged care kits each including:
  - IT equipment with MDIRA-conformant components and software applications to establish a MDIRA-conformant ICE for each patient
  - A mobile device that enables the caregiver to track status and receive alerts from the multiple ICEs (i.e., from multiple patients)
  - MDIRA-conformant ICE that can be configured to meet each patient's unique medical needs

  For brevity, the MDIRA-conformant systems configured from the kits for the two patients are called ICE1 and ICE2, respectively.
- Medical supplies: The medic has sufficient medical expendables (e.g., blood and fluids) for several hours of medical treatment for the patients and the ability to resupply as required.
- Communications: Adequate to request evacuation, resupply, and conduct a virtual care consultation.
- Benefits of the ICE in this scenario:
  - Autonomous medical treatments (fluid resuscitation, vasopressor administration, and ventilator management) permit the medic to leave the burn patient's side to care for the other patient.
  - Provides continuous status tracking of multiple patients with a limited number of personnel and skills.
  - Alerts caregivers to changes in patients' status that may require immediate attention.
  - Enables consult with and transfer of data to a remote medical specialist.
  - Enables continuity of care when transitioning care teams.

Narrative

An improvised explosive device detonates beneath a Humvee. Personnel in the trailing vehicles extinguish the fire and remove the injured passengers. Patient 1 is unconscious and has extensive burns. Patient 2 is conscious and able to extract himself from the vehicle. He sustained some head trauma but shows no indications of other injuries and reports no pain. There is no external bleeding from either patient.

A medic arrives and assesses patient 1 for breathing and pulse. The medic assesses the extent of patient 1's burns and determines he has second- and third-degree burns on about 15% to 20% of his body. She connects him to a multi-parameter patient monitor that is part of ICE1, which includes an autonomous monitoring application. The medic records all assessments, procedures, and intravenous (IV) fluids on the ICE1 touchscreen. The medic begins two large bore lactated Ringer's solution infusions, places a Foley catheter, and initiates a VCC consultation via an app running on ICE1. ICE1 connects to the remote site via an interface to a radio. The monitoring app alerts the medic to patient 1's low oxygen saturation (SpO_2). The medic suspects a partial airway obstruction and places a nasopharyngeal airway. The medic then administers O_2 via a nasal cannula and provides pain medication. While treating patient 1, she asks patient 2 mental-orientation questions to establish a Glasgow Coma Score (GCS).

The medic reviews and verifies patient 1's vital signs trends on ICE1 and continues to administer pain medication via IV periodically, changes IV RL bags as they empty, and records the information on the ICE touchscreen. The Tactical Combat Casualty Card assessment is recorded on the ICE1 touchscreen for patient 1.

Headquarters informs the medic that air evacuation of the patients cannot occur for 16 to 20 hours. With guidance from the VCC consultant, she sedates and intubates patient 1 for the transfer to a secure location. Within 60 minutes of the injuries, the medic and several other personnel transport the casualties and supporting medical equipment to a nearby secure location.

On arrival at the safe site, personnel carry patient 1 on a stretcher to a room. Others assist patient 2 into an adjacent room. With the aid of a helper, the medic attaches the two IV lines to pumps, connects them to ICE1, and configures them for closed-loop fluid resuscitation. The medic then wirelessly downloads the patient's history into ICE1 via radio link and manually enters further observations and treatments. ICE1 is now autonomously delivering fluids and monitoring the patient's status.

With patient 1 being treated and monitored by ICE1, the medic performs a more detailed assessment of patient 2 in the other room. Patient 2's medical condition has deteriorated; he is semi-conscious and has dilated pupils. The medic assembles ICE2, connects it to the patient, enters patient and system setup information, and activates the system for autonomous patient status monitoring. From ICE2's user screen, the medic initiates a VCC consultation. The medic reviews the patient observations, as well as data relayed from ICE2, with the VCC consultant to determine patient 2's plan of care. The VCC consultant recommends intubation of patient 2 to maintain a safe airway and walks the medic through the intubation while a VCC nurse assists the medic by monitoring patient 1. The VCC consultant remotely configures ICE2's screen to emphasize the ventilation parameters that the VCC consultant wants the medic to watch closely. The medic connects the patient to the ventilator and the ventilator to ICE2. From the ICE2 user screen, the medic activates an autonomous ventilation management app.

The medic monitors the status of both patients on a mobile device that wirelessly connects to ICE1 and ICE2 with active monitoring support from a consulting physician when communications are available. The medic continues monitoring both patients, replacing IV fluid bags, until air evacuation 20 hours later. ICE1 and ICE2 evacuate with their respective patients. ICE 1 and ICE2 provide continuity-of-care reports to the evacuation crew, and the systems continue monitoring the patients during transport. Just prior to arrival, ICE1 and ICE 2 upload continuity-of-care reports to the destination hospital via the helicopter’s radio link so the hospital can be ready with the correct equipment and personnel to receive the patients. At the hospital, ICE1 and ICE2 upload their respective data logs, each containing the full details of a patient’s care encounter, to a common data repository.

APPENDIX D. REQUIREMENTS FROM MDIRA VERSION 1.0 OMITTED IN VERSION 2.0

Number	Requirement Statement	Rationale
MR-010	A system ***SHALL*** have a capability to collect patient data and make these data available to all components that have been authorized access.	MR-001 requires exchange of data between components, which could include patient related data. No need for MR-010.
RR-017	A system ***SHOULD*** record relevant clinical data for generating reports.	A software application component within the system would perform this function, and MR-001 ensures that clinical data could get to this application. RR-017 not needed.
MR-022	All displays and user interfaces implemented in the system ***SHALL*** follow International Electrotechnical Commission (IEC) Standard 62366-1 (Reference 14[2]) providing care-givers the ability to (1) quickly and accurately assimilate the patient's medical status and the status of the system and its components, (2) quickly and reliably enter clinical data associated with the patient, and (3) execute the intended clinical workflow(s) with sufficient instructions and feedback.	More definitively stated in Version 2 is that user interfaces are outside MDIRA scope. Including MR-022 is contrary to this, and thus was removed.
MR-023	A MDIRA-compliant system *SHALL* record all entries and actions made by the User.	This is now accounted for in the new requirement MR-081 for a comprehensive data logging capability.
MR-024	A MDIRA-compliant system *SHALL* provide the record of user entries and actions to the Data Logger (see Section 5.5).	This is now accounted for in the new requirement MR-081 for a comprehensive data logging capability.
MR-029	A MDIRA-compliant system design *SHALL* include a safety analyses that prospectively identifies the system's patient safety risks as well as the safety provisions that mitigate these risks as prescribed by the patient safety governing bodies having jurisdiction over the operations of the system.	MR-028.1 requires a system risk analysis. It is expected that safety provisions prescribed by patient safety governing bodies would be part of that system risk analysis.

[2] This reference is not the Reference [14] listed in this document.

Number	Requirement Statement	Rationale
RR-045	System recover protocols ***SHOULD*** operate in conjunction with the patient safety protocol addressed in RR-050.	Patient safety protocols are allocated to a PCM component (a SaMD) that was added in Version 2. The PCM would require information from the Supervisor regarding system health and status. The PCM could notionally direct the Supervisor to take some action to keep the patient safe. See new requirements MR-091 and RR-050.1
MR-047	The Supervisor ***SHALL*** receive patient status data (including patient-related alarms) from the system components.	Allocation of this clinically related task shifted to the PCM component.
MR-048	The Supervisor ***SHALL*** routinely assess patient health status data (including patient-related alarms) from the system components.	Allocation of this clinically related task shifted to the PCM component.
MR-049	The Supervisor ***SHALL*** notify the user of changes in patient status according to a notification protocol that includes management of medically related alarms from the system components.	Allocation of this clinically related task shifted to the PCM component.
RR-051	Patient safety protocols ***SHOULD*** operate in conjunction with the system fault recovery protocol addressed in RR-044.	See rationale for RR-45.
MR-052	The Supervisor ***SHALL*** record time-correlated patient status data and safety protocols executed for status reports.	Allocation of this clinically related task shifted to the PCM component.
RR-059	A self-contained subsystem that includes internal physiological sensors ***SHOULD*** provide data from these sensors to the MDIRA information infrastructure so that other system components might benefit.	If considering a self-contained autonomous system as a *component* of the ICE, the component requirements in Section 5.3 are sufficient. What is stated here is no different than what would be needed from any other component to meet the systems operational requirements. The nuance here adds confusion.
MR-060	Each system component ***SHALL*** verify the data it is using from another source (e.g., another component) as well as the fidelity of that data.	This was conveyed better in MR-061.1.
RR-063	A component that is a self-contained subsystem ***SHOULD*** provide health and status information to the MDIRA information infrastructure that reflects the health and status of all its constituent components.	See rationale for RR-059.
MR-064	Each component of the system ***SHALL*** send a message to the Supervisor if it detects a fault in its own operations.	MR-062 requires that a component report its health and operating status, including alerts. This would account for any faults in the components.

Number	Requirement Statement	Rationale
RR-065	All data displayed to the user through a component's user interface ***SHOULD*** be made available through that component's electronic data interface for use by the system and its components.	This requirement was in response to a requirement in the draft AAMI data logger standard. Its meaning and intent is difficult to comprehend. Because the AAMI standard is referenced, it was decided to not to state the requirement explicitly in MDIRA Version 2.0.
MR-077	The Data Logger ***SHALL*** record user actions on the system and its components as made available by the Supervisor and the system components through their network interface.	This is accounted for by MR-075.1, which is a more general requirement for the Data Logger to record data provided by MDIRA-conformant components.

APPENDIX E. ALARM MANAGEMENT CONSIDERATIONS

E.1 Background

Alarm and information signals are widely used as risk control measures by medical devices to raise user awareness of conditions that may require intervention to prevent patient harm. Alarm conditions can be categorized as either physiological or technical, where the former concerns patient-related conditions (detected by monitoring the patient's physiological variables) and the latter are functional or operational issues with the device (or its components). Regardless of its category, an alarm condition implies that the patient is being potentially exposed to a hazardous situation that requires the user's awareness or response.

IEC 60601-1-8:2006 (Reference [35]) has been adopted by the healthcare industry as the de facto standard for the design and testing of alarm systems in medical systems. The requirements established in this standard cover the design (including human factors), performance, testing and verification, labeling, and disclosure aspects of alarm systems within medical devices.

Although developed for standalone medical devices, IEC 60601-1-8:2006 is also applicable to interoperable medical systems, such as MDIRA ICE-conformant systems. For example, ANSI/AAMI 2700-1 (Reference [5]) requires that an ICE-compliant system, as well as all medical devices and equipment connected to it, comply with IEC 60601-1-8:2006 (Clause 5.5). Therefore, the ("medical functions" related) alarm system in an MDIRA-conformant system shall be in accordance to ICE 60601-1-8:2006.

In addition, multiple consensus standards have been written to provide guidelines to address different aspects of alarm systems in medical devices. For example, AAMI Technical Information Report (TIR) 71:2017 (Reference [36]) discusses how alarm data should be logged, whereas AAMI TIR 66:2017 (Reference [37]) provides guidance on the creation of physiologic data and waveform databases for testing intelligent alarm algorithms. ANSI/AAMI/UL 2800-1:2019 (Reference [10]) (Annex Q, in particular) enumerates a list of specific issues to consider for alarm systems in interoperable medical systems.

These standards provide an important source of information that should be considered during the design, development, and verification of alarm systems in MDIRA-conformant systems.

E.2 Current and Optimal Status of Alarm System in Interoperable Medical Systems

The *current* priorities of developing safe and effective alarm systems in standalone medical devices, as reported in Reference [38], focus on optimizing the alarm management (including the configurations of alarm thresholds) so that the alarm system in a medical device can:

- Reduce false positive alarms and nuisance alarms so that the alarm system can serve as a trusted sentinel and advisor to clinicians.

- Enable adaptive alarm threshold settings customized for individual patients.
- Provide predictive information on patient's conditions.

Current medical devices, however, fail to take full advantage of the rich contextual information that an interoperable medical system is capable of collecting and aggregating, nor do they use the interoperability potentials to support personalized smart alarm condition management that could be tailored to each patient.

Current alarm approaches typically concern the detection and annunciation of alarm conditions at the single device level. For interoperable medical systems, there are many more factors to take into account regarding the alarm system, such as communication of alarm conditions across the system, centralized alarm management, coordinated alarm signals, and alarm conditions caused by interoperability failures. Furthermore, future alarm systems should not simply add "smart" alarms to legacy alarms, which could potentially increase alarm overload and fatigue.

MD PnP research and development on alarm systems in interoperable medical products, such as OpenICE-based systems, focuses on three areas:

- Support the communication and aggregation of alarm conditions detected by connected devices.
- Provide integrated, context-specific alarms at the system level (e.g., via an integrated alarm signal display).
- Automatically optimize alarm settings in ICE-connected devices where possible by the use of smart algorithms, sensor fusion.

A smart alarm clinical scenario using an advanced ICE-based system follows.

- Preconditions: The alarm system of the connected devices can be configured remotely by the ICE platform (e.g., via a smart alarm app).
- Scenario: A pulse oximeter (PO) is applied to a newly admitted casualty. Because the PO is being used in standalone mode, it defaults to a low saturation alarm threshold value of 85% or 90%. The PO is then connected to the ICE when it becomes available. The ICE smart PO app takes over SpO_2 monitoring to optimize tracking of SpO_2 while minimizing false and nuisance alarms. The smart PO app automatically adjusts the PO low SpO_2 alarm to 70% to serve as a safeguard in detecting clinically hazardous low SpO_2 in case of a failure of the smart PO app and to enable the PO manufacturer to continue to provide a core risk-management function (Reference [39]).

In addition, more intelligent alarm algorithms (i.e., apps) can be developed that leverage the context information gathered by the system to derive alarm conditions that no single device is capable of detecting.

This optimal status of alarm systems requires a MDIRA-conformant ICE platform to provide technical flexibility, extensibility, and transparency to smart alarm app developers so that they can easily make use of system-wide context information and remotely configure alarm settings in connected device for better alarm detection and management.

E.3 Considerations for Alarm System in MDIRA-conformant Systems

This section elaborates a set of specific topics to be considered by the alarm system in MDIRA-conformant systems based on the following:

- MD PnP's previous research experience on medical device interoperability
- MD PnP's previous engagement and participation with alarm-related standards activities
- Lessons learned from the design and refinement of alarming capabilities in OpenICE

Note that the topics discussed next focus on the general principles (for consideration) of designing an effective alarm system to improve the safety assurance of systems. The design and testing of intelligent alarm algorithms (i.e., algorithms with complex logic for detecting or inferring specific physiological or technical alarm conditions) in systems are beyond the scope of this discussion.

E.3.1 General

A MDIRA-conformant system should include an alarm system to detect and annunciate alarm signals present in the following:

- Patient physiological monitoring systems (by aggregating the physiological measurements from connected medical devices)
- Connected medical devices and equipment
- Apps hosted in the MDIRA platform
- Infrastructure components in the system, including network infrastructure and the computing environment for hosting apps
- The coordination among devices, infrastructure components, and the system
- The alarm system itself

The alarm system should also detect and derive alarm conditions regarding its interaction with external systems.

If the alarm system uses intelligent alarm algorithms to derive physiological or technical alarm conditions (based on the information from its components and connected devices and equipment), the underlying logic and criteria of such detection should be documented and disclosed to the user.

To enable system-level alarm management (including alarm suppression), a MDIRA-conformant medical device or equipment ideally should have the following capabilities:

- Support remote configuration of the component (device-level) alarm systems by the system, including configuring alarm thresholds and enabling, pausing, or turning off local alarm annunciations.
- Allow its alarm system settings to be configured, either automatically by the system or manually by the user, prior to a patient care episode; and automatically restore to the default settings after the patient care episode.
- Revert to annunciating alarm signals locally when its connection to the system is lost or the system becomes unresponsive; and return to system-level alarming when the issue is fixed. The logic that dictates these functions should be determined by risk management for each particular scenario.
- Acknowledge the receipt of alarm conditions from the system or from other connected devices and equipment.

Design and testing of the alarm system should be an integral part of the risk management process for a system.

- Evaluate the appropriateness and effectiveness of using alarms to mitigate particular risks.
- Document and disclose to the user the set of alarm conditions that the alarm system detects and annunciates, including the criteria of determining alarm conditions.
- Evaluate, document, and disclose to the user the expected performance of the alarm system, including delay in detecting alarm conditions and false positive or negative rates. The alarm system should achieve the expected performance (demonstrated through testing).
- Create a fallback mode of the alarm system [e.g., allocate all alarming capabilities to the system (central) user interface, rather than distributing them across the system, upon a system failure].
- Identify and mitigate any new risks introduced by the alarm system (e.g., excessive suppression of alarms).

Because the alarm system may rely on the communication and coordination of connected devices and equipment to detect and communicate some alarm conditions, testing the reliability of the infrastructure components (e.g., the network infrastructure) supporting such communication and coordination should be included as part of testing of the alarm system.

E.3.2 Alarm Signal Fatigue, Alarm Inactivation, and Alarm Priority Management

Alarm fatigue refers to the situation where caregivers are overwhelmed and therefore become less effective in detecting and responding to the alarm signals generated by the medical devices in the care environment. Alarm fatigue can be expected to present a significant risk for interoperable medical systems, when numerous devices and equipment are connected to the system. Thus, the alarm system in a MDIRA-conformant system should have an alarm management mechanism to mitigate alarm fatigue risks. The design and testing of such a mechanism should be part of the system's risk management process. It also should consider the types and numbers of devices that can connect to the system as well as the types of alarms that they can produce.

An alarm management (including inactivation) mechanism, based on a defined alarm priority management scheme, should help reduce alarm signal fatigue by reconciling the priorities of (concurrent) alarm conditions from multiple sources and annunciating only the most urgent ones. This requires the MDIRA architecture and MDIRA-conformant devices and equipment to share a common alarm priority management scheme that may include the following:

- A connected device that knows how to assign priorities to its alarm in a manner consistent with other connected devices and communicate such priorities to the system. (It is anticipated that the device will be able to assign a priority to a technical alarm, but ICE-based context is required to assign priority to most clinical alarms.)

- A system with a clearly defined mechanism that could allow reconciliation of the priorities of alarms received from connected devices and ensure alarm conditions with higher urgency can be presented (annunciated or displayed) first.

It must be recognized that alarm signal inactivation can lead to new risks being introduced to the system, especially when misapplied or incorrectly configured by the user. Examples include higher-priority alarms being suppressed and all local alarms in a connected device being unintentionally inactivated. Such risks should be identified and mitigated during system-level risk management.

However, suppressed alarms should still be readily available for access by the user (e.g., an icon being displayed on the screen to indicate the presence of suppressed alarms, and further details of these alarms being available for the user).

E.3.3 Usability

The usability of the alarm system should be evaluated to demonstrate that the alarm system achieves the expected effectiveness in attracting the user's attention to alarm conditions, presenting clear information of the alarm conditions to the user, and/or guiding the user to correctly respond to alarm conditions in a timely manner. [An important capability of an ICE system is the ability to present contextual help (see https://youtu.be/afI2lPCx5_M)]. If necessary, user studies should be performed to evaluate the usability of the alarm system. Such an evaluation should cover the following:

- Form of alarm signals (e.g., visual, audio, haptic)

- Urgency alarm conditions (and/or the escalation scheme of alarm signals during alarm annunciation)

- Information accompanying alarm signals (e.g., alarm messages on the display)

- Location(s) of alarm signal (and the display of the accompanied information), either at the system's user interface, the user interfaces on connected devices and equipment, or both

- Acknowledgement, pausing, resume, in activation and termination of alarm signals that can be taken by the user

- Configuration of alarm settings that can be made by the user

- Information accompanying the system, including instruction for use, user's manual, disclosure, and labeling related to the alarm system

E.3.4 Logging

A MDIRA-conformant system should log, for forensic purposes, all alarm conditions presented to the user and alarms that have been suppressed. A particular alarm's log entry should include the origin of the alarm (i.e., the entity that detected the alarm condition), the type and nature of the alarm, and the status of the alarm (annunciated vs. suppressed). The information accompanying the alarm annunciation should also be included as part the alarm log.

AAMI TIR 71:2017 (Reference [36]) should be consulted when designing such logging capabilities.

APPENDIX F. ACRONYMS

AAMI	Association for the Advancement of Medical Instrumentation
ACO	Autonomous Care Operation
AED	Automatic External Defibrillator
AI	Artificial Intelligence
ANSI	American National Standards Institute
ASTM	American Society for Testing and Materials
BICEPS	Basic Integrated Clinical Environment Protocol Specification
CEN	European Committee for Standardization
CSF	Cerebral Spinal Fluid
DDS	Data Distribution Service
DHA	Defense Health Agency
DIM	Domain Information Model
ECG	Electrocardiograph
EHR	Electronic Health Record
EMR	Electronic Medical Record
FDA	Food and Drug Administration
FHIR	Fast Health Interoperability Resource
FSN	Fully Specified Name
GCS	Glasgow Coma Score
GPS	Global Positioning System
HL	Health Level
HTTP	Hypertext Transfer Protocol
ICE	Integrated Clinical Environment

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IHE	Integrating the Healthcare Enterprise
IP	Internet Protocol
ISO	International Standards Organization
IT	Information Technology
IV	Intravenous
JHU/APL	The Johns Hopkins University Applied Physics Laboratory
JPC	Joint Program Committee
JSON	JavaScript Object Notation
LOINC	Logical Observation Identifiers, Names, and Codes
MD PnP	Medical Device Interoperability and Cybersecurity Program
MDC	Medical Device Communications
MDIRA	Medical Device Interoperability Reference Architecture
mDNS	multicast Domain Name Server
MDPWS	Medical Device Profile for Web Services
MDS	Medical Device System
MEE	Medical Electrical Equipment
MES	Medical Electrical Systems
MIB	Management Information Blocks
MIL-SPEC	Military Specification
ML	Machine Learning
MR	Mandatory Requirement
MRDC	Medical Research and Development Command (U.S. Army)
NBP	Noninvasive Blood Pressure

NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
O_2	Oxygen
OA	Open Architecture
OASIS	Organization for the Advancement of Structured Information Standards
OMG	Open Management Group
openSDC	open Smart Device Connect
PCM	Patient Care Manager
PHD	Personal Health Device
PHI	Protected Health Information
PII	Personally Identifiable Information
PnP	Plug-and-Play
PO	Pulse Oximeter
POC	Point of Care
POST	Power-on Self-Test
PTP	Precision Time Protocol
RELMA	Regenstrief LOINC Mapping Assistant
RFC	Request for Comment
RR	Recommended Requirement
RTMMS	Rosetta Terminology Mapping Management System
SaMD	Software as a Medical Device
SCSub	Self-Contained autonomous medical Subsystem
SDC	Service-oriented Device Connectivity
SDO	Standards Development Organization
SNMP	Simple Network Management Protocol

SNOMED CT	Systematized Nomenclature of Medicine – Clinical Terms
SP	Special Publication
SPDP	Simple Participant Discovery Protocol
SSDP	Simple Service Discovery Protocol
SysML	System Modeling Language
TATRC	Telemedicine and Advanced Technology Research Center
TBI	Traumatic Brain Injury
TC	Technical Committee
TCP	Transmission Control Protocol
TIR	Technical Information Report
TLS	Transport Layer Security
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
V&V	Verification and Validation
VCC	Virtual Care Consultation
VMD	Virtual Medical Device
W3C	World Wide Web Consortium
XML	eXtensible Markup Language