Medical device interoperability standards and (high) risks mitigation and mapping for intended use

Konstantinos Makrodimitris, PhD

US FDA/DHHS

FDA DISCLAIMER

The views and opinions presented here represent those of the speaker and should not be considered to represent advice or guidance on behalf of the U.S. Food and Drug Administration.

Motivation

- Leverage interoperability standards in specific contexts/intended use
- Harmonize and standardize device interoperability risks (new or changed)
- Support transparency, consistency in evaluating device interoperability
- Help to identify interoperability risk mitigations by standards (new or buildup)

SCOPE(Risks/Whys)
(potential PAR/Project/White paper)

- Map/Categorize device interoperability risks to **specific intended use contexts**
- Create a geography of interoperability risks for **different information flows** (transmit, receive, control, power, deliver, alert etc.)
- Relate to ISO14971, IMDRF **risk categorization**, IEC62304, Major/moderate/minor level of concern
- Start with **High risk information(serious injury)** related to diagnose, treat, alert, active monitor (specific areas surgical, cardio, neuro, anesthesia etc)
- Leverage **risk mitigations** from specific standards (eg SDC, 10700)
- Map risks to **specific terminology terms/categories**(10101)
- Connect to **regulatory bodies and hospital risk management** and Relate to medical device product codes
- Guide **verification and conformance strategies** by risk based flow

OUT OF SCOPE

- CyberSecurity
- Low risk
- EHR
- Health IT admin
- MDDS
- Patient privacy
- Software architecture, development

Possible standard/map

A. Context/Intended use/Specialization/Product code
   - Surgical
   - Cardio
   - Anesthesia etc.

B. Risk category due on interoperability-LIST
   - High (treat, diagnose, alert, monitor, life sustain…)
     - Alert failure, Control malfunction, Power issue, Diagnosis algorithm input, treatment atrial defib, delay, etc.

C. Standard clause (or other mitigation?)-LIST
   - SDC
   - 10101, 10102
   - Different levels/hierarchy of mitigations(Right, clause…)

DISCUSSION

- Stakeholders
- SDC work aligned
- Terminology work aligned
- Product codes
- Specific intended use priority

APPENDIX

IMDRF SAMD RISK (ideas)

The intended use of the information provided by SaMD in clinical management has different significance on the action taken by the user.

5.1.1 To treat or to diagnose

Treating and diagnosing infers that the information provided by the SaMD will be used to take an immediate or near term action:

- To treat/prevent or mitigate by connecting to other medical devices, medicinal products, general purpose actuators or other means of providing therapy to a human body
- To diagnose/screen/detect a disease or condition (i.e., using sensors, data, or other information from other hardware or software devices, pertaining to a disease or condition).

State of Healthcare situation or condition	Significance of information provided by SaMD to healthcare decision		
	Treat or diagnose	Drive clinical management	Inform clinical management
Critical	IV	III	II
Serious	III	II	I
Non-serious	II	I	I

http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf

5.1.2 To drive clinical management

Driving clinical management infers that the information provided by the SaMD will be used to aid in treatment, aid in diagnoses, to triage or identify early signs of a disease or condition will be used to guide next diagnostics or next treatment interventions:

- To aid in treatment by providing enhanced support to safe and effective use of medicinal products or a medical device.
- To aid in diagnosis by analyzing relevant information to help predict risk of a disease or condition or as an aid to making a definitive diagnosis.
- To triage or identify early signs of a disease or conditions.

5.1.3 To Inform clinical management

Informing clinical management infers that the information provided by the SaMD will not trigger an immediate or near term action:

- To inform of options for treating, diagnosing, preventing, or mitigating a disease or condition.
- To provide clinical information by aggregating relevant information (e.g., disease, condition, drugs, medical devices, population, etc.)

FDA Software Guidance (2005)

Table 1 Major Level of Concern

If the answer to any <u>one</u> question below is Yes, the Level of Concern for the Software Device is likely to be Major.
1. Does the Software Device qualify as Blood Establishment Computer Software? (Blood Establishment Computer Software is defined as software products intended for use in the manufacture of blood and blood components or for the maintenance of data that blood establishment personnel use in making decisions regarding the suitability of donors and the release of blood or blood components for transfusion or further manufacture.)
2. Is the Software Device intended to be used in combination with a drug or biologic?
3. Is the Software Device an accessory to a medical device that has a Major Level of Concern?
4. Prior to mitigation of hazards, could a failure of the Software Device result in death or serious injury, either to a patient or to a user of the device? Examples of this include the following:
a. Does the Software Device control a life supporting or life sustaining function?
b. Does the Software Device control the delivery of potentially harmful energy that could result in death or serious injury, such as radiation treatment systems, defibrillators, and ablation generators?
c. Does the Software Device control the delivery of treatment or therapy such that an error or malfunction could result in death or serious injury?
d. Does the Software Device provide diagnostic information that directly drives a decision regarding treatment or therapy, such that if misapplied it could result in serious injury or death?
e. Does the Software Device provide vital signs monitoring and alarms for potentially life threatening situations in which medical intervention is necessary?

Table 2 Moderate Level of Concern

If the Software Device is not Major Level of Concern and the answer to any <u>one</u> question below is Yes, the Level of Concern is likely to be Moderate.
1. Is the Software Device an accessory to a medical device that has a Moderate Level of Concern?
2. Prior to mitigation of hazards, could a failure of the Software Device result in Minor Injury, either to a patient or to a user of the device?
3. Could a malfunction of, or a latent design flaw in, the Software Device lead to an erroneous diagnosis or a delay in delivery of appropriate medical care that would likely lead to Minor Injury?

IEC62304

„The SOFTWARE SYSTEM is software safety class A if:

- the SOFTWARE SYSTEM cannot contribute to a HAZARDOUS SITUATION; or
- the SOFTWARE SYSTEM can contribute to a HAZARDOUS SITUATION which does not result in unacceptable RISK after consideration of RISK CONTROL measures external to the SOFTWARE SYSTEM.

The SOFTWARE SYSTEM is software safety class B if:

- the SOFTWARE SYSTEM can contribute to a HAZARDOUS SITUATION which results in unacceptable RISK after consideration of RISK CONTROL measures external to the SOFTWARE SYSTEM and the resulting possible HARM is non-SERIOUS INJURY.

The SOFTWARE SYSTEM is software safety class C if:

- the SOFTWARE SYSTEM can contribute to a HAZARDOUS SITUATION which results in unacceptable RISK after consideration of RISK CONTROL measures external to the SOFTWARE SYSTEM and the resulting possible HARM is death or SERIOUS INJURY“

IEC 62304:2006 + A1:2015

MITIGATIONS (The Rights)

The Five Rights of Interoperability

Feb 24, 2016 | Posted by Industry Expert | Healthcare Delivery, HITA Feed

By **Keith Boone**, Healthcare Standards
Twitter: @motorcycle_guy

You can find many different versions of five rights in healthcare:

- Medication Administration: Right Patient, Right Drug, Right Dose, Right Route, Right Time
- Clinical Decision Support: Right Information, Right Person, Right Channel, Right Format, Right Time
- Imaging: Right Study, Right Order, Right Way, Right Report, Right Action.
- Staffing: Right Number, Right Skills, Right Location, Right Time, Right Assignment

What are the five rights for interoperability?

I would argue for these five:

1. Right Information
2. Right Interpretation
3. Right Time
4. Right Workflow
5. Right Value

AAMI 2800-1-2019

H1 Overview

H1.1 The RISK MANAGEMENT framework of this Standard addresses RISK MANAGEMENT activities specifically associated with multi-vendor interoperability while aligning with medical domain RISK MANAGEMENT processes specified in ISO 14971, IEC/TR 80002-1 and IEC 80001-1. While the section organization of this Standard does not match the process flow of ISO 14971 or IEC 80001, selected requirements are designed to augment ISO 14971/IEC 80001 requirements by indicating how ISO 14971/ IEC 80001 requirements may be met in the context of interoperability. This Annex provides an overview of key elements of the RISK MANAGEMENT framework of this Standard and an indication of how the requirements of this Standard support the ISO 14971 RISK MANAGEMENT activities.

H1.2 Some of the key RISK MANAGEMENT issues addressed by this Standard are listed below.

"INTEROPERABLE ITEM"-wise RISK MANAGEMENT – INTEROPERABLE MEDICAL PRODUCTS are built from INTEROPERABLE ITEMS that may be marketed separately from each other as well as from the systems in which they participate. Thus, RISK MANAGEMENT may be performed separately for each INTEROPERABLE ITEM. When INTEROPERABLE ITEMS are integrated, it is necessary not only to be able to reuse the realization of the INTEROPERABLE ITEMS but also assess and integrate part or all of their RISK MANAGEMENT results (e. g., hazard analysis, risk scoring, RISK MANAGEMENT file) and ASSURANCE (e.g., testing artifacts and reports, arguments that RELEASE CRITERIA have been met). Therefore, greater care must be taken to specify RISK MANAGEMENT information at INTEROPERABLE ITEM interface boundaries in a form that can be correctly understood and used to support integration and system level RISK MANAGEMENT activities. In particular, results of hazard IDENTIFICATION, risk analysis, and documentation of risk controls must be exposed at INTEROPERABLE ITEM boundaries and INTEROPERABILITY INTERFACES, and assumptions about the INTEROPERABLE ITEM contexts of use must be clearly IDENTIFIED and described in disclosed SAFETY information (e.g., as addressed in ISO 14971 Information for Safety).

H1.3 Generalization of HAZARDOUS SITUATIONS to RISK CONCERNS –

INTEROPERABLE ITEMS may be designed to be integrated into multiple system contexts. When INTEROPERABLE ITEM RISK MANAGEMENT is performed, the INTEROPERABLE ITEM RESPONSIBLE ORGANIZATION may not know all the potential integrated system contexts (and associated intended uses and PATIENT harms) into which the INTEROPERABLE ITEM may be integrated. ISO 14971 (clauses 4.2 – 4.4) phrases hazard IDENTIFICATION and risk analysis activities in terms of HAZARDOUS SITUATIONS that trace directly to PATIENT harm and INTENDED USE. Because INTEROPERABLE ITEM RISK MANAGEMENT may not address system-level HAZARDOUS SITUATIONS and PATIENT harm directly, this Standard phrases risk analysis activities in terms of RISK CONCERNS that generalize HAZARDOUS SITUATIONS. The RISK CONCERNS may not directly relate to harm, but they

FDA Interoperability Guidance(2016)

Contains Nonbinding Recommendations

Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on: September 6, 2017

Manufacturers' risk analysis should consider the risks associated with interoperability, reasonably foreseeable misuse, and reasonably foreseeable combinations of events that could result in a hazardous situation. Based upon these risks, a manufacturer may want to change the design of the device, the intended interoperability scenarios, or include device limitations and/or warnings to reduce risks to acceptable levels. As discussed in ISO 14971, risk control measures may not be necessary for risks that are broadly acceptable;[8] these decisions should be captured within the risk analysis documentation.

FDA emphasizes that the same process of defining hazardous situations, risks, and mitigations can be used when considering a system that contains more than one connected medical device. There may be additional hazardous situations that arise in these conditions. The manufacturer should specify which mitigations are implemented and which are necessary for safe use but may require implementation by other parties, such as the party responsible for set-up or installation. These should be included in the risk analysis section of the submission.

For devices subject to the risk analysis in 21 CFR 820.30(g), FDA recommends including an analysis of the interface or interfaces on the devices, the intended connections, and any effects that the connection may have on the device performance. The normal risk analysis submitted should include hazards that were considered, possible hazardous situations, the risks that may result from each, and how the hazards and risks were addressed. Your submitted analysis should include the normal elements in a risk analysis and address:

- the risk control measures for reducing unacceptable risks to acceptable levels;
- fault tolerant behavior, boundary conditions, and fail safe behavior such as how the device handles delays, corrupted data, data provided in the wrong format, unsynchronized or time mismatched data, and any other issues with the reception and transmission of data;
- any risks potentially arising from security vulnerabilities[9] that may be