JWG7
Health Device Security Standards Update
APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 1: Roles, responsibilities and activities

1 Scope

Recognizing that MEDICAL DEVICES are incorporated into IT-NETWORKS to achieve desirable benefits (for example, INTEROPERABILITY), this international standard defines the roles, responsibilities and activities that are necessary for RISK MANAGEMENT of IT-NETWORKS incorporating MEDICAL DEVICES to address SAFETY, EFFECTIVENESS and DATA AND SYSTEM SECURITY (the KEY PROPERTIES). This international standard does not specify acceptable RISK levels.

NOTE 1 The RISK MANAGEMENT activities described in this standard are derived from those in ISO 14971 [4]. The relationship between ISO 14971 and this standard is described in Annex A.

This standard applies after a MEDICAL DEVICE has been acquired by a RESPONSIBLE ORGANIZATION and is a candidate for incorporation into an IT-NETWORK.

NOTE 2 This standard does not cover pre-market RISK MANAGEMENT.

This standard applies throughout the life cycle of IT-NETWORKS incorporating MEDICAL DEVICES.

NOTE 3 The life cycle management activities described in this standard are very similar to those of ISO/IEC 20000-2 [10]. The relationship between ISO/IEC 20000-2 and this standard is described in Annex D.
SAFETY, EFFECTIVENESS AND SECURITY IN THE IMPLEMENTATION AND USE OF CONNECTED MEDICAL DEVICES OR CONNECTED HEALTH SOFTWARE

Part 1: Application of risk management

1 Scope


This standard serves to ensure the KEY PROPERTIES of connected MEDICAL DEVICES and connected HEALTH SOFTWARE are maintained during Implementations and Clinical Use as depicted at Figure 1.

This standard is not intended to be a general standard establishing SAFETY, EFFECTIVENESS and security of the individual components of a connected system, but rather to ensure that the SAFETY, EFFECTIVENESS and security of the components is maintained when connected in a system and both for the components and the system. This would include ensuring that pre-existent component HAZARDS and associated RISKS are not exacerbated because of connection and that any emergent HAZARDS and associated RISKS as result of connection are appropriately managed.

This standard is intended for use by HDO of any size, for example a small-scale organisation incorporating a single MEDICAL DEVICE through to a large scale integrated health IT system spanning multiple locations. It is also intended to assist manufacturers in the provision of support to HDOs during the connection of MEDICAL DEVICES and HEALTH SOFTWARE within MEDICAL IT-NETWORKS.
Temporary Annex—Mapping of IEC 80001-1 text to reorganised document (by section).

**2018-01-26**: This table provides mapping of the structures of ISO/DIS 31001 and IEC 80001-1:2010 to this reorganised draft. It is for help in reviewing this draft and is not intended to become part of the final standard.

<table>
<thead>
<tr>
<th>ISO31000: 2018</th>
<th>IEC 80001-1 Content Reorganisation</th>
<th>IEC 80001-1: 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section No:</td>
<td>Section Heading:</td>
<td>Section No:</td>
</tr>
<tr>
<td>n/a</td>
<td>Foreword</td>
<td>n/a</td>
</tr>
<tr>
<td>n/a</td>
<td>Introduction</td>
<td>n/a</td>
</tr>
<tr>
<td>1</td>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Normative references</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Terms and definitions</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Principles</td>
<td>4.</td>
</tr>
</tbody>
</table>

ISO / IEC 80001 Guidance Documents

Guidance documents facilitate understanding & implementation:

80001-2-1  Step-by-Step Risk Management
80001-2-2  Communicating Security Needs, Risks & Controls
80001-2-3  Wireless Guidance
80001-2-4  HCO Implementation Guidance
80001-2-5  Distributed Alarm Systems
80001-2-6  Responsibility Agreements
80001-2-7  Conformance Self-assessment Guidance
80001-2-8  Mapping Security Controls to 19 Capabilities
80001-2-9  Security Assurance Case for 19 Capabilities

Note: Tooling is available, such as those provided by Symantec or NovaLeah (https://www.youtube.com/watch?v=NYwncBtH-TE&authuser=0).
JWG7 Standards Roadmap (from ad hoc report)

Safe Health Software and Safe Health IT Systems
Design, Implementation & Clinical Use

Design & Development
(Responsibility of the Developer)
- Concepts and Requirements Definition
- Development
- Testing, Verification, and Documentation
- Software Production, Release, & Maintenance

Implementation & Clinical Use
(Responsibility of Health Service Organization)
- Procurement (including Manufacturer Compliance)
- Installation, Customization, and Configuration
- Integration, Data Migration, Transition, and Validation
- Implementation, Workflow Optimization, and Training
- IT Systems Operation & Maintenance
- Decommissioning and Disposal

Foundation – Principles, Concepts & Definitions
- IT & IM Governance
- Organization Culture, Roles & Competencies
- System and Software Lifecycle Processes
- Human Factors, Usability & Change Management
- Privacy & Security Management
- Quality Management
- Safety Management Processes Across Software Lifecycle
- Data Lifecycle

Figure 1: Lifecycle Diagram

Figure 2: Sociotechnical system underlying Health IT – Related Adverse Events

81001-1

© Trusted Solutions Foundry, Inc. 2018
The standard framework
(proposed mapping)

Current framework

- 60601, etc.
- 13485
- 14971
- 62304
- 82304
- 80001

- 80001-1
- 80001-2-4 (impl. guide)
- 80001-2-7 (self.assmnt)
- 80001-2-5 (alarms)
- 80001-2-3 (wireless)

80001-2-2 (disclosure) Created
80001-2-8 (sec. req.) Used
80001-2-6 (resp. agrmnt)

81001
HEALTH SOFTWARE –

Part 1: General requirements for product safety

1 Scope

1.1 Purpose

This International Standard applies to the SAFETY of HEALTH SOFTWARE PRODUCTS designed to operate on general computing platforms and intended to be placed on the market without dedicated hardware, and its primary focus is on the requirements for MANUFACTURERS.
1 Scope

This PAS gives recommendations for developers of health and wellness apps, intending to meet the needs of health care professionals, patients, carers and the wider public. It includes a set of quality criteria and covers the app project life cycle, through the development, testing, releasing and updating of an app, including native, hybrid and web based apps, those apps associated with wearable, ambient and other health equipment and apps that are linked to other apps. It also addresses fitness for purpose and the monitoring of usage.

Note: Now a CEN/TC 251 project & possible future JWG7 project.
1 Scope

1.1 * Purpose

This document defines the development and maintenance life cycle requirements for HEALTH SOFTWARE. The set of PROCESSES, ACTIVITIES, and TASKS described in this standard establishes a common framework for HEALTH SOFTWARE life cycle PROCESSES.

3.11 HEALTH SOFTWARE

SOFTWARE intended to be used specifically for managing, maintaining, or improving health of individual persons, or the delivery of care.

Note 1 to entry: HEALTH SOFTWARE fully includes what is considered software as a MEDICAL DEVICE

Note 2 to entry: Examples of HEALTH SOFTWARE include:

1. Non-regulated MEDICAL DEVICE HEALTH SOFTWARE; Mobile applications running on devices without using specific sensors or detectors, Hospital information systems;
2. MEDICAL DEVICE SOFTWARE: software that is an integral part of an Infusion pump or Dialysis machine;
3. Software as a MEDICAL DEVICE: A software application that reviews MRI’s and highlights areas for a clinician to review.

Note 2 to entry: Examples of HEALTH SOFTWARE include: Software only products for health use; Hospital information systems; SW for stimulating activity by Alzheimer patients; Mobile applications running on devices without using specific sensors or detectors.

[SOURCE: IEC 82304-1:2016, 3.6 and A. modified - Note 2 to entry added]
Results of CDV ballot …


2. In IEC, there were 9 countries voting against with comments and 13 countries voting in favor. We did not make the <=25% negative threshold (or >=66.7%).

3. In ISO, there were 4 countries voting against, 16 countries abstaining, and 13 positive votes. So, the document did not make the <=25% negative threshold (or >=66.7%).

4. The team is currently addressing the comments and will have a F2F meeting in October in Italy in conjunction with ISO/TC215 plenary and work group meetings.

5. Team will have a CD3 and then another CDV/DIS.

6. The team will also have a “webinar” or messaging campaign to make sure the document is addressing concerns/comments from the countries and trade organizations. An INF document will be going out with information on this (targeting Webinars for early October).
<table>
<thead>
<tr>
<th>Task</th>
<th>Date</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolve comments and edit document for 3rd CD; Include an Annex Z for EU consideration for harmonization</td>
<td>Ending in October</td>
<td>Purpose is to vet the options and gain confidence in a way forward to a positive vote</td>
</tr>
<tr>
<td>Prepare slide deck for webinar “messaging campaign” to ISO, IEC, COCIR, DITTA</td>
<td>September/October</td>
<td>- Project team meeting with ISO/TC215 JWG7 in Italy (October 25-27 Thur-Saturday)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Documents to ISO/IEC in December</td>
</tr>
<tr>
<td>Complete comment resolution and editing of document</td>
<td>Complete in December</td>
<td></td>
</tr>
<tr>
<td>Expect 3CD in March 2019</td>
<td>IEC administrative tasks ~ 3 months</td>
<td>Request a 2-month review</td>
</tr>
<tr>
<td>3CD comments expected in May 2019</td>
<td>Ending in August 2019</td>
<td>Project team could meet in June with AAMI in Cleveland OH USA</td>
</tr>
</tbody>
</table>
81001-1:2018 CD1

Health informatics — Health software and health IT systems safety, effectiveness and security — Part 1: Foundational principles, concepts and terms

Figure 2 – Health software and systems within their socio-technical ecosystem
1. Scope

1.1 This document articulates the foundational principles, concepts, and terms for health software and health IT system safety across the full lifecycle, from concept to disposal, taking into account the evolving complex internal and external context, including people, technology (hardware/software), organization, process, and external environment. It also addresses the transition points in the lifecycle where transfers of responsibility occur, and the types of bilateral communication that are necessary.

1.2 This document describes the fundamental concepts and principles of managing safety, effectiveness and security (SES) management that are applicable to all parties involved in the health software and systems lifecycle including:

- Organizations designing, developing, integration, implementing and operating these systems – e.g. software developers and manufacturers, system integrators, system operators (including cloud and other IT service providers)
- Health care service delivery organizations, health care providers and others who use these systems in providing health services
- Governments, health system funders, monitoring agencies, professional organizations and customers seeking confidence in an organization’s ability to consistently safe, effective and secure health IT systems and services
- Organizations and interested parties seeking to improve communication in managing safety, effectiveness and security risks through a common understanding of the vocabulary used in SES management;
- Organizations performing conformity assessments against the requirements of ISO/IEC 80001 series;
- Providers of training, assessment or advice in safety, effectiveness and security risk management for HIT software and systems;
- Developers of related SES standards.

1.3 This document specifies the terms and definitions that apply to all future safety, effectiveness and security risk management system standards developed by ISO/TC 215, and other health sector-specific SES standards based on those standards.

Focus is to ensure that the “safety baton” is passed at each critical transition point.
Focus is to ensure that the “safety baton” is passed at each critical transition point.
JWG7 Proposal: IT Security for Medical Devices

Proposed to JWG7 @ 2018 Spring meetings in Maringá by Georg Heidenreich / Siemens ...

Security & Safety

Security

Protection Goals:
- Essential Function
- Information Assets (Data, functions, software)

Medical Device

Confidentiality of data in the device
Integrity of data and functions
Availability of data & services

Unforeseen Event
Forgotten Contributor
Unplanned Situation

Safety

Protection Goals:
- Health
- Safety
- Privacy

IEC 60601
ISO 14971
IEC 80001

NOTE: See complete presentation to JWG7 2018.05 Maringá

Product := System plus Documents
- Intended Use
- Instructions for Use
- Intended Operational Environment
JWG7 Proposal: IT Security for Medical Devices

Security: New standards proposals

Security Threats

Protection Goals:
- Essential Function
- Information Assets (Data, functions, software)

✅ Focus on Manufacturers
✅ Based on work from Germany DKE 811.3.3

Medical Device

Confidentiality of data in
the device

Integrity of data and functions

Availability of data & services

NP-1 Secure Process (Lifecycle)
IEC 62443
SAFECODE

NP-2 Security Functions (Requirements)
IEC 62443
NIST SP800
OWASP
BSI / KRITIS

Source: Georg Heidenreich @ JWG7 2018.05 Maringá
JWG7 Proposal: IT Security for Medical Devices

Product Support for Security

- Product Security Features
  - IEC 82304: Product Safety
- Secure Tools and Components
- Secure Manufacturing
- Documentation: Secure Use

IEC 62304: Software Lifecycle
AAMI Medical Device Cybersecurity Guidance
Medical Device Cybersecurity
A Guide for HTM Professionals

Published: 2018 May

Guidance specifically for:

- Healthcare Technology Management (HTM) professionals
- Developers and Clinical / IT Engineers

Guidance includes:

- Cybersecurity Fundamentals
- Regulatory & Standards
- Managing the Asset
- Risk Assessment & Mitigation
- Trends and future developments
AAMI: Guidance for Newbies & Experts

Foreword (Karl J. West)

1. Medical Device Cybersecurity: A Public Health Perspective (Dale Nordenberg)
2. Objective and Scope of This Guide (Stephen L. Grimes, Axel Wirth)
3. Cybersecurity Fundamentals (Axel Wirth with intro by Lee Kim)
4. Understanding the Patient Care Environment (Stephen Grimes with intro by David Finn)
5. Managing the Technical Environment and Infrastructure (John T. Rasmussen with intro by Sue Schade)
6. Understanding the Regulatory and Standards Environment (Michelle Jump with intro by Suzanne Schwartz)
7. Stakeholders and Their Roles, Responsibilities, Training, and Education in Cybersecurity (Anahi Santiago with intro by Stephen Grimes)
8. Managing the Asset: Inventory and Configuration Management (Stephen Grimes with intro by Purna Prasad)
9. Medical Device Cybersecurity Risk Assessment (Stephen Grimes with intro by Todd Cooper)
10. Medical Device Cybersecurity Risk Mitigation: Establishing Effective Governance (Michael Busdicker, Scot Copeland, Priya Upendra with intro by Jennifer Jackson)
11. Medical Device Cybersecurity Risk Mitigation: Fundamentals of Securing Medical Devices (Ben Esslinger, Axel Wirth with intro Michael McNeil)
12. Medical Device Cybersecurity Risk Mitigation: Incident Response (Timothy Torres with intro by Denise Anderson)
13. Trends and Future Developments in Securing Medical Devices (Ken Hoyme, Shankar Somasundaram, intro by Anita Finnegan)

Appendices (including examples for policies and procedures provided by Mayo Clinic and Scripps Mercy Hospital)
AAMI: Strong industry representation!