Trusted
Solutions
Foundry

JWG7
Health Device Security Standards Update

American National Standard

ANSI/AAMI/IEC 80001-1:2010

2010!

Application of risk management for IT Networks incorporating medical devices — Part 1: Roles, responsibilities and activities

AAMI
Association for the Advancement of Medical Instrumentation

American National Standard ANSI/AAMI/IEC 80001-1:2010

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.

Trusted Solutions Foundry

DRAFT

SAFETY, EFFECTIVENESS AND SECURITY IN THE IMPLEMENTATION AND USE OF CONNECTED MEDICAL DEVICES OR CONNECTED HEALTH SOFTWARE

New title!

Part 1: Application of risk management

1 Scope

2018-07-02: Scope section updated to incorporate feedback from the ISO80001-1 workshop, London 21st/22nd June 2018.

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.

Trusted Solutions Foundry

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- 1:2010to this reorganised draft. It is for help in reviewing this draft and is not intended to become part of the final standard.

ISO31000: 2018		IEC 80001-1 Content Reorganisation		IEC 80001-1: 2010	
Section No:	**Section Heading:**	**Section No:**	**Section Heading:**	**Section No:**	**Section Heading:**
n/a	Foreword	n/a	Foreword	n/a	Foreword
n/a	Introduction	n/a	Introduction	n/a	Introduction
1	Scope	1	Scope	1	Scope
2	Normative references	2	Normative References		
3	Terms and definitions	3	Terms and Definitions	2	Terms and Definitions
4	Principles	4.	Principles		

NOTE: Alignment with ISO 31000, includes ISO 9001 alignment; but not an ISO Directives Annex SL “Management Systems” Standard.

Trusted Solutions Foundry

ISO / IEC 80001 Guidance Documents

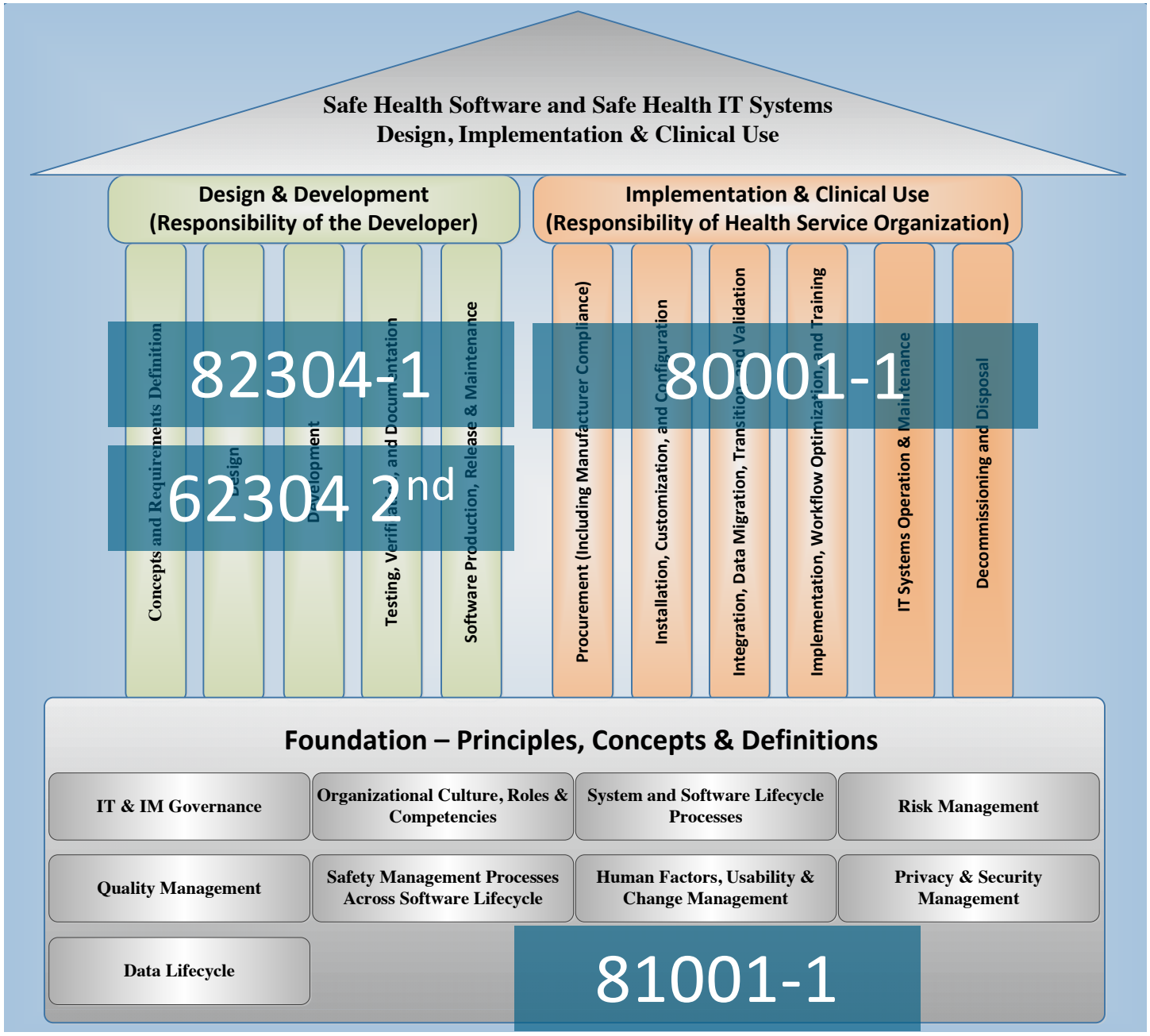
Guidance documents facilitate understanding & implementation:

- 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).

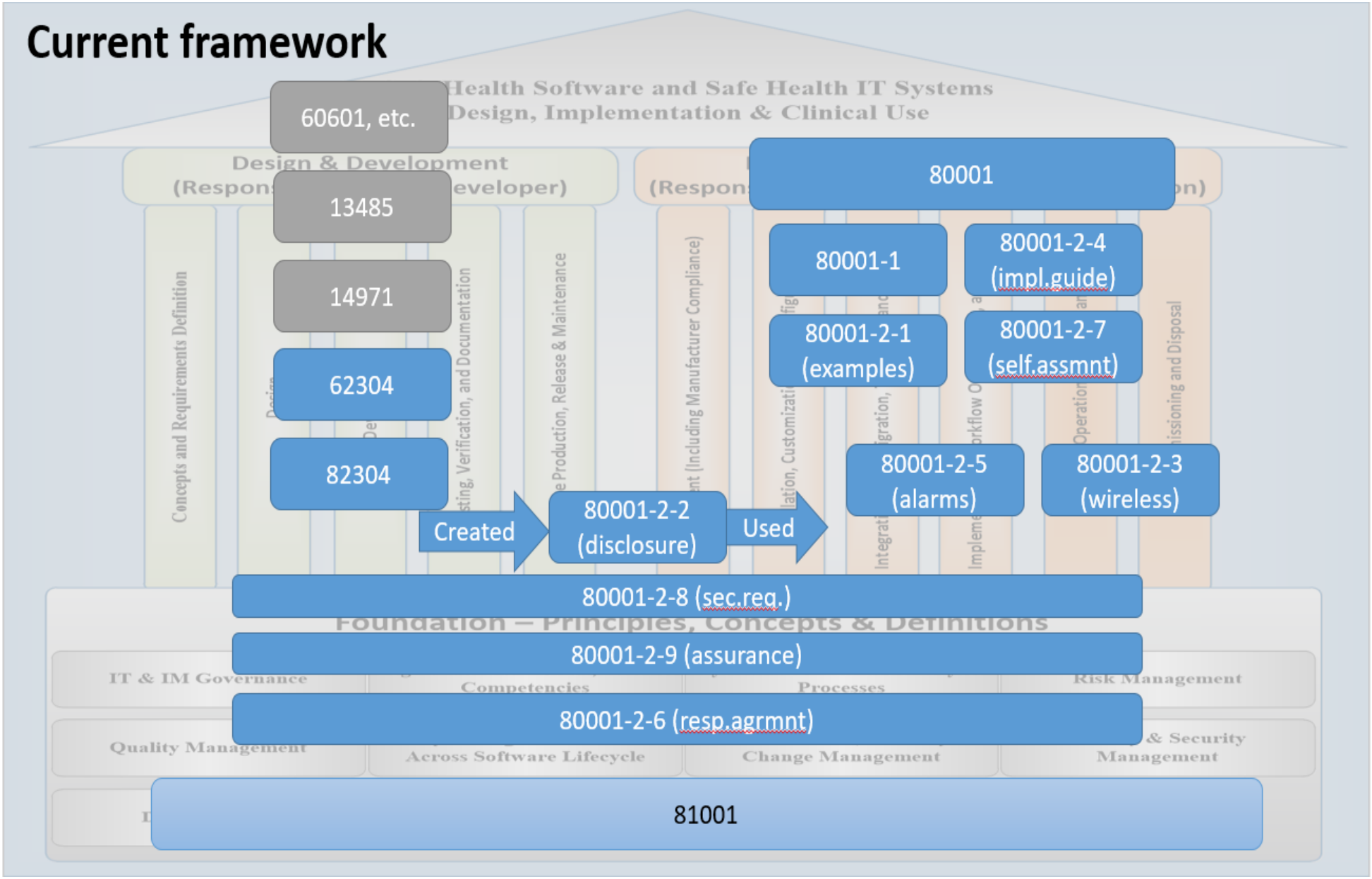
Trusted Solutions Foundry

JWG7 Standards Roadmap (from ad hoc report)



Trusted Solutions Foundry

The standard framework
(proposed mapping)



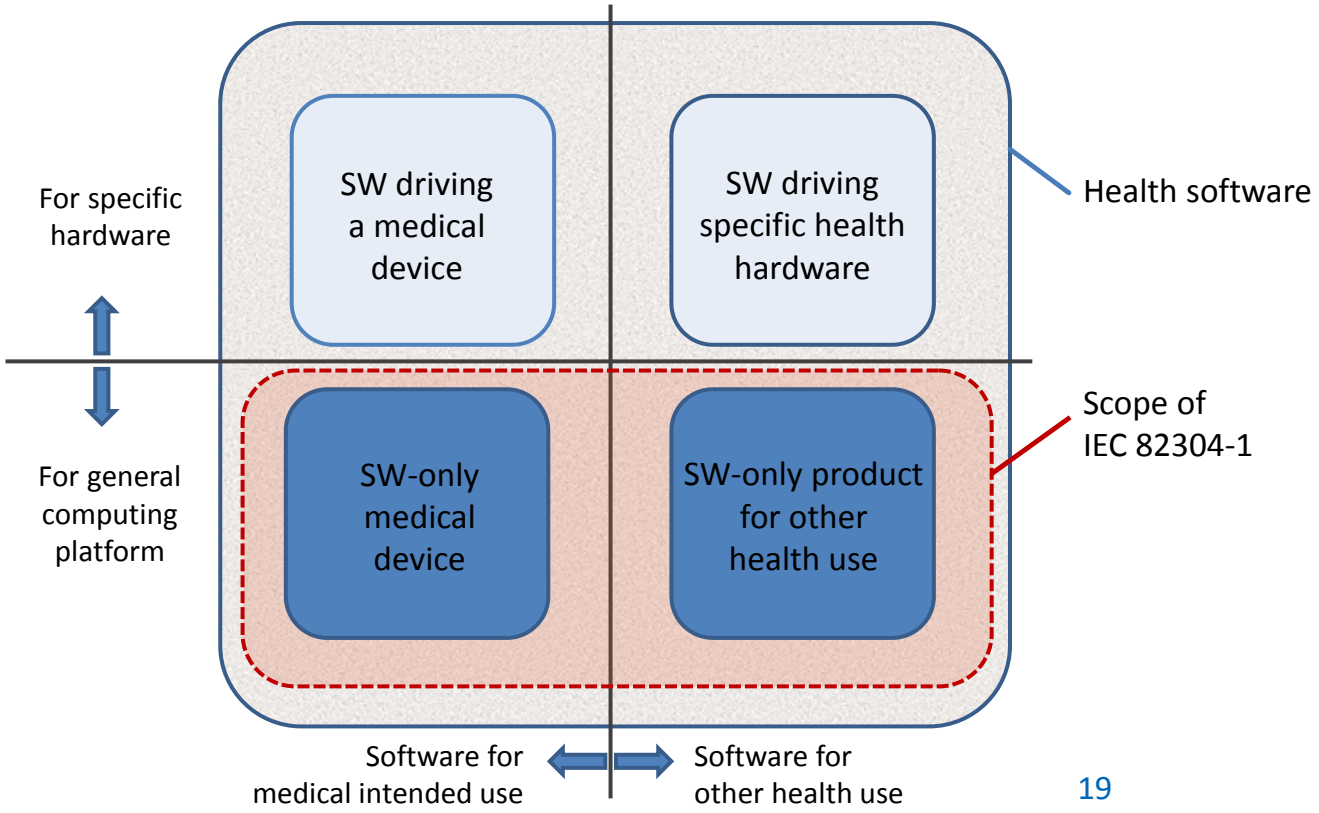
HEALTH SOFTWARE –

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.



PAS 277:2015

Health and wellness apps – Quality criteria across the life cycle – Code of practice

Innovate UK
Technology Strategy Board

bsi.

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.

Trusted Solutions Foundry

HEALTH SOFTWARE – SOFTWARE LIFE CYCLE PROCESSES

1 Scope

1.1 * Purpose

This documentstandard 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 SYSTEM 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. Nnon-regulatedMEDICAL 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. mModified - Note 2 to entry added]

109
110

HEALTH SOFTWARE –
SOFTWARE LIFE CYCLE PROCESSES

Results of CDV ballot …

1. Draft 62304 2nd Edition CDV/DIS did not pass in IEC/SC62A or ISO/TC215
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).

Trusted Solutions Foundry

109 **HEALTH SOFTWARE –**
110 **SOFTWARE LIFE CYCLE PROCESSES**

Resolve comments and edit document for 3rd CD; Include an Annex Z for EU consideration for harmonization	Ending in October	
Prepare slide deck for webinar "messaging campaign" to ISO, IEC, COCIR, DITTA	September/October	Purpose is to vet the options and gain confidence in a way forward to a positive vote
Complete comment resolution and editing of document	Complete in December	**- Project team meeting with ISO/TC215 JWG7 in Italy (October 25-27 Thur-Saturday)** - Documents to ISO/IEC in December
Expect 3CD in March 2019	IEC administrative tasks ~ 3 months	Request a 2-month review
3CD comments expected in May 2019		
Resolve comments and edit document to prepare for 2CDV	Ending in August 2019	Project team could meet in June with AAMI in Cleveland OH USA

Trusted Solutions Foundry

81001-1:2018 CD1

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

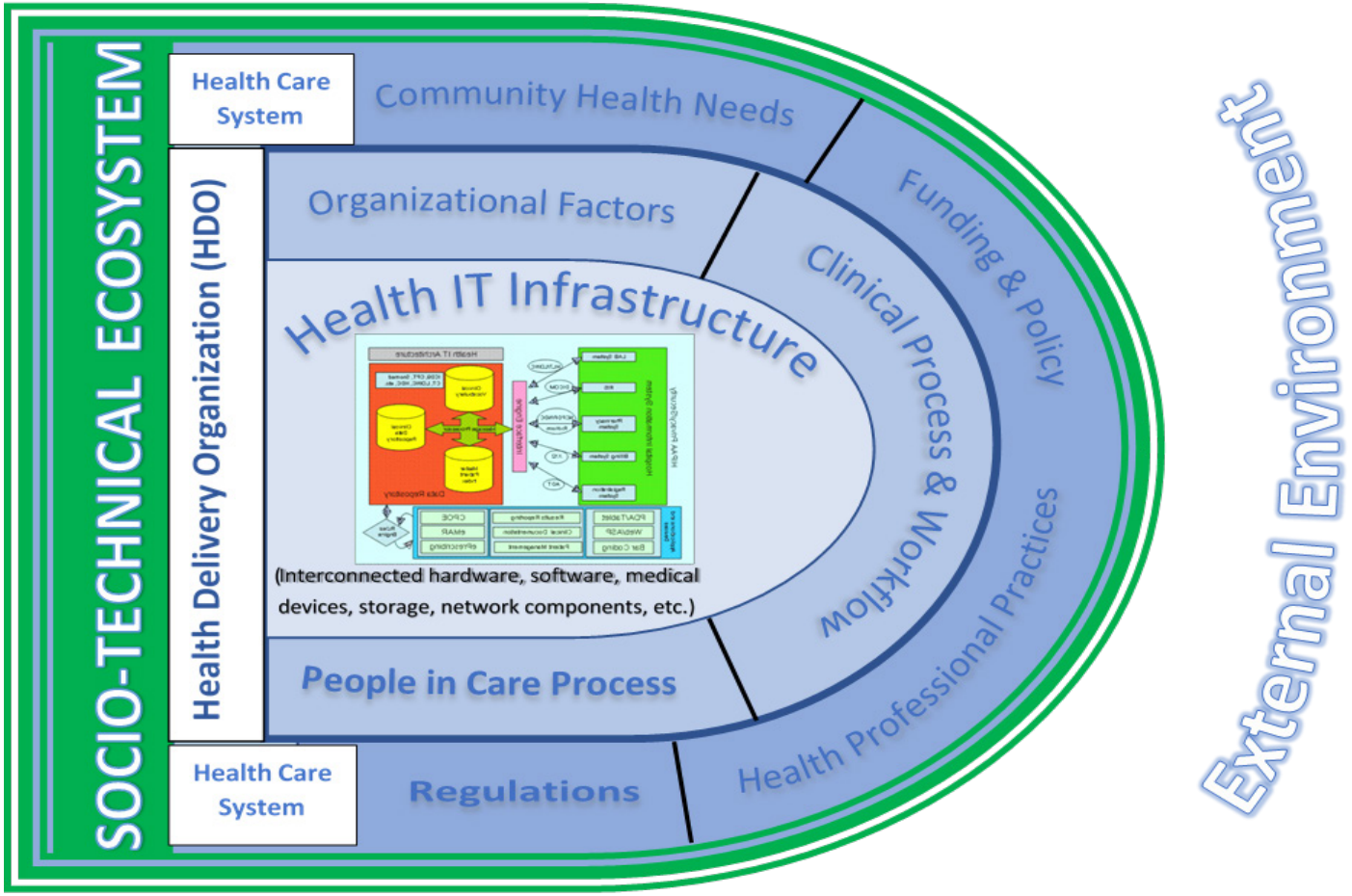
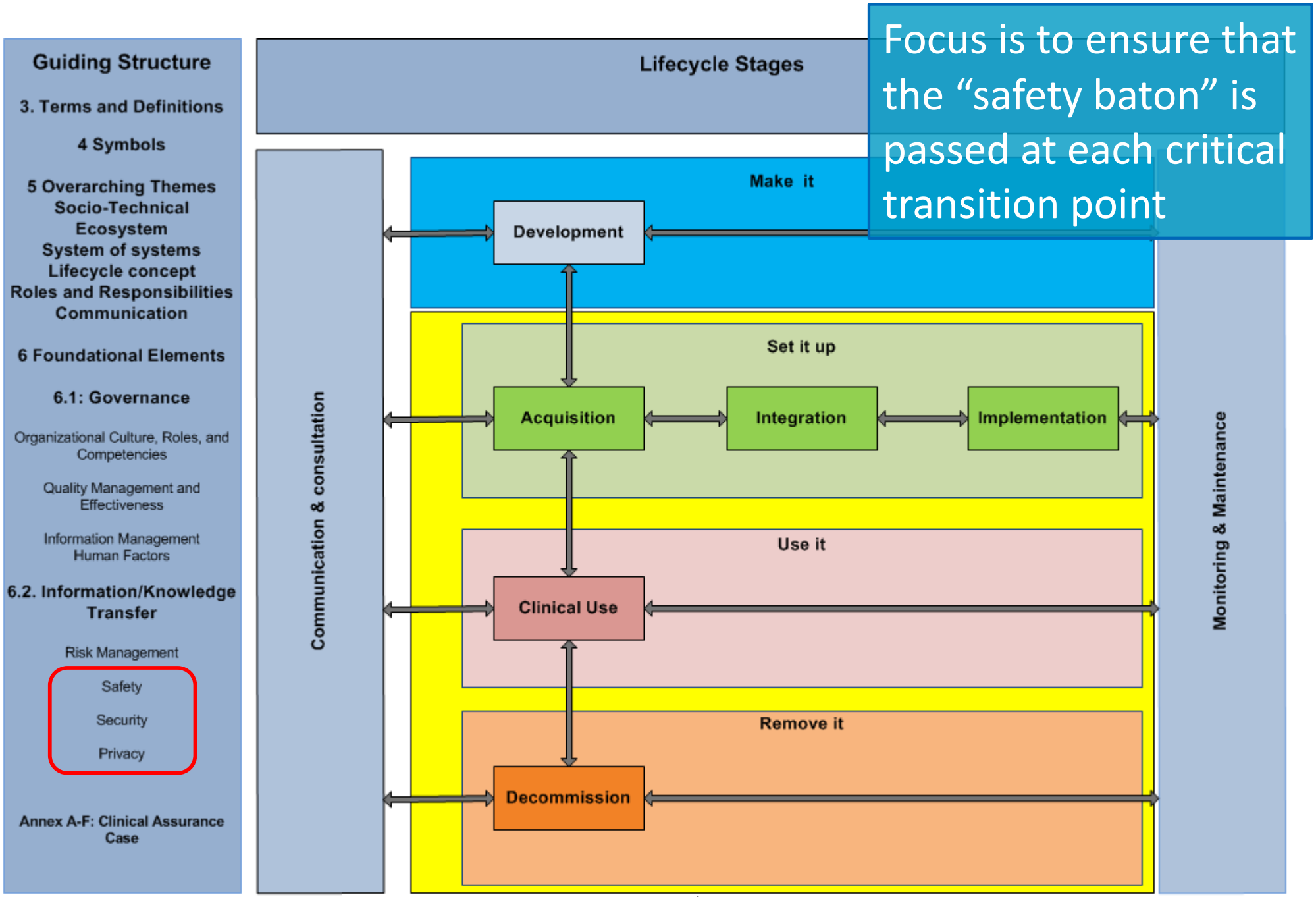


Figure 2 – Health software and systems within their socio-technical ecosystem


Guiding Structure
3. Terms and Definitions
4 Symbols
5 Overarching Themes
Socio-Technical
Ecosystem
System of systems
Lifecycle concept
Roles and Responsibilities
Communication
6 Foundational Elements
6.1: Governance
Organizational Culture, Roles, and Competencies
Quality Management and Effectiveness
Information Management
Human Factors
6.2. Information/Knowledge Transfer
Risk Management
Safety
Security
Privacy
Annex A-F: Clinical Assurance Case
Lifecycle Stages
Communication & consultation
Make it
Development
Set it up
Acquisition
Integration
Implementation
Use it
Clinical Use
Remove it
Decommission
Monitoring & Maintenance
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

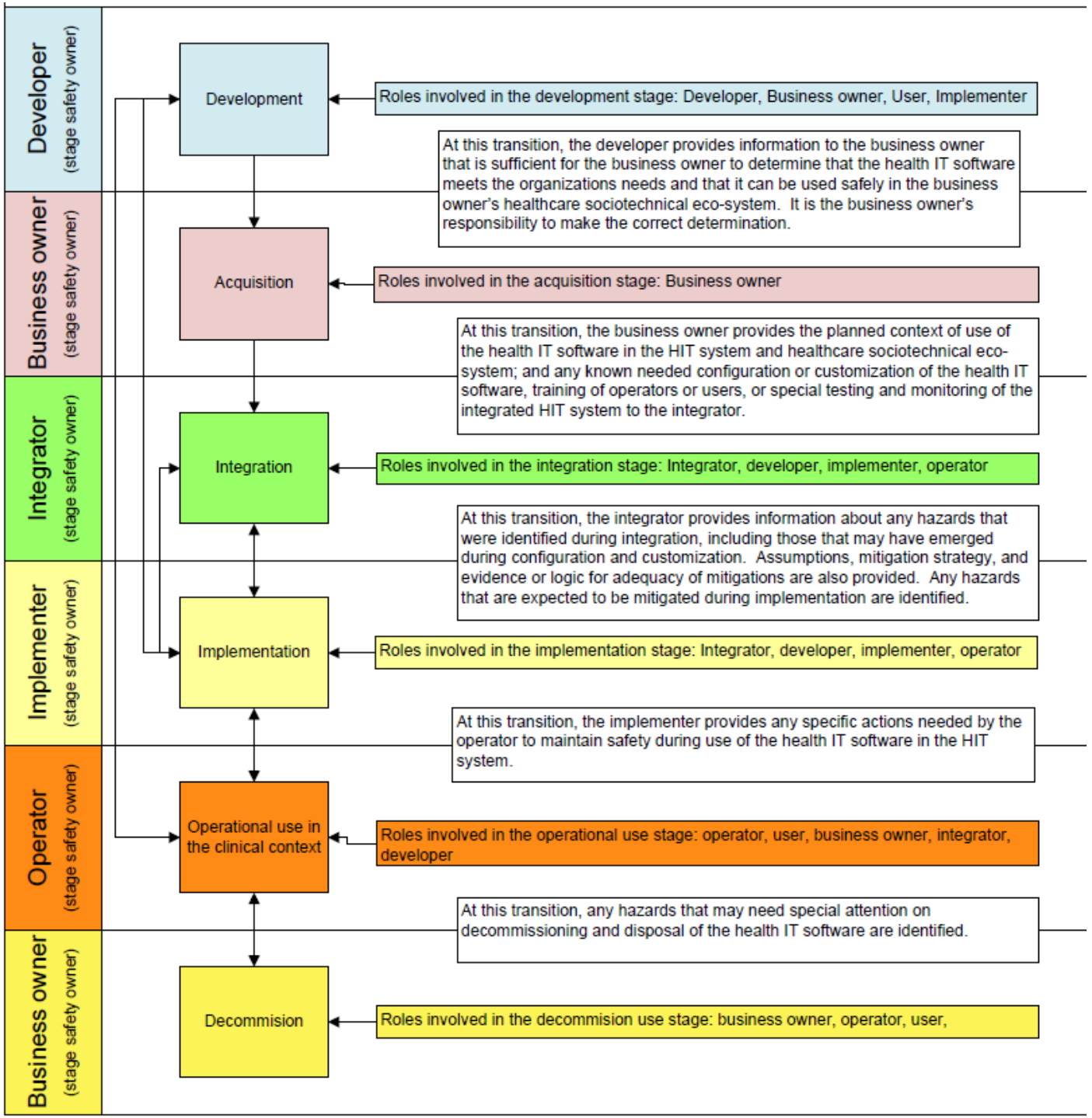
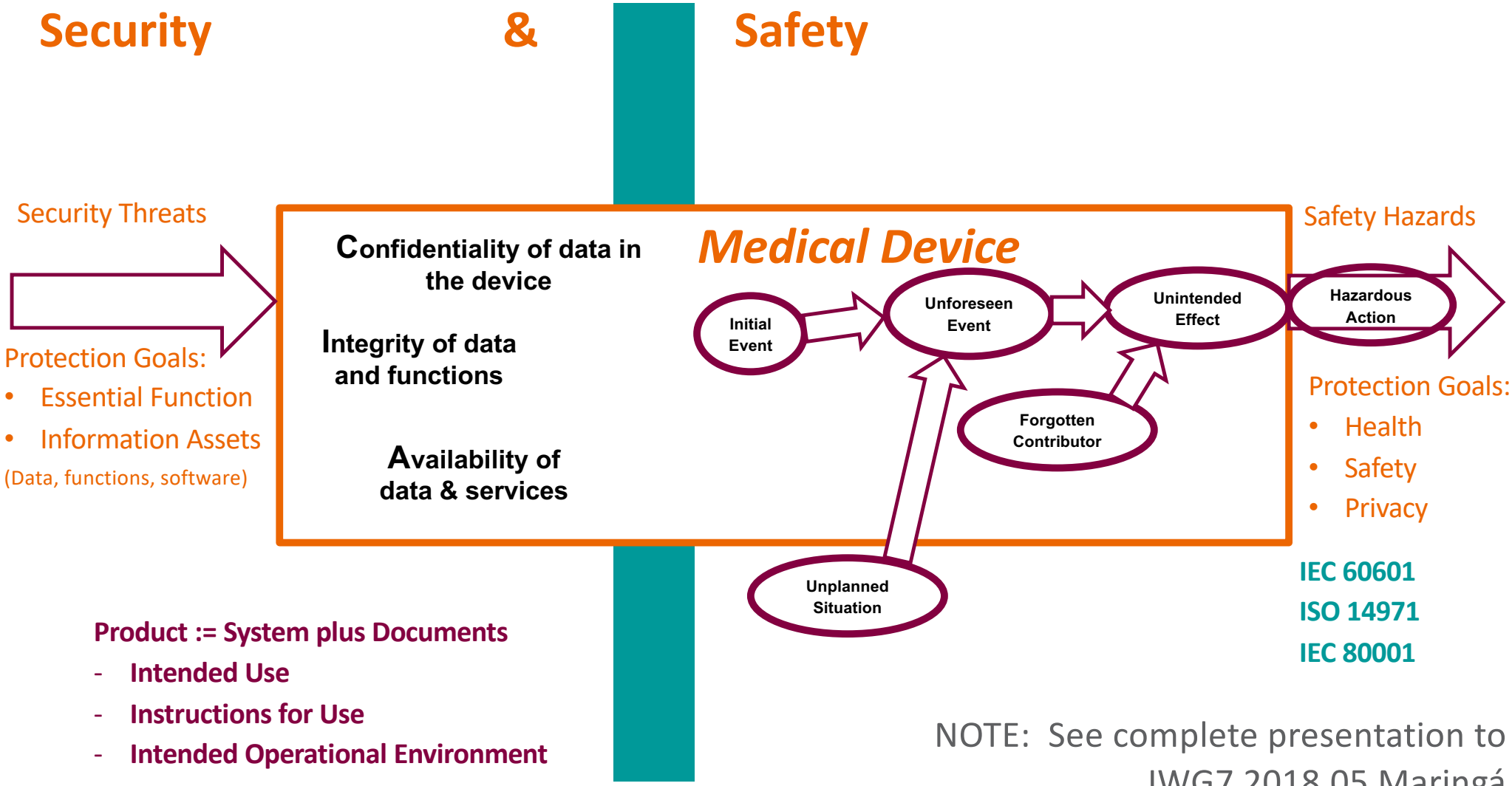


Figure 6 – Health software lifecycle stages and transition points

JWG7 Proposal: IT Security for Medical Devices

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



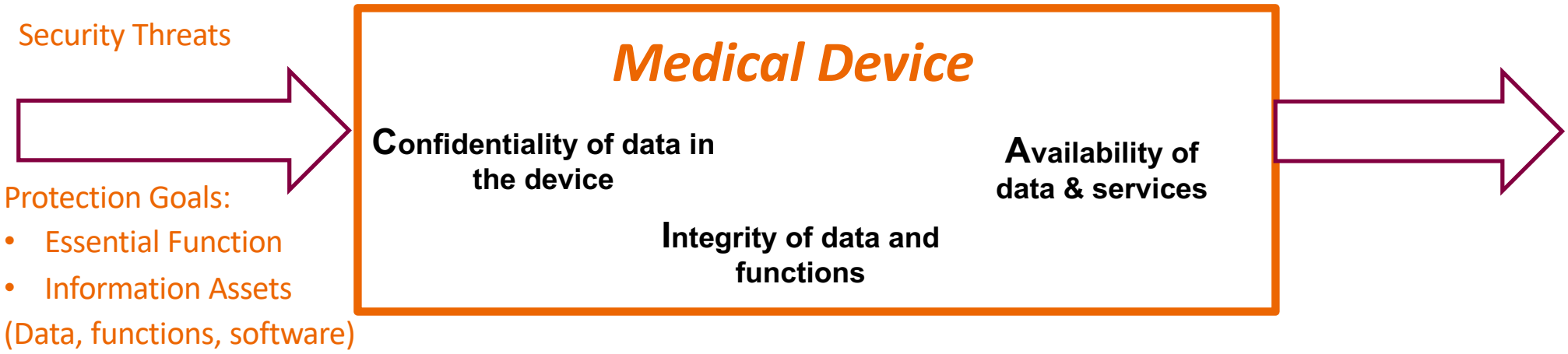
Product := System plus Documents

- **Intended Use**
- **Instructions for Use**
- **Intended Operational Environment**

NOTE: See complete presentation to JWG7 2018.05 Maringá

JWG7 Proposal: IT Security for Medical Devices

Security: New standards proposals



- ✓ **Focus on Manufacturers**
- ✓ **Based on work from Germany DKE 811.3.3**

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

Trusted Solutions Foundry

JWG7 Proposal: IT Security for Medical Devices

Product Support for Security

NP 2

NP 1

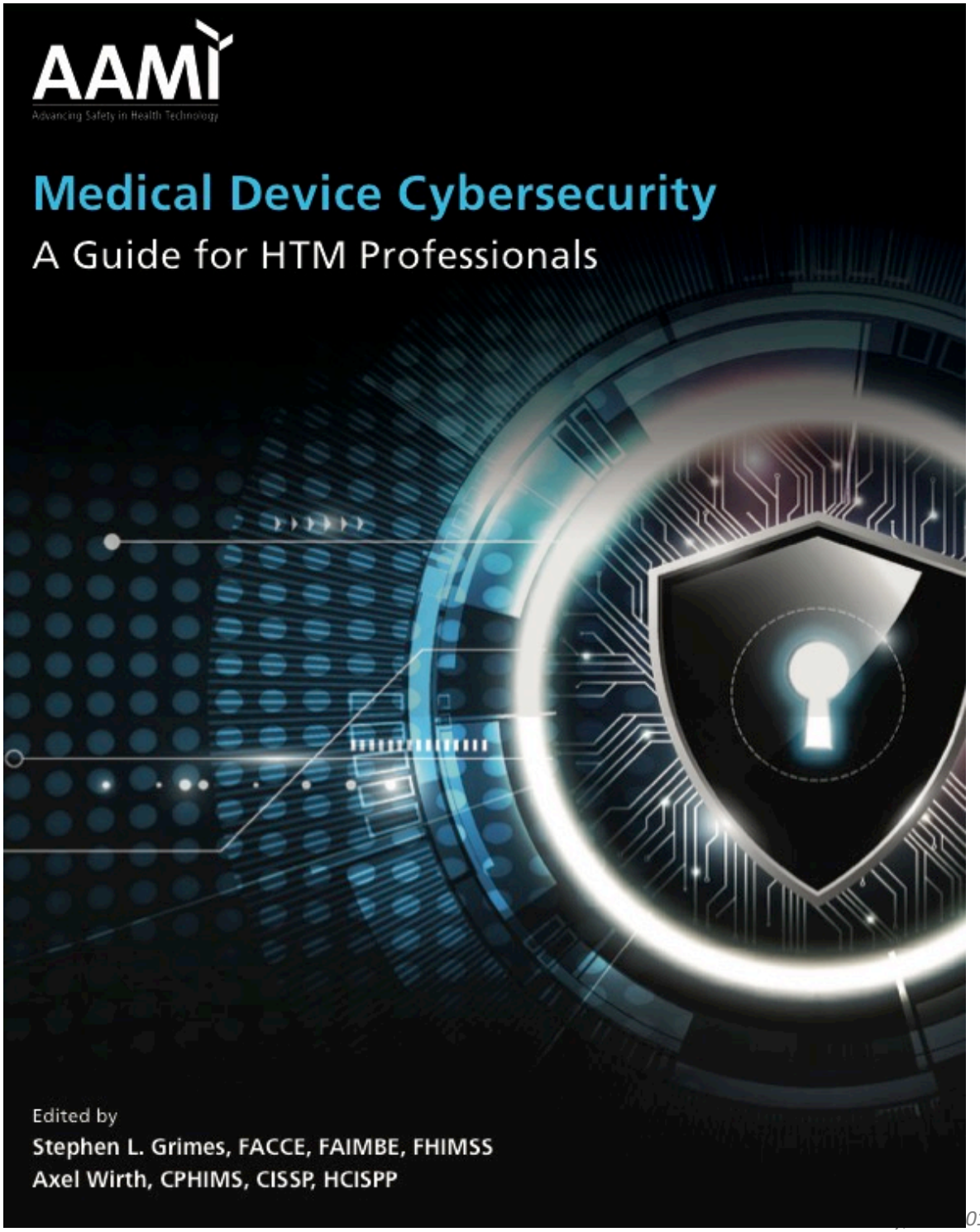
Heidenreich/ DKE

Source: Georg Heidenreich @ JWG7 2018.05 Maringá

Trusted Solutions Foundry

Trusted
Solutions
Foundry

AAMI Medical Device Cybersecurity Guidance



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

Trusted Solutions Foundry

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)

Trusted Solutions Foundry

AAMI: Strong industry representation!

Trusted Solutions Foundry