SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

26-February-2018

SoftwareCPR Standards Navigator provides information and tools related to standards that play a significant role in health software and software intensive medical devices. In addition to information on existing standards, SoftwareCPR Standards Navigator keeps you up to date on new standards activity and gives you expert insight into future changes to existing standards.

http://www.softwarecpr.com/topicsframepage.htm

Standards and regulatory activity overview

Medical devices

2018 should bring some clarity to areas of uncertainty regarding standards. We'll see new or amended versions of key medical device standards and get some idea of how the European Commission will harmonize standards for the Medical Device Regulation. There will be new standards and guidance for cybersecurity in medical devices and also new standards for health IT. Here are some key standards to watch.

- The second edition of IEC 62304 should be completed in 2018. The second edition will expand the scope of the standard to health software.
- Revision of ISO 14971 and ISO/TR 24971 will continue in 2018. Although it may not be completed in 2018, we should have a good idea of the changes being made by the end of 2018..
- Work on the second amendment to IEC 60601-1 will continue in 2018. This amendment is scheduled to be completed in 2019. Amendments will also be made to IEC 60601-1-2, IEC 60601-1-6, IEC 60601-1-8, IEC 60601-1-10 and IEC 60601-1-11. The amendments to these collateral standards are also expected to be completed in 2019. The technical changes should be completed in 2018, with final approvals and publication in 2019.
- There is a debate over whether to quickly complete the amendment to IEC 62366-1, or to hold it until the revision of 14971 is complete. The outcome of this debate will determine whether the 62366-1 amendment is completed in 2019 as currently planned.
- IEC has begun work on a standard for environmentally conscious design related to refurbishment/remanufacturing of medical devices.

Cybersecurity

- Germany has proposed a new cybersecurity standard in IEC and ISO, Health software and health IT systems security – Part 1: Lifecycle requirements for products. The scope includes networked medical devices – but remains independent of the 'medical' qualification of networked/software products in different geographies. The new standard is planned to:
    - not specify product security features
    - follow the structure of IEC 62304 and extend the sections of IEC 62304 as a companion standard
    - build on the outcomes of a 14971-guided safety risk analysis,
    - focus on activities during the product lifecycle
    - not invent specific activities, but refer to IEC to 62443-4-1 and standards from NIST, OWASP, JTC1
- AAMI has begun work on *TIR97 Principles for medical device security – Post-market security management for device manufacturers*. It is expected to be completed in 2018. This guidance is intended to assist manufacturers and other users of the standard in the following:
    - Establishing a corporate level process to manage security interactions with users and others;
    - Creating design features that enable post-market management of security risk and effective integration with HDO network security policies and technologies;
    - Understanding and communicating the security needs of manufacturers and HDOs;

  - Methods needed to observe fielded devices for newly discovered security vulnerabilities and communicate that information to both the HDO and the manufacturer;
  - Methods to assess both safety and security risk to decide when action is required;
  - The development of a coordinated vulnerability disclosure policy;
  - Recommendations on methods to manage device patching;
  - Planning for device retirement.

- AAMI has begun work on SW96, a process standard for application of security risk management to medical devices. The new standard will provide the specific process to support the guidelines and concepts outlined in TIR 57. The standard will supplement and work in conjunction with TIR 57 and there is no intention to replace AAMI TIR57:2016. The objective would be to have TIR 57 to serve in a similar fashion to ISO 24971, which provides guidance and support for implementation of ISO 14971. Then this standard would serve as the process upon which the TIR 57 concepts are applied.
- Work on a new Technical Report on cloud considerations for health information security and privacy has begun. This Technical Report (ISO TR 21332) presents an overview of health specific security and privacy requirements for a cloud computing environment.

Health IT

- A second edition of IEC 80001-1 began in 2016. The second edition will have a revised title and scope, *IEC 80001-1 Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 1: Application of risk management*. The expected date of publication is January, 2020.

Standards Navigator New Documents in January and February 2018

Medical device software

- A committee draft for vote of *IEC 62304 Ed 2: Health Software – Software life cycle processes* has been circulated for ballot. Edition 2 expands the scope of IEC 62304 to include health software that is not regulated as a medical device, and the title has been changed accordingly. This will be the last opportunity to make technical changes.

  The draft standard is available on the SoftwareCPR Standards Navigator web page.

Medical Devices

- A second committee draft of amendment 2 to *IEC 60601-1: General requirements for safety and essential performance* has been circulated for comment. The amendment corrects errors and makes modifications that are considered to important to wait for the next edition.

  The draft standard is available on the SoftwareCPR Standards Navigator web page.

- A second committee draft of an amendment to the second edition of *IEC 60601-1-8: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems* has been circulated for comment. This amendment addresses high priority issues in the standard that need to be considered before the next edition.

  The draft standard is available on the SoftwareCPR Standards Navigator web page.

- A second committee draft of an amendment to the second edition of *IEC 60601-1-11: Requirements for medical electrical equipment and medical electrical systems used in the home healthcare environment* has been circulated for comment. This amendment addresses high priority issues in the standard that need to be considered before the next edition.

  The draft standard is available on the SoftwareCPR Standards Navigator web page.

- The International Medical Device Regulators Forum (IMDRF) has released *Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices* for comment. This guidance document describes fundamental design and manufacturing requirements, referred to as 'Essential Principles of Safety and Performance' that, when met, indicate a medical device is safe and performs as intended. This document has been developed to encourage and support global convergence of regulatory systems. The purpose of this IMDRF guidance is to harmonize the documentation and procedures that are used to assess whether a medical device conforms to the regulations that apply in each jurisdiction.

  The draft guidance document is available on the SoftwareCPR Standards Navigator web page.

Health IT and mobile health applications

- A committee draft of *IEC 80001-1 Ed 2: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software - Part 1: Application of risk management* has been circulated for comment. This committee does not add new content to the standard, but incorporates a new scope and reorganizes the standard as a process standard following the structure of ISO/DIS 31000: Risk management.

  The draft standard is available on the SoftwareCPR Standards Navigator web page.

Medical device and Health Security

- Germany has proposed a new standard for security lifecycle that covers both medical devices and non-regulated health software, and a new guidance for security functions that covers medical devices. The concept for the lifecycle standard is that it will extend IEC 62304 as a companion standard and specify activities based on an ISO 14971-based risk analysis for safety. The concept for the guidance is to provide product related information security aspects to provide better communication between manufacturers of medical devices and Medical IT Network integrators. This proposal will be discussed by the standards committees in meetings to be held in April and May.

  The proposal is available on the SoftwareCPR Standards Navigator web page.

Software Engineering and Information Technology

- A final draft international standard (FDIS) of *ISO/IEC/IEEE 24748-1: Systems and software engineering — Life cycle management — Part 1: Guidelines for life cycle management* has been circulated for ballot. The purpose of this document is to facilitate the joint usage of the process content of the latest revisions of both ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207, by providing unified and consolidated guidance on life cycle management of systems and software.

  The draft standard is available on the SoftwareCPR Standards Navigator web page.

- A final draft international standard (FDIS) of *ISO/IEC/IEEE 24748-2: Systems and software engineering — Life cycle management — Part 2: Guidelines for the application of ISO/IEC/IEEE 15288 (System life cycle processes)* has been circulated for ballot. This document is a guideline for the application of ISO/IEC/IEEE 15288:2015. It addresses system, life cycle, organizational, project, and process concept application. It gives guidance on applying ISO/IEC/IEEE 15288:2015 from the aspects of strategy, planning, application in organizations, and application on projects.

  The draft standard is available on the SoftwareCPR Standards Navigator web page.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents were issued in a previous month and are still being reviewed. They can be found on the SoftwareCPR Standards Navigator until their review period completes.

	Topic	Use / Users	Description
ISO 14971 CD	Risk Management	Manufacturers	*ISO 14971 Medical devices — Application of risk management to medical* devices has been circulated for comment. This is the third edition of ISO 14971. This third edition cancels and replaces the second edition, which has been technically revised. The requirements in this document are clarified with more details, in particular the clauses on overall residual risk, on the risk management report and on production and post-production information.
ISO 24971 CD	Risk Management	Manufacturers	*ISO 24971 Medical devices - Guidance on the application of ISO 1497*1 has been circulated for comment. This document provides guidance to assist manufacturers in the development, implementation and maintenance of a risk management process for medical devices that aim to meet the requirements of ISO 14971:2019
IEC Guide 63 CD	Risk Management	Manufacturers	*Guide 63* provides practical guidance to standards writers on how to include safety aspects in the development of medical device standards including management system standards related to medical devices. This is a draft for comment.
ISO/IEC 25065 CD	Software Engineering	Manufacturers	*ISO/IEC 25065 Systems and software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for Usability: User requirements specification* has been circulated for comment. This document defines the common industry format (CIF) for specifying user requirements for the user interactions with and the interfaces of interactive systems. This document specifies the contents of a user requirements specification for the interactions and user interface and the format for stating requirements.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents were issued in a previous month and are still being reviewed. They can be found on the SoftwareCPR Standards Navigator until their review period completes.

	Topic	Use / Users	Description
MDS2 CD	Cybersecurity	Manufacturers & HDOs	A new revision of *The Manufacturer's Disclosure Statement for Medical Device Security (MDS2)* form and related instructions is being prepared. The MDS2 is used by medical device manufacturers to provide information to healthcare delivery organizations to assist them in accessing and managing risks to privacy and security of data and networks. This is a draft for comment.
MDISS Recommended Practice	Cybersecurity	Manufacturers & HDOs	Recommended Practice for defining the requirements for service providers contributing to the implementation, integration, and maintenance of medical devices and systems used in the context of health care solutions. This draft document has been developed by the Medical Device Innovation, Safety and Security consortium. This is a draft for comment.
ISO/IEC/IEEE 42030 DIS	Systems Engineering	Manufacturers	*ISO/IEC/IEEE 42030 Enterprise, systems and software — Architecture evaluation framework.* This document specifies the means to organize and record architecture evaluations. It covers various kinds of architecture situations, e.g. enterprise, systems, software, products, services, hardware, data, facilities, systems of systems, family of systems, product lines, and encompasses a variety of elements such as, for example, the people, organizations, techniques and processes involved in those architecture situations. It also spans the variety of applications that utilize digital technology such as mobile, cloud, big data, robotics, web, desktop, embedded systems, and so on. It addresses the evaluation of an architecture and not an evaluation of the architecture description's suitability. This is a draft for vote.
ISO/IEC 24733-1 DIS	Software Engineering	Manufacturers	*ISO/IEC 24733-1 Software and Systems Engineering – Certification of Software and Systems Engineering Professionals – Part 1: General Requirements*. ISO/IEC 24773-1 is part one of the ISO/IEC 24773 multipart standard. It contains terms and concepts used or referenced by the other parts of ISO/IEC 24773. It contains the requirements, which are common to all other parts of this multi-part standard, for certifications (schemes and bodies) in the domain of software and systems engineering. This is a draft for vote.