SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

18-December-2017

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

A lot of standards and regulatory activity is continuing in 2017. Here are some of the areas to watch. (Changes are in red)

- IEC 82304-1 *Health Software: General requirements for safety* has been published. It is intended that this standard be harmonized in the EU, but it is not clear when this may happen. Although this standard has not been harmonized in the EU, notified bodies are treating it as "state-of-the-art" and are likely to expect it to be used for software products that are regulated as medical devices.
- A first committee draft of the second edition of IEC 62304 was circulated in 2016. The second edition will expand the scope of the standard to health software. A second committee draft for comment has been circulated. The working group met in June to resolve comments on the second committee draft and will meet again in November. A committee draft for vote will be submitted to IEC before the end of 2017. IEC will go through an editing phase and then a two month translation period, so the draft should be available for review around the beginning of March, 2018.
- IEC TR 80002-2 *Medical device software - Part 2: Validation of software for medical device quality systems* has been published. This TR provides guidance for new requirements in ISO 13485:2016 for validating software used in quality systems. ISO/TR 80002-2:2017 applies to any software used in device design, testing, component acceptance, manufacturing, labelling, packaging, distribution and complaint handling or to automate any other aspect of a medical device quality system as described in ISO 13485.
- A new standard for health software covering all parts of the life cycle was started in 2016, *ISO 81001-1 Health software and health IT systems safety, effectiveness and security – Part 1: Foundational principles, concepts, and terms.* A committee draft for comment will be circulated in 2017. The standard is planned to be published in 2020.
- AAMI is working on a multi-part standard for health software and health IT. These standards are intended for HIT products that are not regulated by the FDA but that are (or may be in the future) certified under ONC rules. Four parts have begun work:
    - AAMI HIT1000-1, Health IT software and systems — Part 1: Fundamental concepts and principles

      This part of the standard has been circulated for vote as a provisional US standard.
    - AAMI HIT1000-2, Health IT software and systems — Part 2: Application of quality systems principles and practices
    - AAMI HIT1000-3, Health IT software and systems — Part 3: Application of risk management
    - AAMI HIT1000-4, HIT1000-4, Health IT software and systems — Part 4: Application of human factors engineering

  Drafts will be circulated in 2017. Publication is hoped to be in 2017 and 2018. Part 1 has been approved as a provisional US standard. Comments were resolved and the updated document will be published as a provisional standard late in 2017. Part 3 is expected to be circulated for ballot as a provisional standard early in 2018.
- 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*. A committee draft for comment will be circulated in 2017. The expected date of publication is January, 2020. The working group will meet in November. Work to restructure the standard as a process standard will begin at that meeting.
- IEC 80001-2-9 *Application of risk management for IT-networks incorporating medical devices - Part 2-9: Application guidance - Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities* has been published. This TR shows how a security assurance case can be used to demonstrate confidence that 80001-2-2 security capabilities have been achieved.

- A European Standard for application of ISO 9001 by Healthcare Delivery Organizations will be published in 2017.
- Work is continuing on revising ISO/IEC Guide 63. This guidance gives recommendations and requirements on how to include safety aspects using risk management in standards for medical devices. The work is to reflect current developments in applying risk management to medical devices considering the concepts in ISO/IEC Guide 51:2014 and ISO 31000:2009. A second committee draft was circulated in April.
- ISO 14971 and ISO/TR 24971 will be revised beginning in 2017. ISO 14971 will be revised with the following plan:

    1) maintain the concepts of and the approach to risk management,

    2) clarify the normative requirements, particularly concerning the following topics:

        - production and post-production information,
        - clinical benefits and risk-benefit analysis,

    3) move guidance in the informative annexes to ISO/TR 24971, *Medical devices -- Guidance on the application of ISO 14971*,

    4) keep the annex with the rationale in ISO 14971, *Medical devices -- Application of risk management to medical devices,*

    5) no change in scope

    6) with a 36 month track (expected publication would be in 2019),

    In addition, the the following items will be considered in the revision of ISO 14971:

    1) include references to ISO/TR 24971 and IEC/TR 80002-1, *Medical device software -- Part 1: Guidance on the application of ISO 14971 to medical device software*;

    2) Clarify the relationship with 62366-1, *Medical devices -- Part 1: Application of usability engineering to medical devices,*

    3) Consider to harmonize the vocabulary with ISO 31000, *Risk management -- Principles and guidelines ,* where appropriate,

    4) Address data privacy and security.

    ISO/TR 24971 will be revised with the following plan:

    1) update the guidance ISO/TR 24971,

    2) merge and update guidance from informative annexes of ISO 14971,

    3) no change in scope,

    4) with a 36 month track (expected publication would be in 2019)

    The joint working group responsible for 14971 and 24971 met in Israel in February to begin work on the revisions. The joint working group met again in June and has a working draft. They plan to meet again late in 2017 and complete the initial committee draft. Committee drafts of ISO 14971 and ISO 24971 have been circulated for comment in December.

- A second amendment to IEC 60601-1 has been started. 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. Committee drafts for comment should be circulated in 2017. A fourth edition of 60601-1 will be started following the completion of the amendment and will be scheduled for completion in 2024. Discussions about the structure of the fourth edition will likely begin in 2017 and decisions made before work is started on the fourth edition. Committee drafts for comment have been circulated.

- Agreement to amend IEC 62366-1 has been reached. The amendment seeks to correct multiple, significant inaccuracies, while strictly limiting modifications to the standard to corrections. It is intended that there be no fundamental changes to the USABILITY ENGINEERING PROCESS as originally conceived in 62366-1. Work on the amendment will start in March. The amendment is planned to be published by mid-2019. A first committee draft for review has been circulated.
- IEC has agreed to develop a standard on environmentally conscious design related to refurbishment/remanufacturing of medical devices.
- AAMI is revising HE75, Human factors engineering – Design of medical devices. A draft for ballot has been circulated.
- The EU Medical Device Regulation and IVD regulation have been approved. The MDR will have a transition period of three years and the IVDR will have a transition period of five years.
- The EU has proposed a new regulation on Cybersecurity. While this regulation is not specific to the health sector, health is mentioned as being critical infrastructure in the proposal. The proposal would provide a revised mandate, objectives and tasks for ENISA, the "EU Cybersecurity Agency". Among these new tasks are to facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products and services. And to support and promote the development and implementation of the EU policy on cybersecurity certification of ICT products and services. The framework for an EU cybersecurity certification is established in this proposed regulation.
- Work on the UL/AAMI 2800 series of standards on medical device interoperability will continue in 2017. It is unclear when drafts will be available for public review and when the first standards might be published. A working draft for the first part of this series of standards has been created. A public committee draft for comments is expected in 2018.
- 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. A working draft of this standard is now available.
- UL has begun developing a series of standards on security, UL 2900. The first of these will be published in 2017.

  UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

  This standard describes requirements regarding the vendor's risk management process for their product; methods by which a product's software shall be evaluated and tested for the presence of vulnerabilities, software weaknesses malware; and requirements regarding the establishment and testing of security risk controls in the architecture and design of a product. This is not a medical device specific standard, but will be referenced by the parts of the series that are intended for medical devices. The standard has been adopted as an ANSI US standard and is expected to be recognized by the FDA in their next update of recognized standards.

  UL 2900-2-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare Systems

  This standard describes the method by which the security risk controls of healthcare system components shall be evaluated and tested for known vulnerabilities, software weaknesses and malware while also establishing a foundational set of verification activities intended to reduce the likelihood of exploitable weaknesses that could be vectors of zero day vulnerabilities that may affect the component. The requirements of UL 2900-2-1 focus on promoting a "defense-in-depth" strategy aimed at reducing the likelihood of a malicious user finding vulnerabilities at communication interfaces, reducing the likelihood of a malicious user accessing critical aspects of the product when a vulnerability is found, and reducing the likelihood of a malicious user increasing their level of access to other products or system assets in case of a successful breach. This standard is in the process to be adopted as an ANSI US national standard.
- Discussions at recent international standards meetings make it clear that medical device cybersecurity standards will be started next year. The exact form of these standards is not yet determined, but will be decided in 2017. Standards addressed to manufacturers may include development process, development risk management and post-market process. Proposals being considered (as of April 2017) include:
  - Guideline for authentication framework of the networked smart healthcare devices
  - Application of privacy management to Personal Health Information
  - Product life cycle activities for product security

  Germany has announced that it will propose 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 will
  - 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

Approval to start work on the standard is expected in the first half of 2018.

- 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.
- A proposal to begin work on a new standard in the area of environmental design has been approved. Work will begin on *IEC 63120 ED1 Environmental conscious design of medical electrical equipment – Particular requirements for refurbishment of medical electrical equipment and systems, for re-use of parts, for a management of critical or hazardous substances contained in medical electrical equipment and systems and for a closed loop Business-to-Business take back system* with a first draft expected in early 2018 and publication planned for 2020. The rationale for this standard is that eco-design regulations require manufacturers on a global basis to decrease the environmental impact of their products. Globally many regulators have adopted ambitious Circular Economy plans, which include revised legislative proposals on waste to stimulate the transition towards a circular economy which is intended to boost competitiveness, foster sustainable economic growth and generate new jobs. By setting internationally accepted standards, manufacturers do not have to navigate through multiple national regulations when launching their products on the market.
- Many system and software engineering standards continue to be developed or revised. These standards are not used in medical device regulation, but may be useful to use as guidance to provide evidence that state of the art process and practices were used in developing a medical device.
- AAMI is working on a standard for classifying software defects in health software. A committee draft for vote was circulated in April.
- CEN will begin work on a new technical specification for health apps. This European Technical Specification will provide a set of requirements for developers of health and wellness apps, intending to meet the needs of health care professionals, patients, carers and the wider public. It will include a set of quality criteria and cover 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 will also address fitness for purpose and the monitoring of usage. This new work will be based on BSI PAS 277 and will be developed in such a way that it may be incorporated into the 82304 series by ISO and IEC.
- NIST has circulated a draft revision of its *Framework for Improving Critical Infrastructure Cybersecurity* for comments. Version 1.1 of the Cybersecurity Framework refines, clarifies, and enhances Version 1.0 issued in February 2014.

Standards Navigator New Documents in November and December 2017

Medical device software

- No new documents this month.

Medical Devices

- A committee draft of the revision of *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. The defined terms are updated and many are derived from ISO/IEC Guide 63:20xx. More attention is given to the benefits that are expected from the use of the medical device. It is explained that the process described in ISO 14971 can be used for managing all risks associated with the medical device. Several informative annexes are moved to the guidance in ISO/TR 24971.

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

- A committee draft of the revision of *ISO 24971 Medical devices - Guidance on the application of ISO 14971* 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, Medical devices — Application of risk management to medical devices. It provides guidance on the application of ISO 14971 for a wide variety of medical devices. These medical devices include active, non-active, implantable, and non-implantable medical devices and in vitro diagnostic medical devices. The members of JWG1 are aware that this CD needs further work, but decided to distribute this draft along with ISO/CD 14971 for review and comments. It is the intention of JWG1 to circulate a second Committee Draft in 2018 together with the Draft International Standard ISO/DIS 14971.

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

- *ISO/IEC Guide 63 Guide to the development and inclusion of aspects of safety in International Standards for medical devices* has been circulated for comment. ISO/IEC 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 sectorial guide is based on risk management principles and ISO/IEC Guide 51:2014 to address the needs of the medical device sector. The defined terms in ISO 14971 are taken from Guide 63. The final draft of Guide 63 will be voted on after comments on the CD of ISO 14971 have been resolved.

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

Health IT and mobile health applications

- No new documents this month.

Medical device and Health Security

- A draft of a new revision of the *NIST Framework for Improving Critical Infrastructure Cybersecurity* has been circulated for comment. This draft revision refines, clarifies, and enhances Version 1.0 issued in February 2014.

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

Software Engineering and Information Technology

- A Committee Draft (CD) of *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.

  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
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.
	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.

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
AAMI SW 96 CD	Medical Devices	Manufactures	AAMI SW 96 Application of security risk management for medical devices. This standard follows a similar risk management process as that defined in ISO 14971. The manufacturer shall use this process for identifying vulnerabilities associated with a medical device, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls. This process shall include the following elements: security risk analysis; security risk evaluation; security risk control; production and post-production information.
ISO/IEC/IEEE 29148 DIS	Medical Devices	Manufacturers	ISO/IEC/IEEE 29148 Systems and software engineering — Life cycle processes — Requirements engineering. This International Standard contains provisions for the processes and products related to the engineering of requirements for systems and software products and services throughout the life cycle. It defines the construct of a good requirement, provides attributes and characteristics of requirements, and discusses the iterative and recursive application of requirements processes throughout the life cycle.
ISO/IEC 26553 DIS	Systems & software	Manufacturers	ISO/IEC 26553 Software and systems engineering – Tools and methods for product line realization This document, within the context of tools and methods of detailed design and implementation for software and system product lines: • provides the terms and definitions specific to realization for software and systems product lines. • defines processes performed during product line realization. Those processes are described in terms of purpose, inputs, tasks, and outcomes. • defines method capabilities to support the defined tasks of each process. • defines tool capabilities to automate/semi-automate tasks or defined method capabilities. This document concerns processes and capabilities of realization tools and methods for a family of products, not for a single system. This is a draft for vote.

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/IEC 26554 DIS	Systems & software	Manufacturers	ISO/IEC 26554 Software and systems engineering – Tools and methods for product line testing This document, within the context of tools and methods of detailed design and implementation for software and system product lines: • provides the terms and definitions specific to testing for software and systems product lines; • defines processes performed during product line testing. Those processes are described in terms of purpose, inputs, tasks, and outcomes; • defines method capabilities to support the defined tasks of each process; • defines tool capabilities to automate/semi-automate tasks or defined method capabilities. This document concerns processes and capabilities of testing methods and tools for a family of products, not for a single system. This is a draft for vote.
ISO/IEC 26556 DIS	Systems & software	Manufacturers	ISO/IEC 26556 Software and systems engineering – Tools and methods for product line organizational management This document within the methods and tools of organizational management for software and systems product lines: • enables the users of this standard to holistically understand, adopt, and enact the processes, tools, and methods for product line organizational management. And this standard helps the users evaluate and select relevant tools and methods based on business and user-related criteria. • helps product line engineers, developers, and tool vendors make informed about capabilities of tools and methods that are required for supporting product line implementation from organizational aspects. • provides product line-specific processes and capabilities of tools and methods in organizational management. This document concerns processes and capabilities of methods and tools for organizational management for a family of products, not for a single system. This is a draft for vote.