SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

12-September-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. They hope to have another draft by early in 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.
- 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.
- 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.
- 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.
- 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.
- 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
- 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.

Standards Navigator New Documents in August 2017

Medical device software

- No new documents this month.

Medical Devices

- No new documents this month.

Health IT and mobile health applications

- No new documents this month.

Medical device and Health Security

- No new documents this month.

.**Software Engineering and Information Technology**

- A Committee Draft of *ISO/IEC 90003 Software Engineering — Guidelines for the application of ISO 9001:2015 to computer software* has been circulated for vote. This version of ISO/IEC 90003 aligns it with the latest version of ISO 9001 which was published in 2015. This International Standard provides guidance for organizations in the application of ISO 9001:2015 to the acquisition, supply, development, operation, and maintenance of computer software. It identifies the issues that should be addressed and is independent of the technology, life cycle models, development processes, sequence of activities, and organizational structure used by an organization. The guidance and identified issues are intended to be comprehensive but not exhaustive.

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

- A Committee Draft of *ISO/IEC/IEEE 21841 Systems and software engineering — Taxonomies of systems of systems* has been circulated for vote. The purpose of this standard is to define normalized taxonomies for systems of systems (SoS) to facilitate communications among stakeholders. It also briefly explains what a taxonomy is and how it applies to the SoS to aid in understanding and communication.

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

- A working draft of a revision of ISO/IEC/IEEE 16085 Systems and software engineering — Life cycle processes — Risk management has been circulated for comment. This International Standard provides a universally applicable standard for practitioners responsible for managing risks associated with systems and software engineering projects and programs over their life cycle. It is suitable for the management of all risks encountered in any type of systems or software

engineering project or program regardless of context, type of industry, technologies utilized, or organizational structures involved. This standard does not provide detailed information about risk management processes, practices, techniques, or tools which are widely available in other publications, but instead focuses on providing a comprehensive reference for integrating the large and wide variety of processes, practices, techniques, and tools encountered in complex systems and software engineering projects and programs into a holistic system for risk management, with the purpose of providing effective and efficient risk management meeting the expectations and requirements of project/program stakeholders.

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

- A second Committee Draft of *ISO/IEC 25030 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) – Quality requirements* has been circulated for vote. This International Standard provides requirements and recommendations for the processes and methods of specifying and documenting quality requirements. This document is the umbrella standard on quality requirements, which includes not only how to define and what to define on quality requirements, but also, for quality in use and product quality, detailed steps to define them, and requirements and guides for using and governing them.

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

- A second Committee Draft of *ISO/IEC 25020 Systems and Software Engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality Measurement* has been circulated for vote. This document gives a guide to select an appropriate quality model among the models defined in ISO/IEC 2501n, which are system and software product quality, data quality, quality in use and IT service quality of SQuaRE.

  This document contains the following:

  - quality measurement reference model;
  - relationship between different types of quality measures;
  - selecting quality measures;
  - constructing quality measures;
  - planning and performing the measurement;
  - interpreting the measurement result.

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

- A Draft International Standard (DIS) of *ISO/IEC 26553 Software and systems engineering – Tools and methods for product line realization* has been circulated for vote. 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.

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

- A Draft International Standard (DIS) of *ISO/IEC 26554 Software and systems engineering – Tools and methods for product line testing* has been circulated for vote. 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.

  The draft standard is available on the SoftwareCPR Standards Navigator web page.
- A Draft International Standard (DIS) of *ISO/IEC 26556 Software and systems engineering – Tools and methods for product line organizational management* has been circulated for vote. 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.

  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
IEC 60601-1_A2 CD	Medical Devices	Manufacturers	Amendment 2 of IEC 60601-1:2005 Medical electrical equipment – Part 1: General requirements for safety and essential performance Amendment 2 addresses high priority issues identified in the third edition of 60601-1 published in 2005 and the first amendment to 60601-1 published in 2012.
IEC 60601-1-2_A1 CD	Medical Devices	Manufacturers	Amendment 1 of IEC 60601-1-2:2014 Medical electrical equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral Standard: Electromagnetic disturbances – Requirements and tests Amendment 1 addresses high priority issues identified in the fourth edition of 60601-1-2 published in 2014.
IEC 60601-1-6_A1 CD	Medical Devices	Manufacturers	Amendment 2 of IEC 60601-1-6:2010 Medical electrical equipment – Part 1-6: General requirements for basic safety and essential performance – Collateral standard: Usability Amendment 2 addresses high priority issues identified in the third edition of 60601-1-6 published in 2010 and the first amendment to 60601-1-6 published in 2013.
IEC 60601-1-8_A2 CD	Medical Devices	Manufacturers	IEC 60601-1-8:2006 Medical electrical equipment – Part 1-8: General requirements for basic safety and essential performance – Collateral Standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems Amendment 2 amendment addresses high priority issues identified in the second edition of 60601-1-8 published in 2006 and the first amendment to 60601-1-8 published in 2012.

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
IEC 60601-1-10 A2 CD	Medical Devices	Manufacturers	Amendment 2 of IEC 60601-1-10:2007 Medical electrical equipment – Part 1-10: General requirements for basic safety and essential performance – Collateral Standard: Requirements for the development of physiologic closed-loop controllers Amendment 2 addresses high priority issues identified in the first edition of 60601-1-10 published in 2007 and the first amendment to 60601-1-10 published in 2013.
IEC 60601-1-11 A1 CD	Medical Devices	Manufacturers	Amendment 1 of IEC 60601-1-11:2015 Medical electrical equipment – Part 1-11: General requirements for basic safety and essential performance – Collateral Standard: Requirements for medical electrical equipment and medical electrical systems used in the home healthcare environment Amendment 1 addresses high priority issues identified in the first edition of 60601-1-11 published in 2015.
IEC 62366-1 A1 CD	Medical Devices	Manufacturers	Amendment 1 of IEC 62366-1:2015 Medical devices – Part 1: Application of usability engineering to medical devices Amendment 1 addresses high priority issues identified in in the first edition of IEC 62366-1 published in 2015 while making no fundamental changes to the usability engineering process as originally conceived in IEC 62366-1:2015.
ISO TS 20405 DIS	Health IT	Healthcare Delivery Organizations	ISO TS 20405 Health informatics – Framework of event data and reporting definitions for the safety of health software This Technical Specification provides a model framework for improving the surveillance and reporting of events with respect to the safety of health software. The Technical Specification defines those data elements needed for identification of particular events including incidents, near-misses and unsafe conditions, as well as outlines good principles, relevant concepts and a process model for the recording, analysis and reporting of event-specific information related to the safety of health software

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 HIT1000-1 CDV	Health IT	Manufacturers and Healthcare Delivery Organizations	AAMI HIT1000-1 Health IT Software and Systems – Part 1: Fundamental concepts and principles This part of AAMI1000 identifies the fundamental concepts and principles for creating, integrating and implementing health IT software and health IT systems to maintain safety, security and effectiveness.
ISO/IEC 29155-1 FDIS	IT	Manufacturers	This document identifies a framework for information technology (IT) project performance benchmarking (e.g. development or maintenance productivity) and related aspects (e.g. data collection and software classification). The framework consists of activities and components that are necessary to successfully identify, define, select, apply, and improve benchmarking for IT project performance. This is a final draft for approval.
ISO/IEC 24748-2 DIS	Software Engineering	Manufacturers	This part of ISO/IEC 24748 is a guideline for the application of ISO/IEC/IEEE 15288:2015. It addresses system, life cycle, organizational, project, and process, concept application, principally through reference to ISO/IEC 24748-1 and ISO/IEC/IEEE 15288:2015. This is a draft for vote.
ISO 25065 CD	Software Engineering	Manufacturers	*ISO 25065 Systems and software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for Usability: User requirements specification*. This document defines the Common Industry Format (CIF) for specifying user requirements for the user interfaces of interactive systems. This document specifies the contents of a User Requirements Specification for the user interface and the format for stating requirements. This is a draft for comment.