SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

15-August-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

- Drafts of the revisions of ISO 14971 and ISO/TR 24971 have been circulated.
- The request to adopt the requirements of IEC 62368-1 as an alternative design solution to IEC 60950-1 for means of operator protection in 60601-1 amendment 2 was approved. This change had been planned for the next edition of IEC 60601-1, but concerns have risen that component manufacturers may begin adopting IEC62368-1 and IEC 60950-1 compliant devices may not be available. The decision to make this change may result in the amendment to IEC 60601-1 being delayed past its expected completion date in 2019.

Cybersecurity

- A proposal has been circulated for a new standard for activities in the product lifecycle of health software (including software as/in a medical device) for the information security of the product. This standard will be consistent with the perspective and structure of IEC 62304 and it will extend the artefacts and activities described in IEC 62304 by those which are related to information security in the product lifecycle. In this respect, no new technical requirements will be specified, but existing technical measures for security in the product lifecycle will be added to the activities known from IEC 62304. A committee draft of the standard is planned for the end of 2018, with publication of the International Standard by the end of 2020.
- A technical report has been proposed to provide an overview of security and privacy requirements for Electronic Health Records (EHR) in a cloud computing service environment. This proposal will be circulated to ISO and IEC national members for approval to initiate work in the next few months. No working draft has been circulated at this time.
- A new IEC technical report on safety related technical security specifications for medical devices has been proposed for the IEC 60601-1 series. This proposed document draws heavily from the IEC 62443 series of standards for security of Industrial Automation and Control Systems (IACS) with appropriate terminology changes.

Health IT

- A first draft has been circulated of a new standard that 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.

Standards Navigator New Documents in July 2018

Medical device software

- No new documents this month.

Medical Devices

- A committee draft for vote of the 3rd edition of *ISO 14971 Application of risk management to medical devices* has been circulated. This third edition cancels and replaces the second edition, which has been technically revised. The main changes compared to the previous edition are as follows:
  - A clause on normative references is included, following the requirements of ISO-IEC Directives, Part 2.
  - The defined terms are updated and many are derived from ISO/IEC Guide 63:20xx. A definition of benefit is introduced.
  - More attention is given to the benefits that are expected from the use of the medical device. The term benefit-risk analysis is aligned with terminology used in some regulations.
  - It is explained that the process described in ISO 14971 can be used for managing all types of risks associated with medical devices, including those related to data and systems security.
  - The method for the evaluation of the overall residual risk and the criteria for its acceptability must be defined in the risk management plan. The method can include gathering and reviewing data and literature for the medical device and similar devices on the market. The criteria for the acceptability of the overall residual risk can be different from the criteria for acceptability of individual risks.
  - The requirements to disclose residual risks are merged into one requirement, after the overall residual risk has been evaluated and judged acceptable.
  - The review before commercial distribution of the medical device concerns the execution of the risk management plan. The results of the review are documented as the risk management report. The manufacturer must determine when subsequent reviews and updates of the risk management report are needed.
  - The clause on production and post-production information is clarified and restructured. More detail is given on the information to be collected and the actions to take when the information is determined to be relevant to safety.
  - Several informative annexes are moved to the guidance in ISO/TR 24971, which has been revised in parallel. More information and a rationale for the requirements in this third edition of ISO 14971 is provided in Annex A. The correspondence between the clauses of the second edition and those of this third edition is given in Annex B.

    The draft standard is available on the SoftwareCPR Standards Navigator web page.
- A committee draft for comment of the second edition of *ISO 24971 Guidance on the application of ISO 14971* has been circulated. This second edition cancels and replaces the first edition, which has been technically revised. The main changes compared to the previous edition are as follows:
  - The clauses of ISO/TR 24971:2013 and some informative annexes of ISO 14971:2007 are merged, restructured, technically revised, and supplemented with additional guidance.

- To facilitate the use of this document, the same structure and numbering of clauses and subclauses as in ISO 14971:20XX is employed. The informative annexes contain additional guidance on specific aspects of risk management.

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

Health IT and mobile health applications

- A first committee draft for comment of *ISO 81001-1 Health software and health IT systems safety, effectiveness and security — Part 1: Foundational principles, concepts and terms* has been circulated. 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.

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

Medical device and Health Security

- A proposal for a new standard, *IEC 80001-5-1 Application of risk management for IT-networks incorporating medical device – Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software - Part 5-1: Activities in the product lifecycle* has been circulated for a vote on whether to initiate work on this standard. The proposed standard will be structured according to the existing health software lifecycle standards IEC 62304, yet it will specify activities towards information security (rather than product safety). It will not copy specific security methods or techniques but refer to clauses in existing and established information security standards.

The proposal and working draft of the standard are available on the SoftwareCPR Standards Navigator web page.

- A proposal for a new part in the IEC 60601 series has been circulated for vote on whether it is needed. *IEC 60601 Part 4-5: Guidance and interpretation – Safety related technical security specifications for medical devices.* This document provides detailed technical recommendations for Medical Devices used in Medical IT Networks associated with the seven foundational requirements (FRs) described in IEC 62443-1-1. This document defines recommendations for Medical Device capability security levels (SL-C).

The proposal and working draft of the standard are 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 11633-1 FDIS	Security	Manufacturers/ HDOs	*ISO 11633-1 Health informatics -- Information security management for remote maintenance of medical devices and medical information systems -- Part 1: Requirements and risk analysis*. This document focuses on remote maintenance services (RMS) for information systems in healthcare facilities as provided by vendors of medical devices or health information systems. When RMS is implemented, the RMS provider and the healthcare facility should jointly perform and reach agreement on a risk analysis for the RMS implementation. This is a draft for vote.
ISO 22696 NP	Security	Manufacturers/ HDOs	*ISO 22696 Guidance for identification and authentication for connectable PHDs*. This document includes guidance for identification and authentication between the bidirectionally connected PHD and gateway by providing possible use cases and associated threats and vulnerabilities. Since some smart devices with mobile healthcare apps and software may connect to the healthcare service network, these devices will be considered as connectable PHDs in this document. This is a proposal for vote.
IEC Guide 120 CDV	Security	Standards writers	*IEC Guide 120 Security Aspects – Guidelines for their inclusion in publications.* The target audience for this document is standards writers. This document provides guidelines on the security topics to be covered in IEC publications, and aspects of how to implement them. These guidelines can be used as a checklist for the combination of publications used in implementation of systems. This is a final draft for vote. This is a draft for vote.