Medical Device Software Standards for Safety and Regulatory Compliance

Sherman Eagles

+1 612-865-0107
seagles@softwarecpr.com
www.softwarecpr.com
Assuring safe software

SAFE

All hazards have been addressed

Adequate process has been implemented (compliance with standards is often considered a demonstration of adequate process.)

Risks have been reduced to acceptable levels

Process is effective

IEC 62304
AAMI TIR 45
IEC 80002-1
IEC 60601-1
IEC80001
IEC 62304 background

- Specifically created for medical device software
- IEC 60601-1-4 and general software engineering standards were not considered adequate
- Significant FDA involvement from start
- Scope includes “stand-alone software” and “embedded software”
- Based on ANSI/AAMI/SW68 with a few significant differences
- Omits requirements duplicated elsewhere (QMS)
- Adds requirements considered essential for medical devices (safety aspects)
Status of IEC 62304

- Approved by both IEC and ISO as an international standard (joint development effort)
- Adopted by CENELEC as EN and harmonized 11/08 under the MDD, AIMDD and IVDD
- Adopted by ANSI as US national standard (replacing ANSI/AAMI/SW 68)
- Recognized by FDA for use in premarket submissions
- China – SFDA adopted 62304
- Translations exist in French, German, Spanish, Chinese and Japanese
- Adopted as a Japan Industry Standard
62304 philosophy

- Safe medical device software requires risk management, quality management and good software engineering
- Good software engineering requires critical thinking – can’t be done by checklist
- Manufacturers know more about their products than regulators
- The variety of medical devices requires a variety of approaches – one size does not fit all
- Resources should be used on what is important
- A standard should have minimum requirements, not best practices
IEC 62304 - What is it?

- A framework – processes, activities and tasks
  - Process is the top level, a process has activities and an activity has tasks. Specific requirements in IEC 62304 are generally at the task level.
- Identifies requirements for what needs to be done and what needs to be documented
- Specifies a software safety classification system
  - additional requirements apply as safety classification increases
IEC 62304 - What is not in it?

- Does not prescribe how to accomplish requirements
  - Not a “how to” with defined methods or practices
- Does not require a specific software life cycle
- Does not specify documents
  - What to document, not where it must go.

- All of these decisions are left to the manufacturer
IEC 62304 - Key concepts

- Quality management and risk management are necessary for safe medical device software
- Software safety is classified according to severity of potential harm
- There are different requirements based on software safety classification
IEC 62304 - Key concepts

- Software systems may be partitioned and the partitions assigned different software safety classifications

- The software life cycle doesn’t end with product release
IEC 62304 Lifecycle

- IEC 62304 is a standard on lifecycles, however
  - It does not define a specific lifecycle model
  - It does not define specific documents
- It does define processes and activities that must be included in a conforming lifecycle
- It implies dependencies between processes
Life cycle principles

- Process outputs should be maintained in a consistent state
  - A change in an output requires related outputs to be updated
- Process outputs should be available when needed as input
- Before release of software, all process outputs should be consistent and all dependencies met
1. Scope
2. Normative References
3. Terms & Definitions
4. General Requirements
5. Development Process
6. Maintenance Process
7. Risk Management
8. Configuration Mgmt
9. Problem Resolution

- Annex A – Rational for Safety Class Activities & Tasks
- Annex B – Guidance
- Annex C – Relationship to other standards
- Annex D – Implementation in a formal Quality System
Two types of requirements

- Process requirements which are necessary to determine the RISKS arising from the operation of each SOFTWARE ITEM in the software;
- Process requirements which are necessary to achieve an appropriately low probability of software failure for each SOFTWARE ITEM, chosen on the basis of these determined risks.
IEC 62304 - Process requirements

- Process requirements differ for different software safety classifications
- All classes – requirements needed for risk management or software safety classification
- Class B and C – requirements that enhance the confidence in the reliability of the software or support the correction of safety-related problems
62304 Software Safety Classification

Software System Overall

- Class A: No injury or damage to health is possible
- Class B: Non-serious injury is possible
- Class C: Death or serious injury is possible

Classification shall be documented.

Software System may have lower worst case risk than device overall, but cannot be higher.

- Both direct and indirect harm are included
- Class C is the default assumption
Navigating 62304

- Each normative section with an asterisk in the title has a corresponding explanatory section in Annex B.
- Annex B can be very helpful in interpreting the main body of the standard.
- Annex C provides comparison to other standards.
  - C.1 13485
  - C.2 14971
  - C.3 60601-1
  - C.4 60601-1-4
  - C.5 12207
- Annex D – Implementation into a Quality System
ANSI/AAMI/IEC 62304:2006

- Development
- Maintenance
- Risk Management
- Configuration Management
- Problem Resolution
Software item

- Any structural part of the software. The top level is called the software system. The lowest level is called the software unit.
SOUP

- Software of unknown provenance
  - Commercial off the shelf software
  - Public domain software
  - Legacy software components with limited information on development process or inadequate process
- Called OTS or COTS in other standards
“As Appropriate”

- Where “as appropriate” is used, the intention is that it shall be done unless there is a documented justification for not doing it.
  - “as appropriate” is used a lot in IEC 62304 to provide an escape for having to do things that don’t make sense for a specific device. But, there must be a documented justification!
IEC 60601-1

Medical Electrical Equipment - General requirements for basic safety and essential performance
Where does IEC 60601-1 fit?

- A product safety standard
- Includes requirements for products that are programmable electrical medical systems (PEMS)
- PEMS decompose into programmable electrical sub-systems (PESS)
- Software is a PESS
- PEMS requirements apply to software (but also to any hardware developed for the PEMS)
When the PEMS clause applies

- PEMS requirements do not apply if the PESS provides no safety function
- PEMS requirements do not apply if it can be shown using 14971 that the failure of the PESS does not lead to unacceptable risk
- All PEMS requirements apply to software

62304 is required in the first amendment to 60601-1
Scope: Medical Devices containing software

- Many of the same techniques used to assure software reliability and quality are relevant to assuring software safety. This report does not discuss general aspects of software quality assurance. Rather it is intended to highlight and explain approaches to assuring that software safety is adequately addressed ... part of an overall software quality assurance process.

Outside Scope

- production or assembly line software
- software tools (e.g. quality assurance systems)
IEC TR 80002-1

- Medical Device Software - Part 1: Guidance on the application of ISO 14971 to medical device software

- Clause structure follows ISO 14971 – for each risk management activity of ISO 14971 additional guidance is provided for software

- Published by IEC in September, 2009
AAMI TIR 45
AAMI TIR 45 Guidance on the use of agile practices in the development of medical device software.
TIR 45 Scope

- provides perspectives on the application of AGILE during medical device software development. It relates them to the following existing standards, regulations, and guidance:
  - ISO 13485:2003,
  - IEC 62304,
  - ISO 14971:2007
  - FDA regulations and software guidance
IEC 80001 series
An international effort

80001 approach

- Establish a framework for maintaining patient safety, technology effectiveness and data security when the point of care is a network node and network use and technology rapidly change
- Utilize this framework to manage risk when changes are made to the network
What properties need to be ensured?

- From IEC 80001-1
- Risk management should be applied to address the following key properties ...:
  - safety;
  - effectiveness (ability to achieve the intended result for the patient and the responsible organization); and
  - data and system security
Who is needed?

- Responsible organization management
- Network integrators and maintainers
- Clinical engineers
- Medical device manufacturers
- Non-medical network technology vendors

None of these parties can address the problem alone, problem solution for networks incorporating medical devices must be shared in a partnership or federated model.
What is a medical device manufacturer required to do?

- If the device is intended to connect to a network, provide information on:
  - Characteristics necessary to make the connection to support the device
  - Security specifications
  - Intended information flow to other medical devices or applications
  - Hazardous situations resulting from a failure of the IT network

- These are equivalent to the requirements in IEC 60601-1:2005 clause 14.13
New challenges

● Supporting the hospital after sale of the device
  – Additional information for hospital risk management
  – Support for virus protection/security updates and patches
  – Defined joint responsibility agreement

● Who will be responsible for these things for the medical device manufacturer?
How will IEC 80001-1 help?

- Will provide an approach that identifies roles, responsibilities and process necessary to address converging technologies
- Will define standardized roles, risk management process and information to allow effective sharing of experiences
- If used widely, will standardize how medical device manufacturers and IT vendors provide information to hospitals
IEC guidance documents

- Four guidance documents are available
  - Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples
  - Guidance for the communication of medical device security needs, risks and controls
  - Guidance for wireless networks
  - Implementation guidance for Healthcare Delivery Organizations

- Additional guidance documents being developed
  - Guidance for distributed alarm systems
  - Self-assessment of IEC 80001-1 in the hospital
  - Security requirements and assurance
Changes to IEC 62304
Revision of IEC 62304

- Initiated in 2012
- Planned publication date of October 2015
  - Working group hopes to be early
- Recommended changes were to scope, software safety classification, legacy software, removal of common defects, addition of an annex on capability maturity assessment and various improvements and clarifications
IEC 62304 Revision

- Revision of 62304 will be done in 3 parts
  - Amendment to 62304 edition 1
    - Change to software safety classification
    - Requirements for legacy software
    - Miscellaneous clarifications and technical changes
  - Capability assessment will become a separate Technical Report
  - Second edition will expand scope from medical device software to health software
- Amendment to be published by October, 2015
- Assessment TR expected in 2015
- Second edition expected in 2016
IEC 62304 Amendment

Software safety classification

● Needed change because too much software was being classified as Class C

● Changes to software safety classification
  – Uses risk instead of consequence to determine software safety class
  – Applies system level risk management without software risk controls prior to software safety classification
In determining the software safety classification of the SOFTWARE SYSTEM, only risk control measures external to the SOFTWARE SYSTEM shall be considered.

Probability of a software failure shall be assumed to be 1.
Requirements for legacy software

- Legacy software is existing software that was created before EN 62304 was harmonized and has been in use.
- Change is needed because legacy software that is not being changed had to go through 62304 process for CE mark.
- Approach is to define requirements to determine if existing documentation on development process and risk management is sufficient, together with post-market information, to achieve the intent of the standard.
- Use requirements of the standard to develop missing documentation.
IEC 62304 Amendment

- Other technical changes
  - Added a requirement for a process to identify and remove common software defects
  - Added a requirement to include software requirements for network aspects of medical devices on networks
  - Removed some requirements related to documentation, such as “intended audience” and “user documentation”
IEC 62304 Amendment

• Changes to clarify
  – Replace “software product” with “medical device software” throughout the standard
  – Clarified use of terms “system” and “product”
  – Clarified use of “segregate” for risk control
  – Removed inconsistencies in verification requirements
IEC 62304 TR

- Provides a process reference model and a process assessment model to allow assessment of an organization’s capability to implement the intent of 62304
- Intended to be used by manufacturers for process improvement or to assess potential software contract developers
- Utilizes process assessment methods from ISO/IEC 15504
IEC 62304 Edition 2

- Second edition will expand the scope from medical devices to health software
- Requested by CENELEC because of concern that different regulators are treating software differently
  - Don’t want requirements for software executing on medical electrical equipment to be different than for the same software executing on a network server
- Will allow 62304 to be referenced by standalone software product standards (e.g. IEC 82304-1) without qualification
- Development of the second edition will occur in parallel with the amendment to the first edition.
More Changes
The changing environment

- Convergence of medical devices and Health IT
- Driven by mobility and wireless connectivity
  - 160 million wearable wireless devices by 2017
    - Homecare
    - Ambulatory monitoring
    - Point of care
- Smart wireless devices will talk to each other as well as health care systems
- We can no longer manage safety device by device
- The new environment must co-exist with the old
The current regulatory model looks at individual elements
  – Categories with reasonable well-known risks
  – Assumes that if each of the components is safe, the whole will be safe
  – This is a known logical fallacy

Regulations must adapt
  – Regulate the system, not the pieces
    ● Not just FDA
  – This will not happen quickly or consistently
  – Regulations always follow technology
Mobile apps

- FDA has a draft guidance on mobile medical applications
- Final guidance is promised to be available by October
- Guidance proposes to require pre-market submission for some apps
FDA’s view of mobile app regulation

- Patient self-management apps
- Simple tracking or trending apps (not intended for treating/adjusting medication)
- Mobile apps not considered "mobile medical apps"

Proposed focus of oversight

Enforcement Discretion

No regulatory requirements

Most mobile apps that meet "device" definition
Regulatory activities related to standalone health software

- FDA considering a guidance for medical device decision support systems
- US regulatory “framework” for health IT
- International Medical Device Regulators Forum (IMDRF) work on standalone software
FDASIA Section 618

Publish a report by January 2014 that expresses "a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology including mobile medical applications"

- promote innovation,
- protect patient safety, and
- avoid regulatory duplication
Workgroup

- Charged with providing expert input on issues and concepts
  - Types of risk that may be posed by health IT that impact patient safety, the likelihood that these risks will be realized, and the impact of these considerations on a risk-based approach;
  - Factors or approaches that could be included in a risk-based regulatory approach for health IT to promote innovation and protect patient safety; and
  - Approaches to avoid duplicative or overlapping regulatory requirements.
Timing of FDASIA report

- Workgroup completed input in August
- Draft report to be completed by end of September
- Final report to be published in January, 2014
IMDRF standalone software work item

- Added to work program in March 2013
- Purpose is to align regulatory
  - Definitions related to standalone medical software
  - Clarify how risk is determined for standalone medical software
  - Develop a risk-based approach for determining appropriate regulatory requirements which should apply to standalone medical software
Timing for IMDRF work item

- Draft definitions were circulated in July, final expected in November 2013
- Draft for how risk is determined in November, final in March 2014
- Draft for how to determine appropriate regulatory requirements in March, final in September 2013
FDA modification of software pre-market review process

- FDA hired a consulting firm to assess their software pre-market review process
- Consultant looked at FDA review practices and also interviewed industry
- One important finding was that industry does not use modern software engineering practices because of uncertainty in how they will be viewed by FDA reviewers
FDA response to report

- Need for a consistent, transparent review process with clear stages
- Need training program for software reviewers
- Need to collaborate with industry for continuous improvement of software
- Need governance structure that provides focus to software
  - Likely to consolidate all software activities in one office
Next steps for Health Software standards
The changing role of standards

- Standards change faster than law and regulation
  - Standards follow technology, but more quickly than regulation
  - Existing standards can evolve to meet new conditions in a changing environment

- Standards are not constrained to components
  - Standards can be developed for systems
    - For example, IEC 80001-1 addresses both devices and networks

- An architecture for health software standards can recognize multiple stakeholders and shared responsibilities
  - Cover the entire lifecycle
  - Identify transition points where risk is shared
A framework for health software standards
Standards activities in progress

- **IEC 82304-1 Health Software - Part 1: General Requirements for Product Safety**
  - Committee draft circulated and comments received
  - Publication expected in 2015 or 2016

- **IEC 62304 Ed. 2 Health software – Software life cycle processes**
  - Will proceed in parallel with the Amendment to Ed. 1.
  - Working draft being created
  - Publication expected in 2015 or 2016

- **ISO TR 17791 Health informatics — Guidance on standards for enabling safety in health software**
  - Survey of existing standards and gaps
  - Approved, publication in 2013
International standards activities starting and future

- IEC 80001 series, additional guidance
  - 80001-2-5 Guidance for distributed alarm systems
  - 80001-2-6 Guidance for responsibility agreements
  - 80001-2-7 Guidance for self-assessment
  - 80001-2-8 Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

- Aligning definitions and standards architecture for Health-IT and medical device software
  - Report due fall of 2014
Future international standards for health software

- New standards activities to address gaps identified in ISO TR 17791
  - The standards developed from a medical device context provide a working basis for enabling safety in health software design and development.
  - Multiple gaps exist in the standards needed for enabling safety in health software implementation and operation.
    - Human factors during network implementation and operation
    - Application of safety in clinical workflow design
    - Network integration and configuration
    - Verification and test of configuration of software
    - Additional development, implementation and operational aspects
Increasing focus on medical device security
US GAO report

- Government Accounting Office studied FDA review of medical device security at request of Congress

- Report issued in 2012 found that FDA had the authority to regulate security related to safety but was not doing it consistently
FDA Draft Guidance on Pre-market review of Cybersecurity

- Released in 2013
- Provides guidance on what cybersecurity information FDA wants to see from medical device manufacturers in a pre-market review
- FDA has also indicated that it will provide guidance on when a cybersecurity vulnerability should be reported and when a vulnerability will result in a recall
Medical Device Security standards activities

- IEC 80001-2-x Guidance on standards for establishing the security capabilities identified in IEC/TR 80001-2-2
- AAMI TIR on medical device security best practices
Thank You

Sherman Eagles
SoftwareCPR
seagles@softwarecpr.com
+1-612-865-0107