Best practices in focus: Notified body auditors and reviewers reflect on medical software auditing

Peter Kramar, PhD

Vienna, 17. 10. 2023

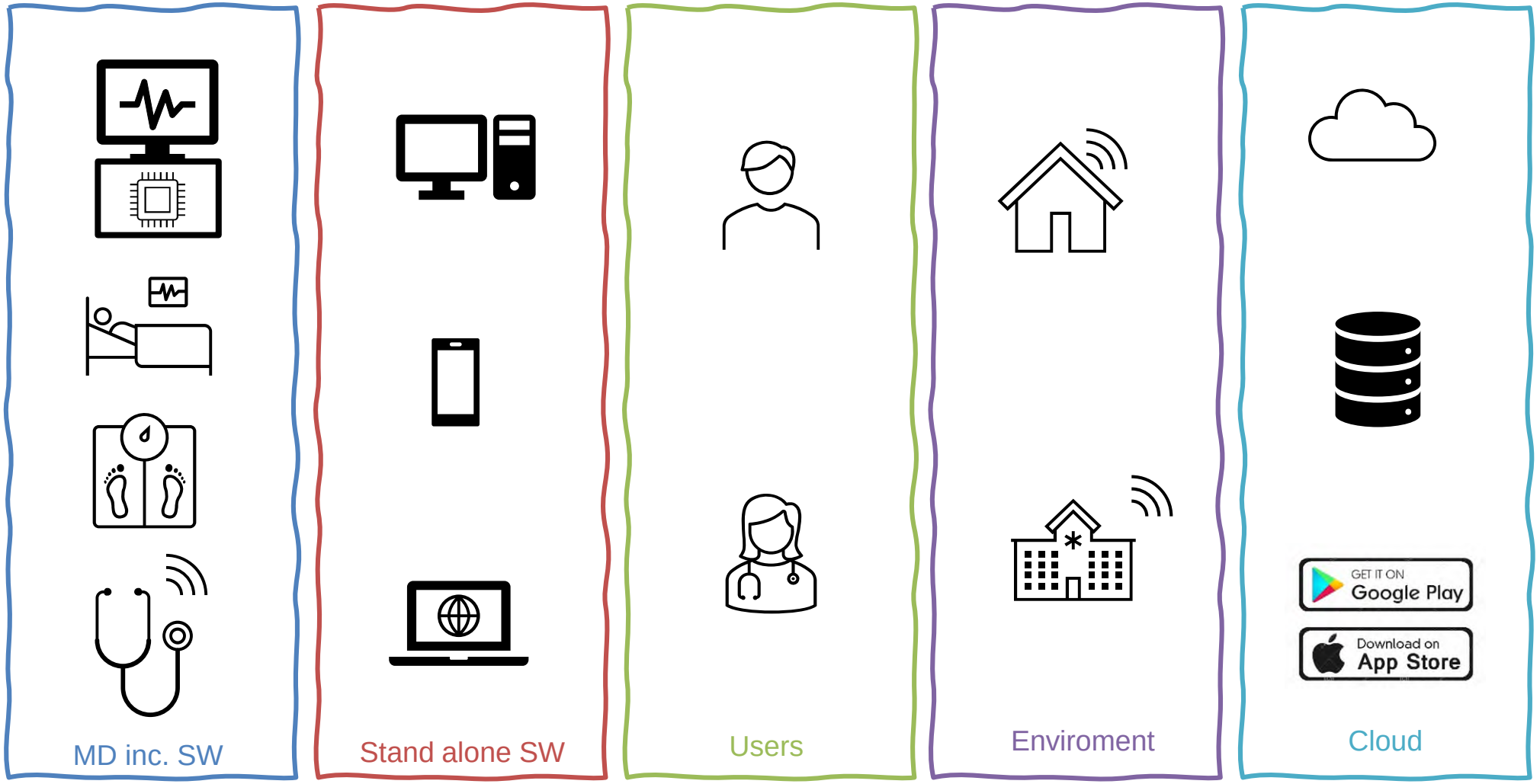
Top New Technologies That Will Impact Healthcare In Future

1. Personal Health Assistants
2. Analytics Of Health Data
3. Organ-on-a-chip Technology
4. Gene Editing
5. Internet Of Medical Things (IoMT)
6. Robotics In Surgery
7. 3D Bioprinting
8. Augmented Reality(AR) In Clinical Training
9. Virtual Reality(VR) In Therapy
10. Health Wearables For Elderly People

Top New Technologies That Will Impact Healthcare In Future

1. **Personal Health Assistants**
2. **Analytics Of Health Data**
3. Organ-on-a-chip Technology
4. Gene Editing
5. **Internet Of Medical Things (IoMT)**
6. **Robotics In Surgery**
7. 3D Bioprinting
8. **Augmented Reality(AR) In Clinical Training**
9. **Virtual Reality(VR) In Therapy**
10. **Health Wearables For Elderly People**

MD Software type combinations



Standards related to SW

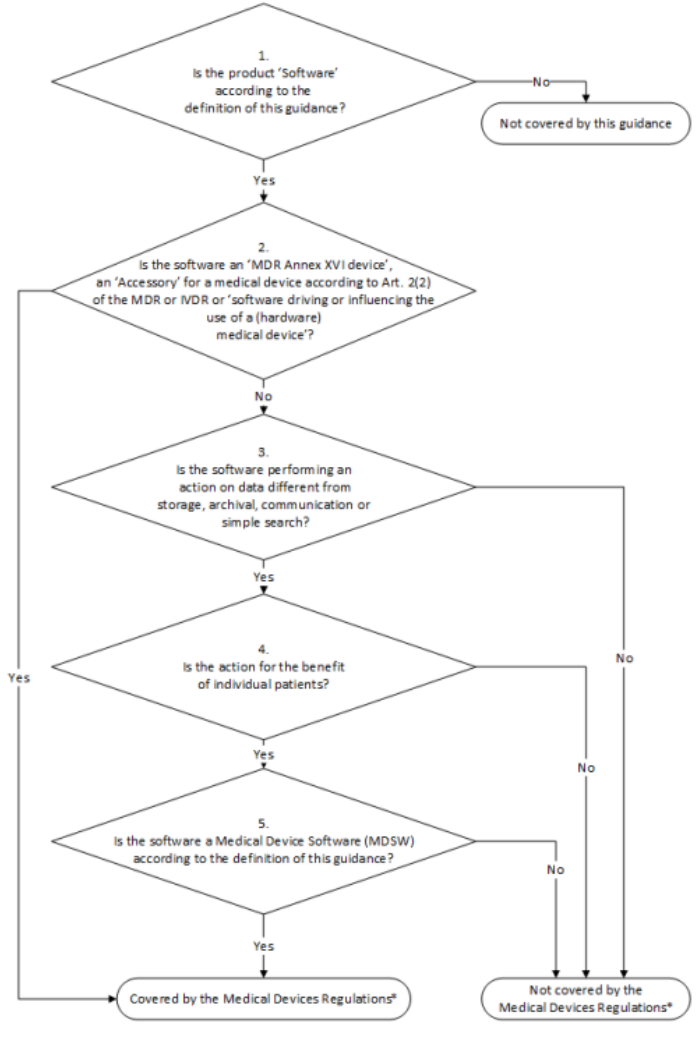
- **EN 62304:2006+A1:2015** – medical device software – software life cycle processes
- **EN 60601-1:2006/A2:2021** Medical Electrical Equipment Medical electrical equipment - Part 1: General requirements for basic safety and essential performance (***clause 14***)
- **IEC/TR 80002-1:2009** Medical device software — Part 1: Guidance on the application of ISO 14971 to medical device software

Guidelines related to SW

- **MDCG 2020-1** Guidance on clinical evaluation (MDR) / Performance evaluation (IVDR) of medical device software
- **MDCG 2019-16** rev.1 Guidance on cybersecurity for medical devices
- **MDCG 2019-11** Qualification and classification of software - Regulation (EU) 2017/745 and Regulation (EU) 2017/746
- **MDCG 2018-5** UDI assignment to medical device software

Qualification and classification of software

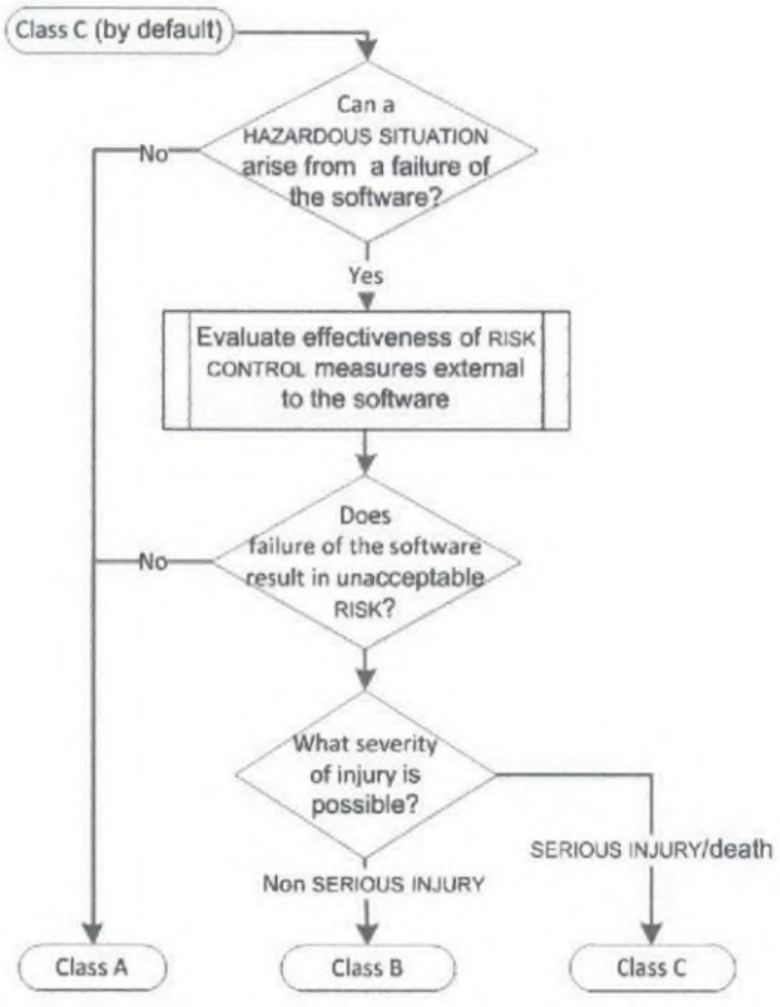
- **MDCG 2019-11** Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR



Classification rules related to software

- **Rule 11** – Software for decisions with diagnosis or therapeutic purposes or software intended to monitor physiological processes
- **Rule 12** – Active devices intended to administer and/or remove substances
- **Rule 13** – All other active devices
- **Rule 15** - Devices used for contraception
- **Rule 22** – Closed loop systems

Software safety classification



IEC 62304:2006+A1:2015

Cybersecurity for medical devices

MDCG 2019-16 rev. 1

MDR codes for notified bodies

Implementing Regulation 2017/2185

MDS

Devices with specific characteristics

MDT

Specific technologies or processes

MDA

- Active implantable
- Active non-implantable for imaging, monitoring and / or diagnosis
- Active non-implantable therapeutic and general active non implantable

Design and intended purpose

MDN

- Non-active implants and long term surgically invasive
- Non-active non-implantable

SIQ (NB 1304)

MDA 0315

MDS 1009

50% application forms

Audited devices incorporating SW at SIQ

- Electroencephalography instruments
- **AI for prediction of the cerebrovascular risk events**
- Diagnostic imaging workstations
- Vital signs monitoring instruments
- **Medical conditions or diseases determination from blood analysis – AI**
- Aneroid sphygmomanometers
- Muscle stimulators
- Decision support system in the evaluation of recorded patient lung sounds
- Various bioimaging and radiotherapy instruments
- Clinical/Diagnostic spirometer
- Surgical laser

Common Audit Findings (TF, QMS)

- Firmware software is not treated as a MDSW
- Software versioning is not defined in the main document and record process
- Usage of CE mark is not correct
- Key function elements of the software were not defined
- There are no software safety classification defined
- Cybersecurity risks were not considered

Common Audit Findings - Development

- Software life cycle phases were not defined
- Software development plan is not prepared
- Software architecture design and integration testing are not defined
- No objective evidence that software developed according to EN 62304:2006 + A1:2015

- Design stages, specifications, including the manufacturing process and their validation, their adjuvants and continuous monitoring and the final product testing was not defined

Common Audit Findings – Verification & Validation

- Software verification plan is not prepared
- Control on Verification and Validation is not sufficient (check list)
- Verification and Validation report for software of version
- Cybersecurity implementation was not part of verification and validation activities
- Browsers for using web applications were not validated
- SOUP libraries are not listed, the validation plan and records are not provided

Common Audit Findings – Clinical Evaluation

- The impact of software functions that are disabled in a medical device must be properly assessed through risk analysis to ensure that the medical device is safe and effective for its intended use
- In the Clinical evaluation report and documentation is no data about cybersecurity (Annex I 17. – 17.4)
- Overview of the similar devices is not provided
- Applicable standards were not listed
- Inadequate search criteria and method of data appraisal in literature

Common Audit Findings – Production

- Inadequate assignment of the UDI to Medical Device Software
- Software labeling is not appropriate
- Release of the software is not recorded and approved
- Criteria and information about software support were not defined, e.g. transitional period and how preventing incompatibility issues
- The prerequisite of the phone OS version has to be stated
- Minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorized access, necessary to run the software as intended should be included in the Instruction for use

SIQ (NB 1304) - Complete Solutions (SW)

- Certification according to MDR – Regulation (EU) 2017/745
  - MDA 0315, MDS 1009,… **free capacities/resources**;
- ISO 13485 Quality Management System for Medical Devices
  - **Accredited certification body**; IQNet Member
- Educational platform/ Training programmes
  - Online workshop: Compliance of Medical Device Software
  - Online training course: Guidelines for managing medical device cybersecurity in design, installation, and maintenance
  - …
- Safety testing capacities
  - Software testing (IEC 62304)