Extending SOUP to ML Models When Designing Certified Medical Systems

Vlad Știrbu, CompliancePal/University of Helsinki, Finland
Tuomas Granlund, Solita, Finland
Jere Helén, University of Helsinki, Finland
Tommi Mikkonen, University of Helsinki, Finland

vlad.stirbu@compliancepal.eu
Outline

- Background and motivation
- 3rd party software
- Machine Learning (ML) in certified medical systems
- Conclusions
Certified medical systems

- Patient safety
- Privacy
- Cybersecurity
Guidances
Communicates the expectations of the regulatory authorities and current practice for supporting implementation

International standards
International standards (ISO and IEC) identified by regulatory authorities that allow manufacturers to declare conformance with relevant regulations

Local legislation
State level legislation that augments the market legislation

Legislation
Applies to the entire market area. MDR in EU or FDA in US

Guidances
Communicates the expectations of the regulatory authorities and current practice for supporting implementation
Standards

- Quality management system
- Risk management
- Product and software development lifecycle
Medical software development lifecycle (ISO 62304)

Safety risk classes: no harm (A), harm (B), serious harm or death (C)
Software of unknown provenance (SOUP)

Software that is already developed and generally available and that has not been developed for the purpose of being incorporated into the medical device (also known as “off-the-shelf software”)

Software previously developed for which adequate records of the development processes are not available
Risk management for ML applications

**Input data**
- Training and the normal use data mismatches

**Algorithm design**
- Human biases - flawed outputs
- Technical flaws - rigour and conceptual soundness
- Usage flaws
- Security flaws - deliberately flawed outputs by input manipulation

**Output decisions**
- Incorrect interpretation and use of the output
Machine learning development lifecycle
Machine learning development lifecycle

ISO 62340
Machine learning development lifecycle

ISO 62340

CD4ML

Functional barriers
Extending the SOUP to ML model

Packaged Model
Test data
Documentation

Integration and risk analysis

Effective safety evaluation
Audit trails

CD4ML
Conclusions

- Machine learning enable complex prediction systems
- Opaque and difficult to comprehend
- Must be handled with the same rigour as SOUP
- Establish solid guidelines codified in DevOps/MLOps pipelines
- Increased complexity on the regulatory activities