Envisioning a Requirements Specification Template for Medical Device Software

Hao Wang[1], Yihai Chen[2], Ridha Khedri[3], and Alan Wassyng[4]

[1] Faculty of Engineering and Natural Sciences, Aalesund University College, Norway

[2] School of Computer Engineering and Science, Shanghai University, China

[3] Department of Computing and Software, McMaster University, Canada

[4] McMaster Centre for Software Certification (McSCert), McMaster University, Canada

12 December 2014
PROFES 2014
Helsinki

Outline

Project Overview

- "*Certification of Safety and Security in Software Intensive Medical Devices*"
  - Collaboration between McMaster Centre for Software Certification, IBM and FDA, with support from Southern Ontario Smart Computing Innovation Platform (SOSCIP) and Software Certification Consortium (SCC)
- Objectives
  - Study on methods and tools to develop safe, secure, and reliable *software-intensive medical devices*, using the insulin pump as a case
  - Protypical processes for development and certification, templates, and tools

Medical Device Software

- European Medical Device Directive (MDD) 93/42/EEC
  - The software is for a purpose explicitly mentioned in a MDD
  - The software is intended to control or influence the functioning of a medical device
  - The software is intended for the analysis of patient data generated by a medical device with a view to diagnosis and monitoring
  - The software is intended for use for/by patients to diagnose or treat a physical or mental condition or disease
- IEC and FDA included software as a category of medical devices

MDS is Safety Critical

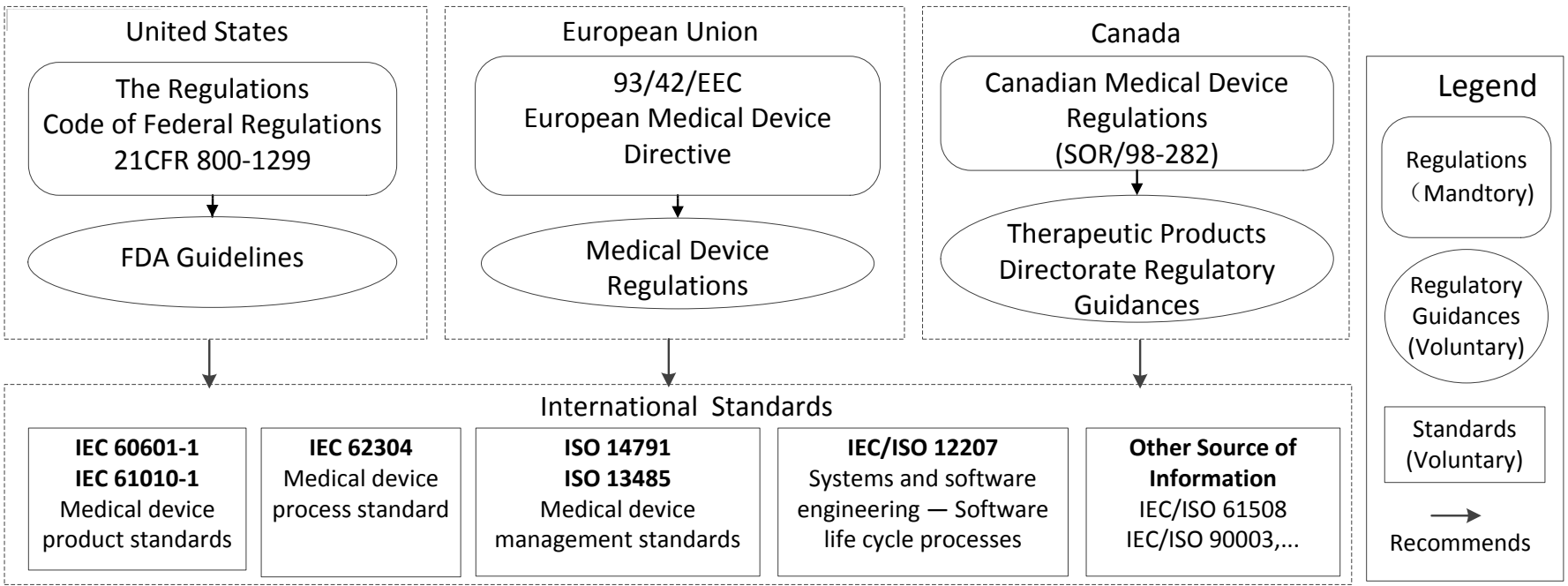
- FDA reported, from Oct.1,2006 to Sept.30,2009
  - Nearly 17,000 insulin pump-related adverse-event reports
  - 12,000+ injuries, 4000+ device malfunctions
  - 310 death reports, 41 device malfunctions
- Popular pumps with wifi were hacked;
- In 2002-2010,
  - 537+ recalls of devices that used software, affected over 1.5 million devices
- Until recently, approval based on development process, e.g., IEC 62304
- FDA introduced more *product focused* approval process for infusion pumps – *assurance cases* are recommended

Requirement Specs are Important!

- Poor RS imperils subsequent stages of development
- A good RS template facilitates elicitation and documentation of requirements
  - Fields like manufacturing or aerospace have standard RS templates
  - No RS template for MDS
- MDS subject to
  - Government and int'l laws and regulations
  - Safety and security concerns

Outline

Standards and Guidelines



Standards and Guidelines

- FDA, USA
  - Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices
  - Guidance for General Principles of Software Validation
  - Guidance for the Use of Standards in Substantial Equivalence Determinations
- Canadian Medical Devices Bureau of the Therapeutic Products Directorate
  - Guidance Document on Recognition and Use of Standards
- Europe, MDD
  - Medical Device Directive (MDD) 93/42/EEC and its latest amendment MDD 2007/47/EC

Existing RS Templates

There are several general/specific-purposed templates

- "the needs of organisations working on different projects can, and do, vary"
- Unfortunately none of these templates can fully satisfy the needs of MDS
- Regulating agencies have not provided RS templates for MDS

General Templates

- IEEE Std 830-1998 template
  - One of the most important reference templates
  - Functional requirements structured in several ways, e.g., system modes or use cases
- Volere template
  - Emphasizes project requirements
  - 3 sections, project drivers, project contraints, project issues, give details like contractual matters and understanding between stakeholders
  - No clear guidance on organization of functional requirements
- Common problems with these two: lack of hazard identification and safety requirements

Domain Specific Templates

- European Cooperation for Space Standardisation (ECSS) standard ECSS-E-40C
  - Interface Requirements Document (IRD), for non-technical audiences like users and project managers
  - Software Requirements Specification (SRS), for designers and developers
  - No detailed guidance on organization of functional requirements; and no details on contents for each subsection
- U.S. Federal Aviation Administration, *Requirements Engineering Management Handbook*
  - Real-time, embedded systems for avionics industry
  - Use isolette thermostat, a medical device, as an example RS
- Naval Research Laboratory and Naval Weapons Center, A-7E software requirements document

Summary of Existing Templates

- Our previous templates
  - Ahmadi proposed a RS template for manufacturing systems
  - Lai proposed a RS template for scientific computation
- Summary of existing templates
  - lack of support for hazard identification and safety requirements
  - lack of support for compliance with applicable regulations and standards

Outline

Objective #1

The template should guide the elicitation of the requirements governed by the relevant regulations and standards

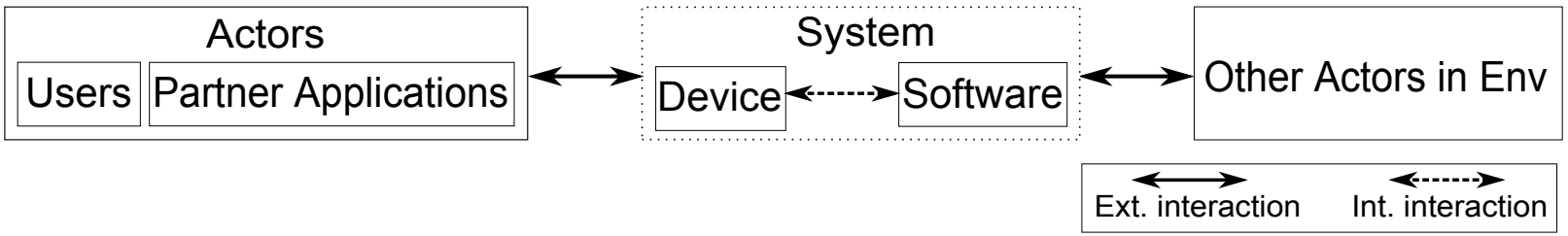
- Regulations cannot include details of technical methods and evaluation criteria
- Standards are more technical, with input from technical experts (often from the industry to be regulated)
- Current standards covering requirements of MDS, but they do NOT presribe the explicit contents for RS
  - IEC62304 "The MANUFACTURER of MEDICAL DEVICE SOFTWARE shall demonstrate the ability to provide MEDICAL DEVICE SOFTWARE that consistently meets customer requirements and applicable regulatory requirements."

Objective #2

The template should guide the elicitation of the requirements from several system perspectives. Each perspective should be the viewpoint of one of the system's environment actor, or partner applications or systems

- Accidents often result from dysfunctional interactions among components, not from individual component failure – System accidents
- Unrealistic expectations about software and the use of computers
- A system approach to the elicitation and documentation of the requirements of medical devices
  - Stimuli from an actor in a system's environment
  - System reacts to the stimuli from actors
  - Some stimuli are NOT a reponse from a previous stimulus, called *initiator-event* (IE)

Objective #2



- For requirements elicitation is to
  - identify the actors (or at least the most relevant ones) of the system's environment, and
  - identify the major initiator-events that affect the system
- A RS template ought to be structured to capture the requirements from each influential actor and that with regard to each IE

Objective #3

The decomposition of the template should be based on the principle of separation of concerns

- A concern in the functional requirements could be an IE or a mode as perceived by one of the actors.
- Each (sub)section in the template has a set of cohesive requirements that are lowly coupled to the rest of the requirements
- For nonfunctional requirements, fine grained decomposition of each expected quality
  - E.g., the security requirements decomposed into access reqs, integrity reqs, privacy reqs, audit reqs, and immunity reqs.
- The result RS will exhibit desirable properties such as modifiability, non-redundancy, verifiability, and ease of validation

Objective #4

The template should guide documenting the safety risk IEs (RIEs) that are handled by the device and support their ranking. As well, it should support articulating the device/environment interactions in response to these safety RIE

- IEC 62304 "the MANUFACTURER shall apply a RISK MANAGEMENT PROCESS complying with ISO 14971"
- Usual risk management emphasizes on the most likely risks

Objective #4

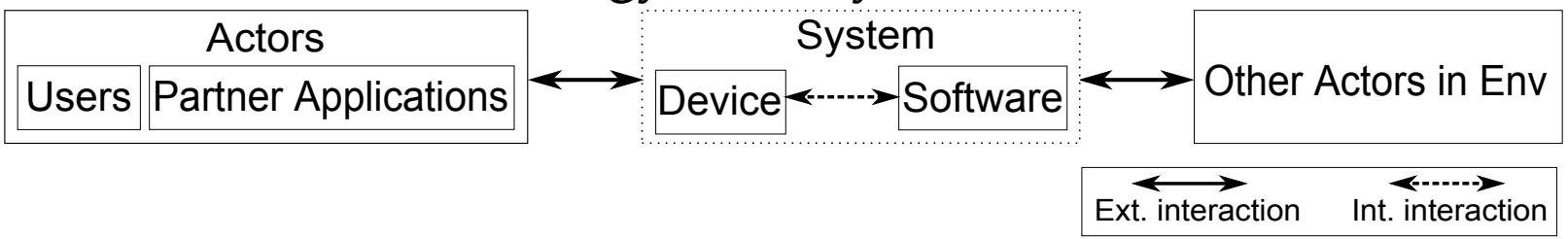
- However, for MDS, we should consider all risks regardless of their probabilities
  - Estimating the probability of occurrence of a harm is quite difficult and often inaccurate
  - Unlikely-to-happen harm can be extremely damaging
  - Include a risk based on whether we can technically come up with the appropriate mitigating measures
  - The *deviations* of European harmonized ISO 14971
    - Deviation 1 indicates that manufacturers should not discard negligible risks
    - Deviation 2 disallows manufacturers to decide the acceptability of risks.
    - Deviation 7 "users shall be informed about the residual risks"
    - Deviation 3 requires reducing risks as far as possible as opposed to as low as reasonably practicable

Objective #4

- Risk Initiator-Event – an IE that leads to a risk
  - Documented accident and incident reports , e.g., FDA MAUDE database
  - Root cause for a RIE
    - RIE workshops
    - Hazard analysis techniques
  - Ranking risks
  - Assess severity of risks
    - IEC 62304 requires "The MANUFACTURER shall assign to each SOFTWARE SYSTEM a software safety class (A, B, or C) according to the possible effects on the patient, operator, or other people"

Objective #5

The template should guide documenting the device's threat targets and specify the reasonable time for accessing the resources it shares with the environment. It should provide the needed requirements for a thorough security assessment according to *Common Criteria for Information Technology Security Evaluation Models*



Objective #5

- No environmental actors can misuse common assets of the device such as data stores and channels of communication
  - *threat targets* (TTs) – data stores and the shared resources
  - Template to help identify all TTs
- Explicit access policies
  - Confidentiality policies
  - Prevention of unauthorized data leakage
  - Detection of unauthorized usage of data
  - Recovery of any data lost or corruptions
- No environmental actor can change the prescribed behaviour of the device or affect its overall qualities (nonfunctional requirements)

Objective #6

The template should guide documenting the privacy requirements that ensure the protection of the user's personally identifiable information

- Related to Obj#5, but more focused on *personally identifiable information*
  - Whether a patient has a Medical Device or not should remain protected from unauthorized users
  - Unauthorized parties should not be able to link a specific-device identifying feature to the user
  - All the standards and regulations regarding of the privacy of medical data should be taken into account

Objective #7

The template should help formally document the functional requirements, while at the same time help document requirements intended for non-technical users. The formalism should at least support formal and automated verification of the space completeness, and the dictionary and behaviour consistency of the functional requirements

- The template needs to help get requirements that can be presented at several technical levels
- Functional requirements can be organised in several ways
  - Isomorphism: (IE, Viewpoint, Use-case) or by (Viewpoint, IE, Use-case), and etc

Objective #8

The template should support a family approach to document software medical devices

- A dilemma
  - On the one hand, we seek systems that are simple, and carry the needed functionality, no more no less
  - On the other hand, we have several classes of users of a MDS
- Product family approach to the development of MDS
  - It helps to deal with unexpected changes to the requirements

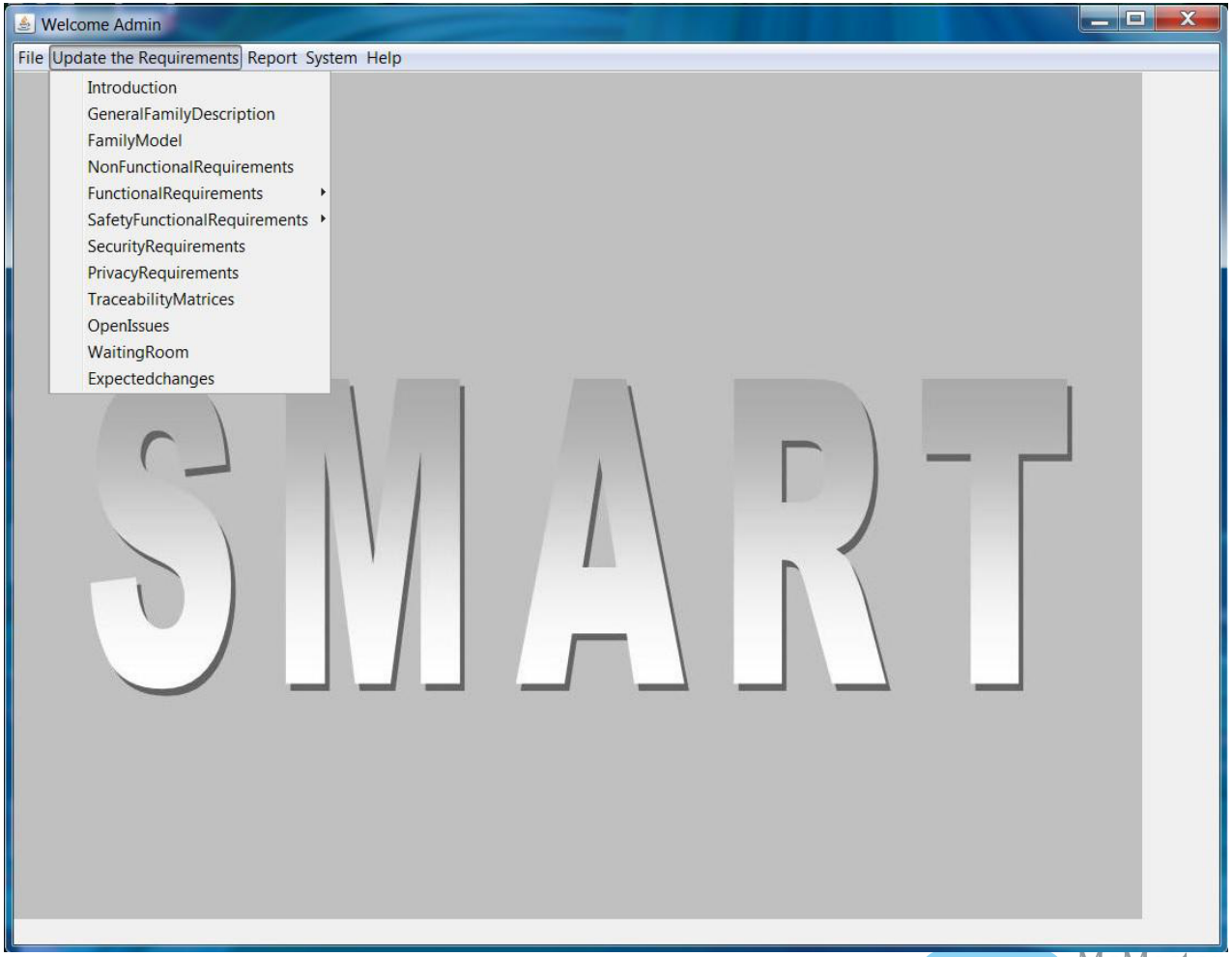
A Structure for a RS Template

We propose a structure in Appendix A (found in our paper) satisfying all above objectives

Obj. 1	Obj. 2	Obj. 3	Obj. 4	Obj. 5	Obj. 6	Obj. 7	Obj. 8
Sec. 2.6 & 7	Sec. 5 & 6	Sec. 5 & 6	Sec. 6	Sec. 8	Sec. 9	Sec. 5 & 6	Sec. 2 & 3

- SMART II
  - Store requirements in XML
  - Access control mechanisms
  - Generate full RS in RTF, PDF
  - Math formula and tabular expressions in LaTeX

SMART II


Welcome Admin
File
Update the Requirements
Report
System
Help
Introduction
GeneralFamilyDescription
FamilyModel
NonFunctionalRequirements
FunctionalRequirements
SafetyFunctionalRequirements
SecurityRequirements
PrivacyRequirements
TraceabilityMatrices
OpenIssues
WaitingRoom
Expectedchanges
SMART

Outline

Conclusions and Future Work

- We propose a set of objectives for MDS RS templates
- We propose a structure for MDS RS templates, with SMART II as a supporting tool
- On-going work
  - Verification mechanism for SMART II
  - Certification and development process for insulin pumps
    - Assurance case template for MDS, submitted to IEEE Design&Test
    - Formalizing and verification of insulin pump requirements, submitted to HCII 2015
  - Building the *Process Improvement Lab* and *Big Data Lab* in AaUC (http://blog.hials.no/), on Big data analytics, Lean and Certification processes, one application area is Maritime

Acknowledgements

- IBM Canada R&D Centre
- Southern Ontario Smart Computing Innovation Platform (SOSCIP)
- Natural Science Foundation of China
- Natural Sciences and Engineering Research Council of Canada
- Ontario Research Fund - Research Excellence

Thank You!

Comments and Questions?

Hao Wang
www.haowang.ca