Medical Cyber-Physical Systems
On the Research Challenges for the Safe Interconnection of Medical Devices

Franziska Kühn\textsuperscript{1,2} Martin Leucker\textsuperscript{1} Daniel Thoma\textsuperscript{1}
\{kuehn, leucker, thoma\}@isp.uni-luebeck.de

\textsuperscript{1}Institute for Software Engineering and Programming Languages
\textsuperscript{2}Graduate School for Computing in Medicine and Life Science
University of Lübeck

July 8, 2014
Outline

OR.NET Project

Legal Regulations in Germany

Formal Methods

Runtime Verification for Interconnected Medical Devices

Implementation and Experimental Results

Discussion
Outline

OR.NET Project

Legal Regulations in Germany

Formal Methods

Runtime Verification for Interconnected Medical Devices

Implementation and Experimental Results

Discussion
Motivation

- Nowadays the networking of medical devices in an operating room is almost always limited to devices from a single manufacturer.
- Networking is only permitted if it is the intended use.
- Clinic operators cannot choose the most economic and qualified products of different manufacturers.
- Surgeons have to use many devices (for example different monitors for different devices instead of one central monitor).
- Due to limited interoperability expensive and cumbersome integration projects are necessary.
- Due to legal reasons a medical device (including complete system-of-systems) has to be successfully tested and certified before its use.
Meningioma Surgery
OR.NET Project Overview

- safe, secure and dynamic networking of medical devices and IT systems in operating room and hospital
- funded by the German federal ministry of education and research (BMBF)
- Project duration: 3 years (started in September 2012)
- Website: www.ornet.org
Project Partners

Industry
- Conworx
- howtoorganize GmbH
- inomed Medizintechnik GmbH
- KARL STORZ GmbH & Co. KG
- KLS Martin Group
- LOCALITE
- MEDNOVO Medical Software Solutions GmbH
- MedPlan Engineering GmbH
- Möller-Wedel GmbH
- MT2IT GmbH & Co.KG
- qcmed GmbH
- Richard Wolf GmbH
- Söring GmbH
- SurgiTAIX AG
- Synagon GmbH
- Unitransferklinik Lübeck
- VISUS Technology Transfer GmbH/R & D
- Ziehm Imaging GmbH

Medical care/operations
- Klinikum Südstadt Rostock, Klinik für Anästhesiologie
- Universitätsklinikum der RWTH Aachen
  - Klinik für Anästhesiologie
  - Orthopädische Klinik
  - Neurochirurgische Klinik
- Universitätsklinikum Schleswig-Holstein
  - IT-Planung und -Strategie
  - Klinik für Chirurgie
- Eberhard-Karls-Universität Tübingen
  - Universitätsklinik für Urologie
  - Universitätsklinik für Radiologie
  - Universitäts-Frauenklinik
- Universitätsklinikum Heidelberg, Zentrum für Informations- und Medizintechnik,
- Universitätsklinikum Leipzig, Klinik für Herzchirurgie
- Rhön-Klinikum AG
Project Partners (cont.)

Research

▶ Fraunhofer FIRST
▶ Fraunhofer MEVIS
▶ Innovation Center Computer Assisted Surgery Leipzig
▶ OFFIS – Institut für Informatik e.V.
▶ RWTH Aachen
  ▶ Lehrstuhl für Medizinische Informationstechnik
  ▶ Lehrstuhl für Medizintechnik
▶ TU Munich
  ▶ Institut für Informatik
  ▶ Lehrstuhl für Automatisierung und Informationssysteme
  ▶ Lehrstuhl für Mikrotechnik und Medizinerätetechnik
  ▶ Minimal-invasive Interdisziplinäre Therapeutische Intervention
▶ Uniklinik der RWTH Aachen, Klinik für Anästhesiologie, Forschungsgruppe Integrierte Teleanästhesiologie
▶ Universität Augsburg, Forschungsstelle für Medizinproduktrecht
▶ Universität Rostock, Institut für Angewandte Mikroelektronik und Datentechnik
▶ Universität zu Lübeck
  ▶ Institut für Medizinische Informatik
  ▶ Institut für Softwaretechnik und Programmiersprachen
  ▶ Institut für Telematik

Standardization

▶ DIN Deutsches Institut für Normung e. V.
▶ IHE Deutschland e.V.
▶ Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE)
Sub-Projects – Overview

SPRJ 1 – Project management

SPRJ 2 – IT integration/networking in OR
Creating an appropriate and standards-based integration concept for
- the interconnection of medical devices (among themselves)
- the interconnection of medical devices and IT systems

SPRJ 3 – Capability for approval
- Consideration of the difficulties in the approval process of modular subsystems with open interfaces, where subsystems are components of integrated operating rooms
- Developing tools and standards which support the new approval process
Sub-Projects – Overview (cont.)

**SPRJ 4 – Standardization**
- Supporting the project partners in reaching an agreement on technical norms and standards to be applied, processes, protocols and terms, thereby ensure interoperability
- Integrating the project results successfully into international standardization processes

**SPRJ 5 – Operator models**
Investigation how the manufacturer’s and operator’s interests can be balanced.

**SPRJ 6 – Demonstrator**
- A prototype implementation showing the safe, secure and dynamic networking of medical devices and their integration with relevant IT systems in an OR.
- Several concepts developed in SPRJ 2 should be realized and evaluated during clinical routine.
Main Objectives

- Freedom of product choice for the clinic operators
- Interoperability for all medical devices (and IT systems)
- Dynamic and simple integration
- Safe and secure (resulting) medical devices
- Standardized interoperability
- International market penetration
Safety Risks in the Context of the Dynamic and Flexibility

- Safety in the medical domain has high priority
- Misbehavior can have severe consequences
- Integration and system tests are not always possible
- Medical devices, which were not tested a priori, are interconnected and operating together in a surgery room
- For example how to ensure
  - that all methods required by another medical device are provided?
  - that system performance requirements are fulfilled?
  - that the behavior of the medical devices fits together (without an exhaustive integration test)?
Contributions of the ISP

- Developing formal methods to avoid hazards induced by the dynamic and flexible networking
- Reaching at least the usual level of reliability when composing new systems and thereby maintaining at least the current level of safety for the patient
- Integrating formal methods in both product development as well as risk management to simplify the approval process
- Enabling the certification body to gain a more complete insight into the applied safety concept
Outline

OR.NET Project

Legal Regulations in Germany

Formal Methods

Runtime Verification for Interconnected Medical Devices

Implementation and Experimental Results

Discussion
Directives, Laws and Norms in Europe

New Approach\(^1\)

- Removing technical barriers to trade in Europe
- Ensuring the free movement of goods between European member states
- Common (technical) requirements for specific product categories (for example medical devices and toys) are described in European directives
- All European member states have to implement the directives into national laws
- Manufacturers have to perform a conformity assessment procedure before bringing a product on the market.

\(^1\)http://www.newapproach.org
Directives, Laws and Norms in Europe

Harmonized norm:

- Support for manufacturers to fulfill the essential requirements of a directive
- The norms are determined and published by the European Commission
- Norms themselves are created by expert committees and
- Published by corresponding (inter-)national standardization bodies

International norms

European directives

EU member state

National laws

harmonize

set limits

implements

are binding in

Leucker et al. July 8, 2014 16/50
Legal Regulations for Medical Device Manufacturers

- Following European directives are the basis for medical devices:
  - 93/42/EWG (Medical Device Directive)
  - 98/79/EG (In-vitro Diagnostic Directive)
  - 90/385/EWG (Active implantable medical devices directive)
- Medical Devices Act (MPG): German implementation of the three European directives for medical devices, supplemented by regulations
Medical Device Directive (93/42/EWG)

93/42/EWG demands the following requirements:

- Provision for quality aspects (EN ISO 13485 (Medical devices - Quality management systems - Requirements for regulatory purposes))
- Implementation of risk management (EN ISO 14971 (Medical devices - Application of risk management to medical devices))
- Provision for software life cycle processes (EN 62304 (Medical device software - Software life-cycle processes))
- Certification of usability (EN 62366 (Medical devices - Application of usability engineering to medical devices))
Describes the process (with activities and tasks) for software development and maintenance

No specific regulations for the implementation

Processes that shall be considered:

- Software development process
- Software maintenance process
- Software risk management process
- Software configuration management process
- Software problem resolution process
Software Development Process

Software Development Planning

▶ Has to ensure, that all required activities are actually performed during development

▶ Shall include for example the deliverables of the activities and tasks, and software integration and integration testing planning

Software Requirements Analysis

▶ Defining and documenting software system requirements from the system level requirements

▶ Shall include for example functional requirements, software system inputs and outputs, interfaces between the software system and other systems

<table>
<thead>
<tr>
<th>5.1</th>
<th>5.2</th>
<th>5.3</th>
<th>5.4</th>
<th>5.5</th>
<th>5.6</th>
<th>5.7</th>
<th>5.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software development planning</td>
<td>Software requirements analysis</td>
<td>Software architectural design</td>
<td>Software detailed design</td>
<td>Software UNIT implementation and VERIFICATION</td>
<td>Software integration and integration testing</td>
<td>Software SYSTEM testing</td>
<td>Software release</td>
</tr>
</tbody>
</table>
Software Development Process

Software Architectural Design
- Overview over the system
- Fundamental decisions for further development, like target platform, external libraries and third party software.

Software Detailed Design
- Refine the structure for the software system based on the software architecture
- Detailed design for each software unit and interfaces
Software Development Process

Software Unit Implementation and Verification

- The manufacturer shall implement each software unit
- Establishing software unit verification process
- Test procedures shall be evaluated for correctness
- Establish software unit acceptance criteria
- Performing software unit verification

Software Integration and Integration Testing

- Integrate software units and verify the integration
- Test integrated software and verify integration test procedures
Software Development Process

Software System Testing

- Establishing tests for software requirements
- Verify software system testing, including
  - the verification strategies and the test procedures used are appropriate
  - all software requirements have been tested or otherwise verified

Software Release

- Ensuring that software verification is complete
- Documentation and evaluation of known residual anomalies
- Archiving software

<table>
<thead>
<tr>
<th>5.1</th>
<th>Software development planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2</td>
<td>Software requirements analysis</td>
</tr>
<tr>
<td>5.3</td>
<td>Software ARCHITECTURAL design</td>
</tr>
<tr>
<td>5.4</td>
<td>Software detailed design</td>
</tr>
<tr>
<td>5.5</td>
<td>Software UNIT implementation and VERIFICATION</td>
</tr>
<tr>
<td>5.6</td>
<td>Software integration and integration testing</td>
</tr>
<tr>
<td>5.7</td>
<td>Software SYSTEM testing</td>
</tr>
<tr>
<td>5.8</td>
<td>Software release</td>
</tr>
</tbody>
</table>
Consequences

- A main objective of OR.NET: Dynamic integration
- IEC 62304 requires that all subsystems that the entire system comprises are considered during testing
- The entire system is not known during development
- Approval requires testing the entire system
- Nowadays: dynamic networking of medical devices is not possible (technical restrictions, legal reasons)?
- OR.NET: development of technical solutions and adapted and new (international) norms and approval processes
When integrating medical devices, IT networks become *medical IT networks*.

Operator of the IT networks are obligated to carry out a risk management to ensure the safety for patient, users and third parties.

Risk management includes

- risk analysis
- risk evaluation
- risk control

IEC 80001 provides support but is not mandatory for operators of a medical IT network.
Outline

OR.NET Project

Legal Regulations in Germany

Formal Methods

Runtime Verification for Interconnected Medical Devices

Implementation and Experimental Results

Discussion
Motivation

- Improving the safety of medical devices
- Helpful for the development of medical devices
- Simplifying the approval process
- Enabling the certification body to gain a more complete insight into the applied safety concept
- Examples for formal methods:
  - Proof carrying code
  - Ontology databases
  - Mediator synthesis
  - Runtime verification
- Rich interface specifications and verification
Proof Carrying Code

- Guaranties safety properties
- Does not depend on reliability of software supplier
- Software supplier provides machine readable proof of defined safety properties
- Before execution the proof is verified
- Proof generation is expensive and involves manual steps
- Proof verification is inexpensive and fully automatic
Ontologies and Mediator Synthesis

- Ontologies model knowledge domains
- Represent knowledge domains using relations between concepts
- Use ontologies to define concepts of application domain
- Use ontologies to define semantic meaning of interfaces of components
- Infer relationship between syntactic interfaces of semantically compatible components
- Synthesize mediator, performing syntactic transformation between interfaces
Runtime Verification

- Allows to monitor the behavior of a system at runtime to examine whether the system under scrutiny is satisfying or violating specified properties
- Monitors can be used to evaluate whether a run of a system under scrutiny satisfies or violates a given correctness property
- Correctness properties are typically given in some linear time logic
- A monitor can be generated by an automata-based monitor construction which translates a given correctness property automatically into an automaton
Possible Use to Enhance the Safety when Connecting Medical Devices

- **Goal:** Checking the compatibility of systems after deployment, without an comprehensive integration test
- **Approach** consists of three steps:
  - Define precisely the interface intended for connectivity
  - Check compatibility of interfaces whenever connecting two devices
  - Check each device for conformance with its interface specification
Interface Definition

- Necessary for the manufacturer’s risk management
- Necessary for software development
- Useful to ensure the intended use of a device
- Basis for checking compatibility of networked devices
- Basis for checking whether a device adheres to its specified interface
- Forms of interface definitions are for example:
  - Interface Automata to specify the intended behavior of a component
  - UML component diagrams to specify for each component the methods including the parameters
  - WSDL to describe the delivered methods of web services
Interface Definition

- A suitable formalism has to be (highly) expressive but still allow for certain analysis techniques and should include at least:
  - the methods which are used/delivered by the medical devices
  - the parameters and return values of the methods (including the intended ranges of data)
  - the pre and post conditions of the provided and used methods
  - some form of the behavior of the component

- The formalism should allow the flexibility that service oriented architectures provide, as they become popular in the field of medical devices
Checking Compatibility of Interfaces

- Checking compatibility of interfaces when connecting devices
- Devices should continue to operate only if their interfaces are compatible
- Compatibility means for example
  - Are the methods required by another device provided?
  - Do the delivered values have the expected types and ranges?
  - Do the requirements of the caller fit the guarantees of the callee? I.e. does the required precondition imply the guaranteed precondition, and is the required postcondition implied by the guaranteed postcondition.
  - Does the behavior of the devices fit together?
- Checking compatibility must be decidable and efficient
Checking Conformance with Interfaces

- Checking the adherence of a device to all the constraints mentioned in the interface specification
- Possibilities checking the adherence:
  - before delivery of the complete system
  - dynamically at runtime
- Checking conformance with an interface specification is not always decidable
- Checking has to be done by all (involved) systems
- Systems should be checked and delivered with a proof of conformance allowing to check that the connecting part is working correctly
Outline

OR.NET Project

Legal Regulations in Germany

Formal Methods

Runtime Verification for Interconnected Medical Devices

Implementation and Experimental Results

Discussion
Runtime Verification

- Lightweight verification technique
- Specifying correctness properties in a high-level language, e.g. LTL
- Algorithmic procedure to synthesize monitors
- Monitoring the execution of the program
- Continuously verifying that the program conforms to its specification
Sequence Diagram

Surgeon

Microscope

starting initialisation
initialisation successful

setValue("ultrasound",60)

setValue("ultrasound",80)

eventValueChanged("ultrasound",60)

eventValueChanged("ultrasound",80)

Ultrasound Dissector

Operating Personnel

set ultrasound to 60

set ultrasound to 80

setValue("ultrasound",80)

eventValueChanged("ultrasound",80)
triggers the dissector

setString(trigger250ms, "ON")

setString(trigger250ms, "CONTINUE")

setString(trigger250ms, "CONTINUE")

setString(trigger250ms, "CONTINUE")

setString(trigger250ms, "OFF")

stops triggering the dissector
Example Properties

∀i :  \( G(i = \text{sendNum} \Rightarrow X \text{sendNum} > i) \)  \( \quad (1) \)
Example Properties

\[ \forall i : \ G(i = \text{sendNum} \implies X \text{sendNum} > i) \]  \hspace{1cm} (1)

\[ G(\text{name} = \text{ultrasound} \implies (0 \leq \text{value} \leq 100 \land \text{value} \mod 5 = 0)) \]  \hspace{1cm} (2)
Example Properties

\( \forall i : \ G(i = \text{sendNum} \Rightarrow X\text{sendNum} > i) \) \hspace{1cm} (1)

\( G(\text{name} = \text{ultrasound} \Rightarrow (0 \leq \text{value} \leq 100 \land \text{value mod 5} = 0)) \) \hspace{1cm} (2)
Example Properties

\( \forall i : \ G(i = \text{sendNum} \Rightarrow X \text{sendNum} > i) \)  \hspace{1cm} (1) 

\( G(\text{name} = \text{ultrasound} \Rightarrow (0 \leq \text{value} \leq 100 \land \text{value mod 5} = 0)) \)  \hspace{1cm} (2) 

\( \forall t : \ G \left( ((\text{on} \lor \text{cont}) \land t = \text{receiveTime}) \Rightarrow X \text{receiveTime} - 250 \leq t \right) \)  \hspace{1cm} (3)
Example Properties

\[ \forall i : \ G(i = \text{sendNum} \Rightarrow X \text{sendNum} > i) \]  

\[ G(\text{name} = \text{ultrasound} \Rightarrow (0 \leq \text{value} \leq 100 \land \text{value} \mod 5 = 0)) \]  

\[ \forall t : \ G \left( ((\text{on} \lor \text{cont}) \land t = \text{receiveTime}) \Rightarrow X \text{receiveTime} - 250 \leq t \right) \]  

\[ \forall c, v : \ G \left( \text{on} \Rightarrow (\neg \text{set}(c) S (\text{set}(c) \land v = \text{value}) \leftrightarrow \neg \text{changed}(c) S (\text{changed}(c) \land v = \text{value})) \right) \]
∀i :  \( G(i = \text{sendNum} \Rightarrow X \text{sendNum} > i) \)
\[ \forall i : \ G(i = \text{sendNum} \Rightarrow X \text{sendNum} > i) \]
\( \forall i : \ G(i = \text{sendNum} \Rightarrow X \text{sendNum} > i) \)
Architecture

- Microscope
  - Web Service
  - Web Service Stack
  - Interceptor

- Ultrasound Dissector
  - Web Service
  - Web Service Stack
  - Interceptor

- Monitoring Web Service
  - LTL
  - SMT Solver
  - RVLib
  - XQuery Processor

- Handler
  - Logfile

Leucker et al. July 8, 2014 42/50
Outline

OR.NET Project

Legal Regulations in Germany

Formal Methods

Runtime Verification for Interconnected Medical Devices

Implementation and Experimental Results

Discussion
Implementation

- Based on Java API for Web Services
  - Allows to attach interceptors to web services and clients
  - Maps automatically between Java objects and their XML representation
  - Provides direct access to the underlying SOAP messages

Diagram:
- Monitoring Web Service
- Ultrasound Dissector
- Monitoring Web Service
- RVLib
- XQuery Processor
- LTL
- SMT Solver
Implementation

- Based on Java API for Web Services
  - Allows to attach interceptors to web services and clients
  - Maps automatically between Java objects and their XML representation
  - Provides direct access to the underlying SOAP messages
- Monitoring Service
  - Reads its specification from XML file
  - Generates corresponding monitor
  - executes monitors when arbitrary message is received
Implementation

- Based on Java API for Web Services
  - Allows to attach interceptors to web services and clients
  - Maps automatically between Java objects and their XML representation
  - Provides direct access to the underlying SOAP messages

- Monitoring Service
  - Reads its specification from XML file
  - Generates corresponding monitor
  - Executes monitors when arbitrary message is received

- Available for download:
  www.isp.uni-luebeck.de/wsrv
Benchmarks – Monitoring

Leucker et al.

July 8, 2014
Benchmarks – Interval of Method Call \textit{trigger250ms}

- Call of method \textit{trigger250ms}:
  - Duration: 12 ms
- Remaining time:
  - Duration: 238 ms
Outline

OR.NET Project

Legal Regulations in Germany

Formal Methods

Runtime Verification for Interconnected Medical Devices

Implementation and Experimental Results

Discussion
Discussion

- Usefulness of formal techniques in the medical domain
- Usefulness of the presented approach
- Legal situation for using these techniques
- The potential of lowering the requirements imposed legally, when incorporating several formal methods
- The legal situation in different parts of the world
Questions?