



Combining Requirements, Use Case Maps and AADL Models for Safety-Critical Systems Design

Dominique Blouin^{1,2} and Holger Giese¹

¹System Analysis and Modeling Group, Hasso-Plattner Institute, Potsdam, Germany

²COMELEC / INFRES Group, Telecom ParisTech School, Paris, France

Importance of Requirements

- Requirements errors are:
 - Most dangerous, expensive, numerous and persistent errors
 - Large majority of accidents in which software was involved can be traced to requirements flaws
 - *Axel van Lamsweerde, *Requirements Engineering: From System Goals to UML Models to Software Specifications*, 2009

- Even more important for the domain of safety-critical embedded systems

- Even more for medical devices, which interact directly with humans leaving little chance to temporize system faults

Example: Ariane 5 Inaugural Flight 501

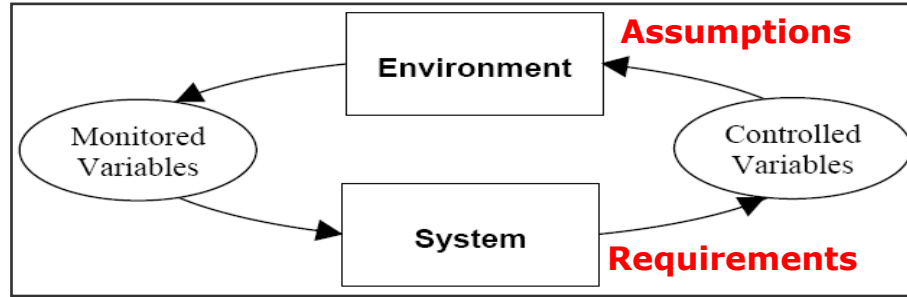
- One of the most expensive software bug of history (≈ 280 M€)
- Reuse of Ariane 4's navigation system (proven reliable)
- Ariane 5 has greater horizontal acceleration values than Ariane 4
- Caused an overflow of data represented in software
- **Mismatched assumptions problem**



Chart 3

Assumptions and Requirements

- Mismatched assumptions are requirements errors
- Assumptions are requirements



Lempia et al., 2008

- Purpose of RE is to provide means for capturing what the system should do:
 - Formulating the problem correctly is the first step towards a solution
 - Design shall provide a valid solution to the problem

Agenda

- 1. FAA Requirements Engineering Management Handbook**
2. Combining Standards for Model-Based Support of REMH
3. Modeling the Isolette Example
4. Error Discovered and Challenges for Model Management
5. Conclusion and Perspectives

FAA Requirements Engineering Best Practices

DOT/FAA/AR-08/34

Air Traffic Organization
NextGen & Operations Planning
Office of Research and
Technology Development
Washington, DC 20591

Requirements Engineering Management Findings Report

David Lempia and Steven Miller
Rockwell Collins

- Literature and industry practice study conducted

DOT/FAA/AR-08/32

Air Traffic Organization
NextGen & Operations Planning
Office of Research and
Technology Development
Washington, DC 20591

Requirements Engineering Management Handbook

David Lempia and Steven Miller
Rockwell Collins

- Set of best practices to enable successful management of requirements

REMH Best Practices and Supporting Languages


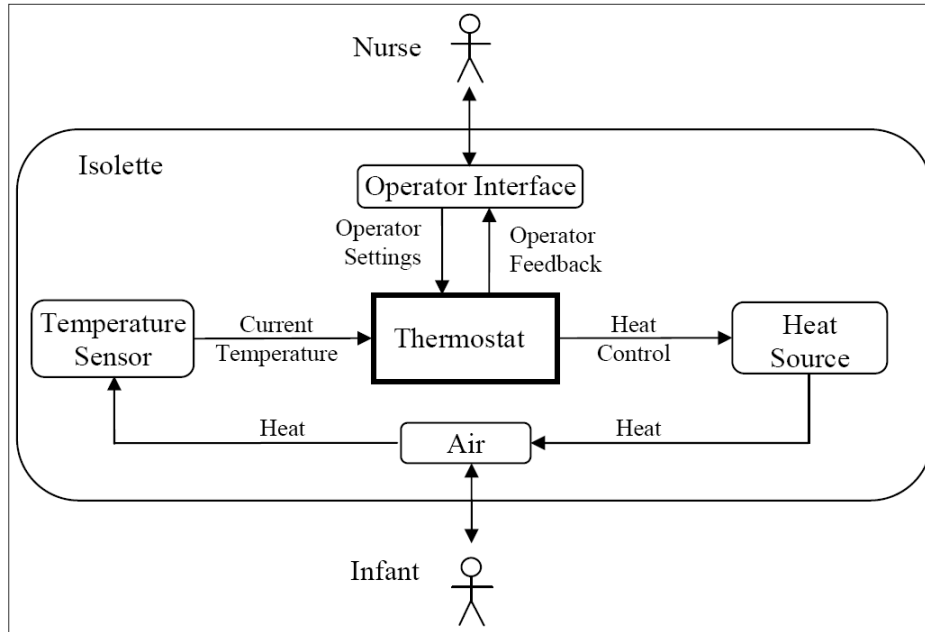
Practice #		Combined Language(s)
1	Develop the System Overview	RDAL, AADL
2	Identify the System Boundary	RDAL, AADL
3	Develop the Operational Concepts	RDAL, URN
4	Identify the Environmental Assumptions	RDAL, AADL
5	Develop the Functional Architecture	RDAL, AADL
6	Revise the Architecture to Meet Implementation Constraints	RDAL
7	Identify System Modes	AADL
8	Develop the Detailed Behavior and Performance Requirements	RDAL, AADL
9	Define the Software Requirements	RDAL, AADL
10	Allocate System Requirements to Subsystems	RDAL, AADL
11	Provide Rationale	RDAL

Chart 7

Best Practices Illustrated via Natural Language Specification Examples



- Isolette thermostat system

Agenda

1. FAA Requirements Engineering Management Handbook
2. **Combining Standards for Model-Based Support of REMH**
3. Modeling the Isolette Example
4. Error Discovered and Challenges for Model Management
5. Conclusion and Perspectives

Many Standards for Model-based Engineering

- Requirements:
 - URN, SysML, etc.
- Embedded systems:
 - AADL, MARTE, AUTOSAR, etc.
- Petri Nets:
 - PNML

- Huge efforts invested in developing these standards and tools
 - E.g.: AADL committee started in 1999
 - 4 meetings per year 2-3 days

- Need to reuse this work; do not reinvent your own language each time

- Architecture Analysis and Design Language
- ADL for safety-critical embedded systems
- SAE-AS5506 Aerospace standard defined by AS-2C subcommittee
- Model software and hardware
- Extensible via definition of annex languages

Benefits of Modeling

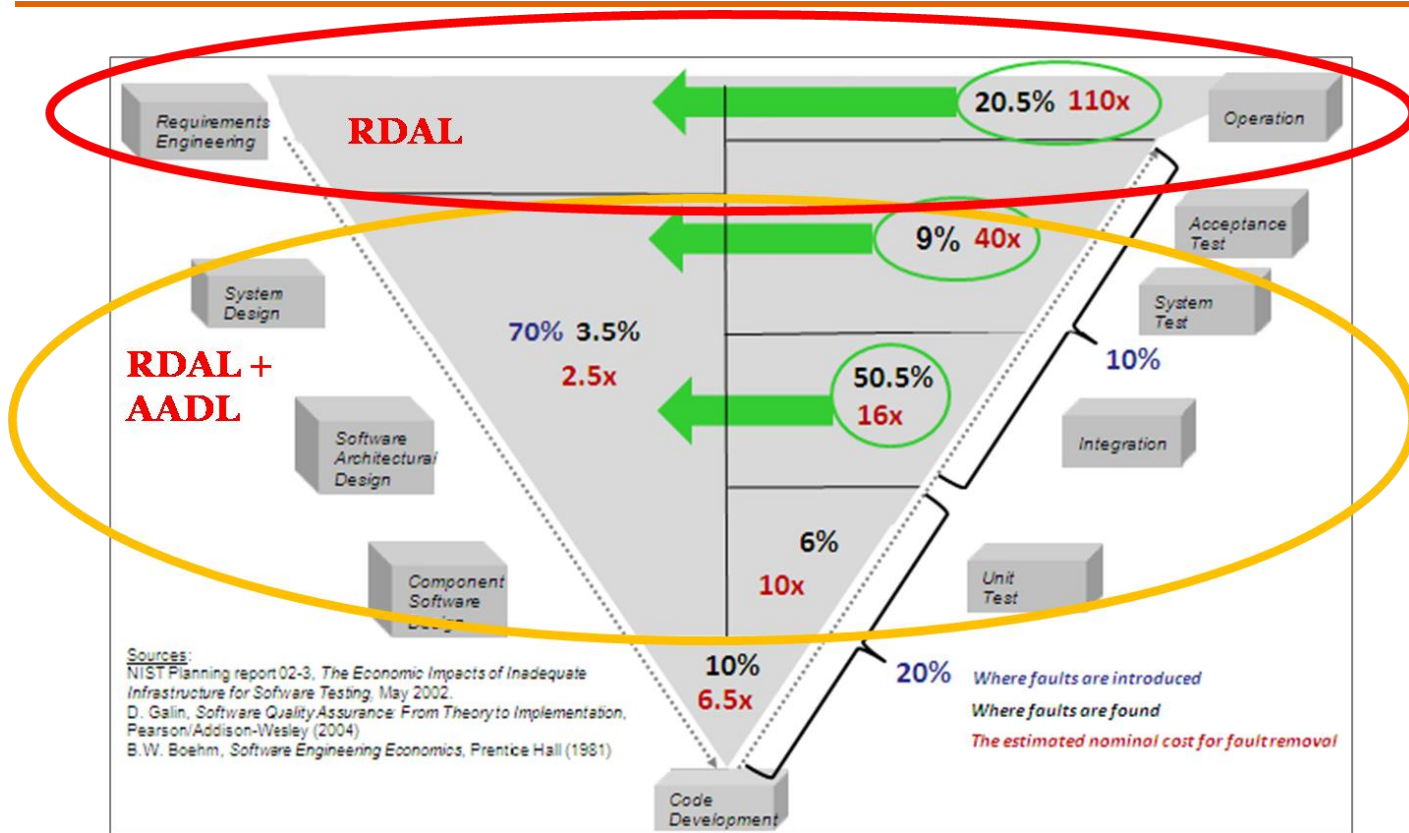


Chart 13

Requirements: RDAL

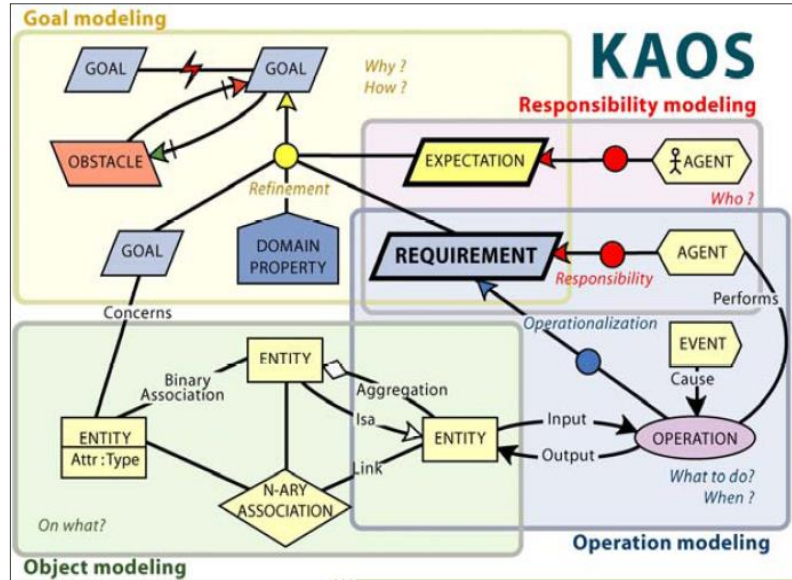
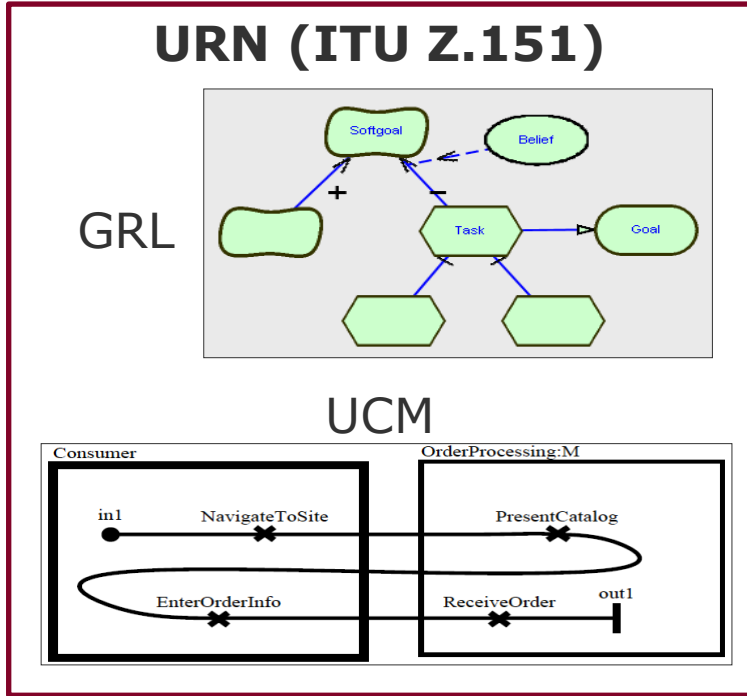
- Requirements Definition and Analysis Language

- *Fragment* language that can be combined with existing languages

- Initially proposed as AADL annex but finally lead to ALISA
 - Architecture-Lead Incremental System Assurance
 - https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_464378.pdf
 - Connects assurance cases with requirements

- RDAL still used for experiments in language composition
 - AADL is growing in a monolithic way...

Why a new Requirements Language?



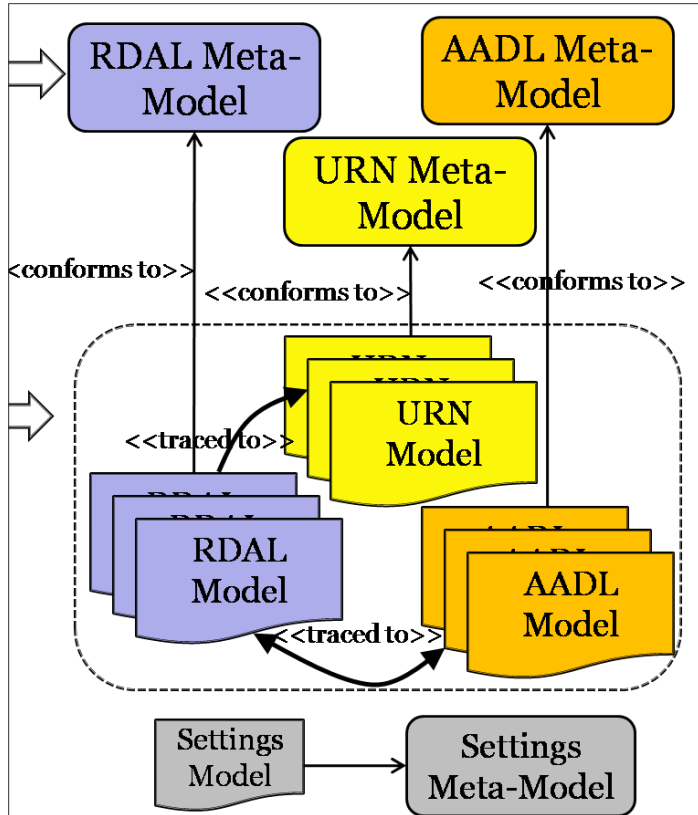
Use Cases: URN (User Requirements Notation)

- ITU Z.150 standard:
 - <http://www.itu.int/rec/T-REC-Z.150/en/>

- 2 sublanguages:
 - GRL (Goal-oriented Requirements Language)
 - UCM (Use case Maps)

- We are interested in UCM
 - Use cases scenarios can be *simulated*

Modular RE Modeling Language



- Usable with several languages (not only AADL)
- Mechanism to specify how to combine the languages
 - Set of predefined traceability references in RDAL
 - System overview, requirements allocation to design, requirement to use case step, goals to use case
 - Typing rules per traceability reference and targeted language

Research Questions

- What benefits can be obtained from the individual languages and from their combination?
- Are state-of-the-art model management techniques sufficient to combine existing independent rich modeling languages while maintaining their independence for reuse?

Agenda

1. FAA Requirements Engineering Management Handbook
2. Combining Standards for Model-Based Support of REMH
- 3. Modeling the Isolette Example**
4. Error Discovered and Challenges for Model Management
5. Conclusion and Perspectives

From Natural Language Specifications to Combined Models

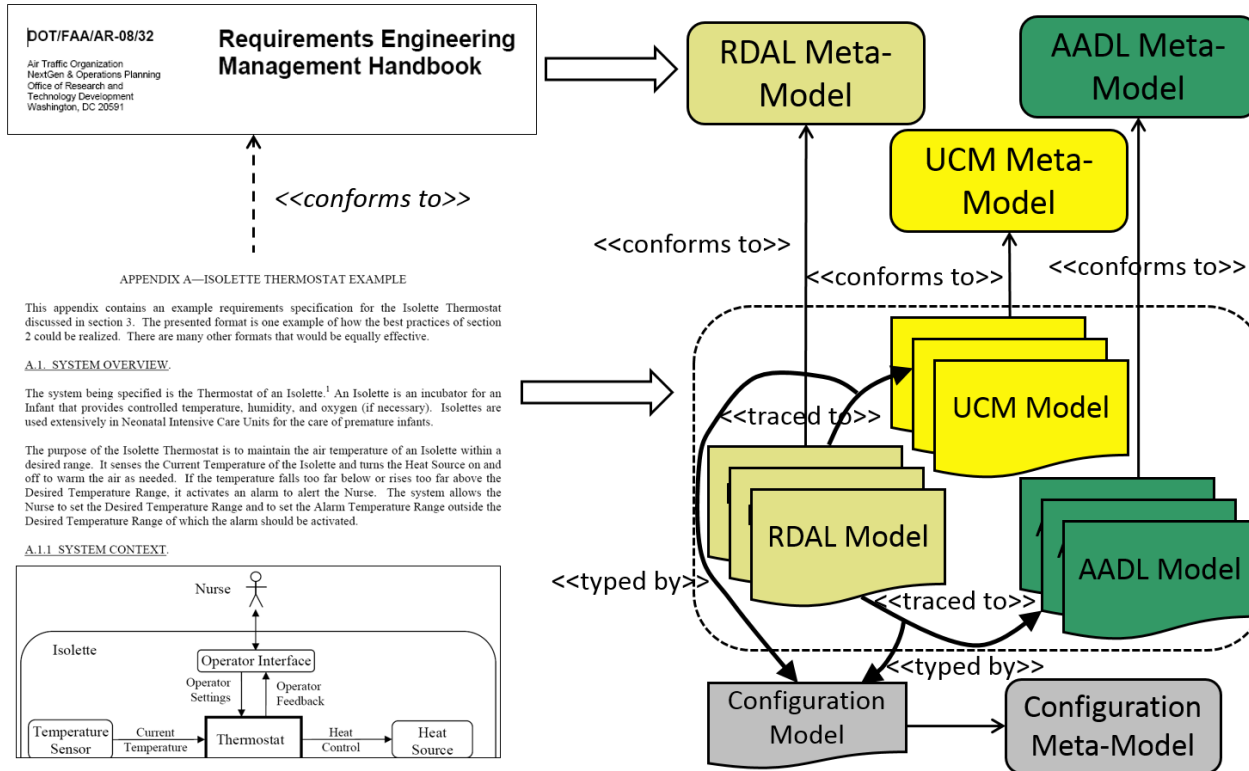
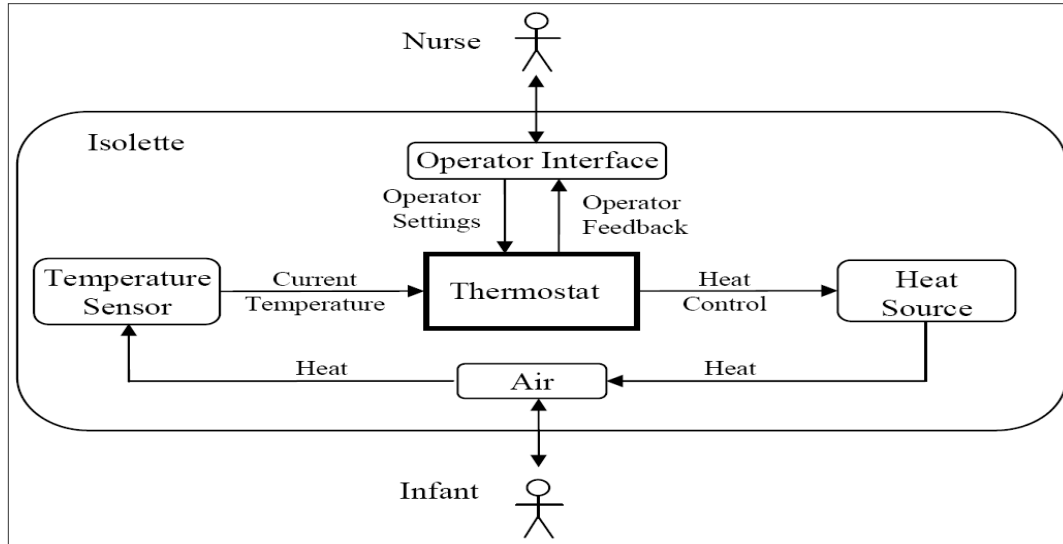


Chart 20

Isolette Thermostat Example



- Maintain constant current temperature
- Additional function introduced for safety reasons:
 - Monitor current temperature

BP #1 and 2: Develop the System Overview / System Boundary

- The system overview serves as an introduction to the system requirements for new people involved in the project.
- Captures high level goals the system should achieve, a brief synopsis, the purpose of the system and its constraints.

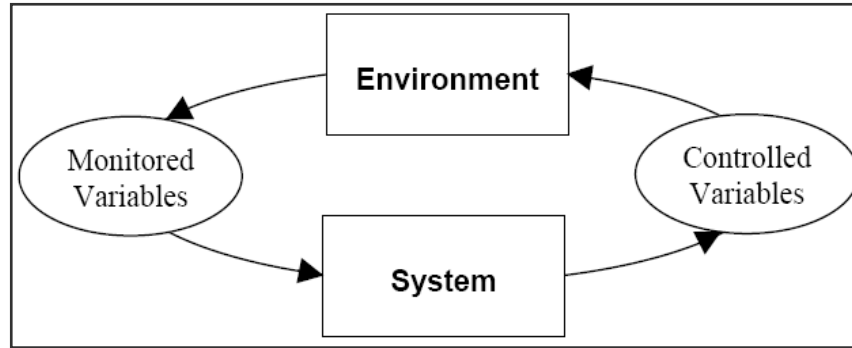
A.1.2 SYSTEM GOALS.

The high-level goals (G) of the system are:

- G1—The Infant should be kept at a safe and comfortable temperature.
- G2—The Nurse should be warned if the Infant becomes too hot or too cold.
- G3—The cost of manufacturing the Thermostat should be as low as possible.

- A crucial step is the definition of a correct system boundary.

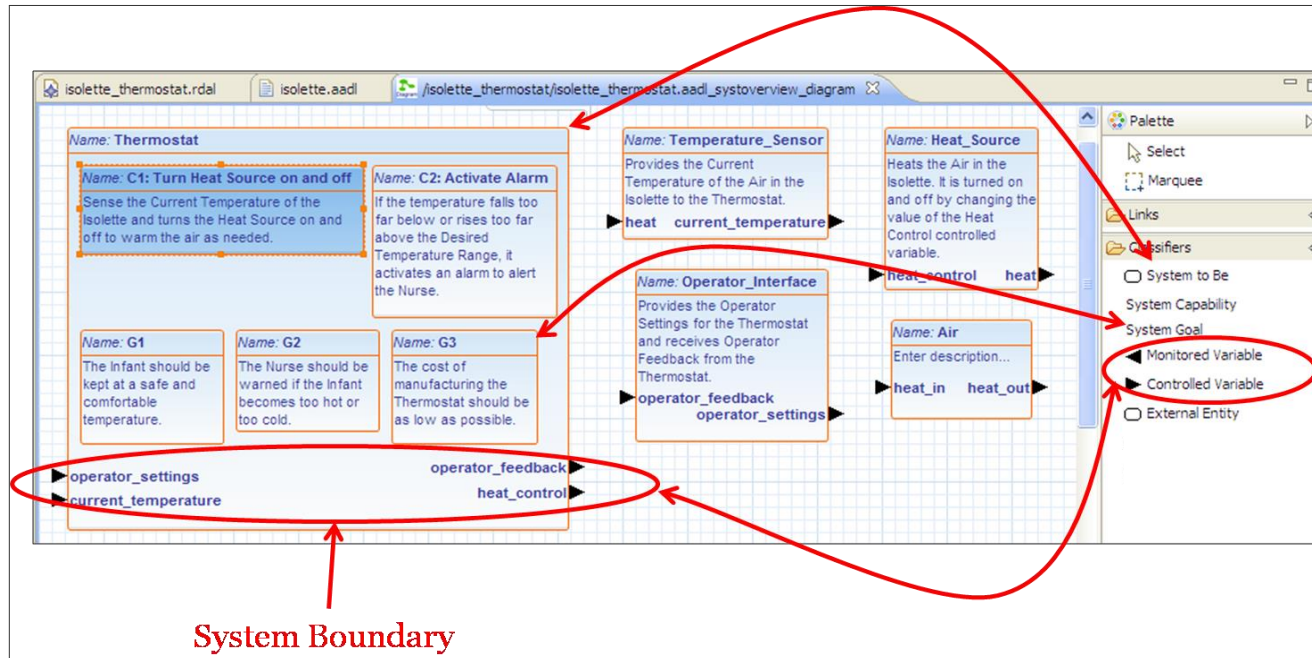
BP #1 and 2: Develop the System Overview / System Boundary



- System requirements define a precise relationship between monitored and controlled variables
- System Boundary == Environment Variables.
- "Getting the system boundary correct is 90 % of the problem!"
 - Stuart Faulk to Steven Miller...

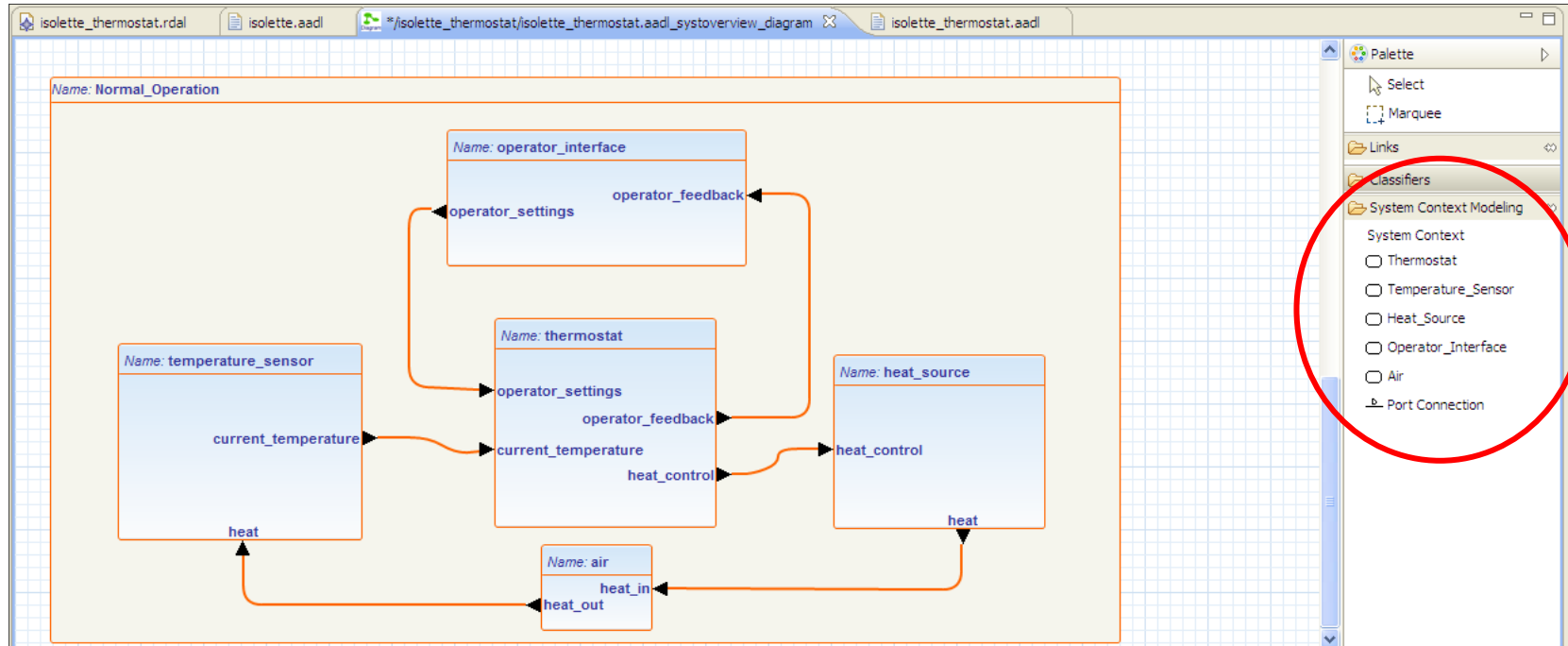
RDAL System Overview Definition

- View editor on model elements from both RDAL and AADL languages



System Context Definition

■ Normal context of operation example

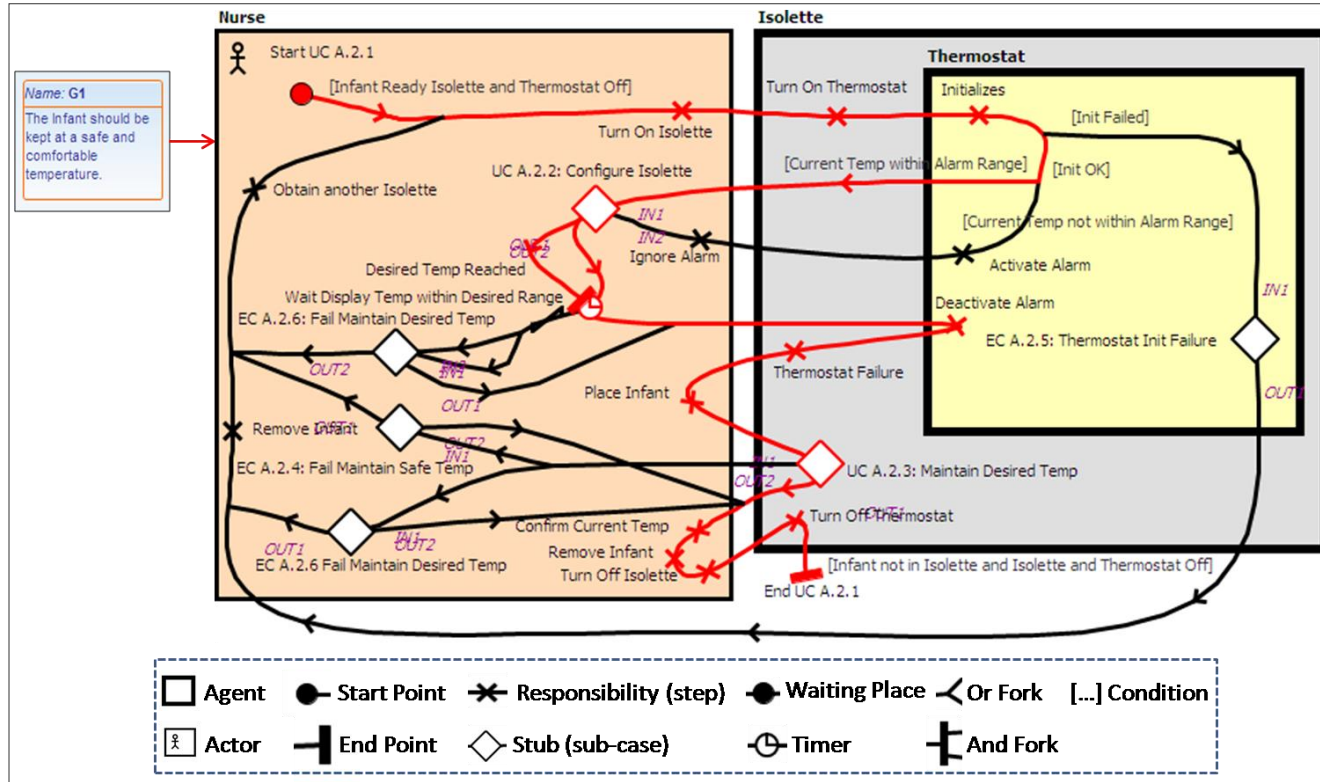


BP #3: Develop the Operational Concepts

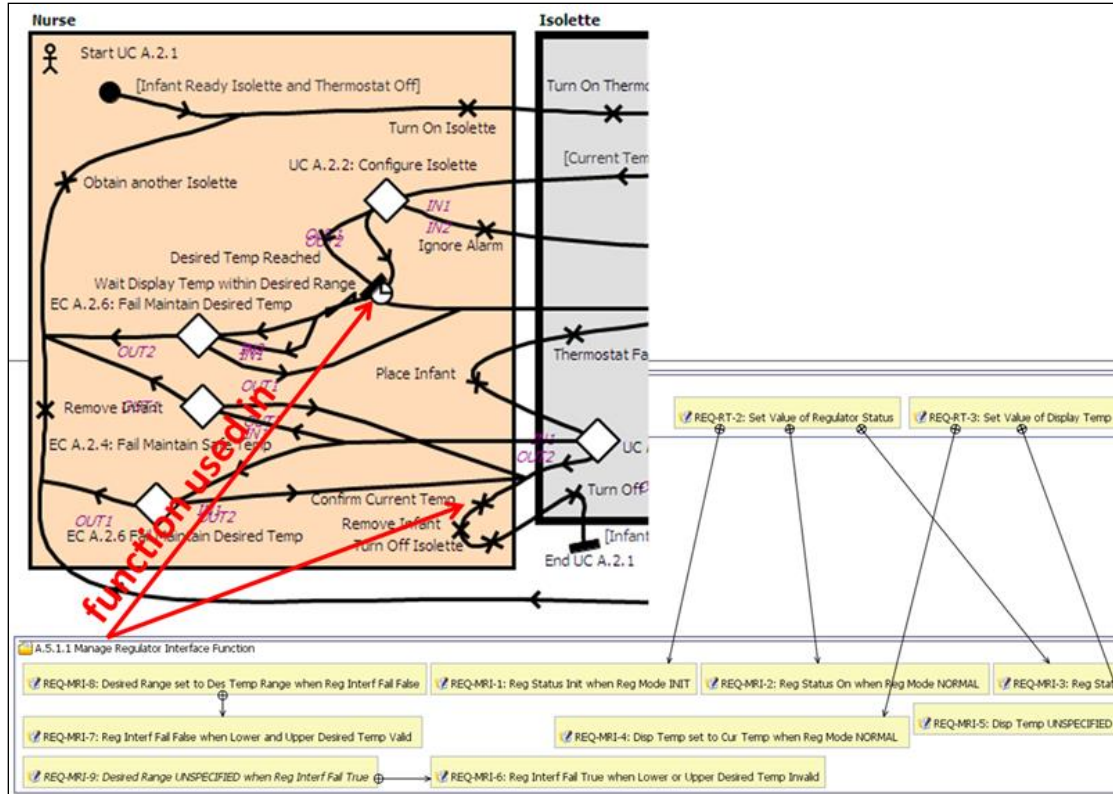
- Use cases are used to discover the functions needed for the system.
- Provides information on the context of use of the functions

- Main Success Scenario:
 1. Nurse turns on the Isolette
 2. Isolette turns on the Thermostat
 3. Thermostat initializes and enters its normal mode of operation (exception case 1) (A.2.5, A.5.1.2 and A.5.2.2)
 4. Nurse configures the Isolette for the needs of the Infant (A.2.2)
 5. Nurse waits until the Current Temperature is within the Desired Temperature Range (A.2.6 and A.5.1.1)
 6. Nurse places the Infant in the Isolette
 7. Isolette maintains Desired Temperature (A.2.3)

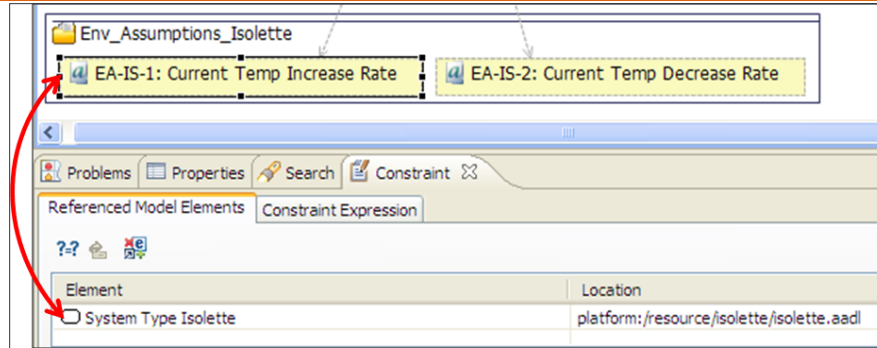
Use Cases Modeling



BP #5: Develop the Functional Architecture Captured as Initial High Level Requirements



Allocate Requirements to Design Model Elements



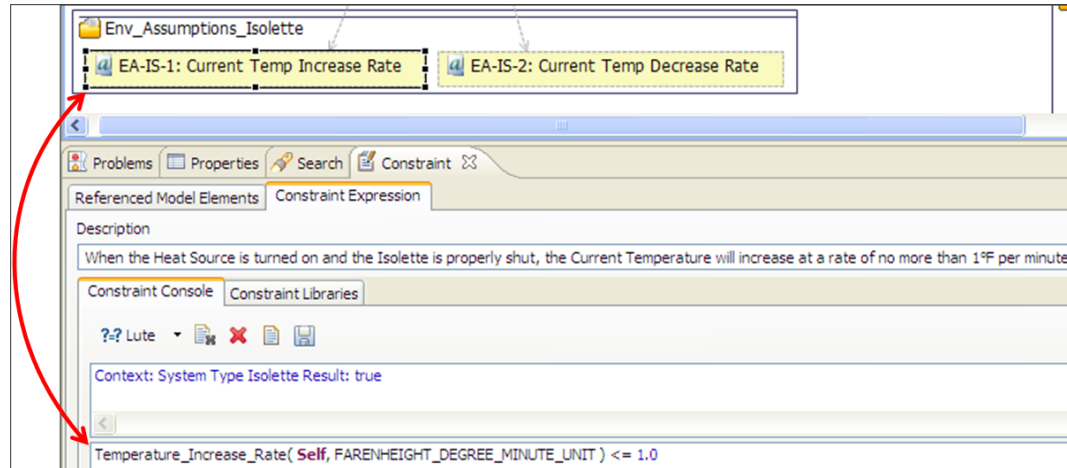
Env_Assumptions_Isolette

EA-IS-1: Current Temp Increase Rate EA-IS-2: Current Temp Decrease Rate

Problems Properties Search Constraint

Referenced Model Elements Constraint Expression

Element	Location
<input type="checkbox"/> System Type Isolette	platform:/resource/isolette/isolette.aadl



Env_Assumptions_Isolette

EA-IS-1: Current Temp Increase Rate EA-IS-2: Current Temp Decrease Rate

Problems Properties Search Constraint

Referenced Model Elements Constraint Expression

Description

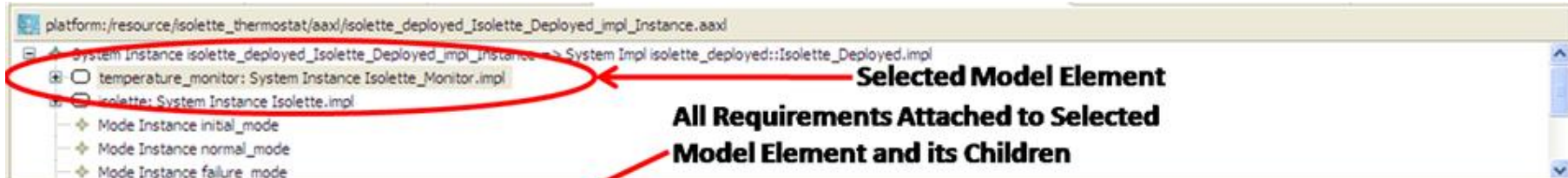
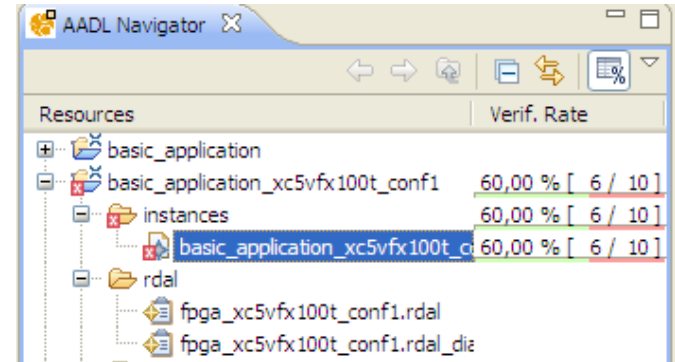
When the Heat Source is turned on and the Isolette is properly shut, the Current Temperature will increase at a rate of no more than 1°F per minute.

Constraint Console Constraint Libraries

Context: System Type Isolette Result: true

Temperature_Increase_Rate(Self, FARENHEIGHT_DEGREE_MINUTE_UNIT) <= 1.0

Automated Verification of Requirements



Selected Model Element
All Requirements Attached to Selected Model Element and its Children

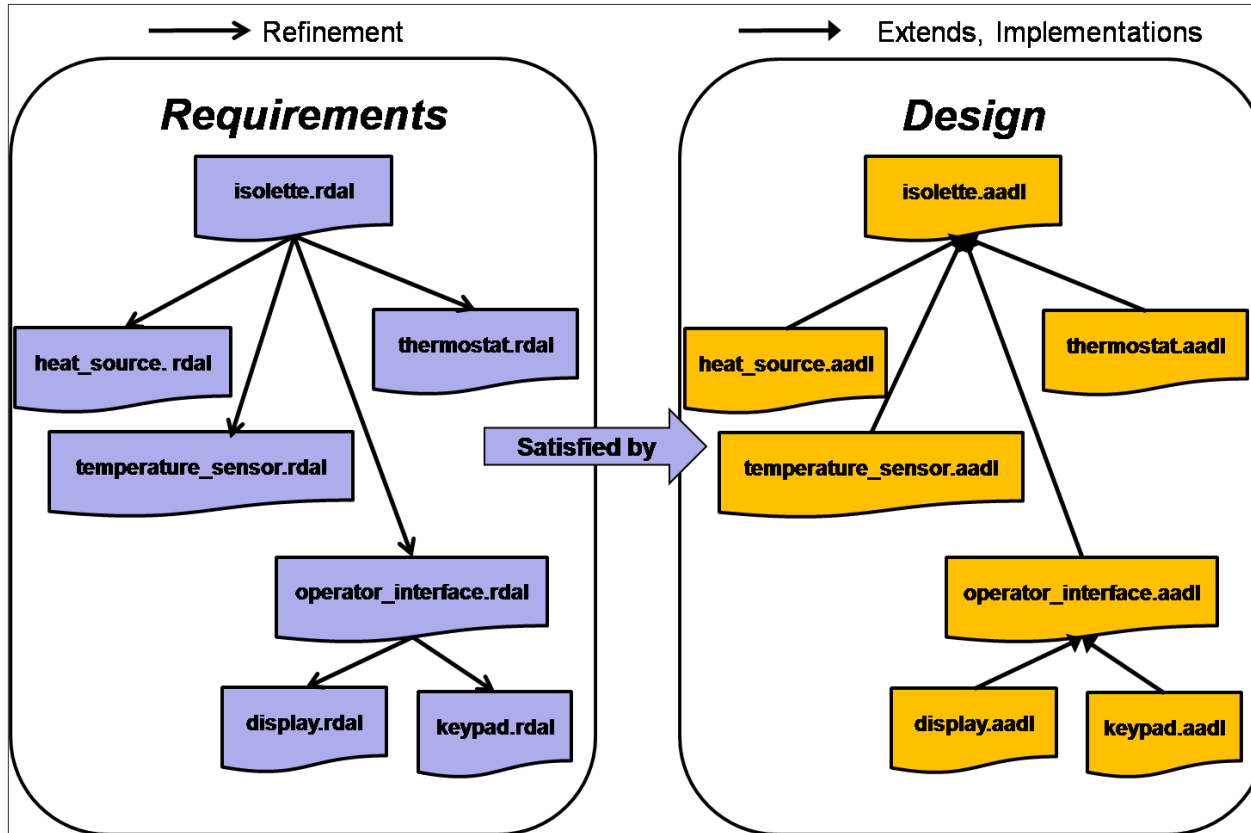
Problems Properties AADL Property Values Traceability

Requirement Referenced Model Elements

Element	Verified	Level (%)	Risk	Type	Description
Requirement MA-2 : Set Alarm when Temperature is out of Safety Range		0.0		Functional	If the Monitor Mode is NORMAL and the Current Temperature is less than the Lower Alarm
temperature_monitor: System Instance					
Requirement MA-4 : Unset Alarm when Temp. is within safety Range		100.0		Functional	If the Monitor Mode is NORMAL and the value of the Current Temperature is greater than
temperature_monitor: System Instance					
Requirement MA-1 : Init Mode Alarm Off		100.0		Functional	If the Monitor Mode is INIT, the Alarm Control shall be set to Off.
temperature_monitor: System Instance					

Chart 30

BP #10: Allocate System Requirements to Subsystems



Agenda

1. FAA Requirements Engineering Management Handbook
2. Combining Standards for Model-Based Support of REMH
3. Modeling the Isolette Example
- 4. Error Discovered and Challenges for Model Management**
5. Conclusion and Perspectives

RQ1: Benefits of Approach

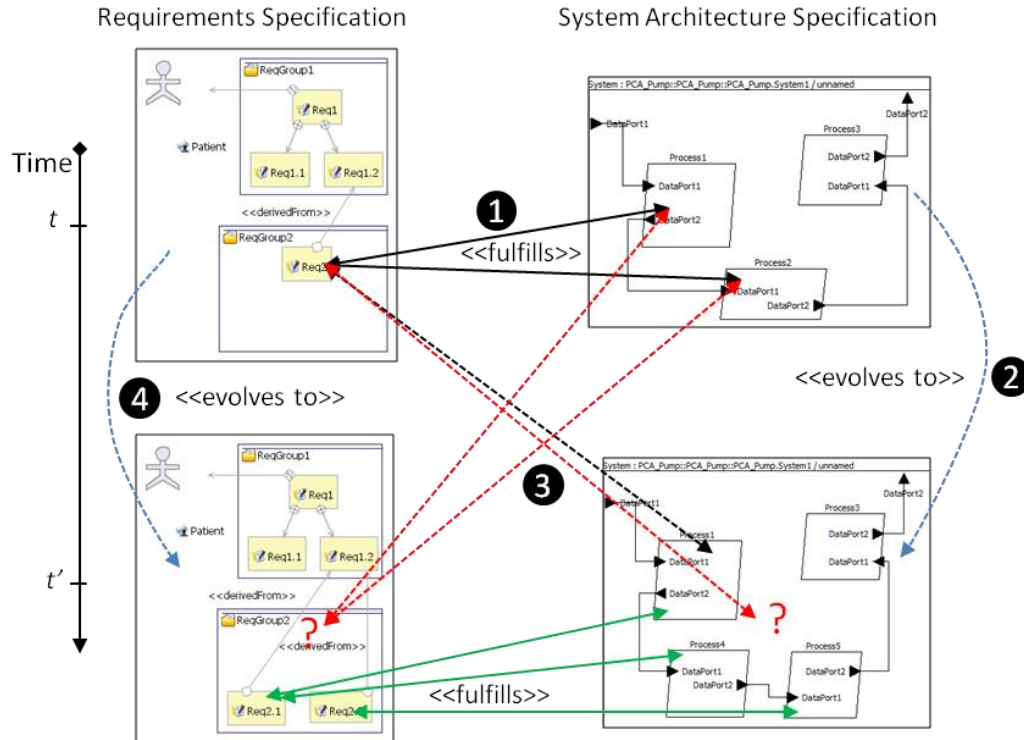
Languages	Nb. Errors	Description
UCM	4	Inconsistencies in pre-and / or post-conditions and variable assignments in use case steps
UCM	6	Omissions of use cases or use case steps
RDAL	1	Incorrect rationale of safety requirement SR2
RDAL, AADL	2	Missing environmental assumptions
RDAL, AADL	1	Vacuous detailed requirement MRI-9

- Remarkable to find so many flaws in the specification of such simple system given as best practice example in an FAA document
- Errors in use cases ripple down to design and tests
- Error in environmental assumptions can lead to catastrophic consequences

- More case studies required for quantitative evaluation

Challenges in Model Management

- RQ2: Model management techniques sufficient?



Model Management Challenges

- How can we ensure model consistency is managed correctly?

- How can we ensure traceability is properly established and maintained in a scalable manner across combined models?
 - RDAL, URN, AADL
 - SysML, AUTOSAR, Modelica, Scade, etc.

- How can we ensure that model operations can be reused and that their execution scales?
 - E.g. automated verification of requirements (RDAL)

Model Management Challenges (cont'd)

- How can we partition existing modeling languages for better reuse?
 - E.g. URN component fragment?

- How can we better compose existing modeling languages for better reuse?
 - RDAL, URN and AADL

- Challenges pertain to MBSE in general

- Existing work is limited and only consists of ad-hoc solutions

Conclusion and Perspectives

- Reusing existing rich modeling languages can be very beneficial
 - Also reuse their tools
 - Combination of languages ensure

- Combining the languages remains a challenge:
 - Syntactically and semantically
 - Must be solved for Model-Based Systems Engineering adoption

- Only few ad-hoc solutions are currently available

- **Foundations on global model management are required**
 - **Keys points: modularity and incrementality**
 - **Unification of approaches into comprehensive megamodeling language**



- Working Group 1: Foundations for MPM4CPS
 - Chair: Holger Giese, Hasso-Plattner Institute
- Contributions welcome (especially from industry)
 - <http://mpm4cps.eu/>

Thank you
for your attention!