

A Component-Based Model-Driven Approach with traceability of concerns: Railway RBC Handover Case Study

YRS 2015, Roma, Italy

Marc Sango

PhD candidate, University of Lille 1 and
IFSTTAR, France

marc.sango@ifsttar.fr



IFSTTAR



Outline



- **What Standards Require About Model Driven Engineering (MDE)?**
- **What is not Addressed by Railway EN-50128 Standard for MDE?**
- **Our Approach: A unified meta-Model and its application process**
- **Evaluation through the RBC-RBC Handover Case Study**
- **Discussion and Conclusion**



What Standards Require About Model-Driven Engineering?

- All Standards for **safety-critical transportation software** acknowledge the model-driven development and V&V approach

- **Railway:** CENELEC EN 50128 Railway applications - Communication, signaling and processing systems - Software for railway control and protection systems

- **Avionic:** RTCA DO-178B Software considerations in airborne systems and equipment certification

- **Automotive:** ISO 26262 Road vehicles - Functional safety

What Standards Require About Model-Driven Engineering?

➤ All Standards for safety-critical transportation software **acknowledge more and less** the model-driven development and V&V approach

➤ **Avionic:** RTCA DO-178B Software considerations in airborne systems and equipment certification

➤ The **new DO-178C** standard is complemented by **DO-331 for Model-Based Development and Verification Supplement**

➤ **Automotive:** ISO 26262 Road vehicles – Functional safety :

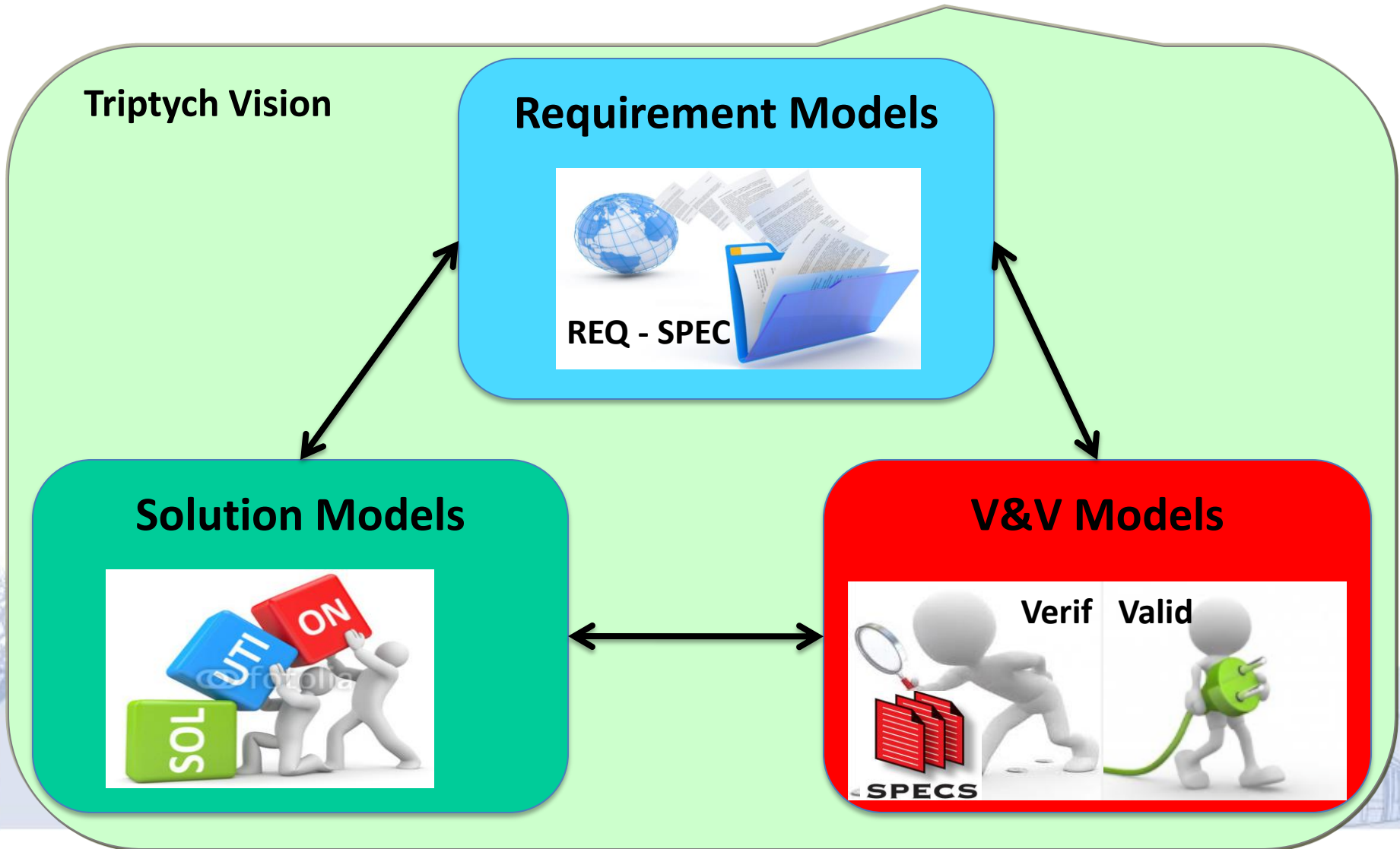
➤ **Part 6:** Product development: software level – **Appendix B: Model-based development**

➤ **Railway:** CENELEC EN 50128:**2011** Railway applications - Communication, signaling and processing systems - Software for railway control and protection systems

➤ **“Model-driven” is used only once in the informative annex**

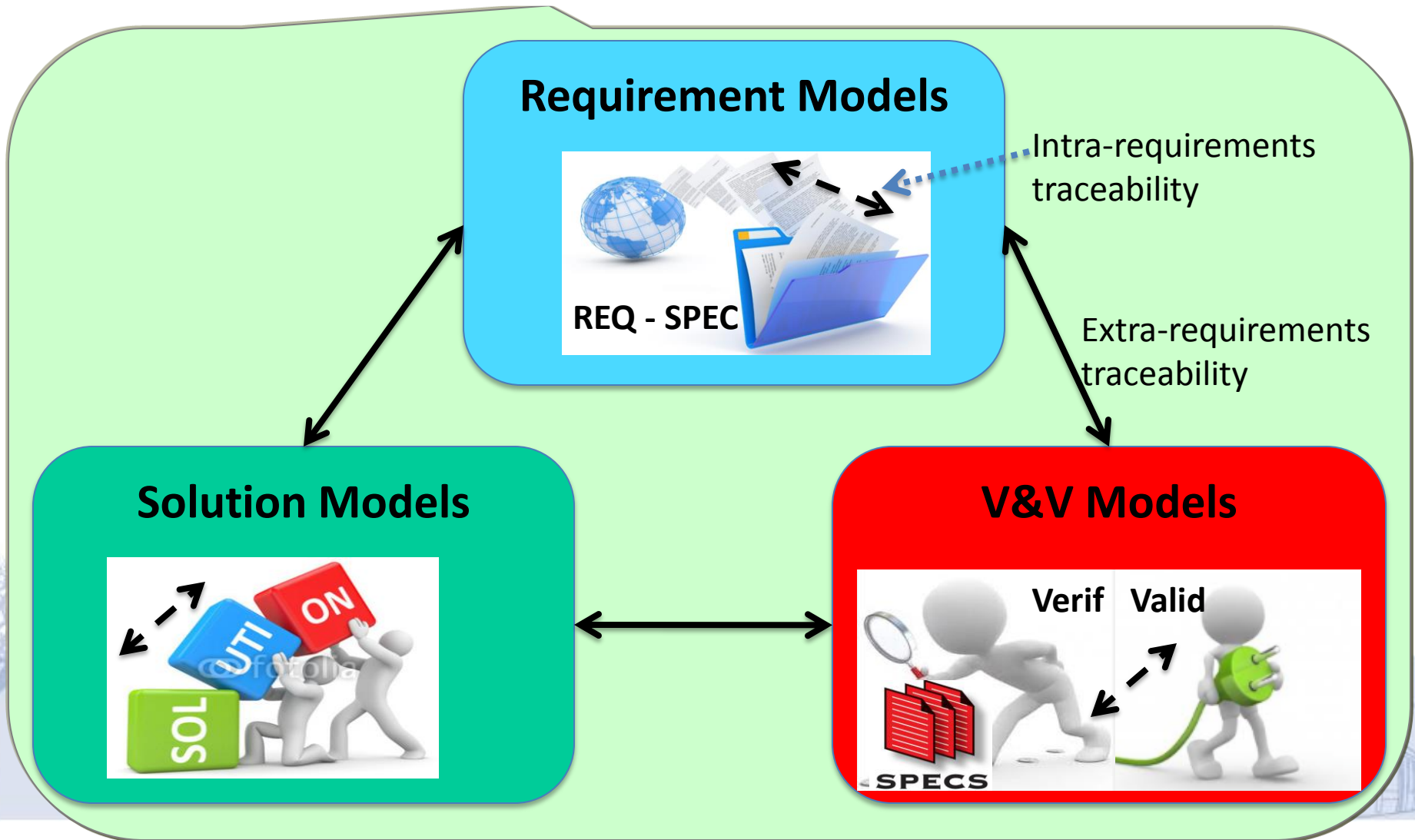
What Standards Require About Model-Driven Engineering?

- All Standards for safety-critical transportation software acknowledge more and less the **model-driven development** and **V&V** approach



What is not addressed by the Standards for MDE?

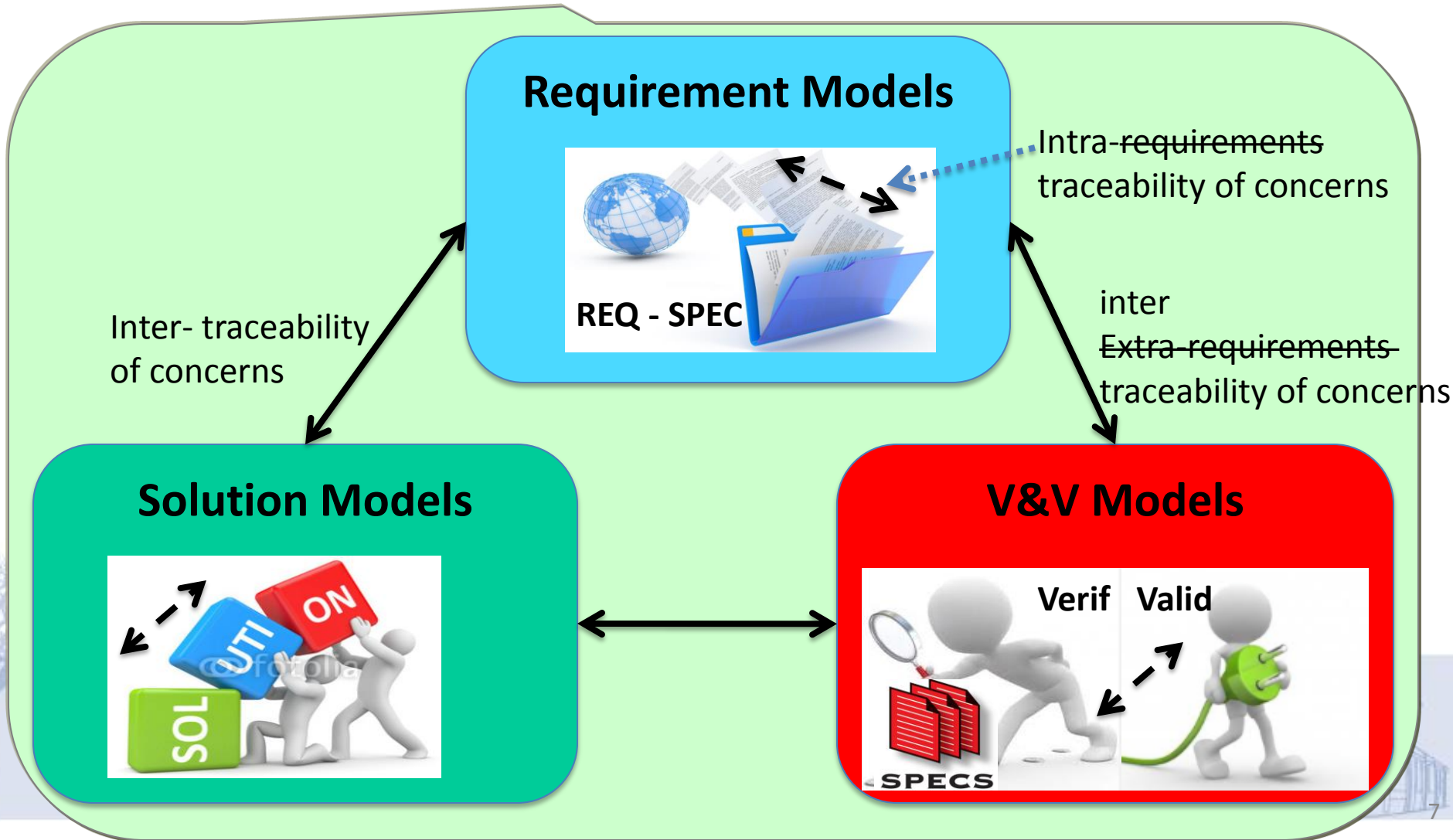
1. How are requirements **traced** in the models?



What is not addressed by the Standards for MDE?

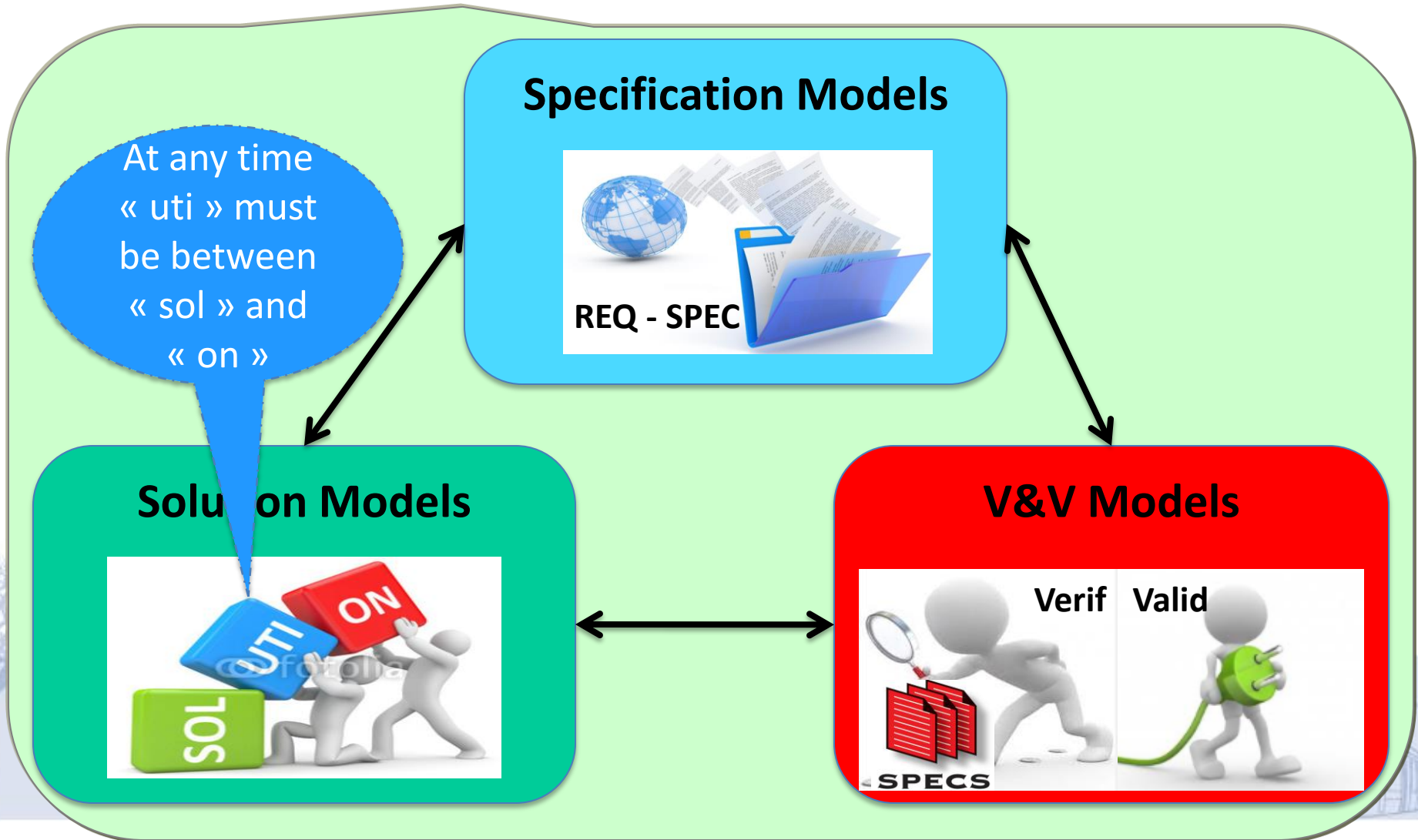
1. How are requirements traced in the models?

Instead of **requirement traceability** we prefer the name **traceability of concerns**



What is not addressed by the Standards for MDE?

1. How are requirements traced in the models?
2. How can **temporal constraints** be modeled and verified?



What is not addressed by the Standards for MDE?

1. How are requirements traced in the models?
2. How can **temporal constraints** be modeled and **verified**?

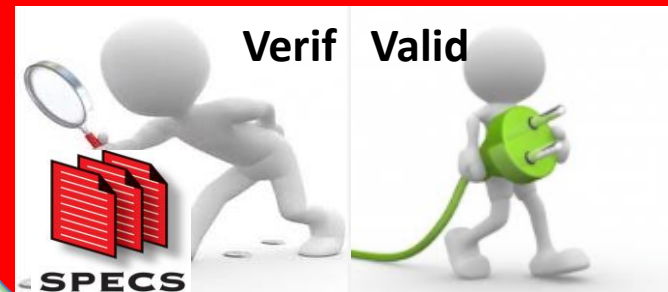
At any time
« uti » must
be between
« sol » and
« on »



Solution Models



V&V Models



What is not addressed by the Standards for MDE?

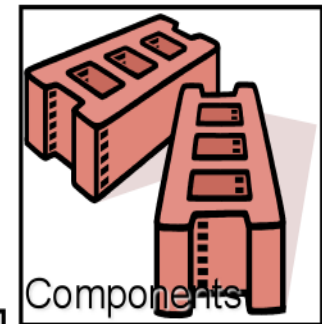
1. How are requirements traced in the models?
2. How can temporal constraints be modeled and verified?
3. How are requirements concretely **reflected** in the models?

Component-Based Development

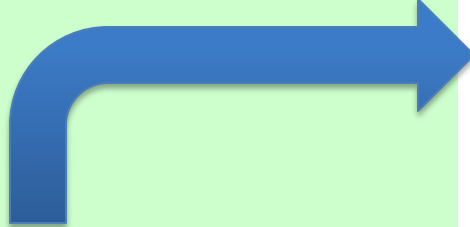
Component model



Component repository



Reflected by



Solution Models



Component Framework

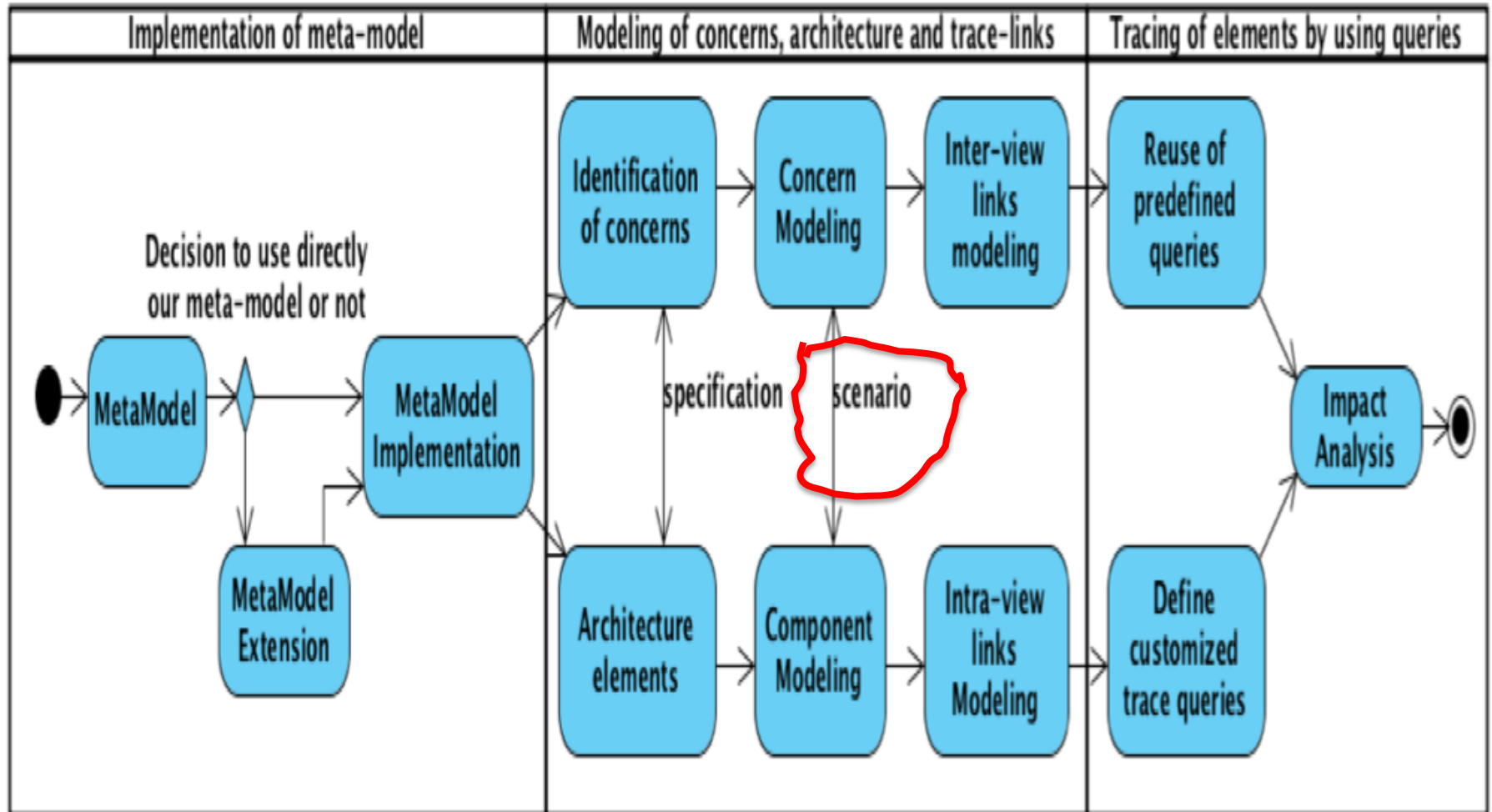
Summary of the motivation context

- We have seen that standards require about MDE for quality reasons
- We have also seen that they do not address specific questions, such as a concrete realization of a solution model.
- Then, we saw that the component-based MDE is one response to this question.
- Let us now introduce our component-based MDE approach



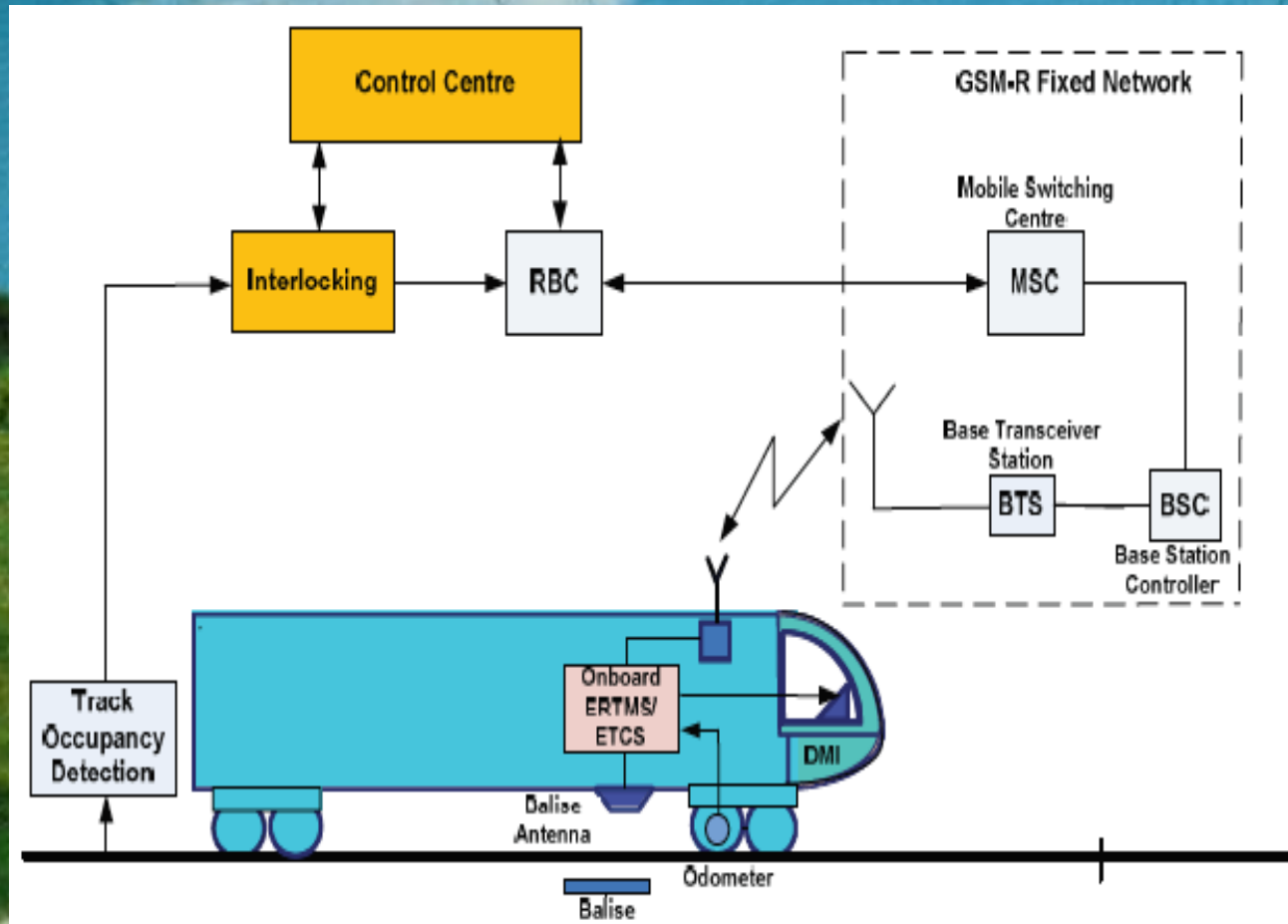
Our approach: Application Process

Generic process that can be used to instantiate the meta-models



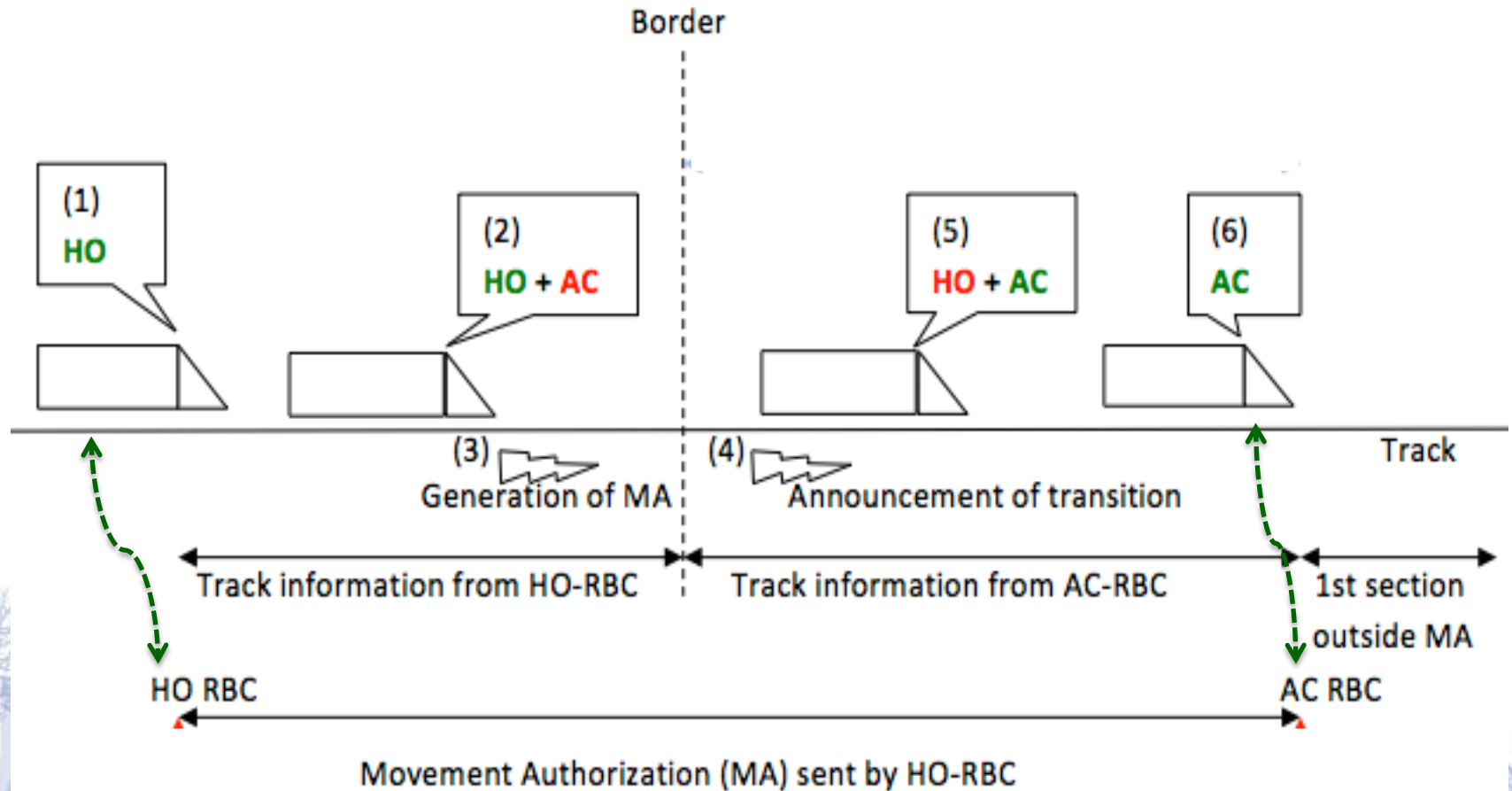
Evaluation: Scenario definition phase

- RBC-RBC Handover scenario in ERTMS/ETCS Systems



Evaluation: Scenario definition phase

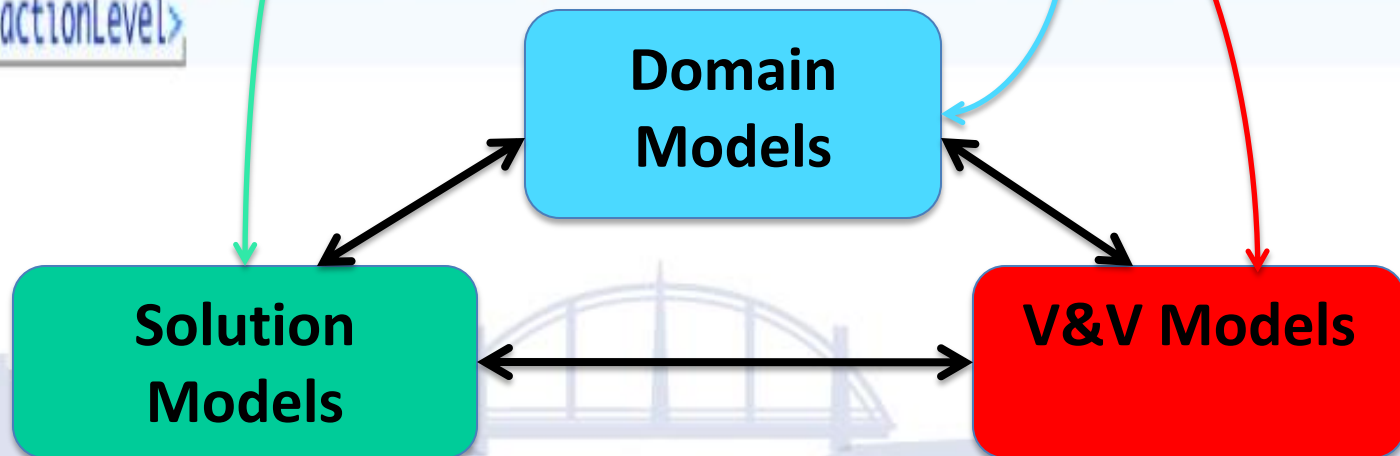
RBC-RBC Handover scenario



Evaluation: Modeling and Verification phase

concern-model.dtd X component-model.dtd X trace-model.dtd X RBC-model-views.xml X

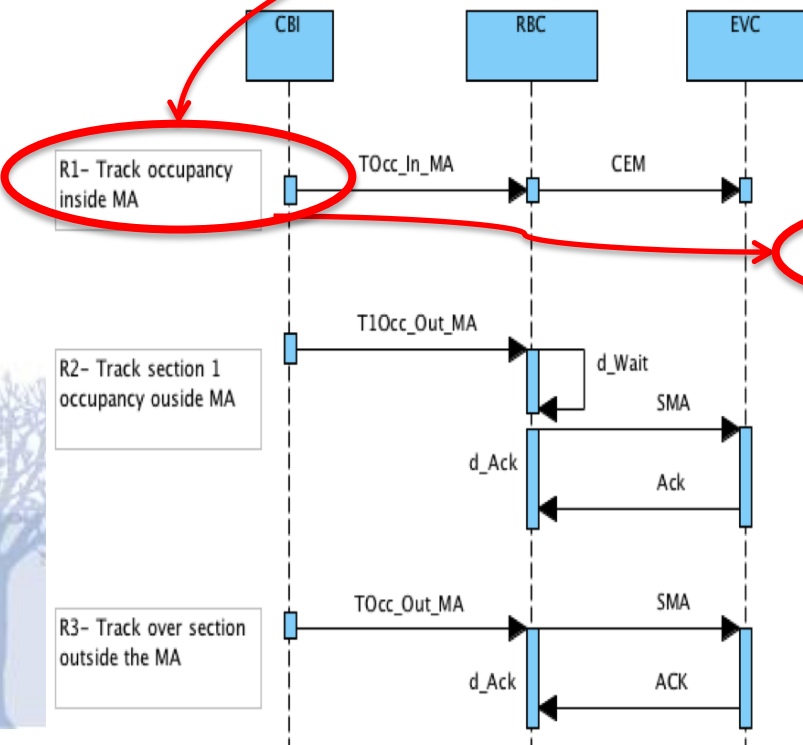
```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE ModelAbstractionLevel PUBLIC "ModelAbstractionLevel" "component-model.dtd">
3 <ModelAbstractionLevel id="RBC_USE_1" ref="" name="RBC handover use case model">
4   <CompView id="Sara_View_ID" ref="RBC-Sara-model-view.xml" type="model design view"></CompView>
5   <CompView id="Uppaal_View_ID" ref="RBC-Uppaal-verification-view.xml" type="model analysis view"></CompView>
6   <CompView id="Ada_View_ID" ref="RBC-Ada-implementation-view.xml" type="model implementation view"></CompView>
7 </ModelAbstractionLevel>
```



Evaluation: Tracing phase

```

    • trace-model.dtd × | • trace-model.xml × | • forwardtrace.xquery × | • predefinedtrace.xquery ×
    24 (: Declaration of forward trace query:)
    25 <math>\sphericalangle</math> declare function oxy:ForwardTraceQuery($oxy:view as xs:string, $oxy:query as xs:string) {
    26     let $link := $TargetQuery ($oxy:query)
    27     return
    28         if (empty ($link)) then $oxy:query
    29         else $oxy:query union oxy:ForwardTraceQuery ($view, $SourceQuery)
    30 };
    31
    32 <math>\sphericalangle</math> <Query_Result>
    33     {oxy:ForwardTraceQuery(".", "NFC_REQ_1")}
    34 </Query_Result>
    35
  
```



	A	B	C	D	E	F
1	Requirement definition			Validation results		
2	REQ ID	Observer pattern	Expected output	Output	Status	Comment
3	R1	CEM must hold even if ACK never occurs.	CEM	CEM	PASSED	Validation with UPPAAL tool
4	R2	Wait a max delay before UEM	ACK(165,172)	UEM(145,146)	FAILED	Validation with UPPAAL tool
5	R3	Response ACK pattern	ACK	ACK	PASSED	Validation with UPPAAL tool
6	R4				UNCHECKED	No value supplied

Traceability Matrix

Evaluation: Cost Benefits Analysis

$$\text{C\&P-COSTSAVING} = FS_{cost} - (S_{cost} + A_{cost} + D_{cost} + Q_{cost})$$

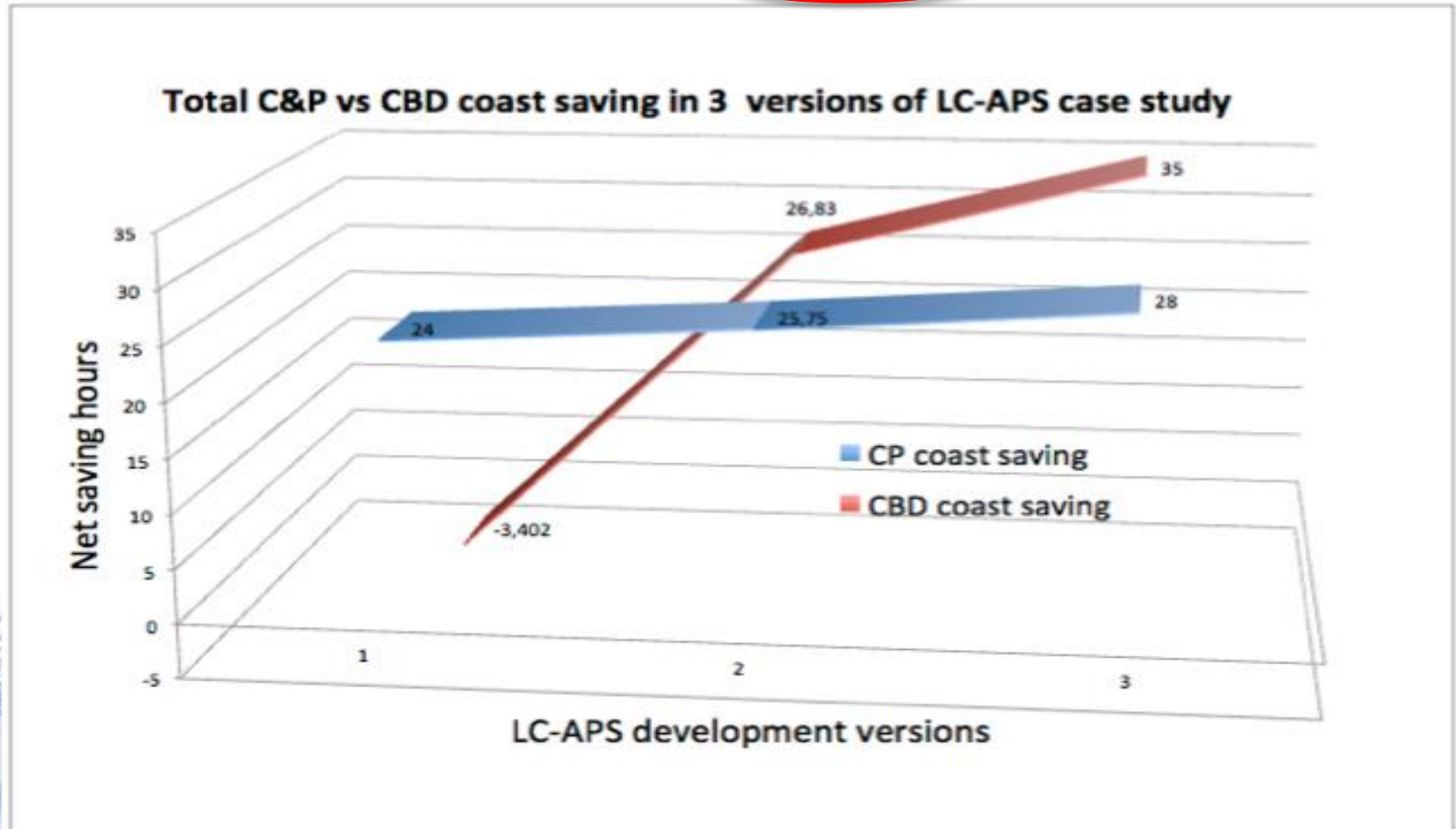
$$\text{CBD-COSTSAVING} = FS_{cost} - (S_{cost} + R_{cost} + GD_{cost} + T_{cost} + A_{cost} + D_{cost} + Q_{cost})$$



Evaluation: Cost Benefits Analysis

$$\text{C\&P-COSTSAVING} = FS_{cost} - (S_{cost} + A_{cost} + D_{cost} + Q_{cost})$$

$$\text{CBD-COSTSAVING} = FS_{cost} - (S_{cost} + R_{cost} + GD_{cost} + T_{cost} + A_{cost} + D_{cost} + Q_{cost})$$



Discussion & Conclusion

Categories	Sub-categories	Approaches	Discussion criteria		
			Traceability	Interoperability	Certification
General-Purpose	OOP-Based	EJB			
		Fractal			
	ADL-Based	AADL	(✓)		
		Pin			
Specialized-Purpose	OOP-Based	Think			
		CHESS			
	ADL-Based	ProCom		(✓)	
		IEC-61499		(✓)	✓
		SARA	✓	✓	✓
		AUTOSAR	(✓)	✓	✓

Our solution is a triple meta-models towards a traceability of concerns but in the same UML based formalism

Discussion & Conclusion

We formally define interoperability of our component model interface. This provides a baseline for other rules, such as component composition.

Categories	Sub-categories	Approaches	Discussion criteria			
			Traceability	Interoperability	V&V	Certification
General Purpose				(✓)		
				(✓)	(✓)	
				(✓)	✓	(✓)
				(✓)	✓	(✓)
Specialized Purpose				(✓)	(✓)	
				(✓)	(✓)	
				(✓)	(✓)	
		ProCom		(✓)	(✓)	
		IEC-61499		(✓)	✓	✓
		SARA	✓	✓	✓	
		AUTOSAR	(✓)	✓	✓	✓

Discussion & Conclusion

The formal model is used in the model transformation into a verification model for which we can use formal verification tool.

Categories	Sub-categories	Approaches	Discussion criteria		
			Interoperability	V&V	Certification
General-Purpose	OO		(✓)		
				(✓)	
				✓	(✓)
				✓	(✓)
Specialized-Purpose	OO		(✓)	(✓)	
			(✓)	(✓)	
				(✓)	
	ADL-Based	ProCom		(✓)	
		IEC-61499		(✓)	✓
		SARA	✓	✓	✓
		AUTOSAR	(✓)	✓	✓

Discussion & Conclusion

As in academic component models certification support is weaker in our model. However, it is crucial to develop a solid understanding of the impact from individual components on the overall dependability of the system for certification reason.

Categories	Sub-categories	Discussion criteria			
		Dependability	V&V	Certification	
General-Purpose			(✓)		
			✓	(✓)	
			✓	(✓)	
Specialized-Purpose			(✓)		
			(✓)		
	ADL-Based	ProCom		(✓)	
		IEC-61499		(✓)	✓
		SARA	✓	✓	✓
	AUTOSAR	(✓)	✓	✓	

Discussion & Conclusion

Traceability



- We have compared the most relevant work related to traceability of concerns,
- and highlight the benefits for component based model driven development.

Interoperability



- In addition to current component models rules, such as composition and reusability,
- we have defined interoperability, by highlighting domain knowledge.

V&V



- Model transformation is used to transform our high level model
- into a TA model for which we have used UPPAAL model checker for verification.

Certification



- The certification support is generally weaker in academic component models,
- mostly due to extensive cost and the need of clear industrial application.

Thanks for your attention



Marc Sango
PhD candidate,
IFSTTAR/COSYS/LEOST
marc.sango@ifsttar.fr

