Functional Safety Management with EA

Dr. Konrad Wieland, LieberLieber

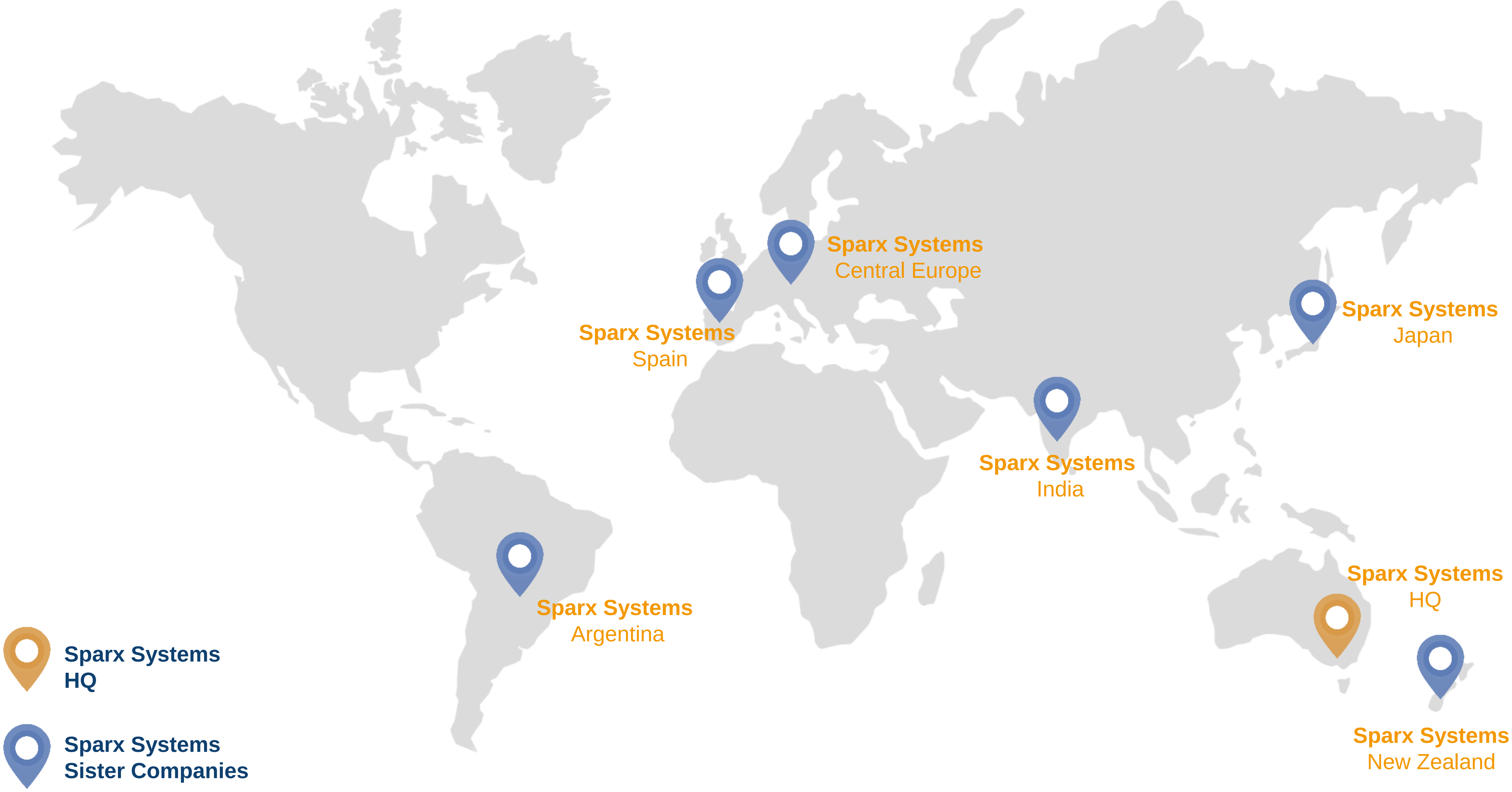
Markus Schwarz, Vector

Stuttgart, 21.2.2017

SPARX SYSTEMS
Central Europe

Enterprise Architect

create | verify | share


Sparx Systems
Central Europe
Sparx Systems
Spain
Sparx Systems
Japan
Sparx Systems
India
Sparx Systems
Argentina
Sparx Systems
HQ
Sparx Systems
New Zealand
Sparx Systems
HQ
Sparx Systems
Sister Companies

Peter Lieber

SPARX SYSTEMS Central Europe

LieberLieber

OMG OBJECT MANAGEMENT GROUP

GfSE Gesellschaft für Systems Engineering e.V. German Chapter of INCOSE

Microsoft Gold Partner

ENTERPRISE ARCHITECT

My Background

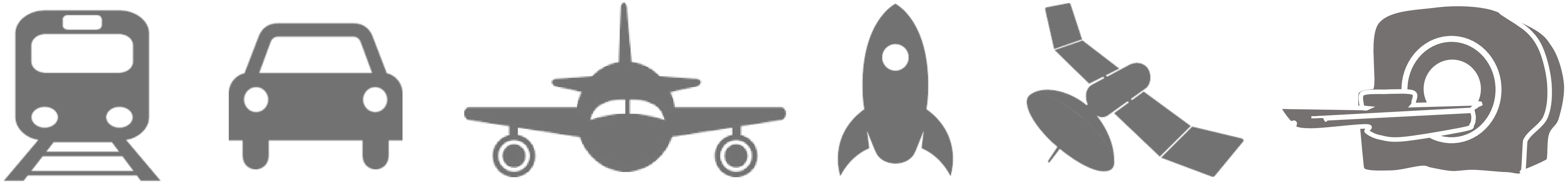
- OOM & Model Engineering, TU Vienna
- 2011 PhD: Model Versioning, TU Vienna
- Sparx Trainer & Consultant
- LieberLieber Product Manager

Agenda

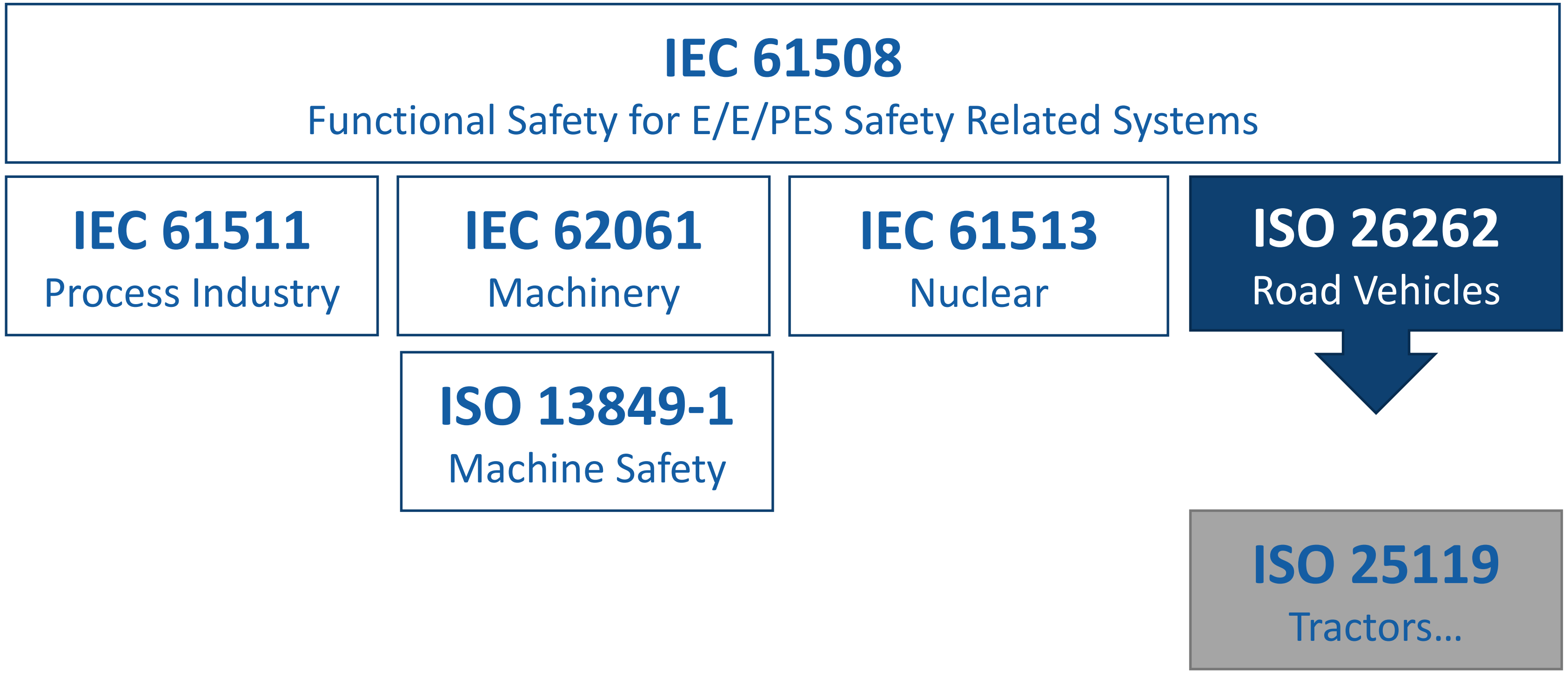
- „Safety needs models“
- Challenges for EA
    - Notation and Profiles
    - Tracability
    - Configuration & Change Management
- And how they are solved at Vector Informatik GmbH

Managing Complexity

We will target Companies manufacturing safety relevant Cyber Physical Systems



ISO 26262 Adaptation of IEC 61508



IEC 61508

Functional Safety for E/E/PES Safety Related Systems

IEC 61511

Process Industry

IEC 62061

Machinery

IEC 61513

Nuclear

ISO 26262

Road Vehicles

ISO 13849-1

Machine Safety

ISO 25119

Tractors…

ISO 26262 is “State of the Art” For Automotive
Developed with OEM

Complexity on the one Hand and Safety on the other

Growing Complexity of Environment and Solutions

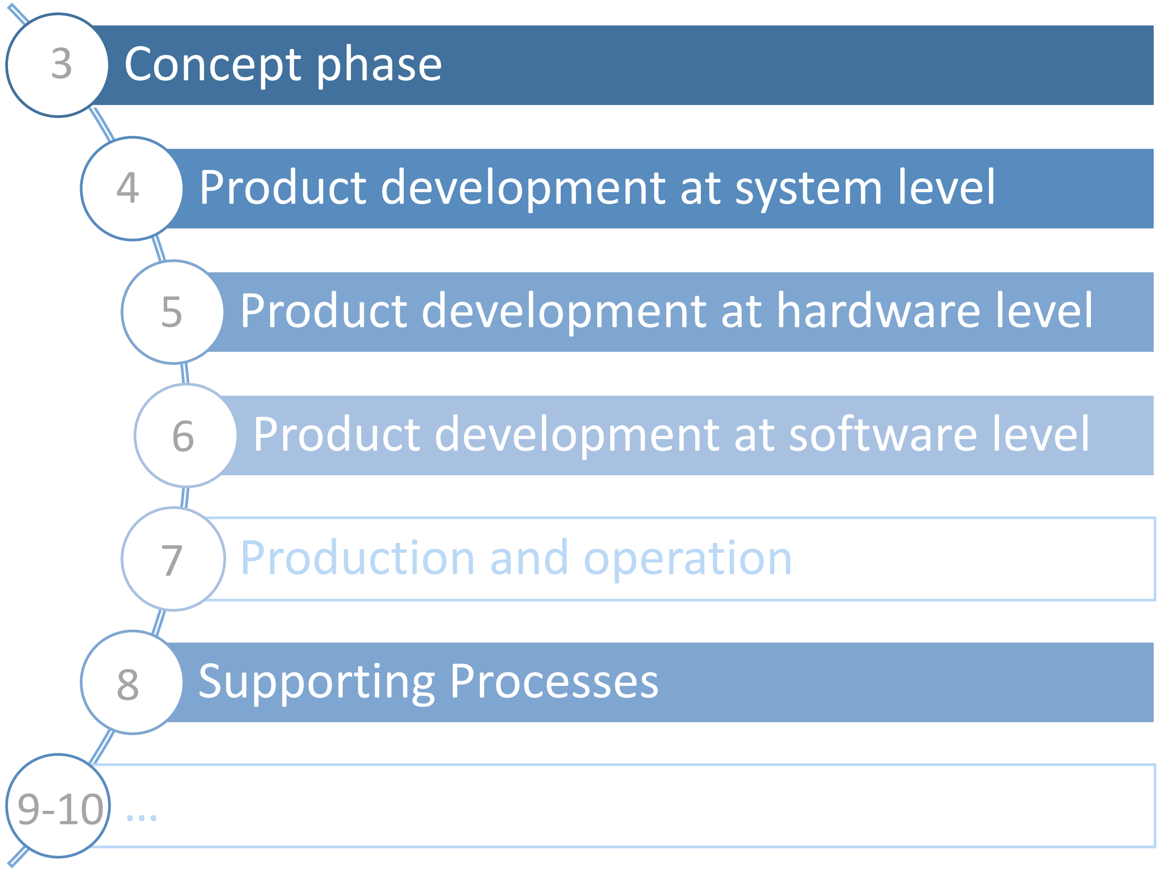
Complex Processes, Distributed Teams

Safety in General and Safety Standards in Particular

- IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
- ISO 26262 - Road Vehicles Functional Safety
- IEC 62304 - Medical Device Software
- EUROCAE ED-12B European Airborne Flight Safety Systems
- IEC 61513 - Nuclear power plants
- IEC 62061 - Safety of machinery
- EN 50128, 50129 - Railway Industry

ISO 26262 Parts relevant for Modeling

Other Standards are similar



- 3 Concept phase
- 4 Product development at system level
- 5 Product development at hardware level
- 6 Product development at software level
- 7 Production and operation
- 8 Supporting Processes
- 9-10 …

3

- Handles Hazard Analysis and Risk Assessment has impact on development process
- Tracking and Traceability of ASI-Level from requirements to tests is necessary

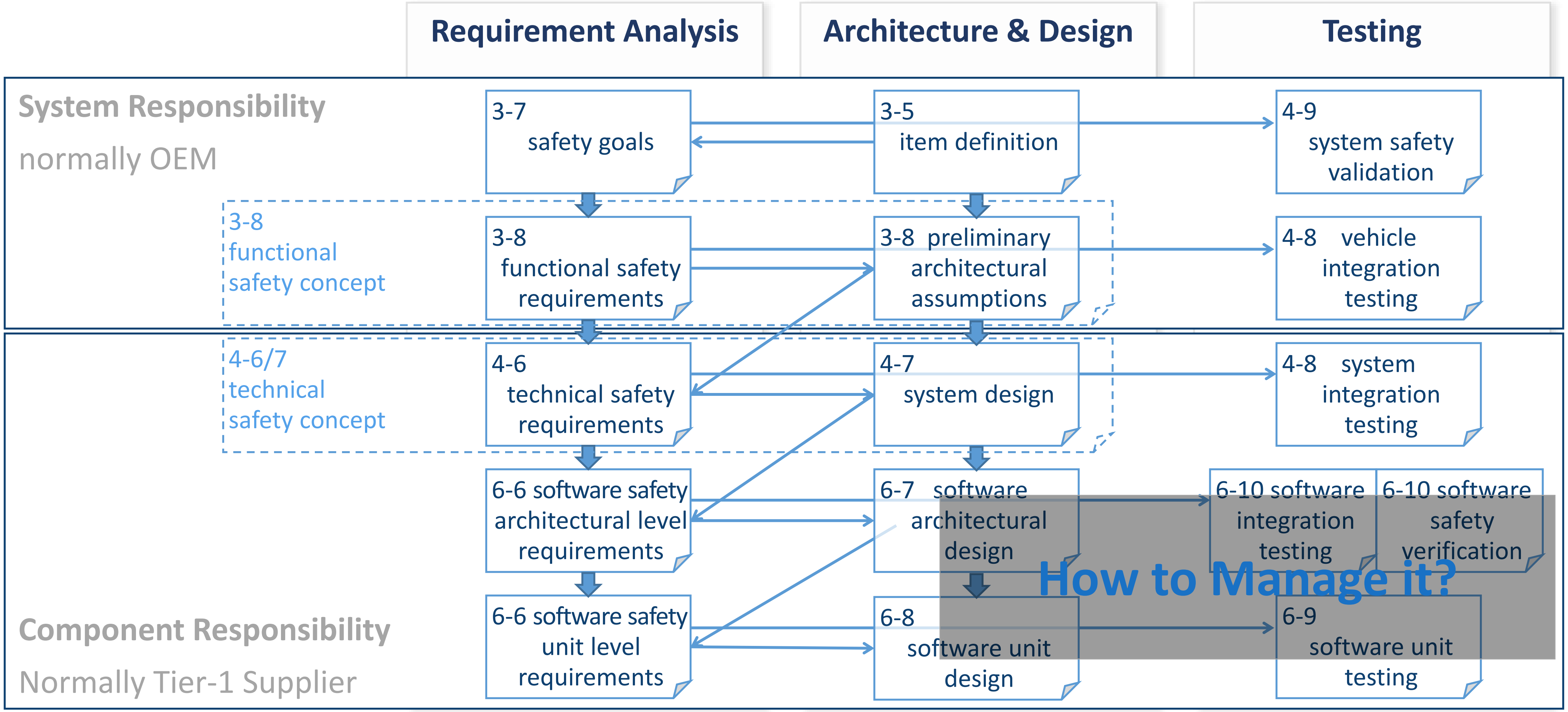
4, 5, 6

- Nested V-Model process highly recommended
- Comprehensible and traceable documentation of all decisions
- Collaborative development of models necessary

8

- Configuration Management and Change Management for all artefacts relevant to development

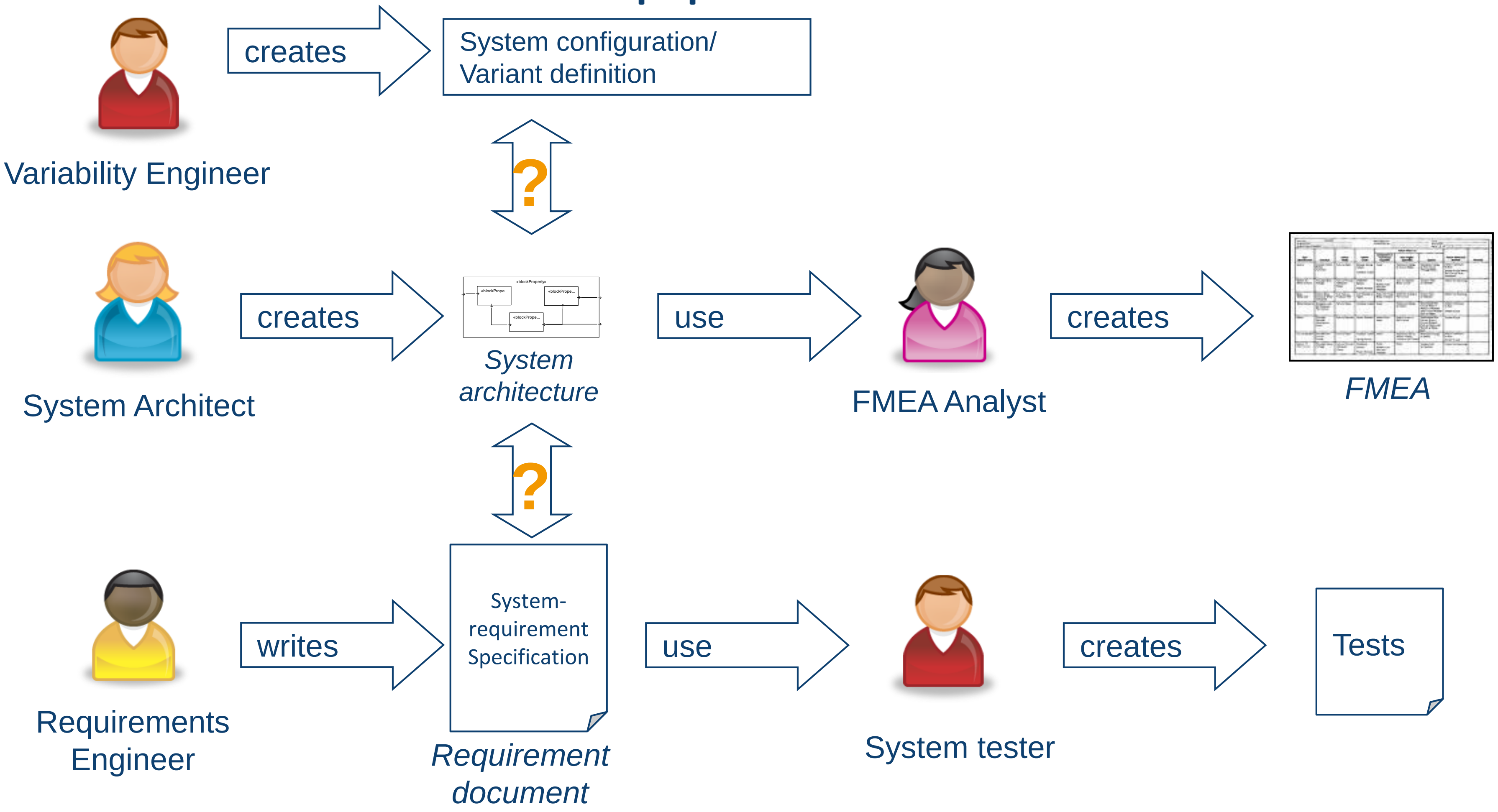
From Concept to Solution as required by ISO 26262



		Requirement Analysis	Architecture & Design	Testing
System Responsibility normally OEM		3-7 safety goals	3-5 item definition	4-9 system safety validation
	3-8 functional safety concept	3-8 functional safety requirements	3-8 preliminary architectural assumptions	4-8 vehicle integration testing
Component Responsibility Normally Tier-1 Supplier	4-6/7 technical safety concept	4-6 technical safety requirements	4-7 system design	4-8 system integration testing
		6-6 software safety architectural level requirements	6-7 software architectural design	6-10 software integration testing 6-10 software safety verification
		6-6 software safety unit level requirements	6-8 software unit design	6-9 software unit testing

How to Manage it?

Document-centric approach?



Variability Engineer creates System configuration/ Variant definition

?

System Architect creates *System architecture*

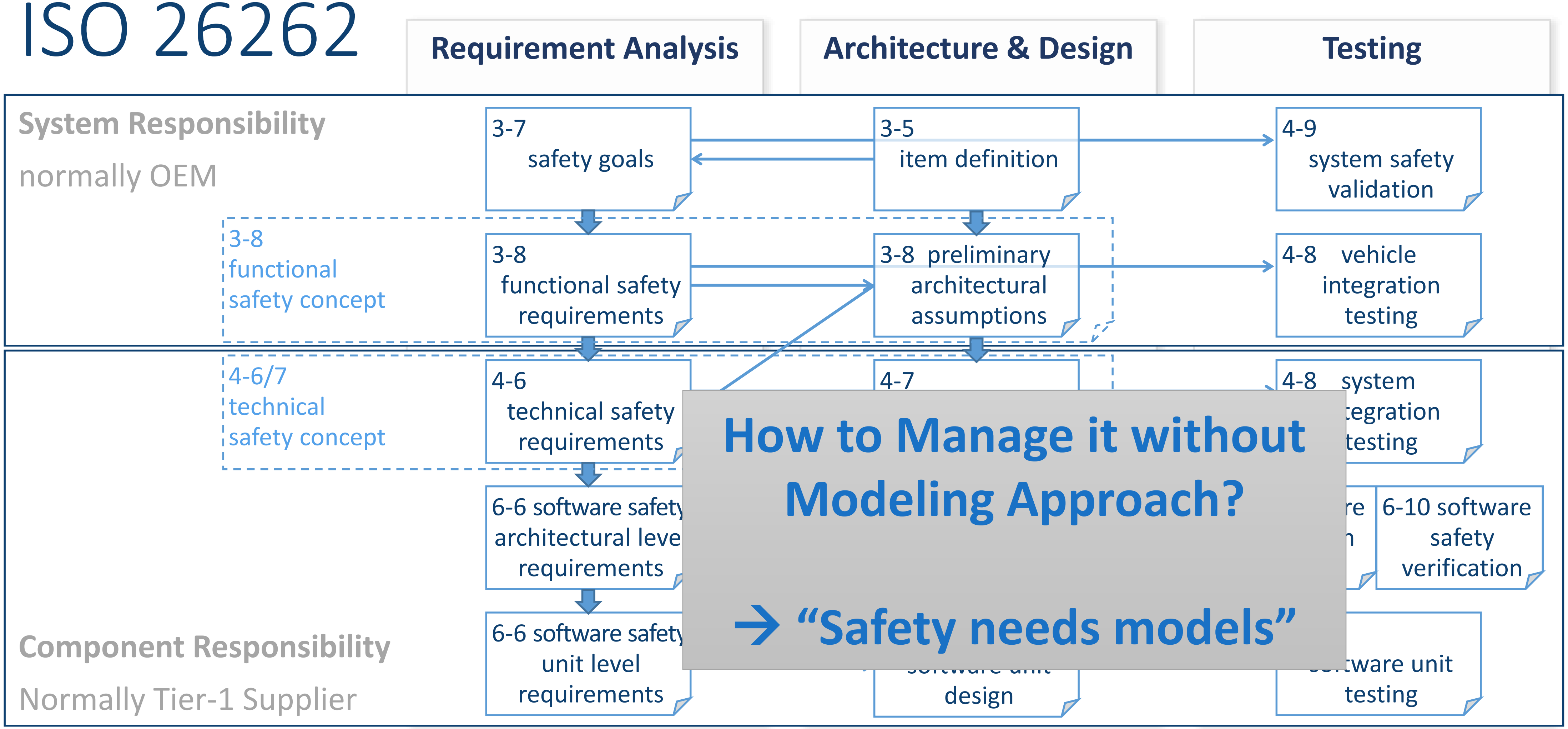
System architecture use FMEA Analyst creates *FMEA*

?

Requirements Engineer writes System-requirement Specification (*Requirement document*)

Requirement document use System tester creates Tests

From Concept to Solution as required by ISO 26262



Requirement Analysis

Architecture & Design

Testing

System Responsibility

normally OEM

3-7 safety goals

3-5 item definition

4-9 system safety validation

3-8 functional safety concept

3-8 functional safety requirements

3-8 preliminary architectural assumptions

4-8 vehicle integration testing

4-6/7 technical safety concept

4-6 technical safety requirements

4-7

4-8 system ·egration testing

6-6 software safet architectural leve requirements

re n

6-10 software safety verification

6-6 software safet unit level requirements

software unit design

software unit testing

Component Responsibility

Normally Tier-1 Supplier

How to Manage it without Modeling Approach?

→ “Safety needs models”

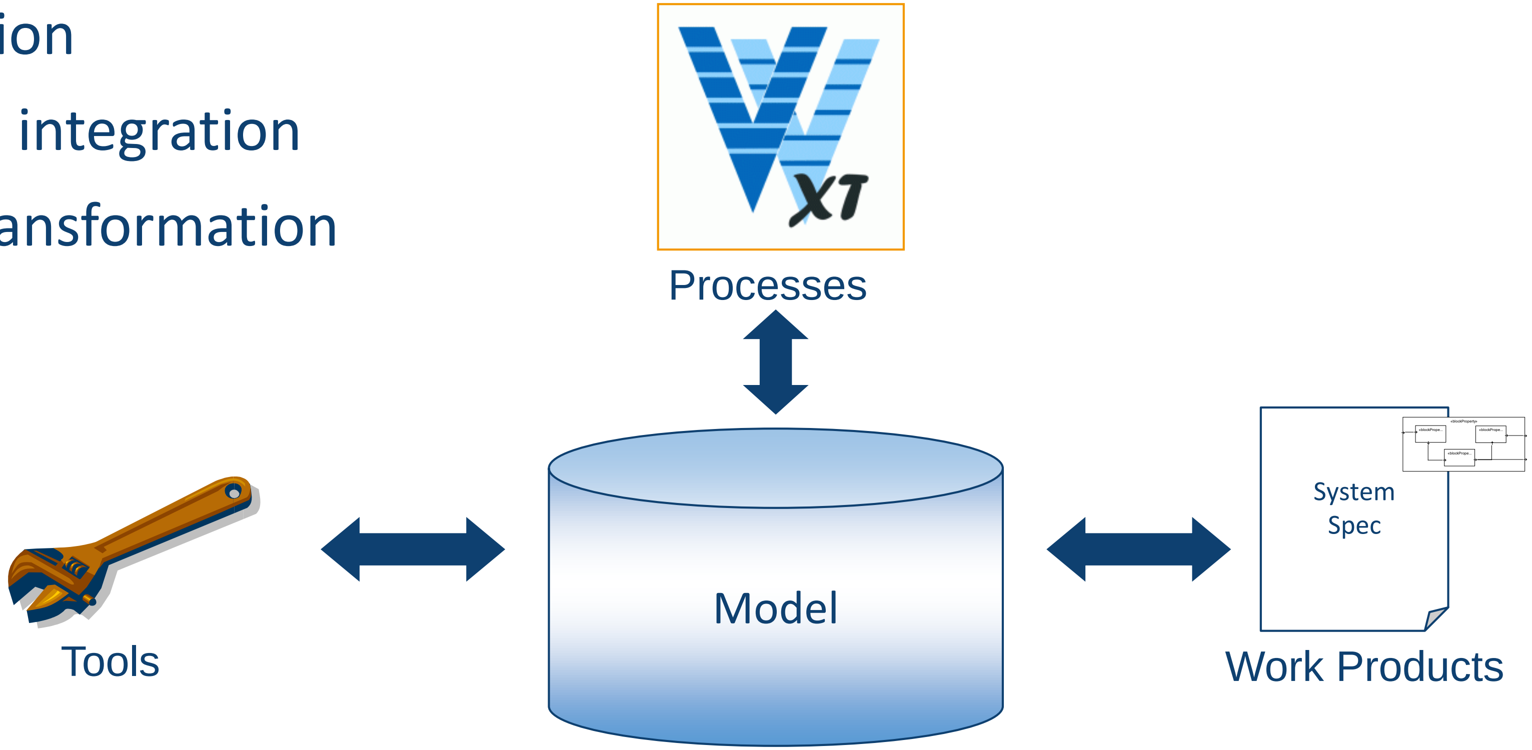
Model-based (Systems) Engineering

Basis: Graph-based Structure

→Automation

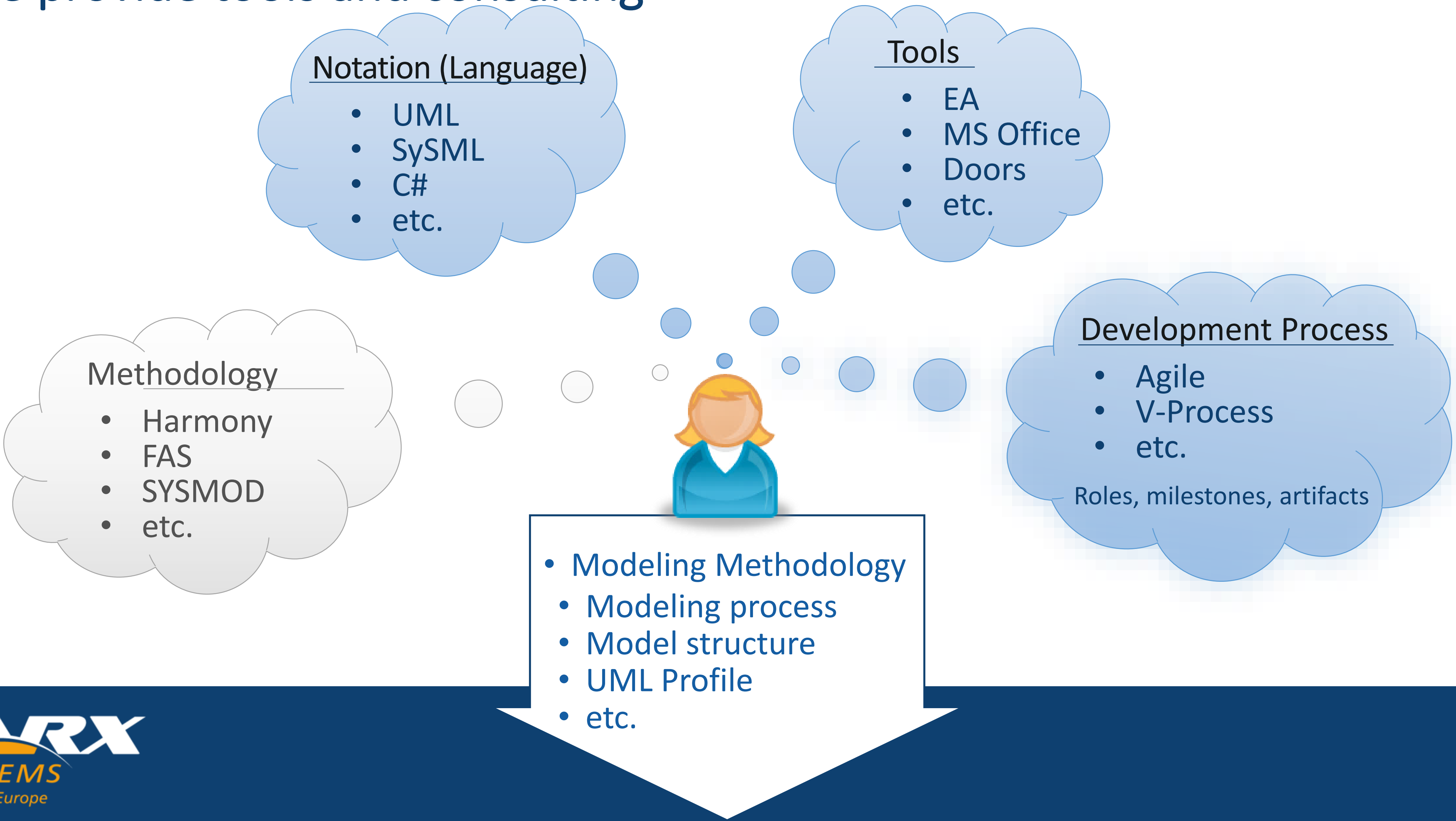
→Tool data integration

→Model transformation



Methodology is **your** Responsibility

we provide tools and consulting



Notation (Language)

- UML
- SySML
- C#
- etc.

Tools

- EA
- MS Office
- Doors
- etc.

Methodology

- Harmony
- FAS
- SYSMOD
- etc.

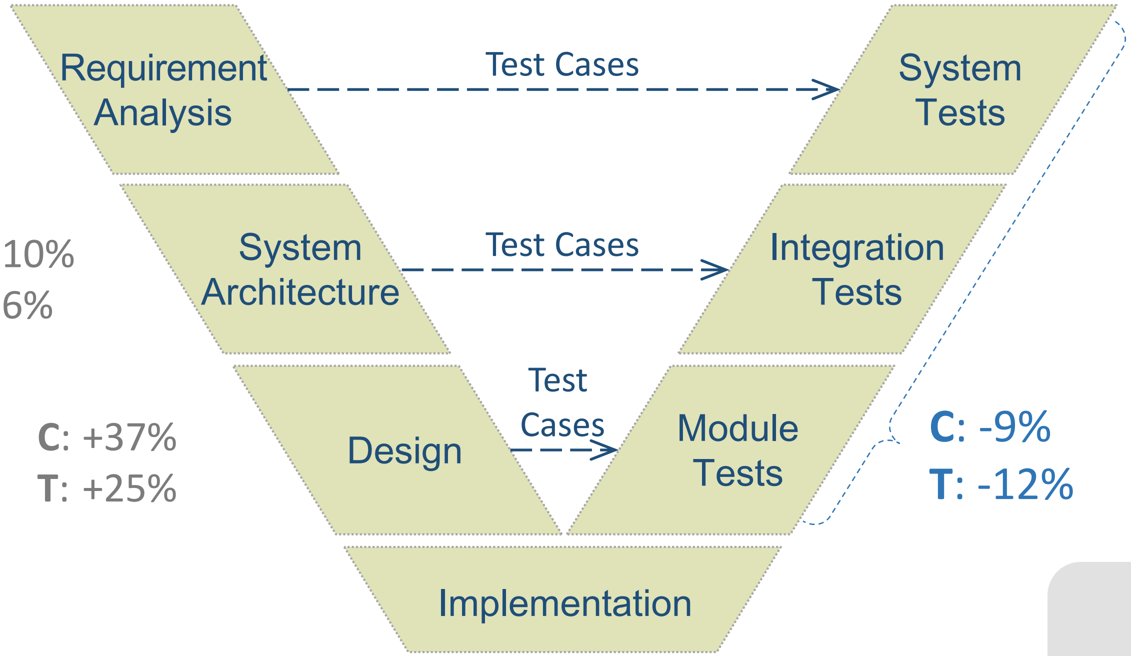
Development Process

- Agile
- V-Process
- etc.

Roles, milestones, artifacts

- Modeling Methodology
  - Modeling process
  - Model structure
  - UML Profile
  - etc.

Time and Cost Reduction of MDE



C: +23%
T: +18%

C: +10%
T: +6%

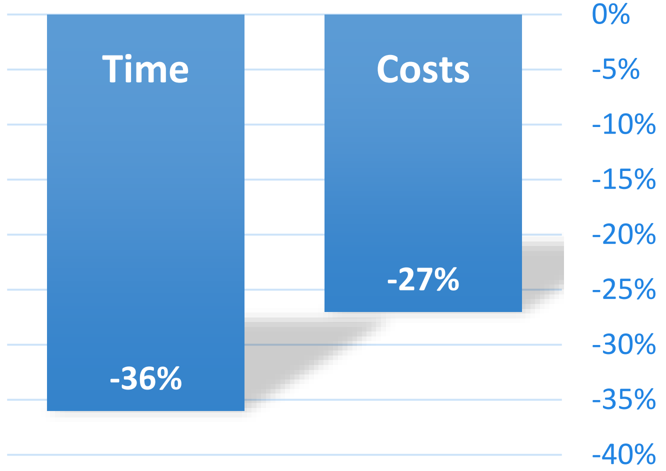
C: +37%
T: +25%

C: -9%
T: -12%

C: -46%
T: -45%

C : Costs
T : Time

Reduction of time effort for whole project

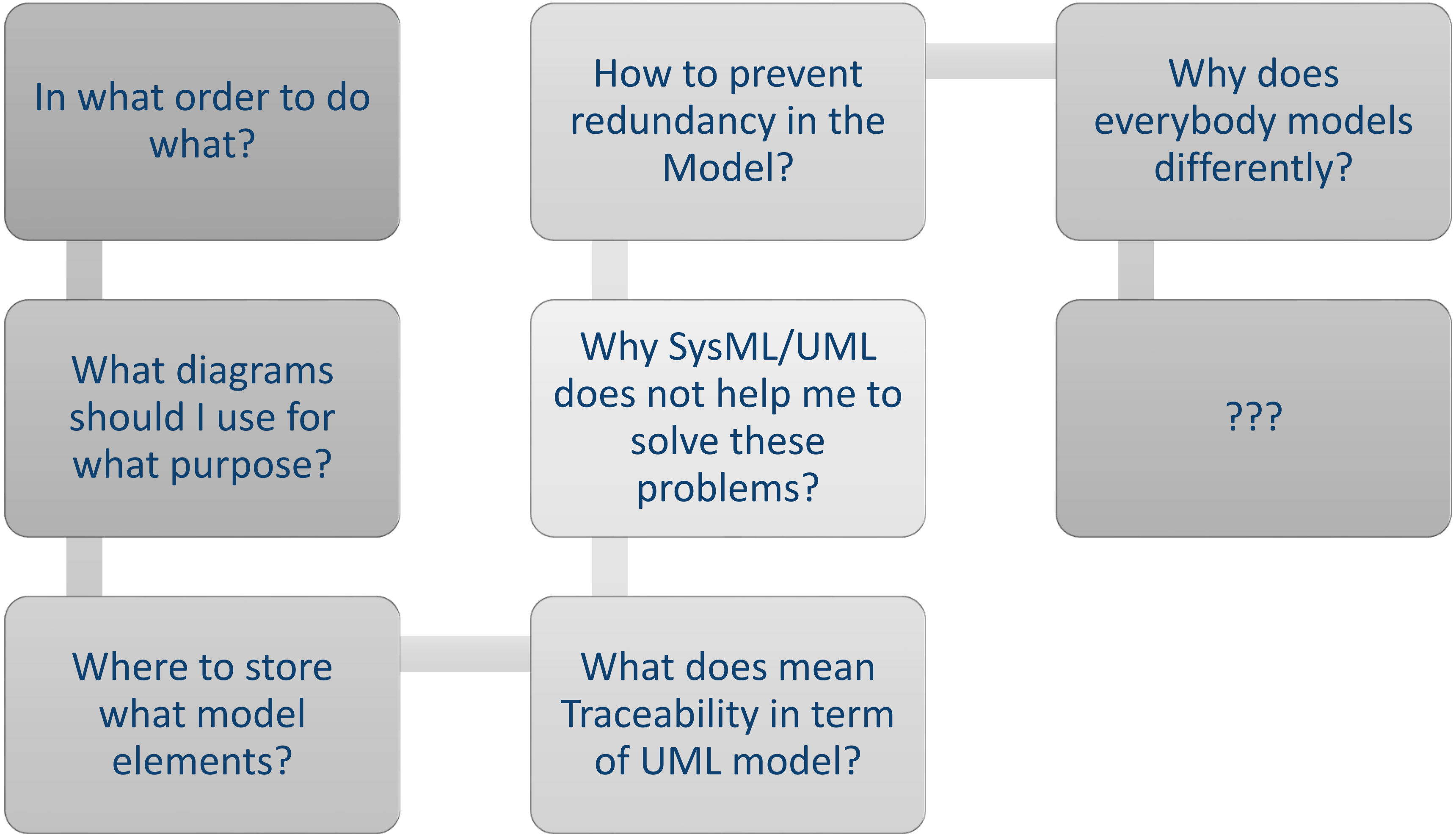


Challenges

- More effort at the beginning - **positive effect later**
- Modeling qualification of employees is required
- Multiple Tools and Methods are required

Sascha Kirstan:
Kosten und Nutzen modellbasierter Entwicklung eingebetteter Softwaresysteme im Automobil. Verlag Dr. Hut Technical University Munich 2011, ISBN 978-3-8439-0121-5, pp. 1-374

Modeling Methodology gives the Answers



In what order to do what?

What diagrams should I use for what purpose?

Where to store what model elements?

What does mean Traceability in term of UML model?

Why SysML/UML does not help me to solve these problems?

How to prevent redundancy in the Model?

Why does everybody models differently?

???

Standards in Model-based Systems Engineering

- UML – Unified Modeling Language
- SysML – Systems Modeling Language
- AUTOSAR Virtual Function Bus modeling
- ReqIF – Requirements Interchange Format

What is SysML ?

- The *Systems Modelling Language* (SysML) is a ***standardized graphical*** language to describe and specify technical systems of all kind, consisting of hardware and software components

- SysML is based on the software modeling language UML (Unified Modeling Language) and reuses parts, but also extends and adds some new possibilities

- With SysML you can specify
  - the structure/the architecture
  - the behavior
  - the reqirements

  of a system and bring them into relations to each other.

- SysML supports the concept of Systems Engineering

Main Challenges for MBE for FSM

- Missing Methodology

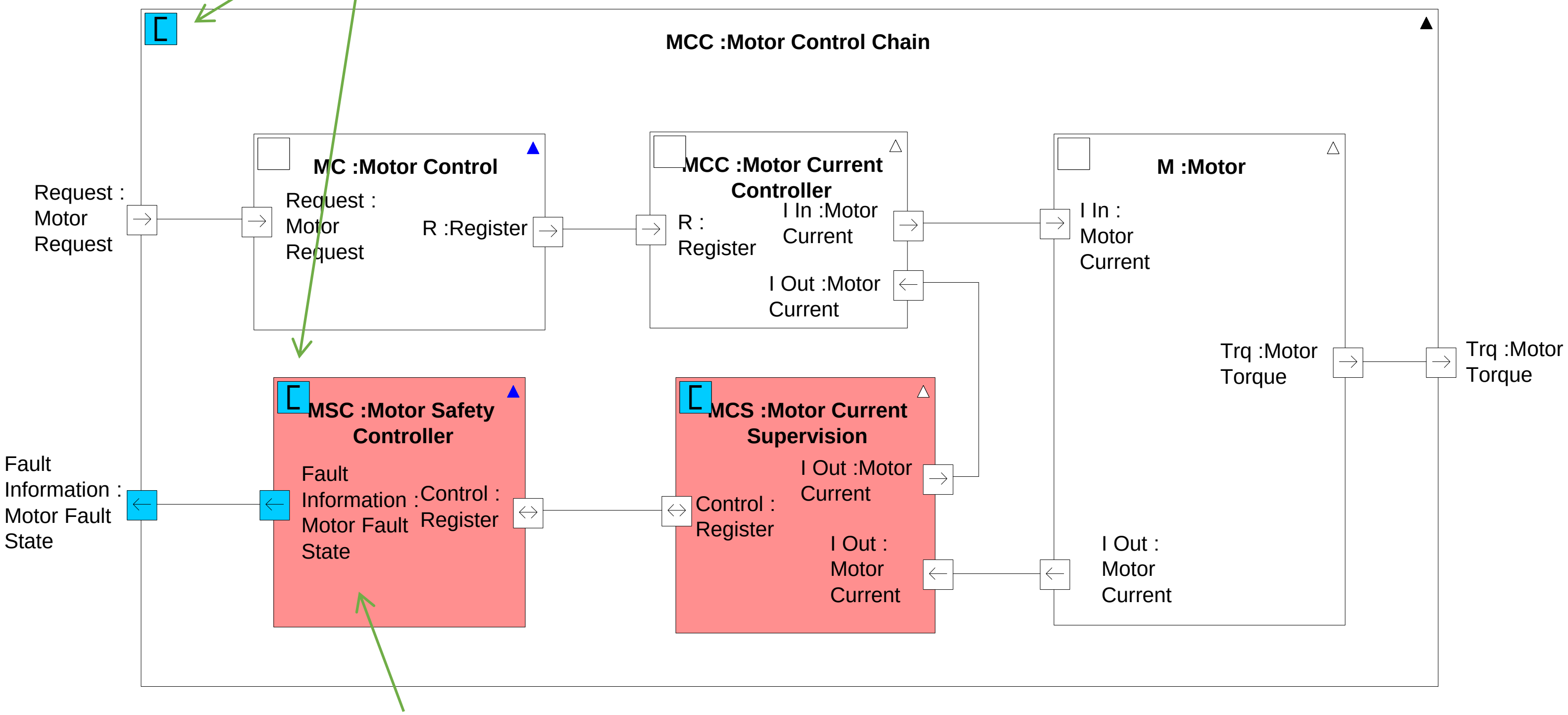
- UML Profiles
- Traceability
- Configuration & Change Management

Tagging

UML and UML Profiles

SysML extensions for FSM/ISO 26262

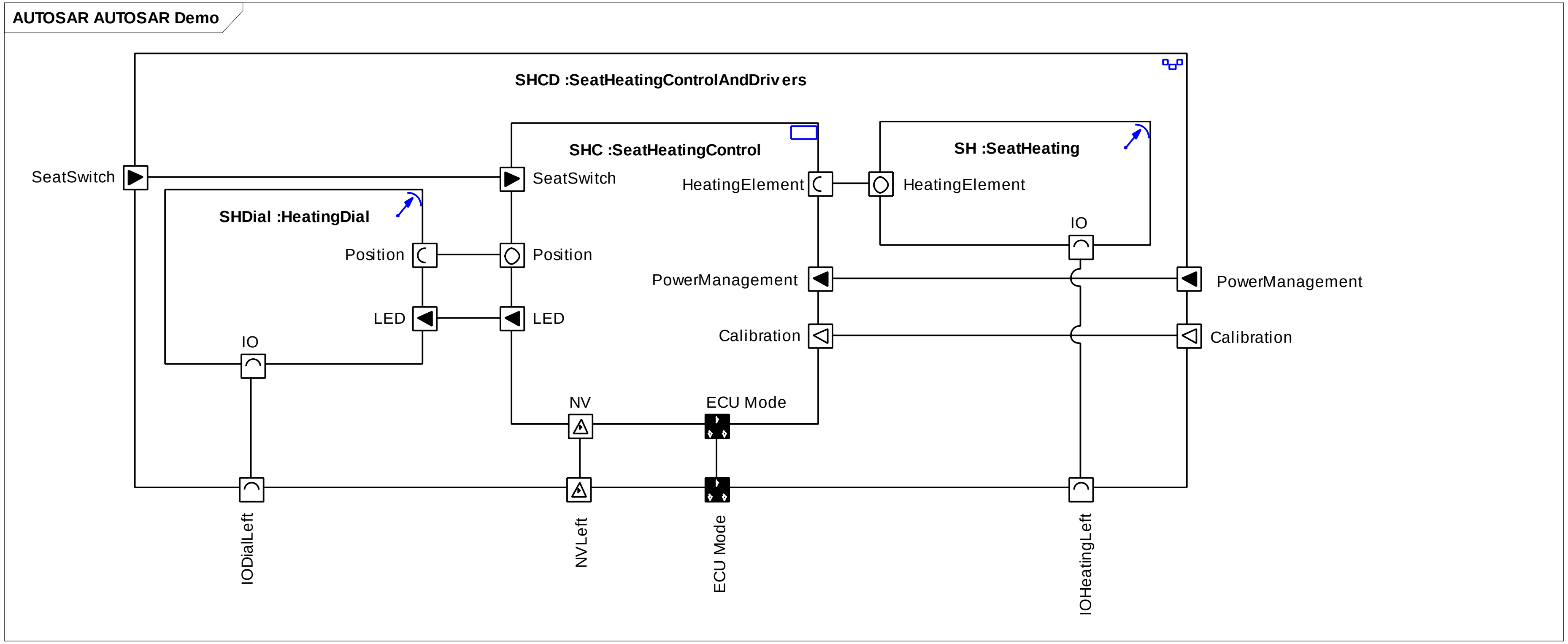
Assignment of ASIL levels to components and ports



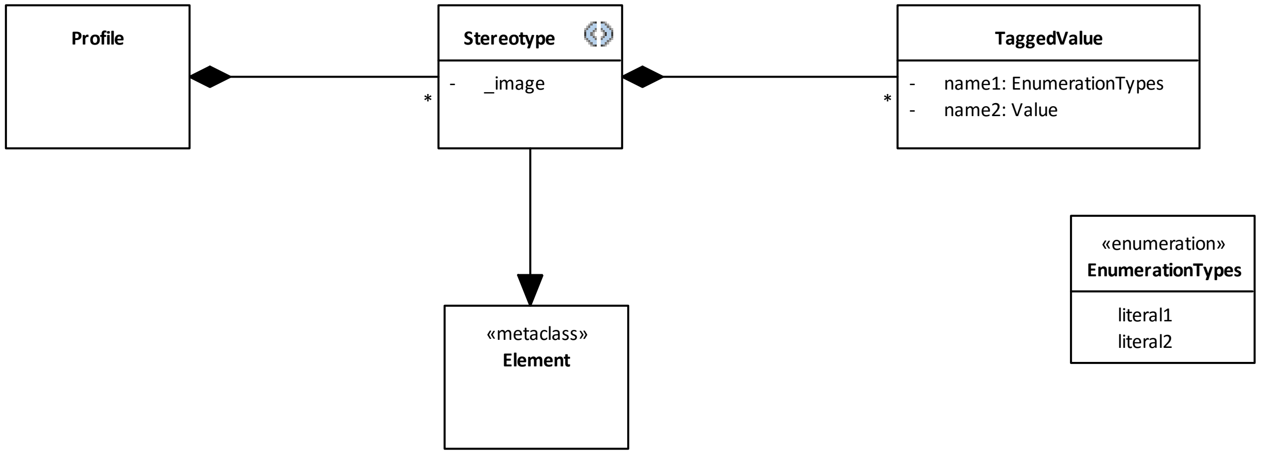
Coloring of Safety Mechanisms

AUTOSAR VFB Modeling with EA

- Tool extension enables AUTOSAR VFB modeling in EA



UML Profiles

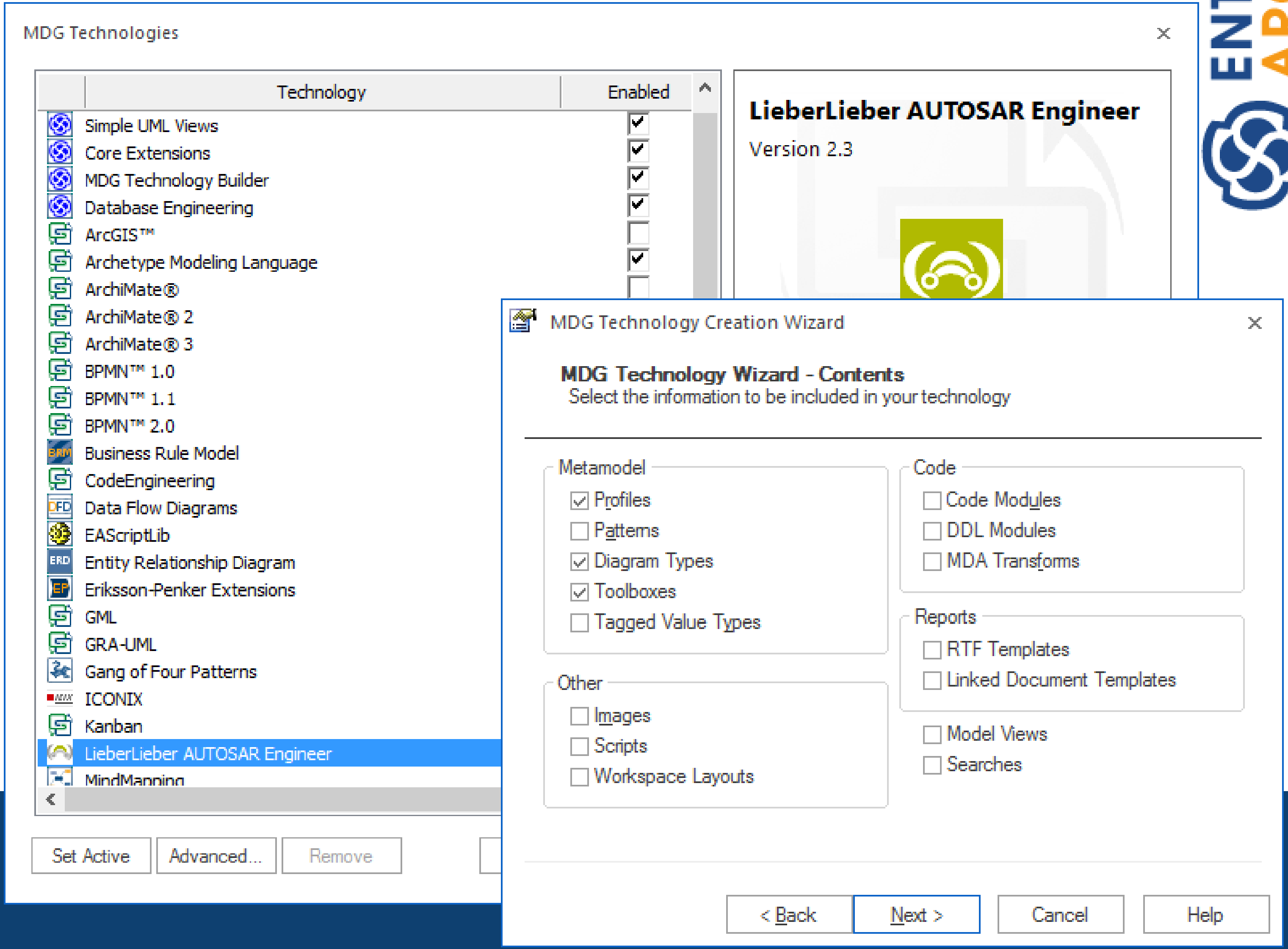


MDG Technolgies

Define

- Profiles,
- Diagrams and
- Toolboxes

for central deployment



MDG Technologies

Technology	Enabled
Simple UML Views	☑
Core Extensions	☑
MDG Technology Builder	☑
Database Engineering	☑
ArcGIS™	□
Archetype Modeling Language	☑
ArchiMate®	□
ArchiMate® 2	
ArchiMate® 3	
BPMN™ 1.0	
BPMN™ 1.1	
BPMN™ 2.0	
Business Rule Model	
CodeEngineering	
Data Flow Diagrams	
EAScriptLib	
Entity Relationship Diagram	
Eriksson-Penker Extensions	
GML	
GRA-UML	
Gang of Four Patterns	
ICONIX	
Kanban	
LieberLieber AUTOSAR Engineer	
MindMapping	

LieberLieber AUTOSAR Engineer
Version 2.3

MDG Technology Creation Wizard

MDG Technology Wizard - Contents
Select the information to be included in your technology

Metamodel
- ☑ Profiles
- □ Patterns
- ☑ Diagram Types
- ☑ Toolboxes
- □ Tagged Value Types

Other
- □ Images
- □ Scripts
- □ Workspace Layouts

Code
- □ Code Modules
- □ DDL Modules
- □ MDA Transforms

Reports
- □ RTF Templates
- □ Linked Document Templates

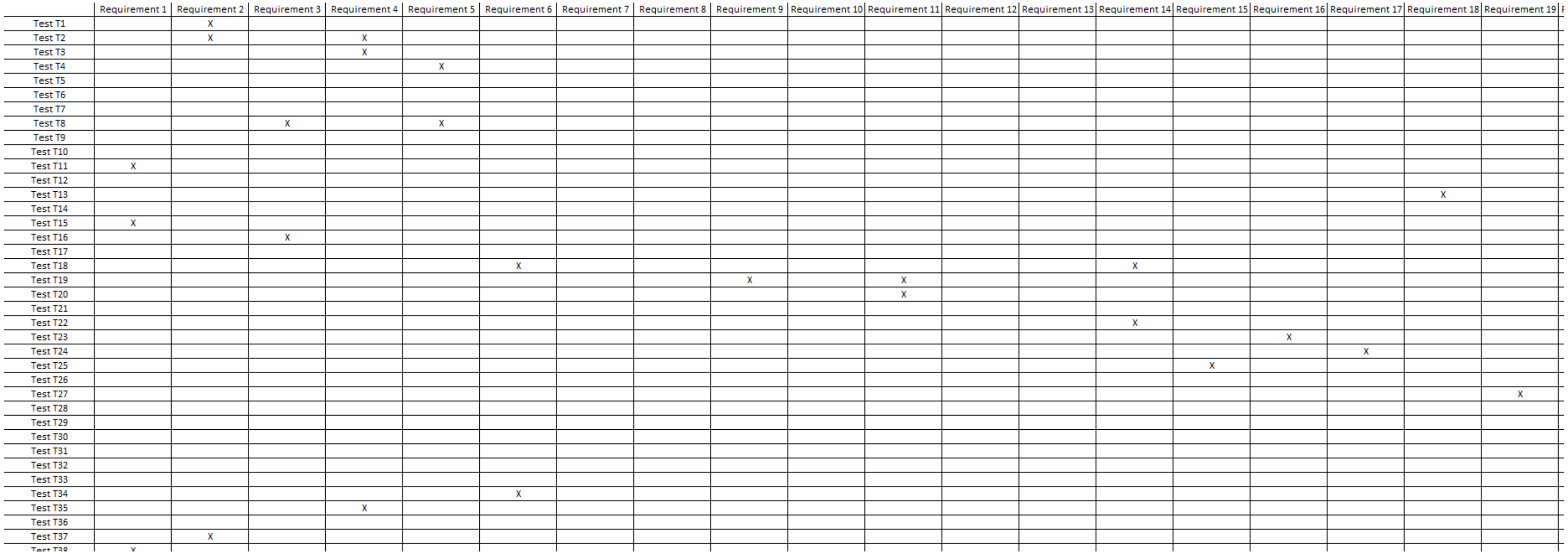
- □ Model Views
- □ Searches

Tracability

… the models intelligence

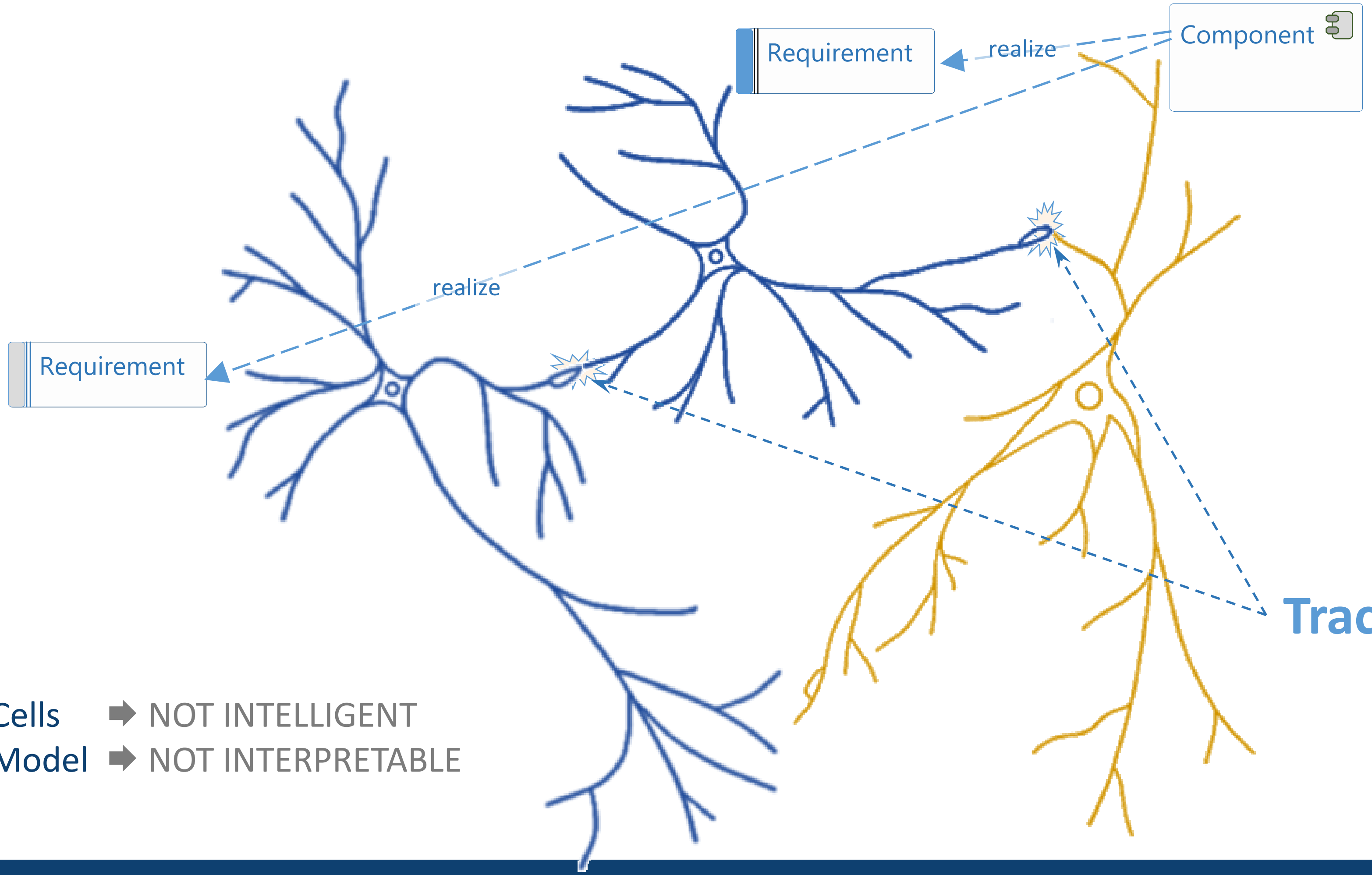
How to ensure consistency?

Traceability-Tables?



	Requirement 1	Requirement 2	Requirement 3	Requirement 4	Requirement 5	Requirement 6	Requirement 7	Requirement 8	Requirement 9	Requirement 10	Requirement 11	Requirement 12	Requirement 13	Requirement 14	Requirement 15	Requirement 16	Requirement 17	Requirement 18	Requirement 19
Test T1		X																	
Test T2		X		X															
Test T3				X															
Test T4					X														
Test T5																			
Test T6																			
Test T7																			
Test T8			X		X														
Test T9																			
Test T10																			
Test T11	X																		
Test T12																			
Test T13																		X	
Test T14																			
Test T15	X																		
Test T16			X																
Test T17																			
Test T18						X								X					
Test T19									X		X								
Test T20											X								
Test T21																			
Test T22														X					
Test T23																X			
Test T24																	X		
Test T25															X				
Test T26																			
Test T27																			X
Test T28																			
Test T29																			
Test T30																			
Test T31																			
Test T32																			
Test T33																			
Test T34						X													
Test T35				X															
Test T36																			
Test T37		X																	
Test T38	X																		

Traceability is the Model Intelligence



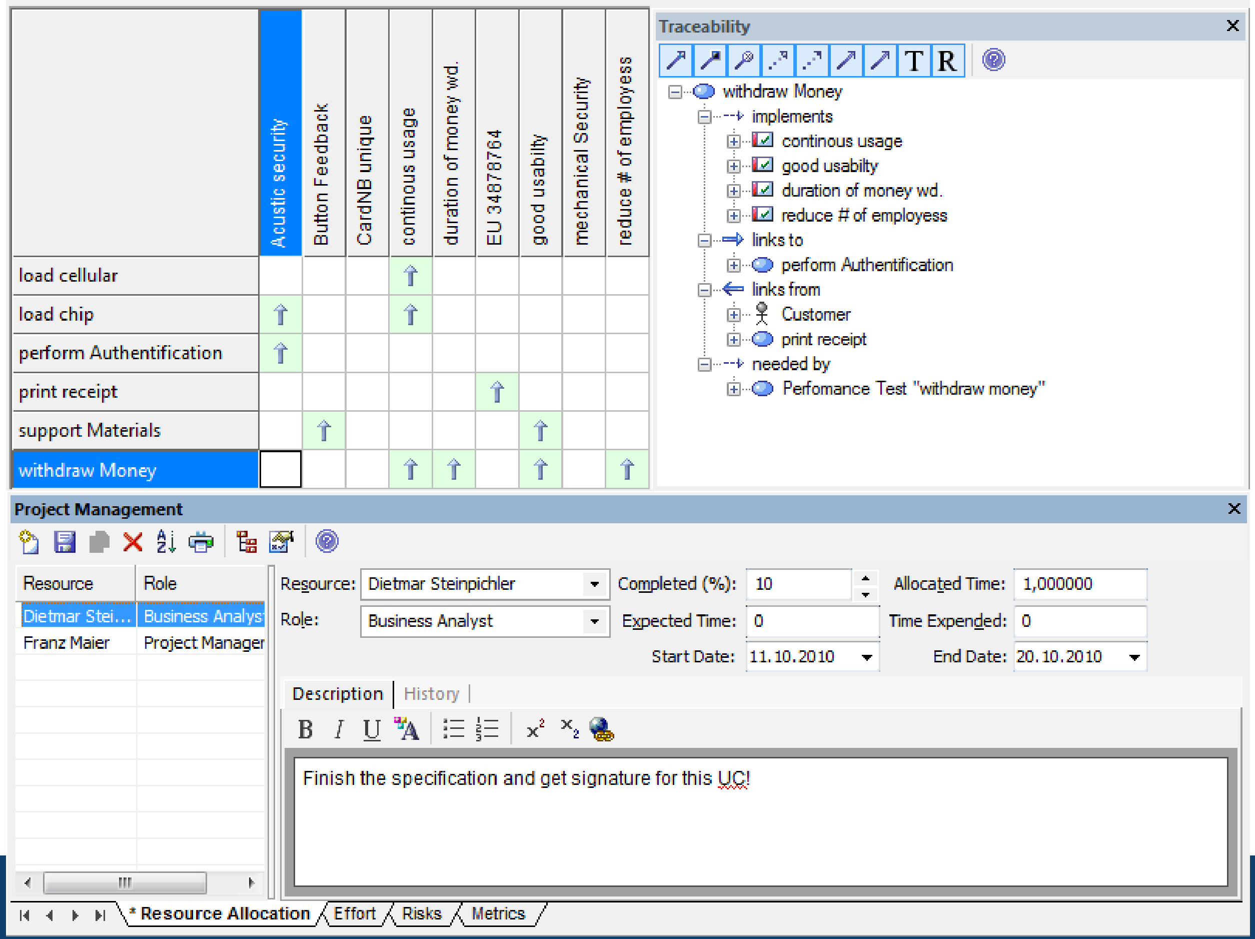
Traceability = Intelligence

Disconnected Cells ➡ NOT INTELLIGENT

Disconnected Model ➡ NOT INTERPRETABLE

Traceability in EA

- Connectors
- Different Traceability Views
- Relationship-Matrix



	Acustic security	Button Feedback	CardNB unique	continous usage	duration of money wd.	EU 34878764	good usability	mechanical Security	reduce # of employess
load cellular				↑					
load chip	↑			↑					
perform Authentification	↑								
print receipt						↑			
support Materials		↑					↑		
withdraw Money				↑	↑		↑		↑

Traceability

- withdraw Money
  - implements
    - continous usage
    - good usabilty
    - duration of money wd.
    - reduce # of employess
  - links to
    - perform Authentification
  - links from
    - Customer
    - print receipt
  - needed by
    - Perfomance Test "withdraw money"

Project Management

Resource	Role
Dietmar Stei…	Business Analys
Franz Maier	Project Manager

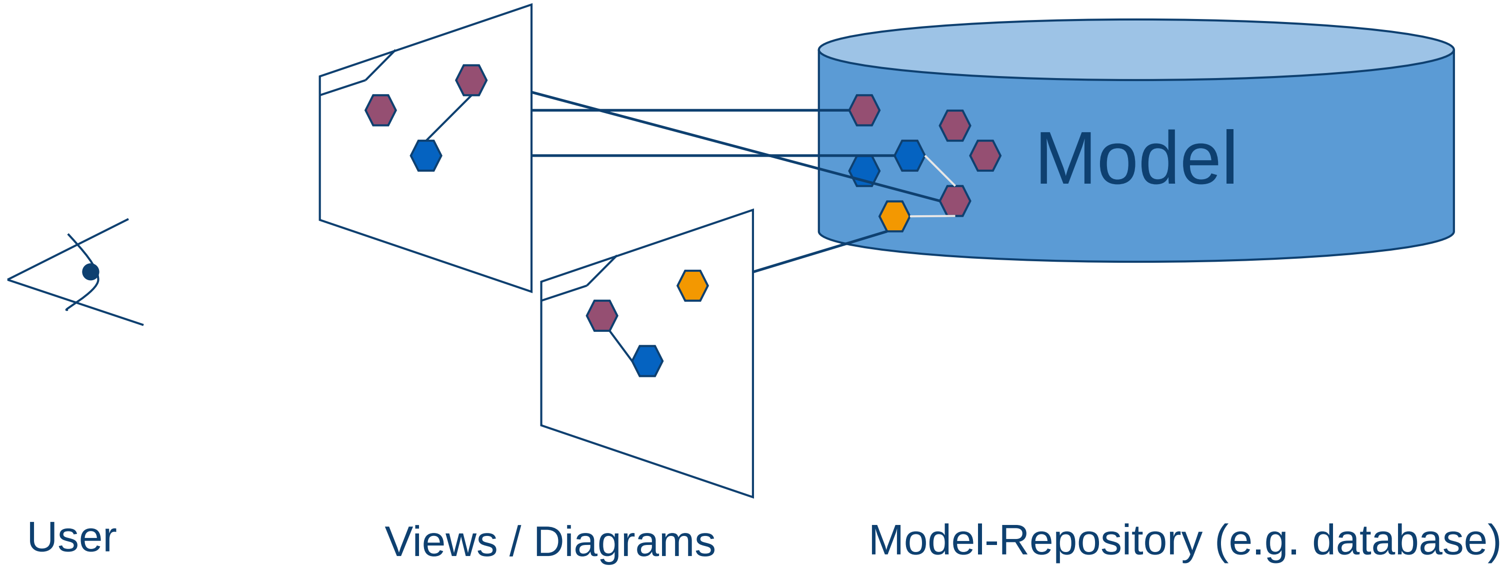
Resource: Dietmar Steinpichler
Completed (%): 10
Allocated Time: 1,000000
Role: Business Analyst
Expected Time: 0
Time Expended: 0
Start Date: 11.10.2010
End Date: 20.10.2010

Description | History

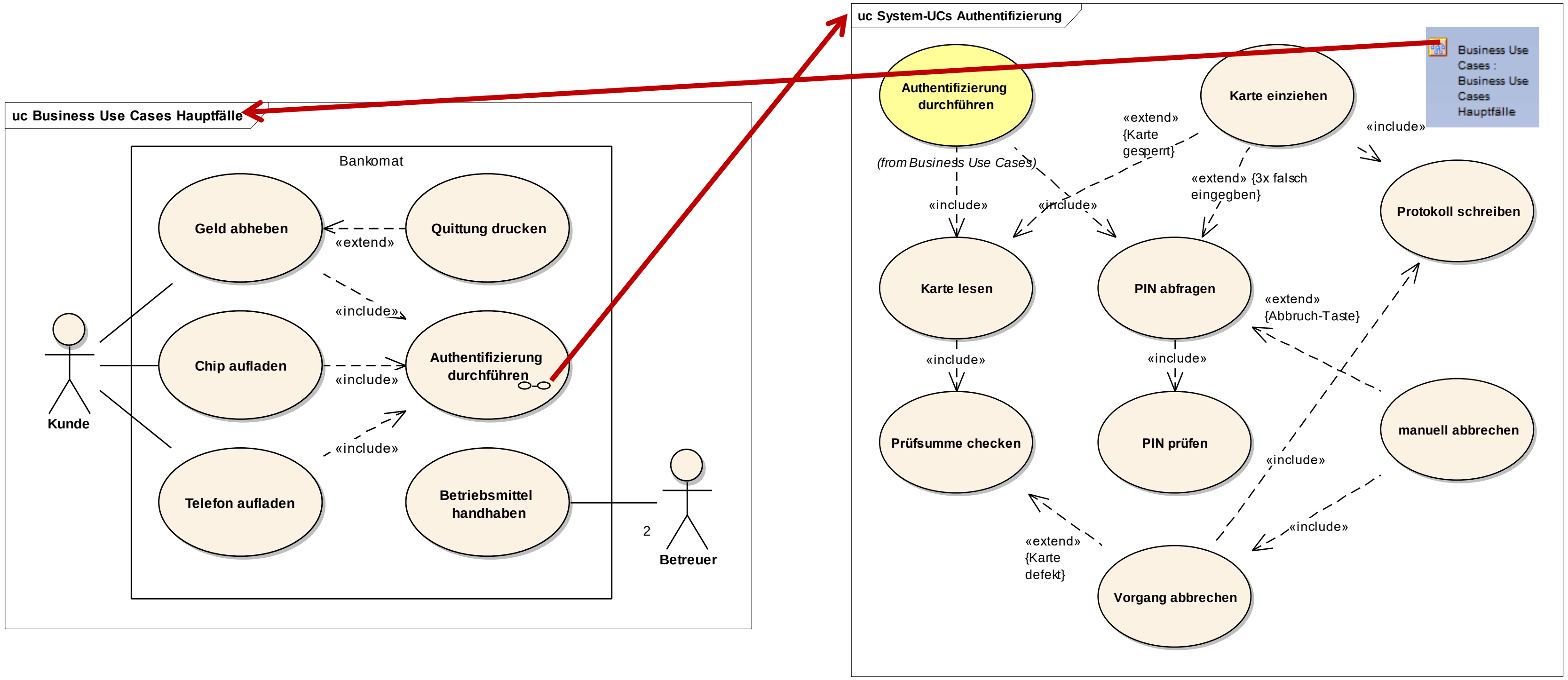
Finish the specification and get signature for this UC!

Model and View

- In case of graphical languages, it has to be distinguished between the model and various views
- *A view is a projection of a model that shows it from a specific perspective or position and omits objects that are not relevant for this perspective.*



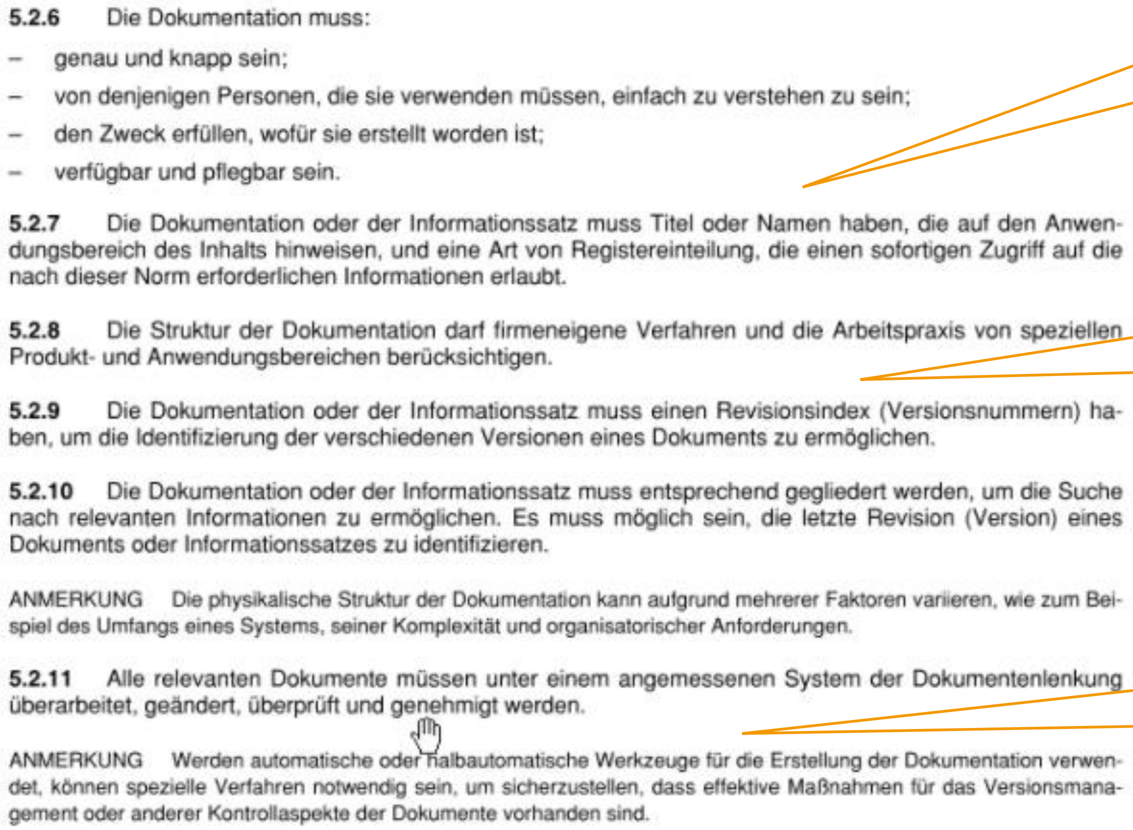
Navigierbarkeit einrichten



Configuration Management

Mit Auszug aus IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems

IEC 61508 and Version Control



5.2.6 Die Dokumentation muss:

- genau und knapp sein;
- von denjenigen Personen, die sie verwenden müssen, einfach zu verstehen zu sein;
- den Zweck erfüllen, wofür sie erstellt worden ist;
- verfügbar und pflegbar sein.

5.2.7 Die Dokumentation oder der Informationssatz muss Titel oder Namen haben, die auf den Anwendungsbereich des Inhalts hinweisen, und eine Art von Registereinteilung, die einen sofortigen Zugriff auf die nach dieser Norm erforderlichen Informationen erlaubt.

5.2.8 Die Struktur der Dokumentation darf firmeneigene Verfahren und die Arbeitspraxis von speziellen Produkt- und Anwendungsbereichen berücksichtigen.

5.2.9 Die Dokumentation oder der Informationssatz muss einen Revisionsindex (Versionsnummern) haben, um die Identifizierung der verschiedenen Versionen eines Dokuments zu ermöglichen.

5.2.10 Die Dokumentation oder der Informationssatz muss entsprechend gegliedert werden, um die Suche nach relevanten Informationen zu ermöglichen. Es muss möglich sein, die letzte Revision (Version) eines Dokuments oder Informationssatzes zu identifizieren.

ANMERKUNG Die physikalische Struktur der Dokumentation kann aufgrund mehrerer Faktoren variieren, wie zum Beispiel des Umfangs eines Systems, seiner Komplexität und organisatorischer Anforderungen.

5.2.11 Alle relevanten Dokumente müssen unter einem angemessenen System der Dokumentenlenkung überarbeitet, geändert, überprüft und genehmigt werden.

ANMERKUNG Werden automatische oder halbautomatische Werkzeuge für die Erstellung der Dokumentation verwendet, können spezielle Verfahren notwendig sein, um sicherzustellen, dass effektive Maßnahmen für das Versionsmanagement oder anderer Kontrollaspekte der Dokumente vorhanden sind.

"Die Dokumentation oder der Informationssatz…"

"…muss einen Revisionsindex haben…"

"…effektive Maßnahmen für das Versionsmanagement…"

Configuration Management, Change Management and Collaborative Modeling

Working collaboratively on a model is hard

Versioning for EA Models is hard and error-prone

Tracking Changes in Models is very complex

RESULT → Modeling with EA is often used without Configuration Management
→ Third Party Tool?!

Versioning in EA

- File Copy
- Baselines
- XMI Export/Import
- Integration with VCS on package level (Lock/Modify/Lock)

LemonTree © by LieberLieber

- Fine-grained 3-way model diff is necessary
- Change tracking is essential
- Features of VCS are necessary for today‘s challenges

> “In general, standards such as IEC 61508 demand the application of configuration management. This refers to all artifacts, including UML models.
> Der LieberLieber Model Versioner is our key to revealing the changes that have been made to a revision.”
>
> Dipl.-Ing. (FH) Stefan Müller, HIMA Paul Hildebrandt GmbH
> Safety-related automation solutions

> “Generell fordern Normen wie IEC 61508 die Existenz eines Configuration Managements. Das bezieht sich auf alle Elemente, also auch auf die UML-Modelle.
> Der LieberLieber Model Versioner ist für uns dabei der Schlüssel dazu, ermitteln zu können, was in welcher Revision geändert wurde.“
>
> Dipl.-Ing. (FH) Stefan Müller, HIMA Paul Hildebrandt GmbH
> Safety-related automation solutions

TOP ENTERPRISE ARCHITECT TOOL

LemonTree©
Fresh Model Versioning
lemontree.lieberlieber.com

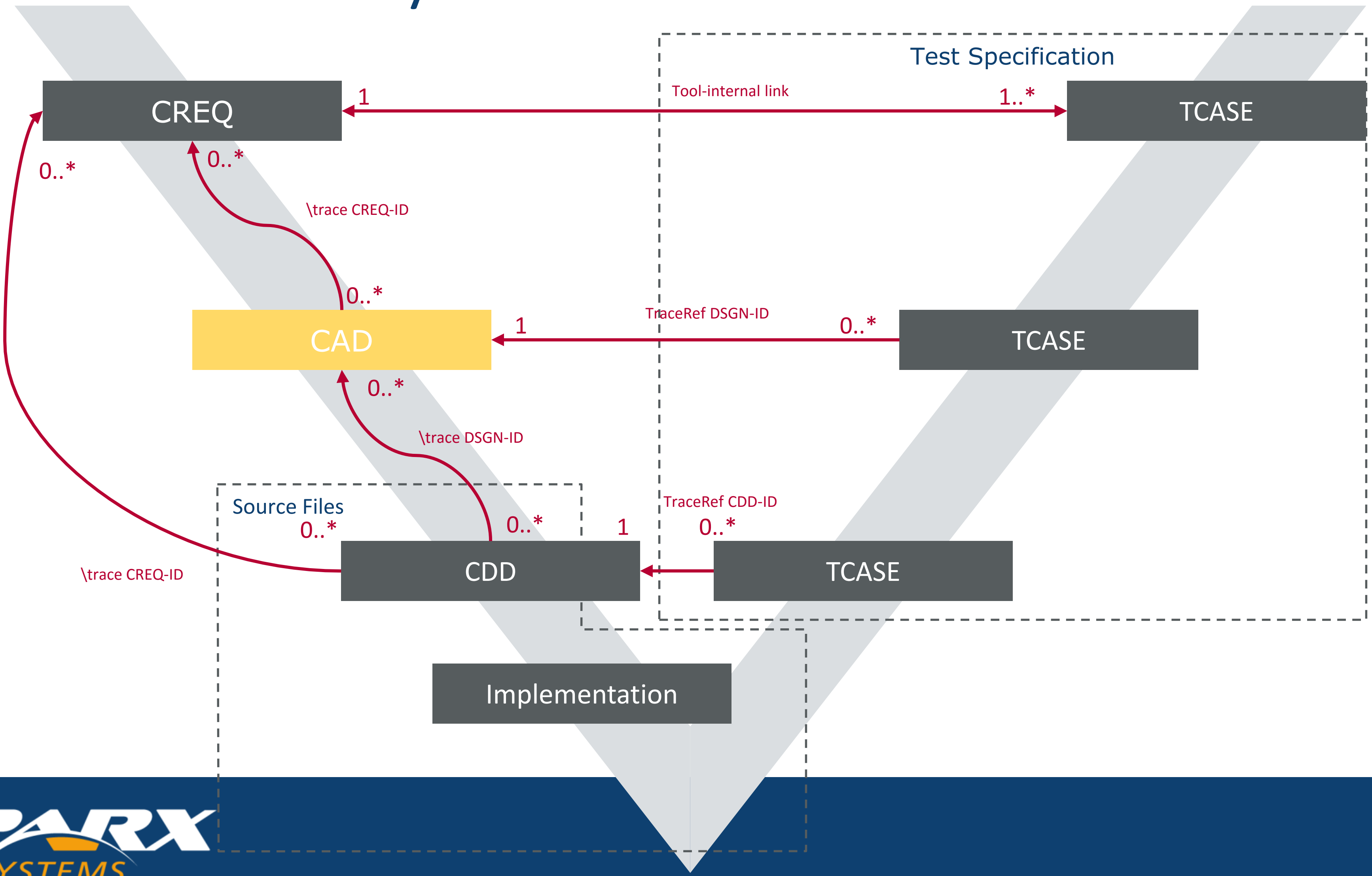
…and how it is solved by Vector

Traceability

Notation of safety-related elements

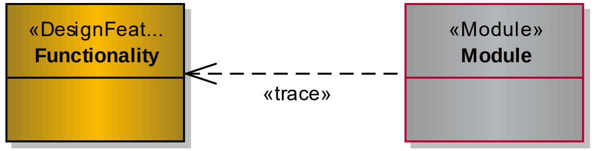
Configuration management

Traceability



Traceability

- Trace EA->EA
  - Trace Dependency



- Trace EA->X
  - Textually within notes

```
\trace CREQ-1234, SPEC-5678
```

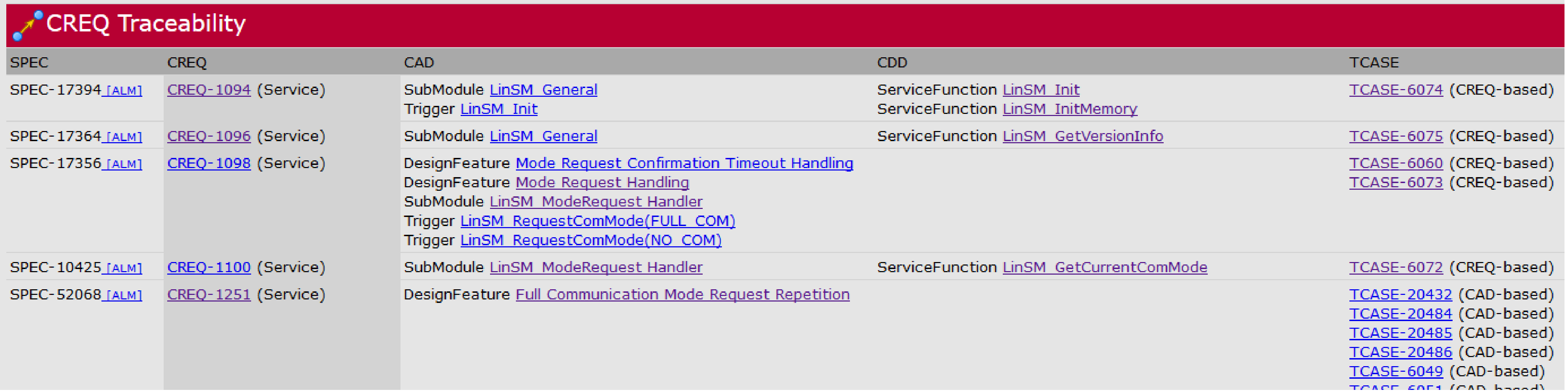
- Trace X->EA
  - Identifier
    - GUID
    - OwnIdentifier (DSGN-<Module><Id>)
      - Automatically calculated (based on EA ID)
      - Might be specifically defined by user (Alias)

```
\trace {2C0069A7-1AEB-4a70-B166-091A3A75AC43}

\trace DSGN-EcuM1234,
       DSGN-EcuMInitInterface
```

Traceability

- Specification Overview

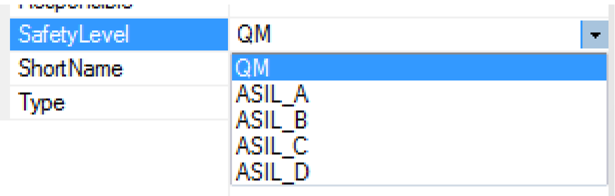


CREQ Traceability

SPEC	CREQ	CAD	CDD	TCASE
SPEC-17394 [ALM]	CREQ-1094 (Service)	SubModule LinSM_General Trigger LinSM_Init	ServiceFunction LinSM_Init ServiceFunction LinSM_InitMemory	TCASE-6074 (CREQ-based)
SPEC-17364 [ALM]	CREQ-1096 (Service)	SubModule LinSM_General	ServiceFunction LinSM_GetVersionInfo	TCASE-6075 (CREQ-based)
SPEC-17356 [ALM]	CREQ-1098 (Service)	DesignFeature Mode Request Confirmation Timeout Handling DesignFeature Mode Request Handling SubModule LinSM_ModeRequest Handler Trigger LinSM_RequestComMode(FULL_COM) Trigger LinSM_RequestComMode(NO_COM)		TCASE-6060 (CREQ-based) TCASE-6073 (CREQ-based)
SPEC-10425 [ALM]	CREQ-1100 (Service)	SubModule LinSM_ModeRequest Handler	ServiceFunction LinSM_GetCurrentComMode	TCASE-6072 (CREQ-based)
SPEC-52068 [ALM]	CREQ-1251 (Service)	DesignFeature Full Communication Mode Request Repetition		TCASE-20432 (CAD-based) TCASE-20484 (CAD-based) TCASE-20485 (CAD-based) TCASE-20486 (CAD-based) TCASE-6049 (CAD-based) TCASE-6051 (CAD-based)

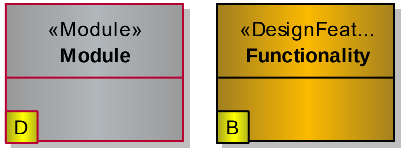
Safety Notation

- Where?
  - Functionality (TSR, CREQ)
  - Module
  - Function
- How?
  - SafetyLevel as Property (TaggedValue)
- Additional
  - ShapeScripts Overlay



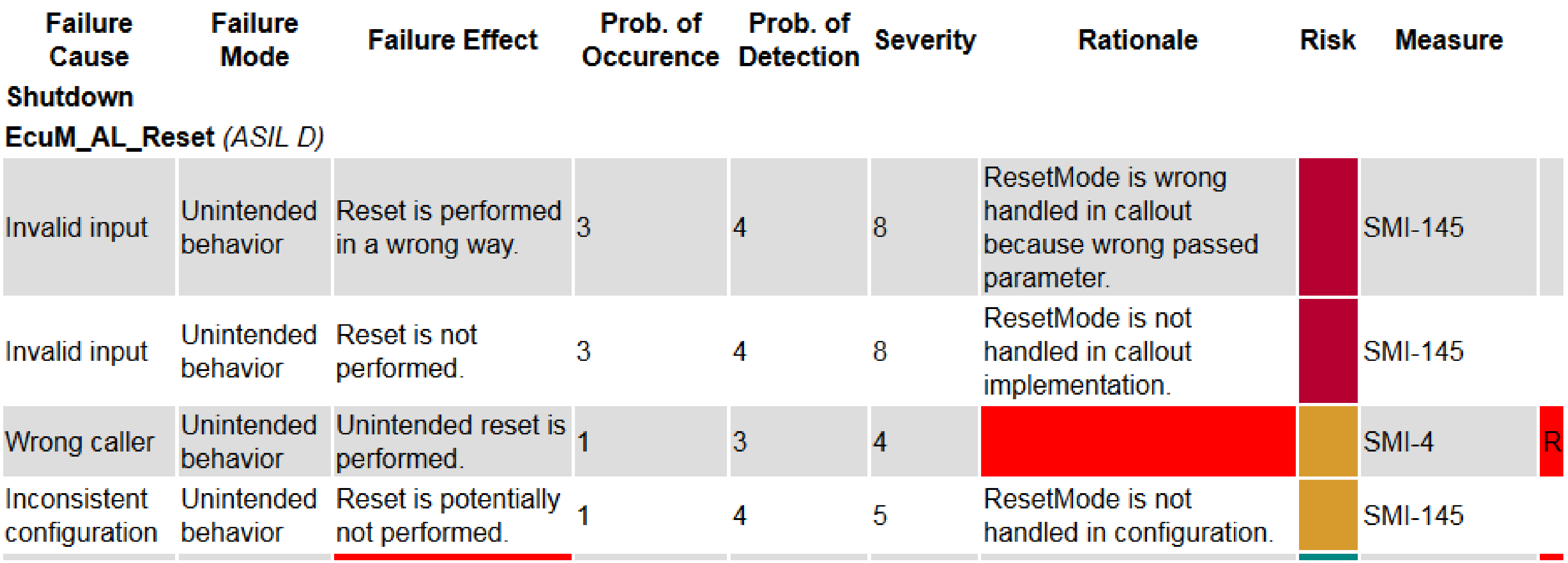
SafetyLevel	QM
ShortName	
Type	

QM
ASIL_A
ASIL_B
ASIL_C
ASIL_D



Safety Notation

- Why?
  - Identify elements for safety analysis.



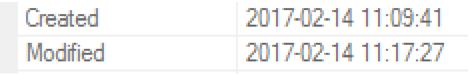
Failure Cause	Failure Mode	Failure Effect	Prob. of Occurence	Prob. of Detection	Severity	Rationale	Risk	Measure	
Shutdown									
EcuM_AL_Reset *(ASIL D)*									
Invalid input	Unintended behavior	Reset is performed in a wrong way.	3	4	8	ResetMode is wrong handled in callout because wrong passed parameter.	🟥	SMI-145	
Invalid input	Unintended behavior	Reset is not performed.	3	4	8	ResetMode is not handled in callout implementation.	🟥	SMI-145	
Wrong caller	Unintended behavior	Unintended reset is performed.	1	3	4	🟥	🟧	SMI-4	R
Inconsistent configuration	Unintended behavior	Reset is potentially not performed.	1	4	5	ResetMode is not handled in configuration.	🟧	SMI-145	

Configuration Management

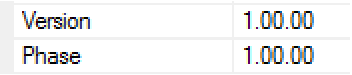
- What are the changes? (e.g. relevant for review, impact analysis)

- EA mechanism
  - Audit
  - Baseline
- Simple mechansims
  - Create/Modify date
- Extended mechansims
  - Create/Modify version
  - DesignLog/SafetyLog

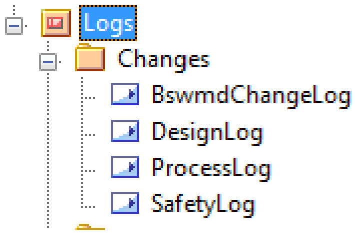
- Export & Compare
  - Focus on „relevant“ data.



Created	2017-02-14 11:09:41
Modified	2017-02-14 11:17:27



Version	1.00.00
Phase	1.00.00



- Logs
  - Changes
    - BswmdChangeLog
    - DesignLog
    - ProcessLog
    - SafetyLog

Conclusion

- Model-based development uses a central model repository to integrate all relevant development data
- You can create relations between all the model elements and so fulfill the process requirements for traceability and consistency
- Tool data integration enables the reuse of existing data as basis for further tools in the development tool chain (e.g. FMEA-tool)
- Model-based development with SysML in a context of ISO26262 helps to ensure the process requirements and leads to consistent system and safety specifications at the end of the day and a improved time-saving workflow.

Contact

lieberlieber.com

blog.lieberlieber.com

konrad.wieland@lieberlieber.com