



VISION

Your partner in smart technology

Benefits of Model-Based Design Approach in Safety-Related System Development

Vision Development Oy

Jari Rauhamäki, Harri Laukkanen, Timo
Riikonen and Antero Äikäs

27.04.2017

Agenda

Theory section

About safety

Software defects

Traceability

Demo

- Can consider in context of various aspects
 - Traffic
 - Downhill skiing
 - Wild animals
 - Chemicals
 - **Machinery and similar systems**
- Can be seen from different viewpoints
 - Perceived - How do people feel about their situation?
 - Substantive - How often and how severe harm has a system produced?
 - **Normative – Does a system conform with the relevant standards and regulation?**

- Definition in a normative context (IEC 61508-4:2010)
 - 'Freedom from intolerable risk'
- Is founded on hazard and risk analysis
 - Hazards and risk need to be known to justifiably mitigate them into a tolerable level
- Identified intolerable risks are mitigated to a tolerable level
 - How should this be achieved?

Risk mitigation approaches

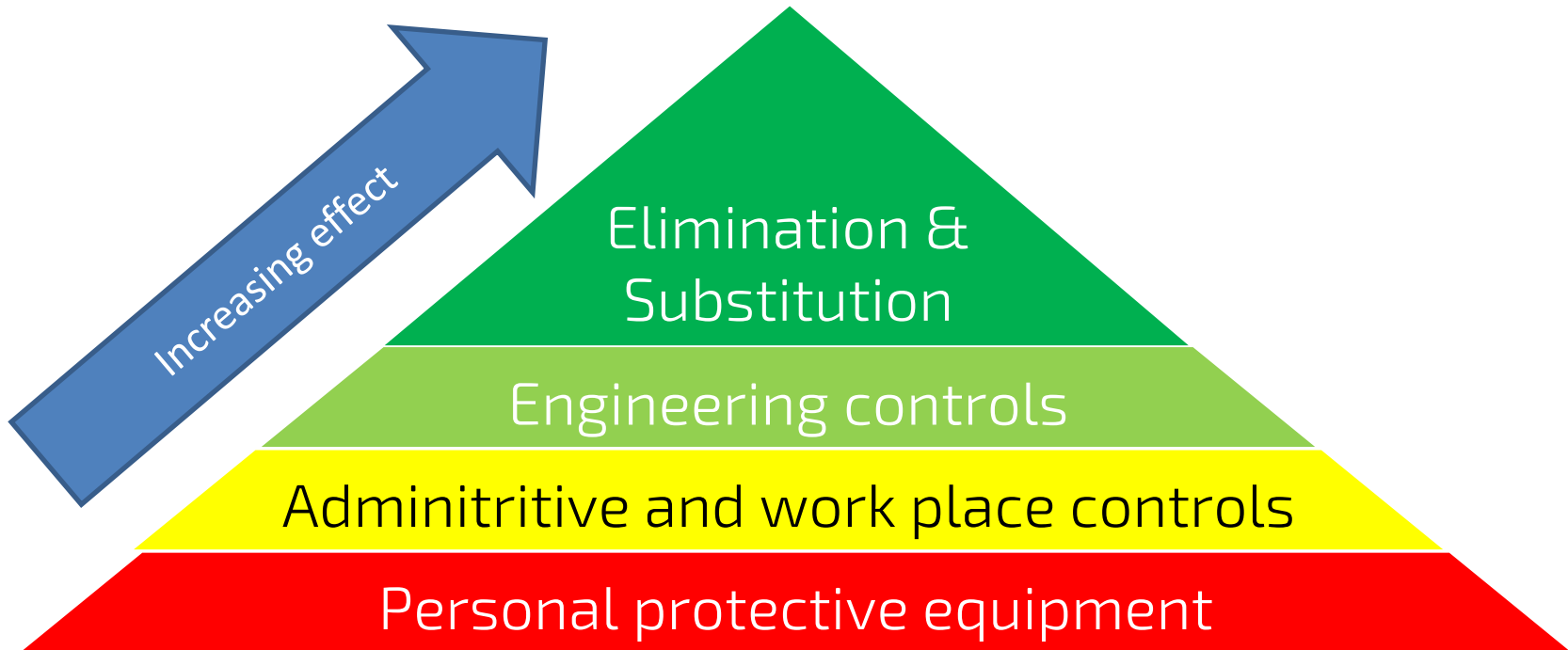


Figure constructed based on:

1. Manuele, F. A., "Risk assessment & hierarchies of control," Professional Safety, vol. 50, no. 5, p. 33, 2005.
2. Nix, D. (2011, Feb) Understanding the hierarchy of controls. Machinery Safety 101. [Online]. Available: <http://machinerysafety101.com/2011/02/28/understanding-the-hierarchy-of-controls/>

- Machinery is often given two typically contradicting requirements:
 - to be efficient and suit the purpose for which they have been designed to
 - to be safe to use and operate
- Keeping the efficiency and advanced functionality while achieving safety of the machine may be challenging
 - Enabling maximum amount of flexibility and possibilities, but keeping safety of the user when needed → Engineering controls and functional safety
 - Increased functionality allows for more fine grained safety features → Software approach often selected for more complex applications
- Therefore, an assumption:
 - Application software needs to be developed to implement a safety function

- Legislative bodies have subjected requirements considering safety of machinery:
 - Machinery directive in European market
 - OSHA in USA market
 - Other legislation and directives in other markets
- Standards help manufacturers to achieve compliance with legislation:
 - IEC 61508
 - EN/ISO 13849
 - IEC 62061
 - ISO 25119
- Requirements regarding the development and life-cycle of the system under development, hardware and software, etc.

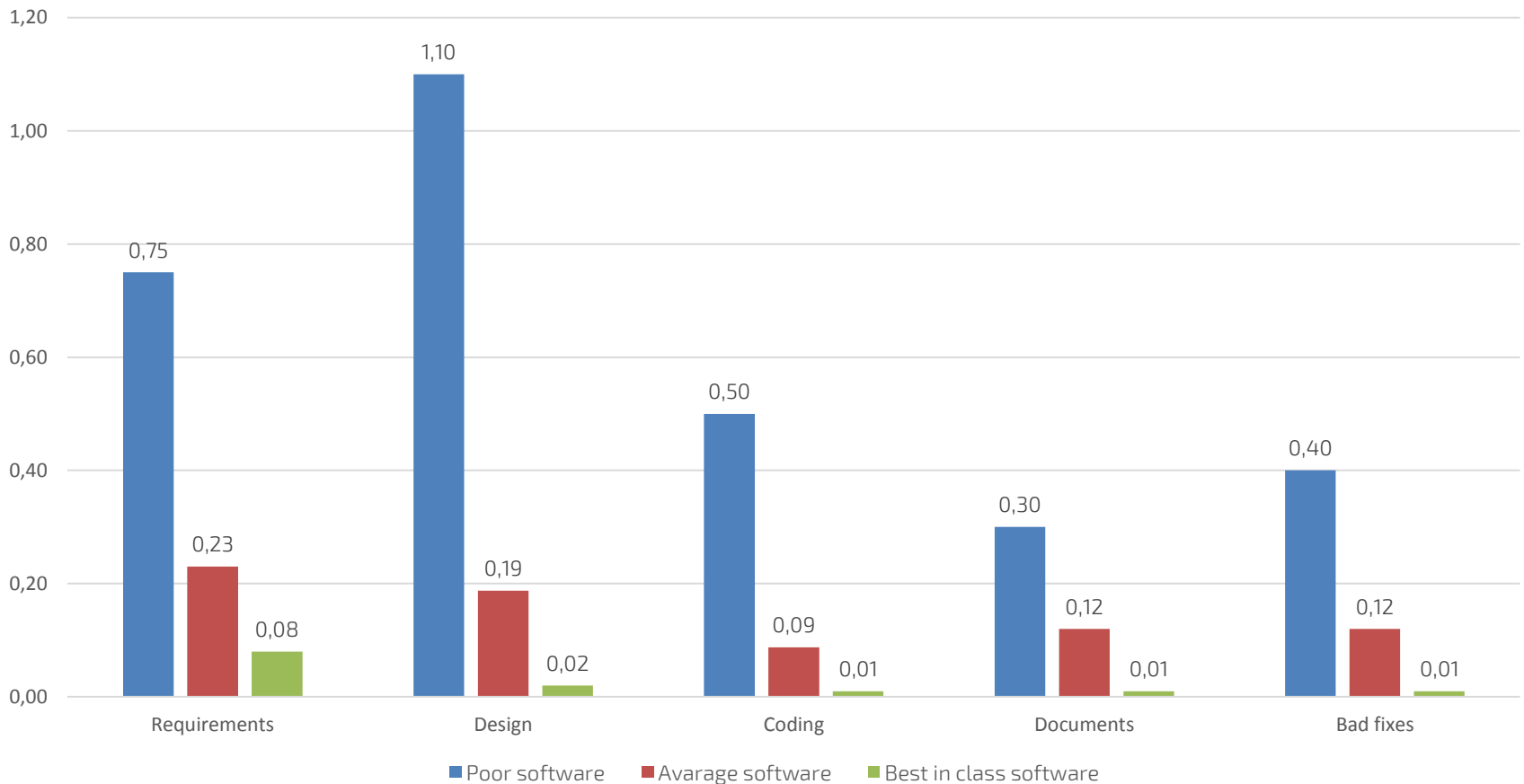
Focus on the most vulnerable phases of design

Traceability

THE BENEFITS OF MODEL-BASED DESIGN

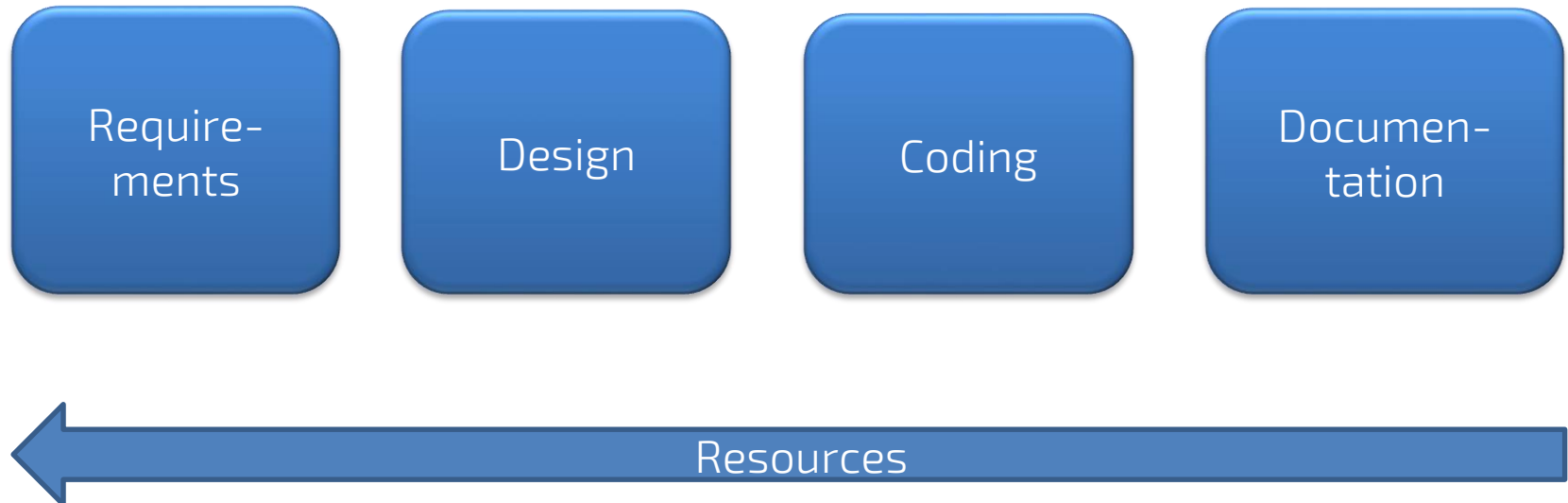
Origins of software defects (20)

Delivered defects in software per function point



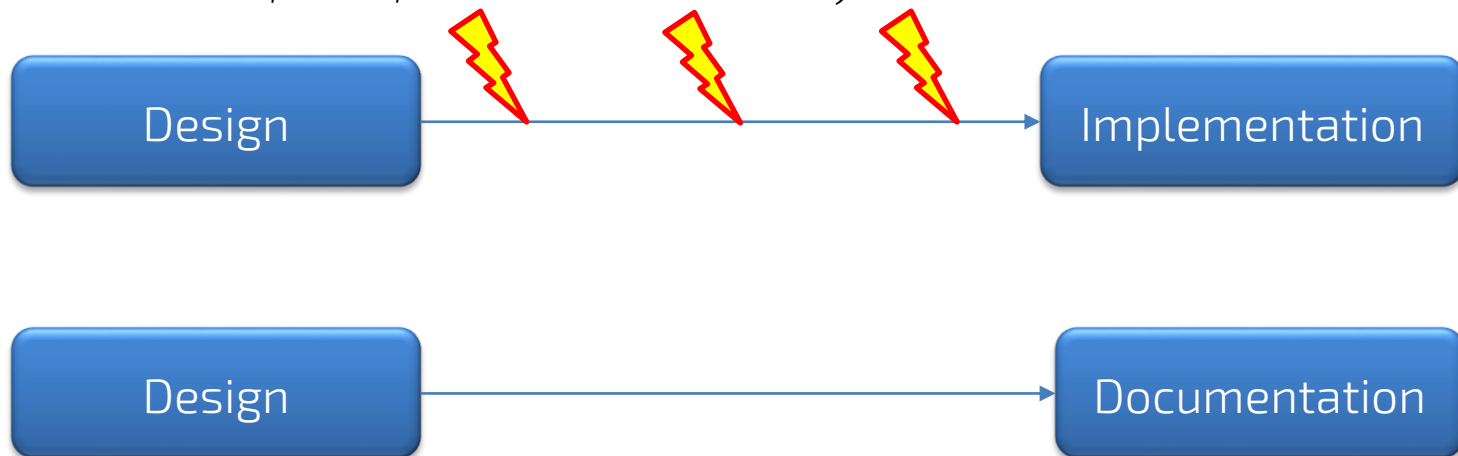
How can model-based design help here?

- In model-based design process the coding and documentation parts can be omitted partly or completely
 - Code for a target runtime/platform is generated from the model
 - Documentation is generated from the model
 - More resources can be allocated to the requirements specification and design phases.



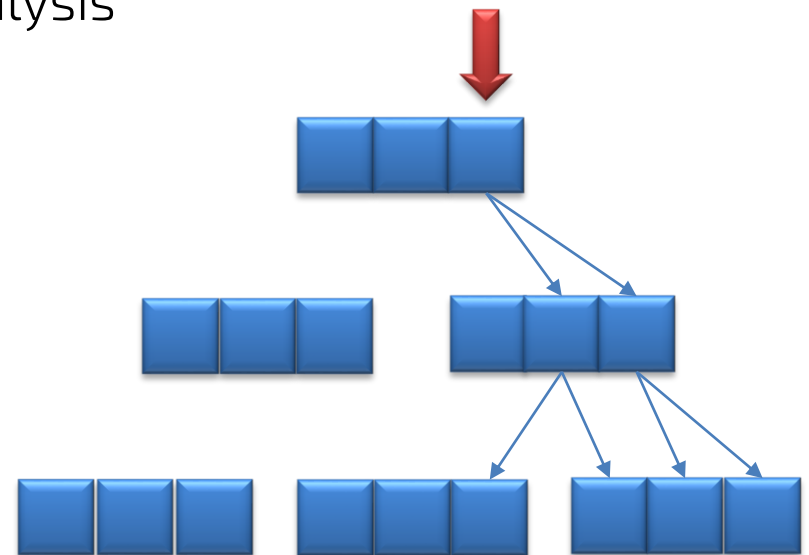
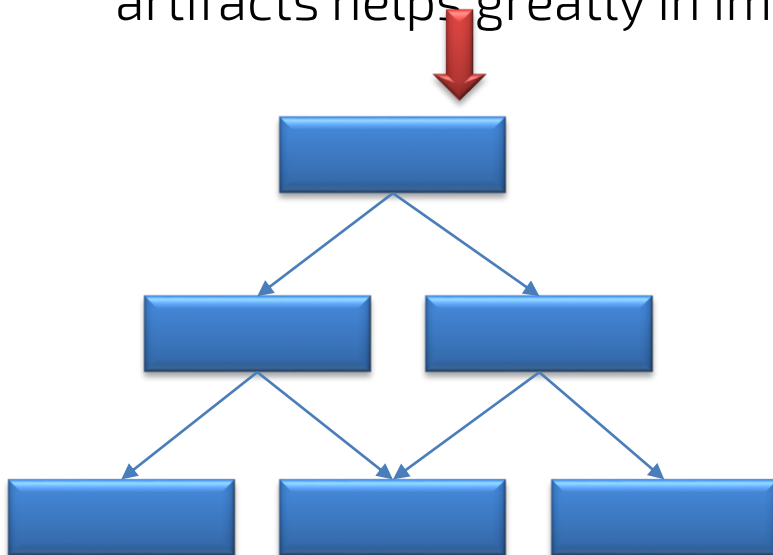
How can model-based design help here?

- Code and documentation is generated by computer (generator software) that should ideally match the specification, the model that is, completely
 - Faults introduced in software implementation phase diminish or at least interpretation errors diminish (assuming the generator introduces no new faults)
 - There should not be any difference between the documentation and the specification of the system (assuming corresponding version of the model, code, and documentation).



- Traceability is a frequent requirement in standards considering development of safety-related parts of (control) system
 - Needed to show compliance with the standard
 - IEC 61508 and ISO 25119
- Helps to assess whether all the requirements have been implemented and tested
- Forms paths between design time artifacts
- Enables (and highly supports) impact analysis to assess the effect of a planned change in the system
- Some work is needed to establish traceability
- Developers need to model and maintain the traceability relations in the software (or system) model

- Done before a safety-related part of a control system is modified
- The purpose is to determine the parts of the system a modification affects
- The results of the analysis is a factor in the needed amount of work to carry out the modification
- A solid and correct traceability between design and software artifacts helps greatly in impact analysis



How to handle traceability?

- The approach to implement traceability can be selected freely
 - Excel, Word

REQ 1.1.1

X needs to be calculated to...

Traces

REQ 1.2.1, REQ 1.2.2

Top level requirements	Subsystem A Requirements	Traceability for upper level	Subsystem B Requirements	Traceability for upper level
1.1.2	1.1	1.1.2	1.1.1	1.2.2
1.1.3	1.2	1.2.1	1.1.2	2.1.3
1.2.1	1.3	1.2.2	1.2.1	2.1.3
1.2.2	1.4	1.2.2	1.2.2	2.1.1
1.2.3	1.5	1.2.1	1.2.3	2.1.2
2.1.1			1.3.1	1.2.1
2.1.2				
2.1.13				

REQ 1.2.1

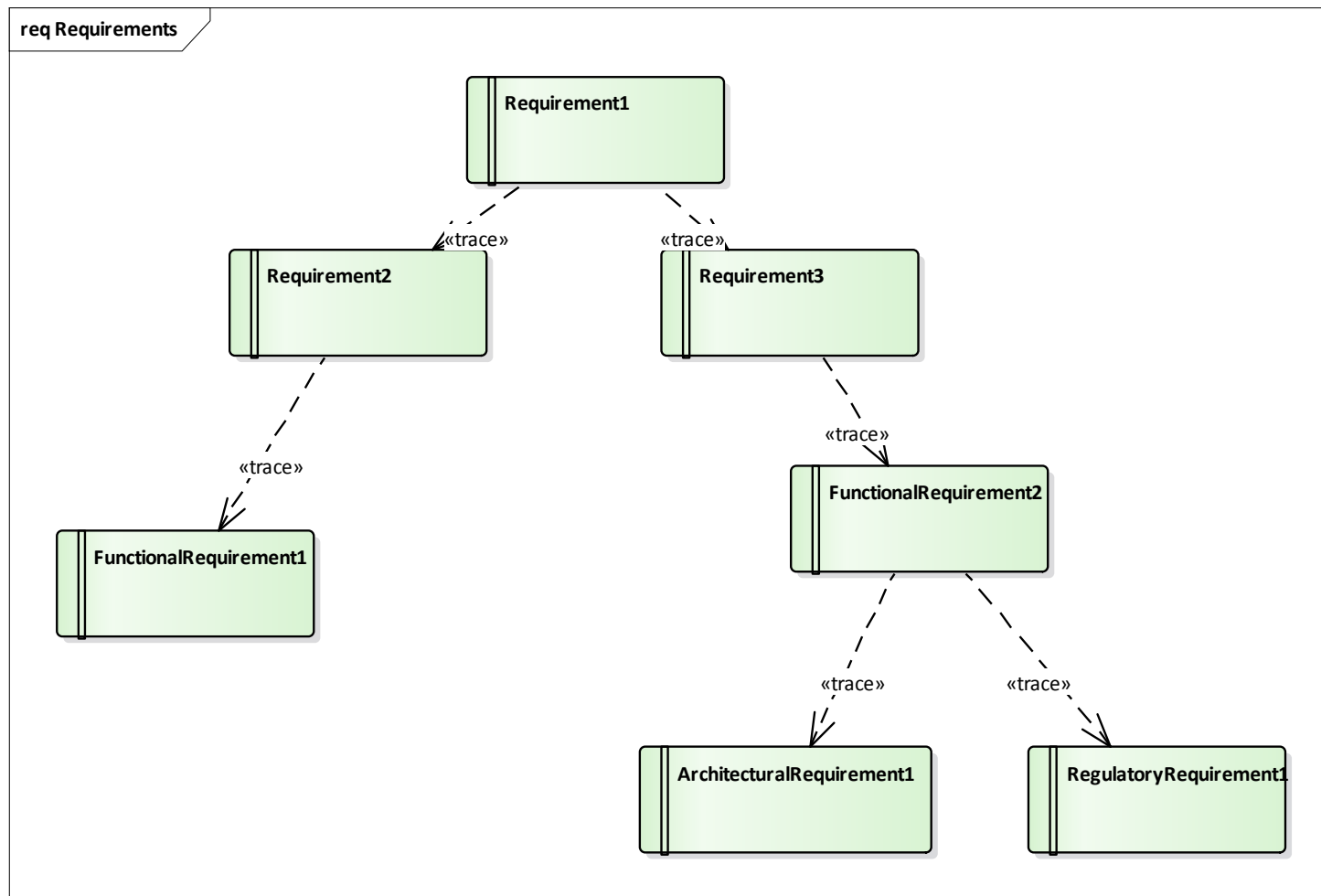
When requested, X shall be calculated within Z seconds for 90% of cases.

REQ 1.2.2

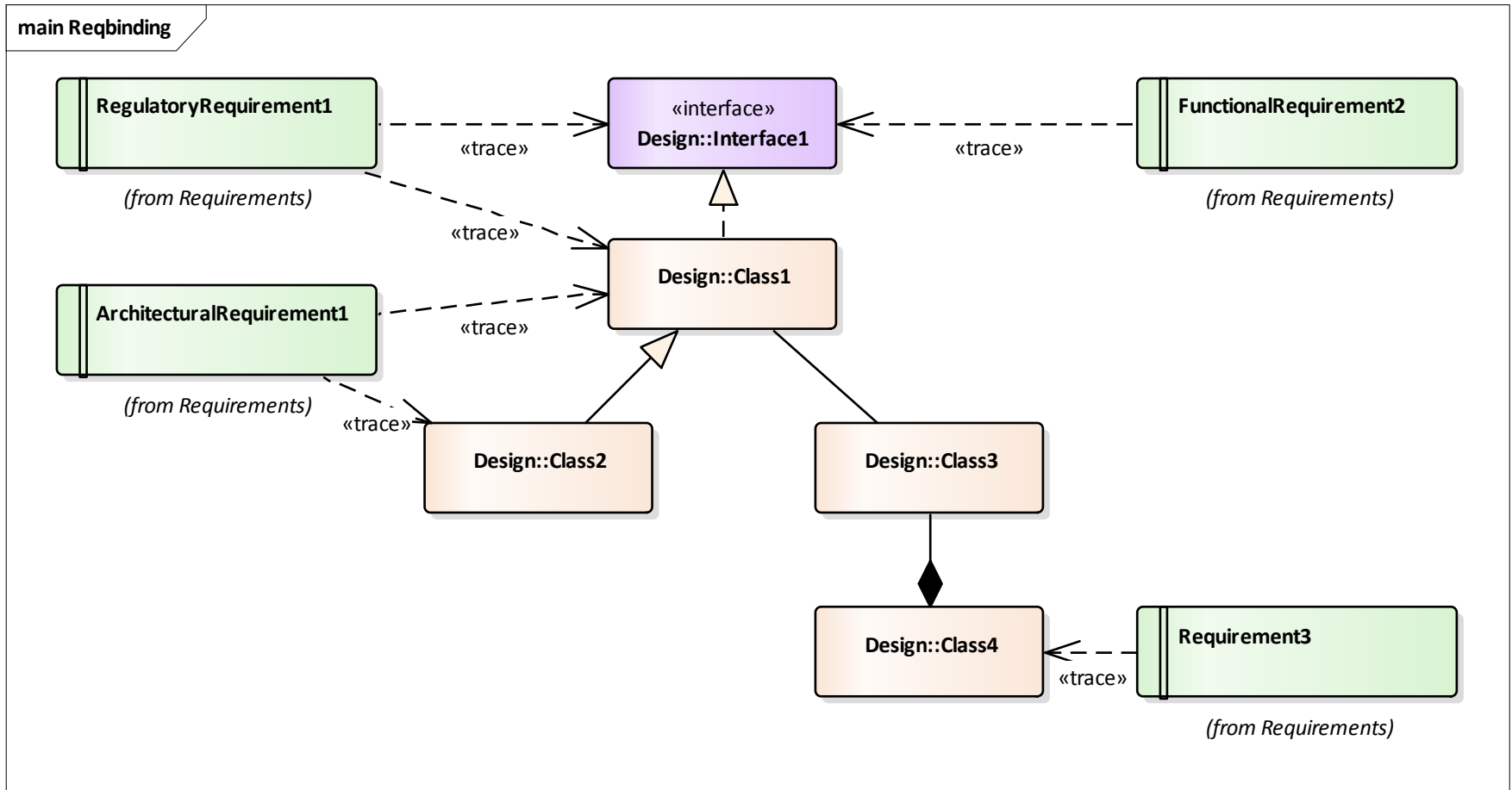
The worst-case calculation time for X shall not exceed Y seconds.

Better alternatives?

- Modeling the traces directly between the design artefacts



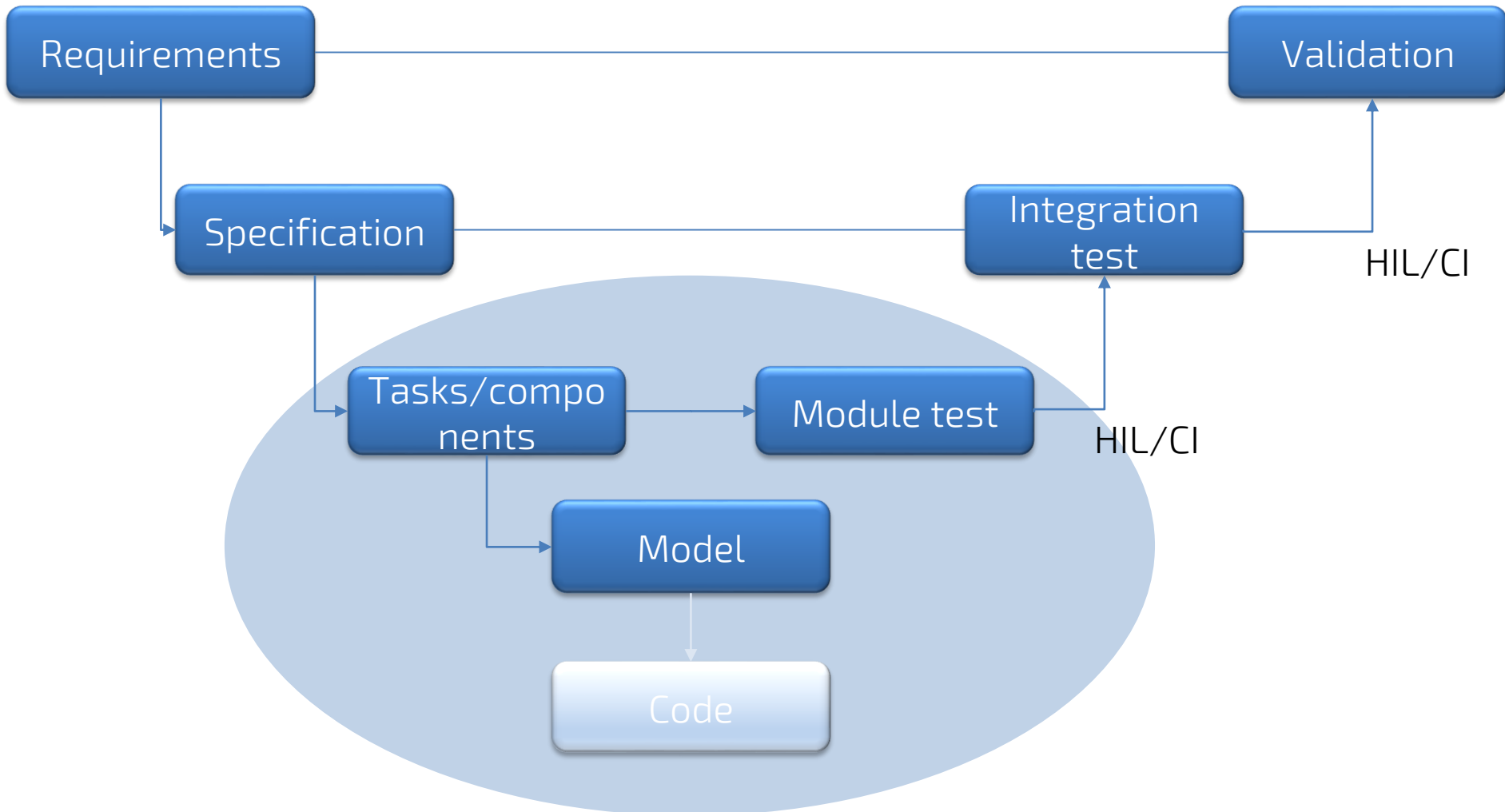
Requirements traced to model elements



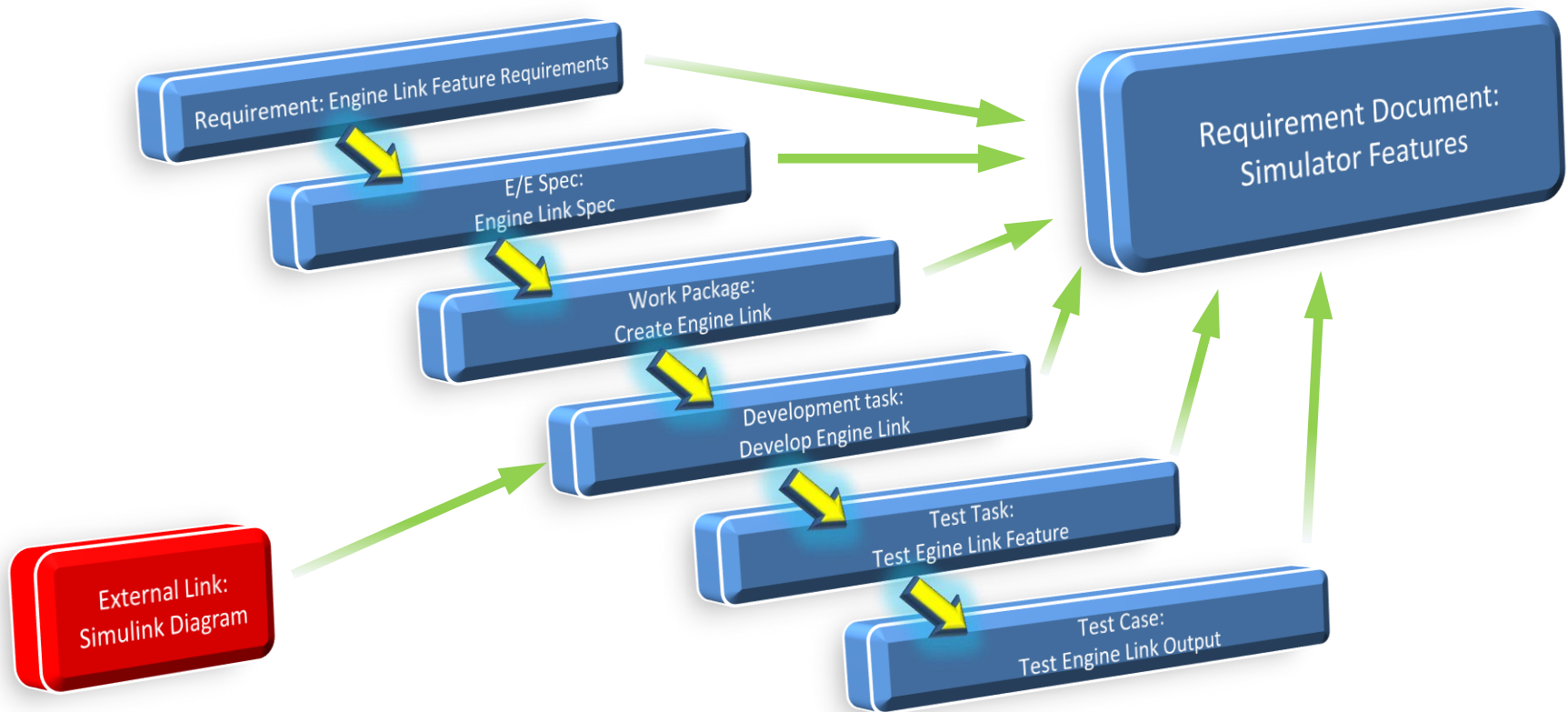
DEMO

- Development process utilizing:
 - Polarion
 - Simulink
 - Polarion connector for Simulink
- Case: Element link
 - A module to communicate with a motor simulation software and a testing environment

Demo case· outline



Engine Link Simulator Feature in Polarion and Simulink



Engine Link Requirement



Valtra_PDO-395 - A vehicle simulator needs an rpm speed link to a motor simulator

↑ Valtra_PDO-400 Valtra_PDO-397 Valtra_PDO-396

Type: Requirement	Requirement Type: Functional	Estimated Time Guess:	Aggregated Time Estimations:
Author: Aikas, Antero	Space:	Estimated Story Points Guess:	Aggregated Spent Time:
Assignee(s):	Document:		Aggregated Remaining Time:
Status: Draft	Planned In:		Aggregated Story Points: 10.0
Resolution:			

Description

A vehicle simulator needs an rpm speed link to a motor simulator. Without this link between the model and the motor simulator the model is not able to work and an engine torque cannot be known. The model must have someway to transfer the rpm speed of its gearbox to the motor simulator and the motor simulator must have an output for the torque signal.

Linked Work Items

Suspect	Role	Title	Project	Revision	Status	Assignee(s)
	is verified by	Valtra_PDO-400 - Test a vehicle simulator's rpm speed link to a motor simulator	Valtra Platform DevOps			
	in implemented by	Valtra_PDO-397 - Add a vehicle simulator's rpm speed link to a motor simulator	Valtra Platform DevOps			
	is detailed by	Valtra_PDO-396 - A vehicle simulator's rpm speed link to a motor simulator	Valtra Platform DevOps			

Engine Link E/E Spec

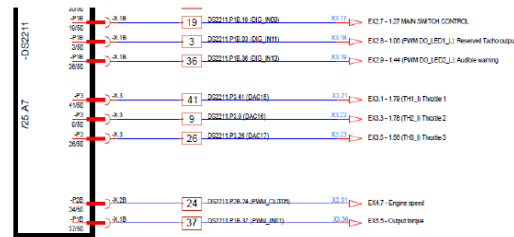
Valtra_PDO-395
Valtra_PDO-396 - A vehicle simulator's rpm speed link to a motor simulator
 Valtra_PDO-400 Valtra_PDO-397

Type: E/E Spec Initial Estimate: Spec Type:
 Author: Aikas, Antero
 Assignee(s):
 Status: Draft
 Resolution:

Description

A vehicle simulator's rpm speed link to a motor simulator transfers a real speed from the model to the motor simulator. This is the speed the motor are able to run at the current load. Thus the model receives receives a motor torque value from the motor simulator which is used to calculate the rpm value which depends on the current load applied to the model. This link will be done using a dSPACE DS2211 card's PWM output and input. To the output the model sends a speed duty cycle and speed period. The motor torque will be received as a duty cycle value and period.

Below is the electric connection scheme for the link.



Linked Work Items

Suspect	Role	Title	Project	Revision	Status	Assignee(s)
details		Valtra_PDO-395 - A vehicle simulator needs an rpm speed link to a motor simulator	Valtra_PDO-395	1	Open	Aikas, Antero
is verified by		Valtra_PDO-400 - Test a vehicle simulator's rpm speed link to a motor simulator	Valtra_PDO-400	1	Open	Aikas, Antero
in implemented by		Valtra_PDO-397 - Add a vehicle simulator's rpm speed link to a motor simulator	Valtra_PDO-397	1	Open	Aikas, Antero

Attachments

Title	File Name	Size	Author	Last Modified	Actions
screenshot-20170428-050428	screenshot-20170428-050404.png [direct link]	53115 B	Aikas, Antero	2017-04-28 05:04	Show revisions

Engine Link Work Package



Valtra_PDO-395 Valtra_PDO-396

Valtra_PDO-397 - Add a vehicle simulator's rpm speed link to a motor simulator

Valtra_PDO-400 Valtra_PDO-399 Valtra_PDO-402

Type: **Work Package** Aggregated Time Estimations: Aggregated Story Points: **10.0**
 Author: **Aikas, Antero** Aggregated Spent Time:
 Assignee(s): Aggregated Remaining Estimate:
 Status: **Accepted**
 Resolution:
 Planned In:

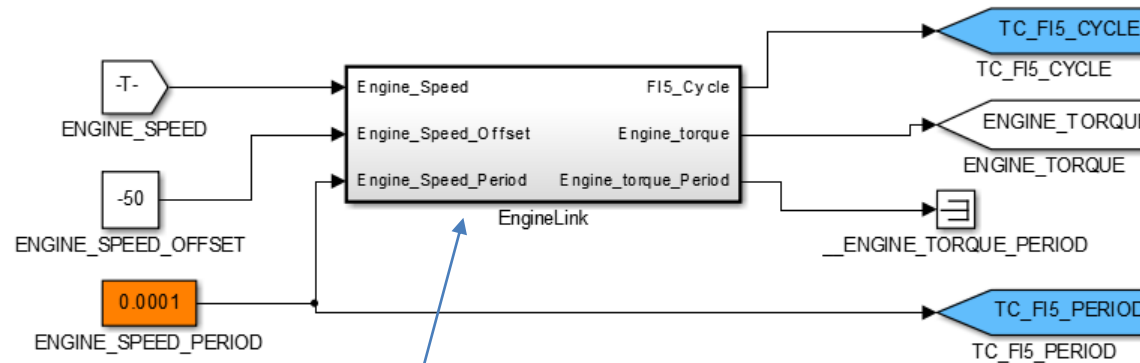
Description

Add a vehicle simulator's rpm speed link to a motor simulator.

Linked Work Items

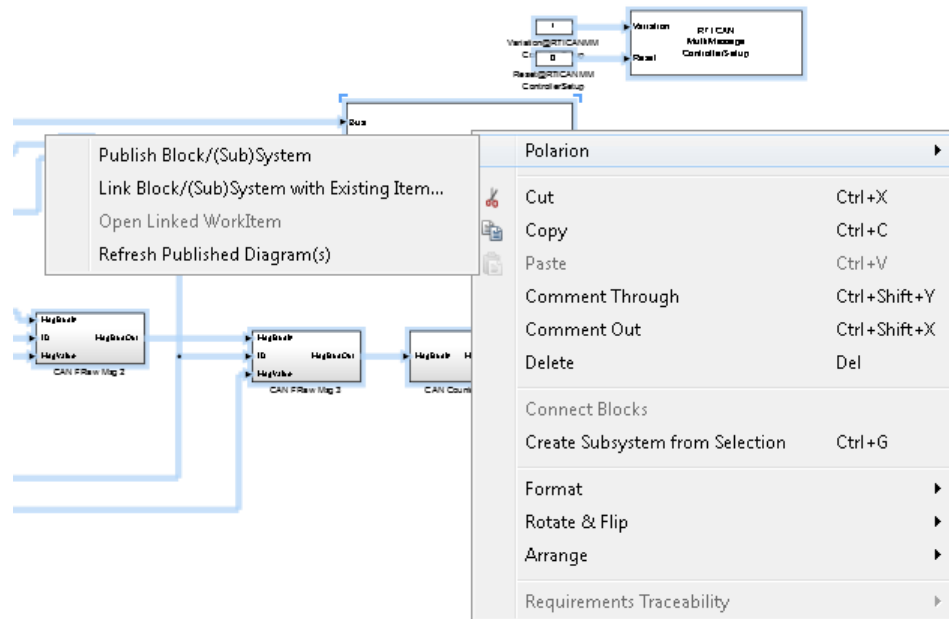
Suspect	Role	Title	Project	Revision	Status	Assignee(s)
	implements	Valtra_PDO-395 - A vehicle simulator needs an rpm speed link to a motor simulator	Valtra Platform DevOps			
	implements	Valtra_PDO-396 - A vehicle simulator's rpm speed link to a motor simulator	Valtra Platform DevOps			
	is verified by	Valtra_PDO-400 - Test a vehicle simulator's rpm speed link to a motor simulator	Valtra Platform DevOps			
	in implemented by	Valtra_PDO-399 - Developing a vehicle simulator's rpm speed link to a motor simulator	Valtra Platform DevOps			Aikas, Antero
	is tested by	Valtra_PDO-402 - Test a vehicle simulator's rpm speed link to a motor simulator	Valtra Platform DevOps			Aikas, Antero

Simulink Engine Link Diagram

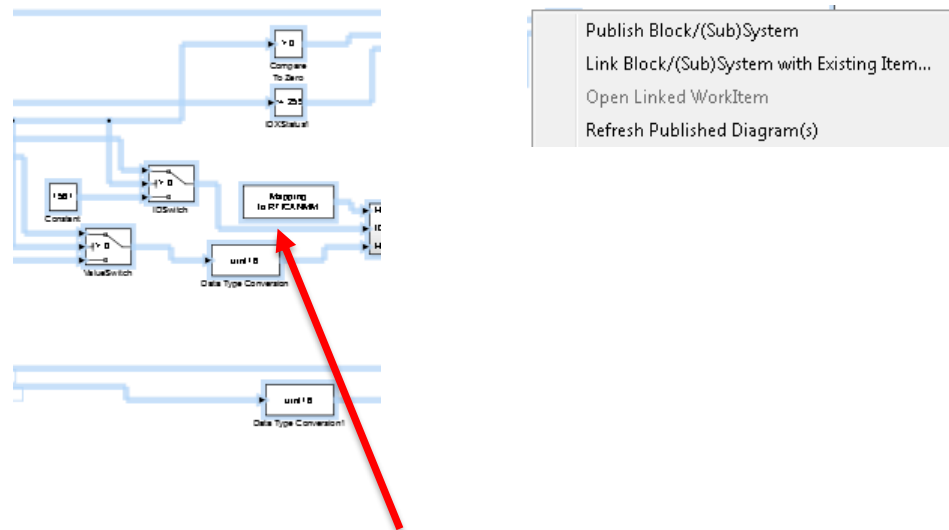


EngineLink subdiagram will be linked to a Polarion document

Menu Integration in Simulink

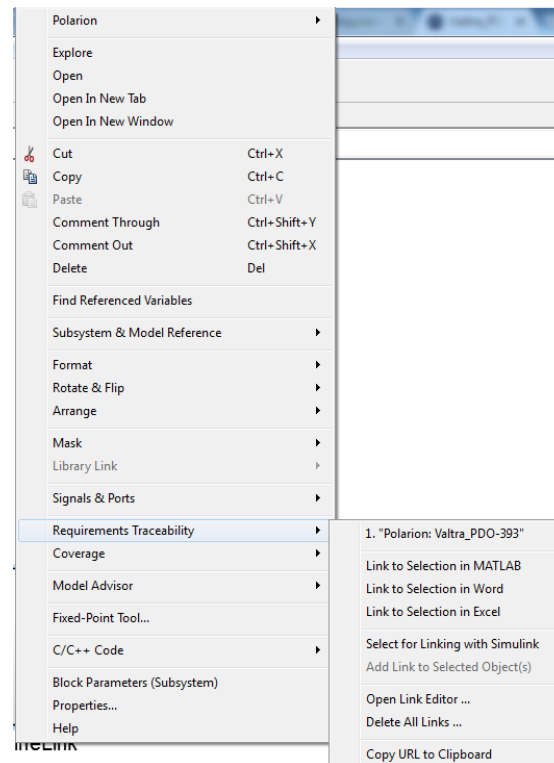


Select Diagram and Polarion Menu Command

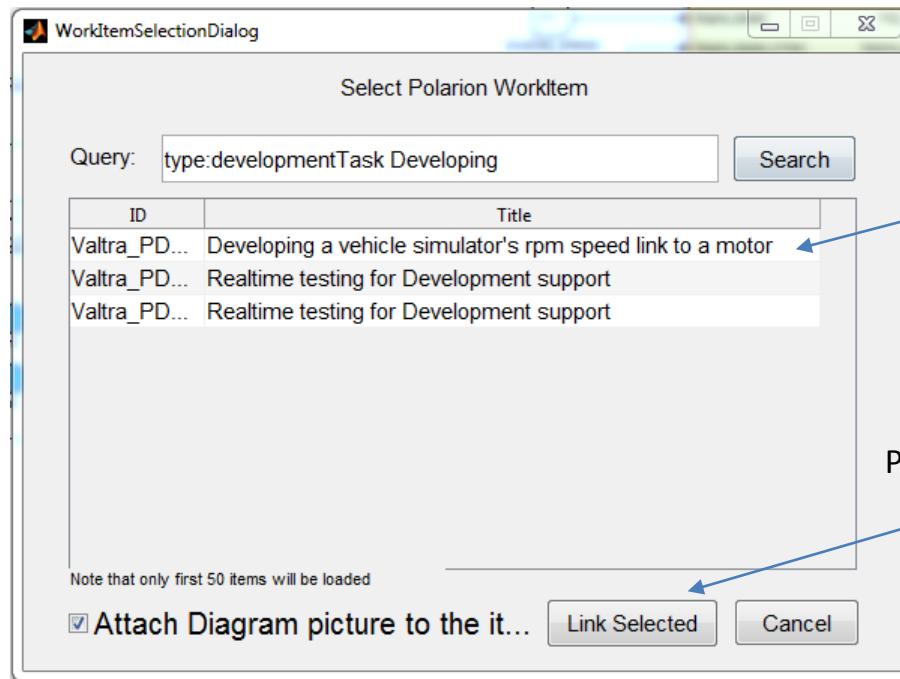


Click inside the selection with the right mouse button

Requirements Traceability



Linking Simulink Diagram To Polaron Document





Select a Polaron document

Press this button to make a link

Engine Link Test Case

 Valtra_PDO-395  Valtra_PDO-396  Valtra_PDO-397

Valtra_PDO-400 - Test a vehicle simulator's rpm speed link to a motor simulator

Type:  Test Case Initial Estimate: Test Type:
Author: Aikas, Antero Test Depth :
Assignee(s):
Status:  Draft

Description

Test a vehicle simulator's rpm speed link to a motor simulator.







- the motor simulator and model should be powered on
- the motor simulator and model should be running
- the PTOs or any external load should not be activated

Test Steps


Step	Description	Expected Result
Turn All Power On	A vehicle must be switched on	
Start Engine	Engine must be started	
Sleep 10 s	Wait 10 seconds until the engine's rpm is stable	
Engine Speed Must Be Around 650	Test if the engine is running at a specified speed	The engine should run at 650 rpm
Engine Torque Must Be Around 150	Test the output torque is in the range	The engine output torque should be about 200 Nm when idling and no external load is applied
Stop Engine	Engine is stopped after the test	
Turn All Power Off	A vehicle must be switched off	

Test Records

Linked Work Items

Suspect	Role	Title	Project	Revision	Status	Assignee(s)
	verifies	 Valtra_PDO-395 - A vehicle simulator needs an rpm speed link to a motor simulator	Valtra Platform Development	1		
	verifies	 Valtra_PDO-396 - A vehicle simulator's rpm speed link to a motor simulator	Valtra Platform Development	1		
	verifies	 Valtra_PDO-397 - Add a vehicle simulator's rpm speed link to a motor simulator	Valtra Platform Development	1		

Test Case Results in Polaron

 **Execute Test**

Current Test Run - no Test Run selected - Start Test Case

# Step	Description	Expected Result	Actual Result	Step Verdict
1 Turn All Power On	A vehicle must be switched on		OK <small>Add Attachment</small>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2 Start Engine	Engine must be started		OK <small>Add Attachment</small>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3 Sleep 10 s	Wait 10 seconds until the engine's rpm is stable		OK <small>Add Attachment</small>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4 Engine Speed Must Be Around 650	Test if the engine is running at a specified speed	The engine should run at 650 rpm	OK <small>Add Attachment</small>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
5 Engine Torque Must Be Around 150	Test the output torque in the range	The engine output torque should be about 200 Nm when idling and no external load is applied	OK <small>Add Attachment</small>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
6 Stop Engine	Engine is stopped after the test		OK <small>Add Attachment</small>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
7 Turn All Power Off	A vehicle must be switched off		OK <small>Add Attachment</small>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Test Case Verdict

This test went trough without problems!

Add Attachment Recent Open next queued Test when finished

Passed **Failed** **Blocked**

Possible to Track Test History in Polarion



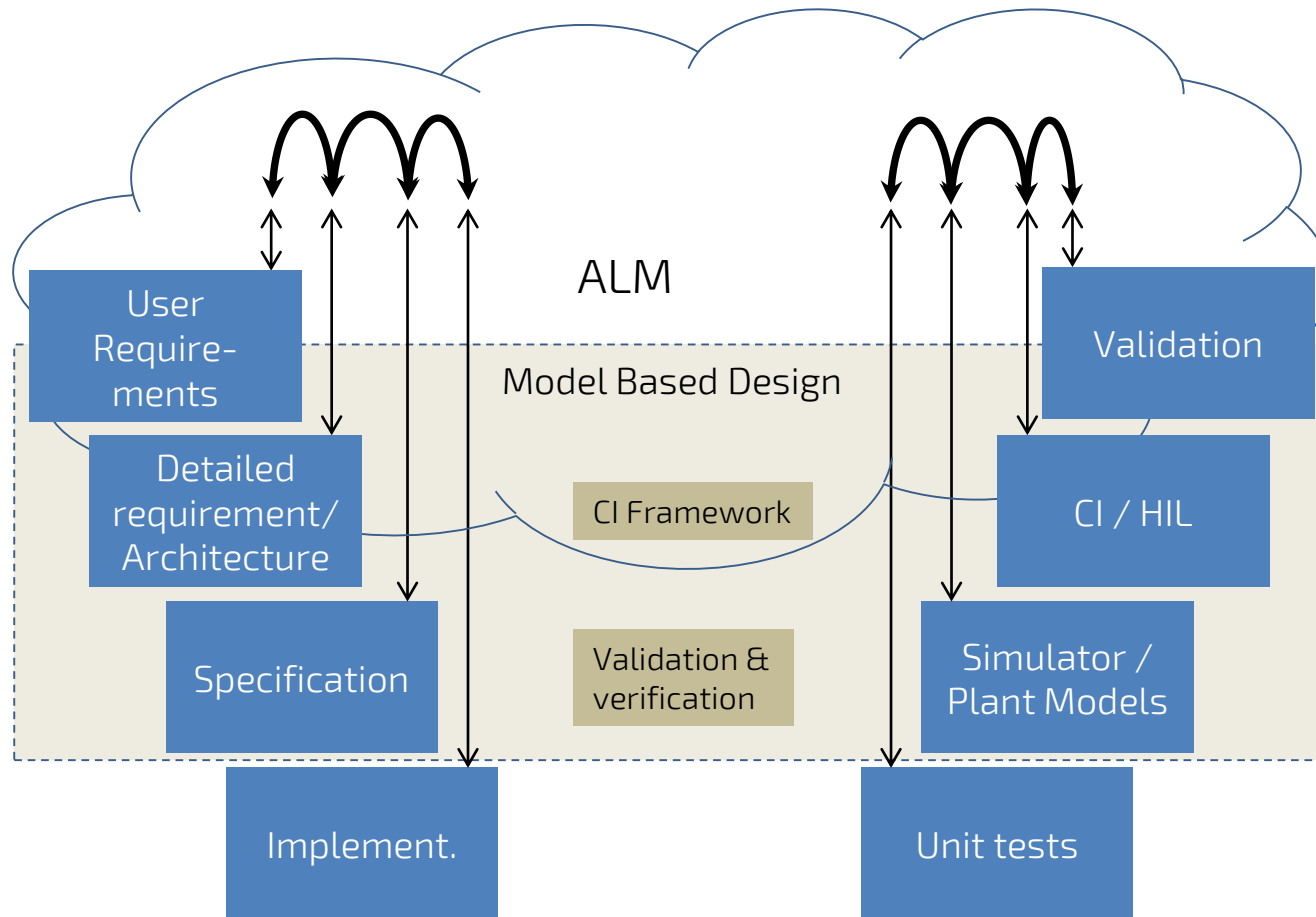
Test Records ▲

Show:

Testexecution History ▲

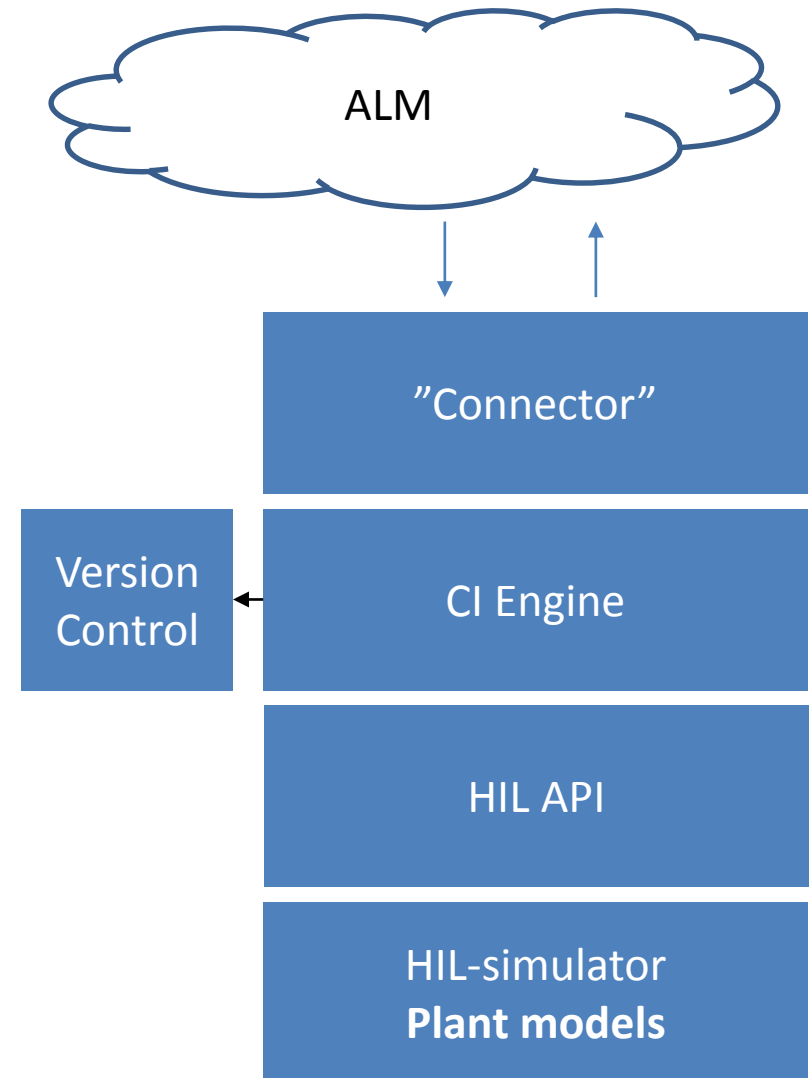
null

- Traceability between design artifacts is considered as a core part of the development process
 - Supports achieving sufficient traceability for safety-related applications
- When all the linked parts of a component/subsystem/element are ready, the documentation can be produced and should be ready for review
 - Supports documentation and project management
- The structure of the Simulink model should be designed to support use with Polarion → Subsystems modularization



Continuous Integration

- Integration tests are run automatically against HIL simulator
- Test cases are automatically executed from ALM system
- HIL API is used for test commands and result feedback





VISION

Your partner in smart technology