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
Safety

• 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?
Safety in the context of machinery

• 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:
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
Normative safety in machinery context

• 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
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 speciation, 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

- 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
Typically, traceability needs to cover the whole development process from requirements to implementation and to verification and validation.
Impact analysis

- 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

<table>
<thead>
<tr>
<th>Top level requirements</th>
<th>Subsystem A Requirements</th>
<th>Traceability for upper level</th>
<th>Subsystem B Requirements</th>
<th>Traceability for upper level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.2</td>
<td>1.1</td>
<td>1.1.2</td>
<td>1.1.1</td>
<td>1.2.2</td>
</tr>
<tr>
<td>1.1.3</td>
<td>1.2</td>
<td>1.2.1</td>
<td>1.1.2</td>
<td>2.1.3</td>
</tr>
<tr>
<td>1.2.1</td>
<td>1.3</td>
<td>1.2.2</td>
<td>1.2.1</td>
<td>2.1.3</td>
</tr>
<tr>
<td>1.2.2</td>
<td>1.4</td>
<td>1.2.2</td>
<td>1.2.2</td>
<td>2.1.1</td>
</tr>
<tr>
<td>1.2.3</td>
<td>1.5</td>
<td>1.2.1</td>
<td>1.2.3</td>
<td>2.1.2</td>
</tr>
<tr>
<td>2.1.1</td>
<td></td>
<td></td>
<td>1.3.1</td>
<td>1.2.1</td>
</tr>
<tr>
<td>2.1.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

REQ 1.1.1
X needs to be calculated to...

Traces
REQ 1.2.1, REQ 1.2.2

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
• 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

Requirement Document: Simulator Features

Requirement: Engine Link Feature Requirements

E/E Spec: Engine Link Spec

Work Package: Create Engine Link

Development Task: Develop Engine Link

Test Task: Test Engine Link Feature

Test Case: Test Engine Link Output

External Link: Simulink Diagram
**Engine Link Requirement**

**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 a way 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**

<table>
<thead>
<tr>
<th>Suspect</th>
<th>Role</th>
<th>Title</th>
<th>Project</th>
<th>Revision</th>
<th>Status</th>
<th>Assignee(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>is verified by</td>
<td>Valtra PDO-400 - Test a vehicle simulator's rpm speed link to a motor simulator</td>
<td>Valtra Platform DevOps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>in implemented by</td>
<td>Valtra PDO-307 - Add a vehicle simulator's rpm speed link to a motor simulator</td>
<td>Valtra Platform DevOps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>is detailed by</td>
<td>Valtra PDO-396 - A vehicle simulator's rpm speed link to a motor simulator</td>
<td>Valtra Platform DevOps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A vehicle simulator's rpm speed link to a motor simulator is a real speed from the model to the motor simulator. This is the speed the motor is able to run at the current load. The model 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 digital (DS161) card if necessary and input. To the output the model sends a speed duty cycle and speed period. The motor torque will become an input duty cycle value and period.

Below is the electric connection scheme for the link.

Linked Work Items:

- [Linked Work Item](valtra_PDO-396 - A vehicle simulator's rpm speed link to a motor simulator)
- [Linked Work Item](valtra_PDO-400 - Test a vehicle simulator's rpm speed when parameters set to a different number)
- [Linked Work Item](valtra_PDO-397 - Add a vehicle simulator's rpm speed when parameters set to a different number)

Attachments:

<table>
<thead>
<tr>
<th>Title</th>
<th>File Name</th>
<th>Size</th>
<th>Author</th>
<th>Last Modified</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Linked Work Item](valtra_PDO-396 - A vehicle simulator's rpm speed link to a motor simulator)</td>
<td>1115B.jpg</td>
<td>12B</td>
<td>Akan, Antero</td>
<td>2017-04-20 13:04</td>
<td>Show revisions</td>
</tr>
</tbody>
</table>
Valtra PDO-397 - Add a vehicle simulator's rpm speed link to a motor simulator

Type: Work Package
Author: Aikas, Antero
Aggregated Time Estimations: 10.0
Aggregated Spent Time:
Aggregated Remaining Estimate:
Status: Accepted
Resolution:
Planned In:

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

Linked Work Items

<table>
<thead>
<tr>
<th>Suspect</th>
<th>Role</th>
<th>Title</th>
<th>Project</th>
<th>Revision</th>
<th>Status</th>
<th>Assignee(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>implements</td>
<td>Valtra PDO-395 - A vehicle simulator needs an rpm speed link to a motor simulator</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
</tr>
<tr>
<td>implements</td>
<td>Valtra PDO-396 - A vehicle simulator's rpm speed link to a motor simulator</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
</tr>
<tr>
<td>is verified by</td>
<td>Valtra PDO-400 - Test a vehicle simulator's rpm speed link to a motor simulator</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
</tr>
<tr>
<td>in implemented by</td>
<td>Valtra PDO-399 - Developing a vehicle simulator's rpm speed link to a motor simulator</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
</tr>
<tr>
<td>is tested by</td>
<td>Valtra PDO-402 - Test a vehicle simulator's rpm speed link to a motor simulator</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
<td>adinifruit.com</td>
</tr>
</tbody>
</table>
Simulink Engine Link Diagram

EngineLink subdiagram will be linked to a Polarion document
Select Diagram and Polarion Menu Command

Click inside the selection with the right mouse button
Linking Simulink Diagram To Polarion Document

Select a Polarion document

Press this button to make a link
Engine Link Development Task

[Image of Simulink subsystems diagram]

The linked Simulink subsystems diagram
Engine Link Test Case

Test Case: Valtra PDO-400 - 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.

Description

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn All Power On</td>
<td>A vehicle must be switched on</td>
<td></td>
</tr>
<tr>
<td>Start Engine</td>
<td>Engine must be started</td>
<td></td>
</tr>
<tr>
<td>Sleep 10 s</td>
<td>Wait 10 seconds until the engine's rpm is stable</td>
<td></td>
</tr>
<tr>
<td>Engine Speed Must Be</td>
<td>Test if the engine is running at a specified</td>
<td>The engine should run at 650 rpm</td>
</tr>
<tr>
<td>Around 650</td>
<td>speed</td>
<td></td>
</tr>
<tr>
<td>Engine Torque Must Be</td>
<td>Test the output torque is in the range.</td>
<td>The engine output torque should about 200 Nm when</td>
</tr>
<tr>
<td>Around 160</td>
<td></td>
<td>idling and no external load is applied.</td>
</tr>
<tr>
<td>Stop Engine</td>
<td>Engine is stopped after the test</td>
<td></td>
</tr>
<tr>
<td>Turn All Power Off</td>
<td>A vehicle must be switched off</td>
<td></td>
</tr>
</tbody>
</table>

Test Records

Linked Work Items

<table>
<thead>
<tr>
<th>Subject</th>
<th>Role</th>
<th>Title</th>
<th>Project</th>
<th>Revision</th>
<th>Status</th>
<th>Assignee(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>verify</td>
<td></td>
<td>Valtra PDO-396 - A vehicle simulator needs an rpm to speed reference</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>verify</td>
<td></td>
<td>Valtra PDO-396 - A vehicle simulator rpm speed link to motor simulator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>verify</td>
<td></td>
<td>Valtra PDO-397 - Add a vehicle simulator's rpm speed to motor simulator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Test Case Results in Polarion

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Expected Result</th>
<th>Actual Result</th>
<th>Stop/Verdict</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Turn All Power On</td>
<td></td>
<td>OK</td>
<td>![Checkmark] ![Cross] ![Stop]</td>
</tr>
<tr>
<td>2</td>
<td>Start Engine</td>
<td></td>
<td>OK</td>
<td>![Checkmark] ![Cross] ![Stop]</td>
</tr>
<tr>
<td>3</td>
<td>Sleep 10 s</td>
<td></td>
<td>OK</td>
<td>![Checkmark] ![Cross] ![Stop]</td>
</tr>
<tr>
<td>4</td>
<td>Engine Speed Must Be Around 650</td>
<td></td>
<td>OK</td>
<td>![Checkmark] ![Cross] ![Stop]</td>
</tr>
<tr>
<td>5</td>
<td>Engine Torque Must Be Around 150</td>
<td></td>
<td>OK</td>
<td>![Checkmark] ![Cross] ![Stop]</td>
</tr>
<tr>
<td>6</td>
<td>Stop Engine</td>
<td></td>
<td>OK</td>
<td>![Checkmark] ![Cross] ![Stop]</td>
</tr>
<tr>
<td>7</td>
<td>Turn All Power Off</td>
<td></td>
<td>OK</td>
<td>![Checkmark] ![Cross] ![Stop]</td>
</tr>
</tbody>
</table>

Test Case Verdict

This test went through without problems!
Possible to Track Test History in Polarion
1.9 Simulator Engine Link

Vehicle_%d_355: 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 drive torque to transfer the rpm speed of its gearing to the motor simulator and the motor simulator must have an output for the torque signal.

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 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 as a duty cycle value and period.

Below is the electric connection scheme for the link:

![Electric Connection Scheme](image)

Add a vehicle simulator’s rpm speed link to a motor simulator:

- Developing a vehicle simulator’s rpm speed link to a motor
- 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.
Observations

• 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
Traceability

User Requirements
Detailed requirement/Architecture
Specification
Implement.

ALM
Model Based Design
CI Framework
Validation & verification

Validation
CI / HIL
Simulator / Plant Models
Unit tests
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