Accelerating Safe Railway Application Development using Model-Based Design

Daran Smalley
Brakes Subsystem Manager

May 10 2023
Agenda

1. About Us
2. Global Trends
3. Our Traditional Workflow
4. Model-Based Design
   Modelling instead of documenting
   Failing Fast
5. Future Model-Based Design
   Even Earlier modelling
   Failing Faster
01 About us
Leading the way to greener and smarter mobility solutions

mobility by nature
We are where mobility is needed

Over 74,000 employees worldwide
From 166 nationalities
70 countries
140 sites
250 depots

19,700 engineers
More than 9,400 patents
Over 150,000 vehicles in commercial service
Partner to over 300 cities

Over 74,000 employees worldwide
EUROPE 44,350 employees
AMERICAS 11,900 employees
AMECA (AFRICA, MIDDLE EAST, CENTRAL ASIA) 4,850 employees
APAC (ASIA PACIFIC) 13,000 employees

As of 31 March 2022

© ALSTOM SA 2023. All rights reserved. Information contained in this document is indicative only. No representation or warranty is given or should be relied on that it is complete or correct or will apply to any particular project. This will depend on the technical and commercial circumstances. It is provided without liability and is subject to change without notice. Reproduction, use, alter or disclosure to third parties, without express written authorization from Alstom, is strictly prohibited.
A global leader in the transportation sector in the digital age

Leading societies to a low carbon future

Alstom develops and markets mobility solutions that provide sustainable foundations for the future of transportation.

Our comprehensive product portfolio ranges from high-speed trains, metros, monorail and trams, to turnkey systems, services, infrastructure, signalling and digital mobility solutions.
Alstom in Västerås - Rolling Stock & Components

- One out of three Global Component Development Sites for Traction equipment
- A Global Test and Technology Centre for Powertrain Systems
- Product responsibility for Mitrac control electronics

Site scope:

- Development of Powertrain Systems including converter- and traction-motor design with validation & verification at in-house, large scale, PowerLab
- Traction equipment manufacturing, from prototyping to after market
- Train Control and Communication electronics
- TCMS Applications including Control, I/O and visualization products
About Me

Daran Smalley
Daran.Smalley@alstromgroup.com
Brakes Subsystem Manager

- Mechatronics Engineer from Monash University in Melbourne, Australia. Now enjoying the freezing cold in Sweden.
- 3 years Electrical Engineer at Rio Tinto aluminium smelter.
- Gap Year travelling Europe
- 7 years Control Software Engineer working in Bombardier/Alstom Traction Control for Traction.
  - Software control engineer transforming Traction Control to a Model Based Design development approach
  - Train performance simulations for Bids and Tenders
  - Customer interface verifying and closing requirements
Global Trends
Megatrends affecting the global rail market

<table>
<thead>
<tr>
<th>Digitalisation / Automation</th>
<th>Emission reduction</th>
<th>Urbanisation</th>
<th>Connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seamless journey</td>
<td>Globalisation</td>
<td>Environmental awareness</td>
<td>Safety</td>
</tr>
</tbody>
</table>

Source: UNIFE, Roland Berger
Growing system and software complexity

Source: McKinsey & Company

Driverless cars will require one billion lines of code, says JLR
Jaguar Land Rover says autonomous vehicles will need 1,000 times more computer code than Apollo 11

Source: Auto Express

The changing face of test: testing advanced aerospace systems
Aerospace electronics and avionics continue to advance at a rapid pace, with few signs of slowing. As aerospace systems grow in complexity, engineers face myriad challenges in the test, validation, and verification of these modern devices. This trend is changing the face of test, and accelerating the need for flexible, scalable test solutions.

Author — Courtney E. Howard
Apr 14th, 2017

Source: Intelligent Aerospace
Our Traditional workflow
Typical Design Process

REQUIREMENTS

INTEGRATION AND TEST

IMPLEMENTATION

CONTROL

Electrical

Mechanical

Cannot validate design against requirements

Cannot test or optimize fully integrated design

Can only find problems using hardware prototypes

Manual coding is slow, buggy, and hard to verify

Typical Design Process

- REQUIREMENTS
- CONTROL
  - Electrical
  - Mechanical
  - Code
- INTEGRATION AND TEST
- IMPLEMENTATION
  - Emb. Code
- Cannot validate design against requirements
- Cannot test or optimize fully integrated design
- Can only find problems using hardware prototypes
- Manual coding is slow, buggy, and hard to verify
Traditional design and verification
How to reduce time and cost with quality?
Model-Based Design
Modelling instead of documenting
Failing Fast
Model-Based Design Benefits

**REQUIREMENTS**
- Detect errors right away with continuous verification

**SYSTEM LEVEL DESIGN**
- Optimize design in a single simulation environment
- Lower costs using HIL tests

**IMPLEMENTATION**
- Save time by automatically generating embedded code

**TEST & VERIFICATION**
- Cannot validate design against requirements
- Manual coding is slow, buggy, and hard to verify
- Can only find problems using hardware prototypes
- Cannot test or optimize fully integrated design
- Optimize design in a single simulation environment
- Lower costs using HIL tests

**INTEGRATION AND TEST**
- Emb. Code
- HIL System
Fail Fast - Detect errors early with Model-Based Design (MBD)
Model-Based Design compared to traditional approach
Software Development Process for Safety-Critical Applications
EN 50128 / EN 50657

7.2. Software Requirements

Software Architecture Design and Integration

7.5. SW Component Implementation

7.5. Software Component Design and Testing

7.6. Software Integration

7.7. Software Component Testing

7.7. Software Validation

Output Work Products
Software requirements
Traceability
Interfaces
Analysis report

Output Work Products
Software architecture
Interfaces
Traceability

Output Work Products
Detailed Design
Dynamic Behavior
Software Unit
Interfaces
Traceability

Output Work Products
Test specification
Test result
Traceability

Model Verification
Code Verification
Model-Based Design: Software development

Source Requirements

Automatic Requirement Document

Software Development Process for Safety-Critical Applications

EN 50128 / EN 50657

© ALSTOM SA 2023. All rights reserved. Information contained in this document is indicative only. No representation or warranty is given or should be relied on that it is complete or correct or will apply to any particular project. This will depend on the technical and commercial circumstances. It is provided without liability and is subject to change without notice. Reproduction, use, alter or disclosure to third parties, without express written authorization from Alstom, is strictly prohibited.
Model-Based Design: Software development

Source Requirements

Design

Automatic Checks

Automatic Requirement Document

Automatic Design Documents

Automatic review Documents

Software Development Process for Safety-Critical Applications
EN 50128 / EN 50657

Automatic review Documents

summaryReport.html
Model-Based Design: Software development

Source Requirements

Automatic Requirement Document

Design

Link

Automatic Checks

Test Environment

Test Manager

Automatic Design Documents

Automatic review Documents

Automatic Test Specification

Code Coverage

SIL

PIL

Emb. Code

Integration Test

Software Development Process for Safety-Critical Applications

EN 00128 / EN 50607

© ALSTOM SA 2023. All rights reserved. Information contained in this document is indicative only. No representation or warranty is given or should be relied on that it is complete or correct or will apply to any particular project. This will depend on the technical and commercial circumstances. It is provided without liability and is subject to change without notice. Reproduction, use, alter or disclosure to third parties, without express written authorisation from Alstom, is strictly prohibited.
Model-Based Design: Software development

Source Requirements

Automatic Requirement Document

Design

Automatic Checks

Test Environment

Test Manager

Automatic Design Documents

Automatic review Documents

Automatic Test Specification

Code Coverage

SIL

PIL

Emb. Code

Automatic Test Report

Integration Test
Model Based Design: Simulate together - Share models

Customer interface

Large train simulator

Simulation of other sections of the train
Timeline – How far we have come
10 Year Journey and more to come

2013 - 2018

- MathWorks Model-Based Design Workflow running on controllers controlling 4MW traction systems
- Traction System functions verified with MBD
- First Software Development Process using MBD
- Targeted First order project
- Training and upskilling Traction Control Department

2019

- MATLAB 2019b
- 4 order project using MBD
- train simulators using Traction System models from Simulink
- Train global control departments on MBD

2020

- Evaluate MathWorks System Composer & Design Verifier.
- 3 Train simulators using traction MBD models

2021

- Alstom Purchase Bombardier
- 1st Safety Certificate for safe MBD software process

2022

- MATLAB 2022b
- Jenkins Servers using Simulink projects
- Simulink products for all Alstom
- Alstom global review best practices

2023

- New department utilises latest MathWorks workflows and experience from traction.
05

Future Model-Based Design
Even Earlier modelling
Failing Faster
Software Requirements Analysis

Software Development Process for Safety-Critical Applications

EN 50128 / EN 50657

Software Requirements - Validation Tests

Reuse of Architecture and Integration Tools

Model Verification

Software Architecture Design and Integration

Software Component Design and Testing

Software Component Testing

Automated Code Generation

Code Verification

Software requirements

Interfaces

Traceability

Analysis report

External Documents

Import / Export

Author

Analyze

Trace

Requirements

Management Tools

Output Work Products

Index Summary

1 Requirement 1: Lock when in use compatible

2 Requirement 2: Unlock during normal shutdown

Description: Main State Machine software component

Rationale:

• Divide operational states of BMC into:
  - Standby State
  - Fault State
  - Charging State
  - Driving State

• Manage transitions between operational states from supervisory controller, contactor state measurement.
Software Architecture Design

**External Documents**
- [doc]
- [xls]
- [database]

**Requirements Management Tools**

**Design**

**Define**

**Describe**

**Evaluate**

**Output Work Products**
- Software architecture
- Interfaces
- Traceability

© ALSTOM SA 2023. All rights reserved. Information contained in this document is indicative only. No representation or warranty is given or should be relied on that it is complete or correct or will apply to any particular project. This will depend on the technical and commercial circumstances. It is provided without liability and is subject to change without notice. Reproduction, use, alter or disclosure to third parties, without express written authorisation from Alstom, is strictly prohibited.
7.7 Software Validation

Specify

Select

Test

External Documents

- doc
- .xls

Requirements Managements Tools

Output Work Products

- Test specification
- Test result
- Traceability