MATLAB EXPO 2019

Simplifying Requirements Based Verification with Model-Based Design

Fraser Macmillen
Requirements & Model-Based Design

Requirements

Models

Tests

Simulink Requirements

Simulink Test

Simulink Requirements
Verification & Validation Products

86 slides of new features in 2019…

R2019a  R2019b
Simulink Requirements is aware of baseline in DOORS 9

MATLAB EXPO 2019
Unlock and Edit Referenced Requirements

Augment referenced requirements with additional details

- Add additional custom attributes without modifying imported content
  - Update restores data from external source and preserves additional content

- Export to ReqIF for roundtrip workflow of local edits with third party tool

See: Roundtrip Workflows with ReqIF Files
Test Specification Report

- Generate report in PDF, ZIP or DOCX format consisting of test specifications (models, inputs, baseline, assessments etc)

- Customization through templates for report formatting

- Custom sections to add extra content that are user specific

<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ExampleTestFile</td>
</tr>
<tr>
<td>1.1. Example TestSuite</td>
</tr>
<tr>
<td>1.1.1. Example BaselineTest</td>
</tr>
<tr>
<td>1.1.2. Example EquivalenceTest</td>
</tr>
<tr>
<td>1.1.3. Example SimulationTest</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Baseline Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal Name</td>
</tr>
<tr>
<td>baseCap.mat</td>
</tr>
<tr>
<td>Input Conversion Subsystem:2</td>
</tr>
<tr>
<td>vehiclespeed</td>
</tr>
</tbody>
</table>

MATLAB EXPO 2019
But what are my requirements for this talk?

1. I shall expand awareness and capability in the use of our tools that support verification of requirements

2. I shall not repeat content from previous EXPOs

3. I shall deliver content appropriate to a masterclass

4. I shall make it interesting!
Minimising
the less we have to deal with the simpler it is

Insight
insight leads to understanding and makes our work simpler

Automation
to speed up the process and avoid errors makes our work simpler
Simplifying Requirements Based Verification with Model-Based Design

Minimising

the less we have to deal with the simpler it is

Insight

insight leads to understanding and makes our work simpler

Automation

to speed up the process and avoid errors makes our work simpler
Minimising – being at the right level

Requirements at the right level

Verification at the right level

Tracing to the right level
Minimising – handling multiple levels

Example

Control system requirements specify the need for filtering of certain signals

The design uses a reusable custom filter to implement the requirement

There are lower level requirements for the filter behaviour itself

Let’s start by creating some links to an instance of the custom filter in the design
Minimising
Minimising – handling multiple levels

When linking a requirement to a Simulink block...

- Can link from either end
- The Simulink block is always the source
- The requirement is always the destination
- The link is saved in the file associated with the source:
  i.e. [modelFileName].slmx
Minimising – handling multiple levels

Linking Between Requirements At Different Levels

The prime purpose of traceability is to infer what is the origin/parent/source of an object.

i.e. a link is from child to parent, from source to destination

i.e. the source is the lower level requirement
the destination is the upper level requirement

The link is saved in the file associated with the source

So: click on source (lower-level requirement) first and create link from the parent requirement…
Minimising
Minimising - Links
Minimising Links
Minimising

Using re-usable components can help
- minimise requirements
- minimise requirement links
Minimising
Simplifying Requirements Based Verification with Model-Based Design

Minimising
the less we have to deal with the simpler it is

Insight
insight leads to understanding and makes our work simpler

Automation
to speed up the process and avoid errors makes our work simpler
## aggregateTests

### TAGS
- Rotor speed dependency
- Component Tests
- FreqResponse
- TimeResponse

### COVERAGE SETTINGS*

#### COVERAGE TO COLLECT
- Record coverage for system under test
- Record coverage for referenced models

Coverage filter filename: [Model Settings]

#### COVERAGE METRICS
- Decision
- MCDC
- Signal Range
- Simulink Design Verifier
- Saturation on integer overflow
- Relational Boundary

#### TEST FILE OPTIONS*
- Close all open figures at the end of execution
- Store MATLAB figures
- Generate report after execution

### Description

#### REQUIREMENTS

#### CALLBACKS

### PROPERTY | VALUE
---|---
Name | aggregateTests
Location | C:/Users/macmill/OneDrive - MathWorks/...
Enabled | √
Tags | Type comma or space separated tags. You can
Insight - Observers
Observers: Separate verification logic from design

- Access nested signals
- Without modifying interface
Insight – Logical & Temporal Assessments
Translate textual requirements into unambiguous Assessments

• Compose assessments using form based editor

• View assessments as English-like sentence

• Review and debug temporal assessment results

• Link to requirements
### Temporal Assessments

<table>
<thead>
<tr>
<th>Index</th>
<th>Summary</th>
<th>Implemented</th>
<th>Verified</th>
<th>Type</th>
<th>Parameter</th>
<th>Parameter Units</th>
<th>Keywords</th>
<th>Verification</th>
<th>SID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>References to WindTurbineControllerRegulator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Front Matter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Wind Turbine Controller Functional Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.1</td>
<td>Wind speed filtering attenuation shall be ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.2</td>
<td>Wind speed filtering attenuation shall be ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.3</td>
<td>Wind direction filtering attenuation shall ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.4</td>
<td>Wind direction filtering attenuation shall ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>Supervisory Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.1</td>
<td>Normal Operation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.2</td>
<td>In normal “auto” operation the turbine ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.3</td>
<td>The turbine shall enter the Standby mode ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.4</td>
<td>The turbine shall enter Brake mode if A...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.5</td>
<td>The turbine shall enter the Generating ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.6</td>
<td>Abnormal Conditions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.7</td>
<td>The turbine shall stop if wind speed exceeds ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3</td>
<td>Pitch Control System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.1</td>
<td>when in power generation mode the rotor ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.2</td>
<td>Under initial load (zero aerodynamic)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.3</td>
<td>Under initial load (zero aerodynamic)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.4</td>
<td>Open-loop gain margin shall be greater than ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.5</td>
<td>Open-loop phase margin shall be greater than ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4</td>
<td>Yaw control System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4.1</td>
<td>The yaw rate magnitude shall be less than ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4.2</td>
<td>The commanded yaw torque per actuator ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>User Interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Operator inputs to system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>The operator panel shall provide a switch ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>Information displayed to operator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3.1</td>
<td>Justifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Summary:** The turbine shall enter the Generating mode [GeneratorTrip FALSE] if the generator speed is greater than 1200 rpm and less than 2200 rpm.
Insight - What if verification is by analysis, not simulation?
What if verification is by analysis, not simulation?
Simplifying Requirements Based Verification with Model-Based Design

Minimising
the less we have to deal with the simpler it is

Insight
insight leads to understanding and makes our work simpler

Automation
to speed up the process and avoid errors makes our work simpler
Simplification – Automation

Examples:

- *Checking parameter values against requirements*

- *Continuous Integration*
Simplification – Automation

Programmatic Interface:
- Find and interrogate requirements and links
- Use to create custom artefacts or utilities

Example…
The rotor cut-in wind speed shall be [windSpeedCutIn].
Continuous Integration (CI) originated as a software development process in which developers integrate their code into a shared repository on a regular basis.

Each commit into a repository is verified by an automated build and test.

These tests may be a pre-cursor to pushing the changes to a main branch.

Continuous Integration can be applied to Mode-Based Design workflows.
Simplification – Automation – Continuous Integration (CI)

How quickly can one set up a continuous integration project to run Simulink Tests against requirements?

How many lines of MATLAB code are required?
How quickly can one set up a continuous integration project to run Simulink Tests against requirements?

< 5 minutes!

How many lines of MATLAB code are required?

- None!
Simplification – Automation - Continuous Integration (CI)

Best practices can minimise the work required

Model-Based verification tools continue to develop to provide insight
- more tool integration
- more ways of accessing information you need intuitively & unobtrusively
- more control over granularity

Automation can be quick to set up, and offers significant benefits
Key products covered in this presentation:

- **Simulink Requirements**
- **Simulink Test**
- **Simulink Coverage**
- **System Composer**

Learn more at Verification, Validation and Test Solution Page:

[mathworks.com/solutions/verification-validation.html](http://mathworks.com/solutions/verification-validation.html)

fmacmill@mathworks.com