Wiederverwendung von Testfällen bei der modellbasierten SW-Entwicklung

DGLR Workshop "Verifikation in der modellbasierten Software-Entwicklung"
Garching, 04 October 2011
Dipl.-Ing. Peter Hermle, Key Account Manager Aerospace
Agenda

- Introduction / Company Overview
- Model Based Software Development Process
- Key features of SILVER ATENA SDE
- Functional Tests, Offline Simulation
- Test Case Reuse for SW Unit Test
- Reference Projects for Model Based Software Development
- Summary / Conclusion
### SILVER ATENA Service Portfolio

#### Safety-critical Electronic Systems Engineering

<table>
<thead>
<tr>
<th>Engineering</th>
<th>Consulting</th>
<th>Products</th>
</tr>
</thead>
</table>
| - Systems Engineering  
- Hardware Development  
- Software Development  
- Safety Engineering | - System Consulting  
- Technology Consulting  
- Process Consulting | - Electronic Control Units  
- Development Tools  
- HiL Test Systems  
- Simulators  
- Test Benches |
### Employees & Locations

<table>
<thead>
<tr>
<th>Location</th>
<th>Employees</th>
<th>Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>56 %</td>
<td>Aerospace, Aero Engines</td>
</tr>
<tr>
<td>UK</td>
<td>13 %</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td>10 %</td>
<td></td>
</tr>
<tr>
<td>India</td>
<td>21 %</td>
<td></td>
</tr>
</tbody>
</table>

In total **more than 450** Employees

#### SILVER ATENA Locations

- **Hamburg**: ~50 Employees
  - Domains: Aerospace, Aero Engines
- **Bremen**: ~10 Employees
  - Domain: Aerospace
- **Stuttgart**: ~25 Employees
  - Domain: Automotive
- **Munich**: ~155 Employees
  - Domains: Aerospace, Aero Engines, Automotive
System Development: V-Model for ECUs

ECU Development

Customer

System Requirements
Requirements ECU
Software Requirements
Software Design
Coding / Implementation
Integration Test Unit Test
SW Acceptance Test
Acceptance Test ECU
System Test
Validation
SILVER ATENA Software Development Process
Standards and Scope

**Software Development based on V-Model:**

- Process according V-Model conformal to
  - ISO 26262 (Automotive)
  - IEC 61508 (Industrial)
  - RTCA DO-178B (Aerospace)

**Scope**

- Definition of an efficient development process with the required planning documentation according to all standards (Automotive, Industrial, Aerospace)
- Definition of quality goals
- Definition of configuration management (CM) and quality assurance (QA)
SILVER ATENA Software Development Process
Planning Documents / Standards / Guidelines

Development Processes and Planning Documents:

- Project Handbook (internal use only)
- Safety Program Plan / PSAC
- SW Development Plan
- SW Verification Plan
- Quality Assurance Plan
- Configuration Management Plan

Standards / Guidelines:

- Software Requirements Standard
- Software Design Standard / Software Modeling Standard
- Software Coding Standard (Software Programming Manual)
- Guidelines, Work Instructions and Checklists
Model Based Software Development
Overview

The Matlab/Simulink Model becomes the executable SW Detailed Design

ECU Requirements & ICD

SW Requirements & HW/SW - SW/SW ICD

SW Architecture & SW Detailed Design

Model (SDM)

The Matlab/Simulink Model

Source Code

ECU Test on Target-HW / HiL

SW Integration & SW Requirements Test on Target-HW / HiL

SW Unit Tests on Target-HW
Key Features of SILVER ATENA
Software Development Environment (SDE)

- SW Design with SDE based on Matlab/Simulink (~80% of SW Design)
- Design documentation generated from Software Design Model (SDM)
- Model Design Standard conformance check at very early stage of development by Simulink Model Checker (SMS Checker)
- Requirements based testing at very early stage of development using Offline Simulation Toolchain (OTE)
- Autocode Generation from SDM in Matlab/Simulink with Mathworks product „Embedded Coder“ using a customized configuration
- No further efforts to generate standard conformal code
- Coding Standard conformance check supported by Code Walk Through Parser
- Reuse of Test Cases for Structural Coverage Analysis
- Reuse of Test Cases and Test Results SW Unit Tests

**IMPORTANT:** No Tool Qualification necessary as no Verification Step is skipped (Full Review on Design Documents and Source Code)
Functional Tests, Offline Simulation

**Verification of Detailed Design vs. SW Requirements**

- Detailed Design is an executable Simulink Model
- Input and expected output data are derived from SW Requirements
- Verification procedure: Simulation/Execution of the Detailed Design and comparison of expected data with actual data

→ Result: Early and more accurate verification of the software design

**Test Case Reuse for SW Unit Tests**

- Prerequisites:
  - One Unit in the Simulink Model corresponds to one Code Unit
  - Functionality of the SW Design is identical with the Source Code
- Benefit: Saves time during Unit Test (reuse of test description)
Features of the Offline Simulation Toolchain

**Automatic Test Frame generation**
- No manual interaction needed
- Simulink Buses are handled by the Tool

**Test Case Template generation**
- Extraction of all input and output signals
- Extraction of all constants used in the Model
- Test Case Templates in MS-EXCEL

**Test Execution**
- Possibility to modify constants
- Comparison of expected and actual data

**Conversion of test data to Unit Test data**
- No manual interaction needed
Offline Simulation Toolchain (OTE)

SW Requirements

Testcase (EXCEL-File)

Offline Test Input

Template Generation

Offline Test Environment

OTE

Inputs

Time | 0 | 1 | 2
---|---|---|---
in1 | 1 | 2 | 3
in2 | 0 | 1 | 1

Expected Outputs

Time | 0 | 1 | 2
---|---|---|---
out1 | 1 | 4 | 9
out2 | 1 | 5 | 10

Simulated Outputs

Time | 0 | 1 | 2
---|---|---|---
out1 | 1 | 3 | 9
out2 | 1 | 5 | 10

Testresult (EXCEL-File)
Offline Test Environment GUI
SW Design Model Review and Analysis

**Verification of SDM vs. Modeling Standard**

- SMS Checker is implemented as M-File into Matlab/Simulink
- The rules of the Modeling Standard (and implicit also partially even some of the rules of the Coding Standard) are implemented
- SMS Checker can be customized
- SMS Checker generates Report Files
Code Review and Static Analysis

Verification of Source Code vs. Coding Standards

- Code Walk Through Parser (CWT Parser) as Eclipse Plug-In
- The rules of the Coding Standard are implemented in the CWT Parser
- The CWT Parser can customized to match different Coding Standards
- Usable for both manually written and autocoded Source Code
- CWT-Parser automatically generates Checklists with info whether
  - Check is passed
  - Check is failed
  - Check has to be performed manually
- These generated Checklists are designed to be the input of the actual Code Walk Through / Review

- IMPORTANT: Code Review for all the Source Code is still considered to be a "manual" Code Review in order to avoid tool qualification
CWT Parser GUI

```c
/* Output and update for referenced model: 'CL29 DEMAND_SELECTION_BANK X' */

void CL29_DEMAND_SELECTION_BANK_X_step(const S_F32 *q_o, const S_F32 *q_lim_x, 
{
    /* SPRI_0083: Identifiers shall not exceed 31 characters (this identifier has 33 characters). */

    if ((*q_lim_x) < (*q_o)) 
        (*q_x) = (*q_lim_x);
    if ((*q_x) > (*q_track)) 
        (*q_track) = (*q_x); 

    /* SPRI_0084: 'Root/Maximum Operator 1' */
    if ((*q_x) > (*q_track)) 
        (*q_track) = (*q_x);

    /* SPRI_0085: 'Root/Minimum Operator 2' */
    if ((*q_x) = (*q_track));
}
```

Writtable   Smart Insert  33:23
66M of 170M
Model Based Software Development
Usage of SDM

Executable SW Detailed Design for Simulation, Autocode, SW Unit Test

- ECU Requirements & ICD
- SW Requirements & HW/SW - SW/SW ICD
- SW Architecture & SW Detailed Design
- Modeling Standard
- SMS Checker
- Coding Standard
- Code Review & Static Analysis
- Functional Testing
- Offline Simulation
- Model (SDM)
- Review
- Test Case Reuse
- SW Integration & SW Requirements Test on Target-HW / HiL
- SW Unit Tests on Target-HW
- Structural Coverage & Dynamic Analysis
- Autocode
- CWT Parser
- Source Code
Example Unit Detailed Design
Example Test Frame
Example Test Vector (EXCEL Table) for Offline Simulations and SW Unit Tests

![Excel Table Example]

The Excel table contains columns for various test cases, input and output variables, and associated values. Each row represents a specific test case, with columns detailing the test conditions and outcomes.
Example Result File (EXCEL Table)

```
<table>
<thead>
<tr>
<th>Time</th>
<th>Value1</th>
<th>Value2</th>
<th>Value3</th>
<th>Value4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>1.2</td>
<td>3.4</td>
<td>5.6</td>
<td>7.8</td>
</tr>
<tr>
<td>0.2</td>
<td>2.3</td>
<td>4.5</td>
<td>6.7</td>
<td>8.9</td>
</tr>
<tr>
<td>0.3</td>
<td>3.4</td>
<td>5.6</td>
<td>7.8</td>
<td>9.0</td>
</tr>
<tr>
<td>0.4</td>
<td>4.5</td>
<td>6.7</td>
<td>8.9</td>
<td>1.2</td>
</tr>
<tr>
<td>0.5</td>
<td>5.6</td>
<td>7.8</td>
<td>9.0</td>
<td>1.2</td>
</tr>
</tbody>
</table>
```

Note: The table represents a sample Excel result file with values at different times.
Features of the Unit Test Toolchain

**Template Generation**
- Test Description template
  - Extraction of input and output signal
  - Extraction of constants used in the code
  - Test Cases in MS-EXCEL
- Executable Test Frame
  - Normal case: no manual interaction needed
  - Stubs: added manually

**Test Procedure Generation**
- Conversion of Test Description to Trace32 Debugger Skript

**Test Execution**
- Separate execution of functional, High Level Language Coverage and Object Code Coverage Tests
- Possibility to run in batch mode
SW Unit Test Environment

- Standard Windows PC used as test platform
- GUI Lauterbach Trace32 In Circuit Debugger
- LDRA Testbed
SW Unit Test and Dynamic Analysis Process

- Test cases from Offline-Tests
- Source Code
- Instrumented Source Code
- LDRA Testbed
- Tool
- Sim2TC
- pre-filled Excel tables
- for model code
- for manual code
- Test data for Unit- and Module-Tests
- Testframe (C-Code)
- Testframe Generator
- Target-HW
- Test report functional coverage
- Results dynamic Analysis
- LDRA Testbed
- Tool
- Perform Unitest
- InOutParser FillOutSkeleton
- Tool
- Test data for Unit- and Module-Tests
- Lauterbach Control file
- Tool
- UT-Preparation ProcGen
- Tool
- Tool
- Tool
SILVER ATENA Tool Chain (SDE) for IEC 61508 / DO-178B Autocode

Autocode for SIL-X / DAL X Applications

- Toolchain generates IEC 61508 / DO-178B qualifiable C-Code (Ada optional)
- Reduction of development efforts approx. 30 %
- Reduction of development time approx. 50 %
- More than 50 software releases already developed and delivered
Reference Project: Automotive ECU for BMW

BMW CleanEnergy ECU for Hydrogen 7-Series Passenger Car

System Development Innovation
- First Automotive ECU compliant with IEC 61508 / SIL-3
- Dual lane system for „fail-operative“ concept
- 86 % of SIL-3 software autocoded from Matlab/Simulink with SILVER ATENA SDE
- Master Control Unit for all hydrogen relevant components
- Scope of Project: From Concept to Series Production (Small Series < 150 Units)
- Fully qualified Software Release within just a few weeks by use of SDE
Reference Projects: ECUs for Aero Engines

**Engine Control Unit Development**
- Development based on V-Model approach
- Model Based Software Development
- Simulation of Models for Engine Control Unit and Environment
- Generation and Integration of qualifiable Auto Code
- Development and operation of HiL Test Systems
- HW Development
- HW/SW Test and Verification
Summary / Conclusion

- Model Based SW Development can speed up ECU Software Development and help reduce both coding and testing efforts

- Offline Simulations and Test Results during Development Phase can be reused during Verification Phase for SW Unit Tests

- The SILVER ATENA Software Development Environment (SDE) in contrast to other Toolchains or formal methods does NOT require any tool qualification

- **SILVER ATENA** has successfully demonstrated the use of Model Based SW Development with the SDE for Automotive and Aerospace Projects
Many Thanks for Your Attention! Any Questions?

The technology we develop today, will be progress tomorrow.

Engineering | Consulting | Products
Contact

Dipl.-Ing. Peter Hermle  
Key Account Manager Aerospace

SILVER ATENA  
Electronic Systems Engineering GmbH  
Dachauer Str. 655  
D-80995 Munich, Germany

Tel.: +49 89 18 96 00 – 82 75  
Fax: +49 89 18 96 00 – 85 17  
p.hermle@silver-atena.de  
www.silver-atena.de

GERMANY

- Bremen  
  Aviation Center  
  Airbus-Allee 5  
  D-28199 Bremen

- Hamburg  
  Hein-Sass-Weg 36  
  D-21129 Hamburg

- Stuttgart  
  Hanns-Klemm-Str. 5  
  D-71034 Boeblingen

UK

SILVER ATENA Ltd.  
Cedar House  
Swindon Rd  
Malmesbury  
Wiltshire  
SN16 9RS

INDIA

SILVER ATENA  
Electronic Systems Pvt. Ltd.  
Plot No. 23 & 24  
EPIP 1st Phase  
KIADB, Whitefield  
Bangalore 560066

SPAIN

SILVER ATENA  
Avenida de España 23, 3º  
28100 Alcobendas, Madrid