Model Based Systems Engineering: Bringing Together Safety Critical Embedded Software and Full System Simulation

Eric BANTEGNIÉ
President & CEO, Esterel Technologies
VP Systems Business Unit, ANSYS
When software & electronics become dominant in a product architecture

- Larger solution space – more design degrees of freedom
- Multiplicity of architectural interfaces have to be designed, tested and maintained
- Electronics & software are increasing the risk of catastrophic failure modes and the cost of safety certification

Manage Complexity to design innovative, market leading products

Coordinate Interdisciplinary Engineering to reduce design changes and development costs

Early & Reliable Verification to deliver high quality, safe, and reliable products to the market faster
Coping with Systems engineering challenges

Manage Complexity

Requirements and Specifications

System Functional & Architectural Design

Sub-System Design

Component Integration & Verification

Early and Reliable Verification

System Validation

Coordinate Interdisciplinary Engineering

Detailed Design & Optimization

Mechanical Electrical Software

Detailed Design & Optimization
Systems V Practices and Owners

Requirements Mgmt and Functional Design Practices

- Requirements analysis
- Requirements traceability
- Variant management
- Operational and usage analysis
- Functional decomposition
- Functional simulation
- Architectural design & selection
- Rapid prototyping
- Physical system simulation (0D plant models)

Validation Groups

Engineering Groups

Integration and Validation Best Practices

Virtual:
- Virtual system integration & simulation
- 0D – 3D co-simulation
- Reduced order modeling

Physical:
- Component Hardware testing
- Calibration

Mixed:
- SiL
- HiL
- TiL

Detailed Design and Optimization Best Practices

Hardware Design
- CAD
- Single physics
- Multiphysics
- Optimization

Electronics Design
- ECAD
- EDA
- Circuit analysis
- 3D physics
- Multiphysics
- Optimization

Software Design
- Model-based controls design
- Model-based display design
- Automatic code generation and certification
- Software configuration management
System Functional and Architectural Design
Model Based System Engineering

**DESIGN**

**VERIFY**

**INTEGRATE**

- Model Checking
- Model Diff
- System/Software Sync Up (including I/Os)
SCADE System delivers powerful functional and architecture modeling capabilities.
Step 1: Define what the system shall do

- Draw the functions and interfaces with SCADE System
Step 2: Define how the system is built

Draw the system architecture in SCADE System
Step 3: Bring further details
Step 4: Verify design consistency

Result of check for ANSYS2013SystemDemo

18 error(s) detected - 0 warning(s) detected - 0 info(s) detected

<table>
<thead>
<tr>
<th>Category</th>
<th>Code</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>CHK_101</td>
<td>Model element is not displayed on any diagram at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_101</td>
<td>Model element is not displayed on any diagram at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_101</td>
<td>Model element is not displayed on any diagram at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_22</td>
<td>Flow port Energy for the part [ANSYS2013SystemDemo::FunctionalDecomposition::SystemVehicle::ProduceEnergy] is not connected to any other port at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_101</td>
<td>Model element is not displayed on any diagram at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_22</td>
<td>Flow port Control for the part [ANSYS2013SystemDemo::FunctionalDecomposition::SystemVehicle::CommandMovement] is not connected to any other port at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_22</td>
<td>Flow port Environment for the part [ANSYS2013SystemDemo::FunctionalDecomposition::SystemVehicle::Move] is not connected to any other port at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_101</td>
<td>Model element is not displayed on any diagram at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_22</td>
<td>Flow port Energy for the part [ANSYS2013SystemDemo::FunctionalDecomposition::SystemVehicle::ProduceEnergy] is not connected to any other port at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_22</td>
<td>Flow port Control for the part [ANSYS2013SystemDemo::FunctionalDecomposition::SystemVehicle::CommandMovement] is not connected to any other port at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_22</td>
<td>Flow port Environment for the part [ANSYS2013SystemDemo::FunctionalDecomposition::SystemVehicle::Move] is not connected to any other port at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_101</td>
<td>Model element is not displayed on any diagram at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_22</td>
<td>Flow port Energy for the part [ANSYS2013SystemDemo::FunctionalDecomposition::SystemVehicle::ProduceEnergy] is not connected to any other port at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_22</td>
<td>Flow port Control for the part [ANSYS2013SystemDemo::FunctionalDecomposition::SystemVehicle::CommandMovement] is not connected to any other port at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_22</td>
<td>Flow port Environment for the part [ANSYS2013SystemDemo::FunctionalDecomposition::SystemVehicle::Move] is not connected to any other port at [link]</td>
</tr>
<tr>
<td>Error</td>
<td>CHK_101</td>
<td>Model element is not displayed on any diagram at [link]</td>
</tr>
</tbody>
</table>
System – Software Synchronization

- Avoid duplication of efforts and inconsistencies between system structural models and software behavioral models
- System design and Software components evolve independently
- On-demand re-synchronization of interfaces

Interfaces described in SCADE System model
Safety Critical
Embedded Software Design
SCADE Suite-based Cruise Control
HIL Simulation Support

- Download & run SCADE generated code on to a real physical system and/or a HIL infrastructure

Ex: National Instruments HIL (PXI, Compact RIO) with real sensors & actuators
HMI Software Design

- Model Checking
- Simulation
- SCADE Display KCG

PROTOTYPE & DESIGN

VERIFY

GENERATE

Certification Kits
- DO-178B
- DO-178C
- IEC 61508
- EN 50128
- ISO 26262
- Certification Kits
SCADE Display-based Dashboard panels
Full Support of Mobile Platforms

One-click application generation

Desktop PC, Laptops

Rugged / Embedded Platforms

One-click code generation

Mobile Devices
Verify requirements traceability with SCADE LifeCycle
What is unique about SCADE?

• SCADE is developed specifically to be able to address critical system and software applications
• SCADE Suite and Display Code Generators are certified/qualified according to the following international safety standards:
  – ISO 26262 certification up to ASIL D – Automotive (TUV Sud)
  – IEC 61508 certification up to SIL 3 – Industrial & Energy
    • IEC 60880 full compliance – Nuclear Instrumentation & Control
    • IEC 62304 full compliance – Medical Systems
    • EN 13849 full compliance – Industrial Machines Safety
  – DO-178B / DO-178C qualification up to Level A – Aerospace & Defense
  – EN 50128 certification up to SIL 3/4 – Rail Transportation
• Same products qualified at the highest level of safety across 5 market segments by 10 safety authorities, worldwide
What costs reduction does this bring?

- Application software can be modelled, simulated and debugged on host using a notation that has been designed for safety critical systems.
- Generated code will behave like the Applications Models.
- All unit testing to verify the coding process are eliminated.
- Time spent on HIL, testing the correctness of application software decreases by more than 80% versus manual methods.
## Comparative Software Development Effort per Level including Testing

<table>
<thead>
<tr>
<th>ISO 26262 Level</th>
<th>No cert Effort</th>
<th>ASIL A Effort</th>
<th>ASIL B Effort</th>
<th>ASIL C Effort</th>
<th>ASIL D Effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comparative Effort</td>
<td>Baseline</td>
<td>No cert +10%</td>
<td>ASIL A +36%</td>
<td>ASIL B +80%</td>
<td>ASIL C +30%</td>
</tr>
<tr>
<td>Effort</td>
<td>100</td>
<td>110</td>
<td>150</td>
<td>270</td>
<td>350+</td>
</tr>
</tbody>
</table>
ISO 26262 Methodology Handbook

• Contents:
  - Development and verification steps
    - Model-based development with SCADE
    - Simulation and Model Test Coverage
    - Formal verification
    - Automatic code generation with KCG
    - C compiler verification activities
  - Set of guidelines for developing efficient models, generating efficient code, etc.
SCADE Suite at Subaru Electric Vehicles

- Subaru chose SCADE Suite for the design of its electric vehicle engine controls:
  - Vehicle dynamics
  - Engine functions
  - Vehicle energy consumption
    » heating & air conditioning
    » breaking
    » body controls
  - Battery load management
SCADE Suite at LIEBHERR Construction

• Liebherr chose SCADE Suite as its corporate standard embedded software development environment
• For all its design centers for earth moving machines, cranes and any heavy duty product
Full System Simulation and Virtual Prototyping
E/E System Physical Simulation with Simplorer

Co-Simulation

Matlab®

RBD

Maxwell

CFD

Simulation Data Bus/Simulator Coupling Technology

C/C++ User Defined Model

Matlab®

Circuits:

Blocks:

States:

Model Extraction: Equivalent Circuit, Impulse Response Extracted LTI, Stiffness Matrix

Electromagnetic (FEA)

Mechanical (FEA)

Thermal (FEA/CFD)

Fluidic (CFD)

VHDL-AMS

IF (domain = quiescent_domain)
V0 == init_v;
ELSE
Current == cap*voltage'dot;
END USE;
VHDL-AMS:

• Mixed signal modeling language standardized by the IEEE/IEC
• IEEE standard 1076.1, IEC Standard 61691-2
• Rich Electronics library development: Electrical, Power electronics, HEV, etc..
SCADE Suite & Display integrate with ANSYS Simplorer for accurate plant modeling and co-simulation.

Control Software Engineering

Requirements and Specifications

System Functional & Architectural Design

Sub-System Design

Component Integration & Verification

Detailed Design & Optimization

Sub-System Triang., & Verification

SCADE Suite

Simplorer

Electronic Control Unit

Mechanical

Electromechanical

Fluidic
Battery Physics – Thermal
Reduced Order Model for CFD
Sensor Physics and Behavior via Reduced Order Model (ROM)
Electric Machine Physics and Behavioral ROM

Electrical terminal

Rotating system terminal

\[ \psi(i, \theta) \]

\[ \tau(i, \theta) \]
The System Simulation Model
Build the Virtual Prototype

SCADE Rapid Prototyper Simulation Interface
A Complete Virtual Prototype!
Requirement

Req 23: On request, the valve should close in 500us
In Summary

### Systems Functional Engineering

- **Functional Allocations**
- **Architecture**
- **Detailed Architecture**

### Software Engineering & System Simulation

- **SCADE Suite**
- **Simplorer**
- **SCADE Display**

### Detailed Design & Optimization

- **Mechanical**
- **Electrical**
- **Software**

### System Validation

- **Requirements and Specifications**
- **Sub-System Integration & Verification**
- **Component Integration & Verification**

### Detailed Design 3D Multiphysics

- **Maxwell**
- **Fluent**

### Systems Functional Engineering

- **Functional**
- **Allocations**
- **Architecture**
- **Detailed Architecture**

---

**2013 Automotive Simulation World Congress**

October 29 - 30 • Frankfurt am Main, Germany