SCADE Safety and Audit Considerations for DO-178C

David Henderson
28th Sep 2017 – Safety Critical Club
General Agenda

• Model Based Development and Verification Concepts

• ANSYS and SCADE Products Overview
  o Software and SCADE V-Cycle

• Introduction to DO-178C, DO-331, DO-330

• Focus on SCADE Code Generator qualification

• ANSYS Esterel Support for Certification

• DO-178C compliant MBDV Workflow

• Conclusion
A Model is an acceptable means to completely express software requirements or architecture.

Req_001: The XX module shall Wait 10ms before entering in blabl state

Req_002: The XX module ....

Derived Req_003: ...
MBDV Concept #2

The MBDV supplement applies to any Model that is used to define software artefacts *whatever the process that produced it*

Interfaces between System and Software processes must be updated to address the case where a system team produces a software model.
MBDV Concept #3

Models should be developed from a complete set of requirements and constraints external to it
MBDV Concept #4

Simulation is an appropriate means to support Model verification

Model Parent Requirements
Model Verification Process

Model Parent Requirements

Development

Verification

Simulation Cases

Simulation Procedures

Simulation Results
SW Verification Process

During the SW verification process, it is required to show:

- Compliance & Robustness of EOC (Executable Object Code) with Model Parents Requirements
- Compliance & Robustness of EOC with Model
Model Coverage Analysis

Model Coverage Analysis provides a way to detect **unintended functions** in a Model.
Verification of Models and Target Testing

• **Verification** will be achieved by a **combination** of Model simulation and other traditional means.

• **HW/SW Integration** test objectives **cannot** be achieved by Model simulation.
ANSYS Simulation Platform Overview

*From Comprehensive Component-Level Design & Simulation ...*
ANSYS Simulation Platform Overview

... To Complete Systems Simulation

45,000 Customers
2,500 Employees
Embedded Software Challenges by Industry.....

- **Aerospace & Defense**: 500% increase in software lines of code (SLOC) in aerospace in 10 years.
- **Automotive**: 100Mi software lines of code (SLOC) in modern vehicles.
- **Railways**: Ever increasing certification costs and project delays/costs overrun.
- **Industrial Equipment**: More than 380K software and system engineers work in the oil and gas industry.
- **Energy & Nuclear**: Software-based Instrumentation and Controls have become State of the art.
- **Healthcare**: Software Failures are Responsible for 24% of all Medical Device recalls.
Managing Design Complexity

Assuring Functional Safety and Security

Reducing Embedded Software Costs

Reducing Physical Validation Costs

Optimizing Overall System Performance

Systems & Software Development Challenges
Complexity Increase – Not Unique to Aerospace

• ECUs: > 100
• Software Size: 100 Mi LOC
• Multiple integrated Networks
• Sensor Fusion & Surround Sensing
• Increasing # of Variants
• …

![Software Size (Mi Lines of code)](chart)

- MODERN HIGH-END CAR: 100 Mi LOC
- MAC OS X: 85
- LARGE HADRON COLLIDER: 50
- WINDOWS 7: 40
- F 35 FIGHTER: 24
- BOEING 787: 14
- CHEVY VOLT: 10
- MARS CURIOSITY ROVER: 5
- F22 RAPTOR: 2
For autonomous Driving: Validation and Testing Challenges

Billions of miles of testing needed for autonomous vehicle safety

**Driving to Safety**

*How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?*

- Autonomous vehicles would have to be driven hundreds of millions of miles and sometimes hundreds of billions of miles to demonstrate their reliability in terms of fatalities and injuries.

---

Akio Toyoda, President of Toyota @ Paris Auto Show

“It is estimated that some 8.8 billion miles of testing, including simulation, are required”

---

Image Source: Wikipedia Creative Commons
Provide systems and software engineers with model-based development and verification solutions that reduce costs, risks, and time-to-market
SCADE - Safety Critical Applications Development Environment

• SCADE products and solutions are developed specifically to address critical system and software applications

• SCADE Suite and Display code generators are certifiable according to the following international safety standards:
  o **DO-178B / DO-178C** qualification up to Level A – Aerospace & Defense
  o **EN 50128** certification up to SIL 3/4 – Rail Transportation
  o **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
  o **ISO 26262** certification up to ASIL D – Automotive

• Same products qualified at the highest level of safety across 6 market segments by 10 safety authorities, worldwide

FIRST DO-178C CODE GENERATION QUALIFICATION KITS AVAILABLE ON THE MARKET
What is ANSYS SCADE used for?

Embedded Software Application Development

Embedded Controls and Displays

High Quality, High Dependability Mission or Safety Critical Applications (with or without software certification requirements)
ANSYS Systems & Embedded Software Capabilities

Model-Based Systems Engineering

System Safety
- medini™ analyze

System Simulation & Digital Twins

Model-Based Software Engineering

3D Physics Simulation

System Architecture

System/Software Architecture

SW Components (FMI)

ROM
Integrated Workflow for SW-intensive Systems
ANSYS SCADE Products
Goals for MBSE SCADE to address in A&D

<table>
<thead>
<tr>
<th>STRATEGIC</th>
<th>TECHNICAL</th>
<th>ECONOMICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Compliance with Software Safety Certification and Quality requirements at lowest cost</td>
<td>• Automated Production of readable, portable, high performance and high quality Code</td>
<td>• 50% Development and V&amp;V Costs Reduction overall</td>
</tr>
<tr>
<td>• Improved Communication &amp; Collaboration among system and software teams, customers, suppliers and certification authorities</td>
<td>• Documentation Quality and Accuracy</td>
<td></td>
</tr>
<tr>
<td>• Product Line Development support</td>
<td>• Early Detection of Design Flaws</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Improved Long-term Maintainability of applications</td>
<td></td>
</tr>
</tbody>
</table>
ANSYS SCADE Architect

System/Software Architecture Design

Operational Requirements Analysis

Architecture Design & Data Propagation

Model Checks

Model Diff/Merge

System / Software Bi-directional Sync Up

ICD Generation

GENERATE

CONFIGURE

DESIGN

ANALYZE

ANSYS Confidential
SCADE Architect Diagrams

- Use Case
- Sequence
- State Machine
- Activity
- Block Definition
- Internal Block
- Parametric
- Tables
Model-Based System Engineering

**MBSE: Requirements Based Workflow**

- **Operational Analysis**
  - SCADE ARCHITECT
  - Traceability
  - Supports

- **System Design**
  - SCADE ARCHITECT
  - System Functions
  - System Architecture
  - Allocation
  - Traceability
  - Supports

- **Software Design**
  - SCADE SUITE
  - Synchronization (detailed interfaces & SW Architecture)
  - Traceability

- **User Requirements**
  - Traceability

- **System Requirements**
  - Traceability

- **Software Requirements**
  - Traceability
Modeling Capabilities

• **Graphical formalism**
  - Block diagrams, to specify the algorithmic part of applications, such as control laws and filters
  - Hierarchical state machines, to model the control part of applications
  - Decision diagrams
  - Packages, data types, constants
  - Arrays & iterators
  - Libraries

• The **unique integration of data flow and safe state machines** allows you to model the whole application with the **same formalism**
SCADE Suite IDE Overview
SCADE Architect - SCADE Suite Integration
An Integrated Workflow for SW-intensive Systems
ANSYS SCADE Display

SCADE Display

HMI Software Design

- Model Checks
- Simulation
- Plant Model Co-simulation (incl. FMI)

PROTOTYPE & DESIGN

VERIFY

GENERATE

SCADE Display KCG

DO-178B & C
- IEC 61508
- EN 50128
- ISO 26262
- Certification Kits

Simulation

Plant Model Co-simulation (incl. FMI)
ANSYS SCADE Test

**SCADE TEST**

**Prototyping & Test Creation**
- Rapid Prototyping
- Interactive Test Creation

**Testing Environment**
- Test Execution on Host
- Model Coverage

**Target Execution**
- Test Execution on Target (RTRT, LDRA, VectorCAST & Generic)

**Host Execution**
- Test Execution on Host
- Model Coverage

© 2015 ANSYS, Inc. September 27, 2017  ANSYS Confidential
ANSYS SCADE LifeCycle

System & Software Lifecycle Management

Requirements Traceability

Configuration & Change Control

Project Documentation Generation

TRACE

CONTROL

DOCUMENT
Typical Pains in a Traditional Software Development

- Low maturity or low accuracy of requirements
- No way to simulate and rapid proto in short loop iteration
- Non efficient design process (pseudo code)
- Manual coding error prone
- Risk of exceeding the budget
- High level number of test on target
- Late detection of functional bugs with time consuming verification (manual process)
- Time consuming activity with low added value
- Time consuming modification with bad impact for Product Manufacturer

Development → Modifications
SCADE based Solution to Solve Pains

- Accurate HLR thanks to rapid prototyping
- Better collaboration with Model Based
- Early detection thanks to model simulation
- Automatic code generation from model
- Reduced customers trial on plane
- Re-use of test scenario to run on target
- Fast Hw and Sw integration
- Removing of LLR-based Testing
- Removing of source code review

Development → Modifications

50%
Software V-cycle with ANSYS SCADE

System Development

Software Requirements

Overall Software Architecture

SCADE Allocated High-Level Requirements

SCADE Architecture Design

SCADE Detailed Design

SCADE Model Simulation

SCADE Test Cases

SCADE Target Testing

Overall Software Integration Testing

SCADE Auto-Coding & Integration

Software Life Cycle Management

Software Planning
Software V-Cycle with ANSYS SCADE
Software V-Cycle with ANSYS SCADE
Where Time Goes in Embedded Software Projects

<table>
<thead>
<tr>
<th>Phase</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept Definition</td>
<td>5%</td>
</tr>
<tr>
<td>System Design (Requirements, Functions and System Architecture)</td>
<td>12%</td>
</tr>
<tr>
<td>System Requirements allocated to Software (HLRs)</td>
<td>14%</td>
</tr>
<tr>
<td>Software Design (LLRs)</td>
<td>15%</td>
</tr>
<tr>
<td>Coding</td>
<td>10%</td>
</tr>
<tr>
<td>Software Unit Testing (Low Level testing)</td>
<td>10%</td>
</tr>
<tr>
<td>Software / Software Integration &amp; Testing</td>
<td>7%</td>
</tr>
<tr>
<td>Hardware/Software Integration &amp; Testing</td>
<td>10%</td>
</tr>
<tr>
<td>Documentation &amp; Reviews</td>
<td>7%</td>
</tr>
<tr>
<td>Project Management</td>
<td>10%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>100%</td>
</tr>
</tbody>
</table>

Source: AGARD – Advisory Group for Aerospace R&D (USA)
# Where Does SCADE Cut Costs?

<table>
<thead>
<tr>
<th>Phase</th>
<th>Comments</th>
<th>Reference Cost Breakdown (Manual process)</th>
<th>Cost Breakdown (SCADE-based process)</th>
<th>SCADE Gain</th>
<th>Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept Definition</td>
<td></td>
<td>5</td>
<td>5</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>System Design (Requirements, Functions and System Architecture)</td>
<td>Functional &amp; Architectural Definition, System Safety Analysis</td>
<td>12</td>
<td>8</td>
<td>35%</td>
<td></td>
</tr>
<tr>
<td>System Requirements allocated to Software (HLRs)</td>
<td>Control Laws, Logic definition, HLRs (text, equations…)</td>
<td>14</td>
<td>9</td>
<td>35%</td>
<td></td>
</tr>
<tr>
<td>Software Design (LLRs)</td>
<td>Detailed SW architecture, Functional design, Requirements-based tests creation</td>
<td>15</td>
<td>18</td>
<td>-20%</td>
<td></td>
</tr>
<tr>
<td>Coding</td>
<td>Detailed Coding</td>
<td>10</td>
<td>2</td>
<td>85%</td>
<td></td>
</tr>
<tr>
<td>Software Unit Testing (Low Level testing)</td>
<td>Functional Unit testing</td>
<td>10</td>
<td>2</td>
<td>85%</td>
<td></td>
</tr>
<tr>
<td>Software / Software Integration &amp; Testing</td>
<td>Testing of the above</td>
<td>7</td>
<td>1</td>
<td>85%</td>
<td></td>
</tr>
<tr>
<td>Hardware/Software Integration &amp; Testing</td>
<td>incl. On target debugging</td>
<td>10</td>
<td>5</td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td>Documentation &amp; Reviews</td>
<td>Design documentation and Quality reviews</td>
<td>7</td>
<td>1</td>
<td>85%</td>
<td></td>
</tr>
<tr>
<td>Project Management</td>
<td></td>
<td>10</td>
<td>5</td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL :</strong></td>
<td></td>
<td><strong>100</strong></td>
<td><strong>50</strong></td>
<td><strong>50%</strong></td>
<td></td>
</tr>
</tbody>
</table>
Aerospace Systems Applications

Cockpit & Avionics
- Cockpit Displays
- Head-up Displays
- Flight Management
- Flight Warning
- Navigation, Guidance & Inertial Unit
- On-Board Airport Navigation
- Data Concentrators

Flight Control Systems
- Autopilots
- Air Data and Inertial Reference
- Flight Control / High Lift / Slat&Flaps
- High Lift Hydraulic Control System
- Active Control Side Stick

Engine Control Systems
- Engine Control (FADEC)
- Nacelle Controls
- Thrust Reversers

Mechatronic Control Systems
- Anti-Icing
- Braking and Landing Gear
- Doors and Slides
- Hydraulic Controls

Air & Cabin Control Systems
- Cabin Pressure and Climate Control
- Oxygen Control
- Water & Waste Controls
- Environmental Control Systems
- Fire Protection & Control Systems

Power Control Systems
- Fuel Management
- Power Management, Electrical Load Management
- Auxiliary Power Units (APU)
- Power Conversion Systems
- Starter Generators

Maintenance Systems
- Health Monitoring & Utility
- On-Board Maintenance

Training & Simulators
- 2D simulators
- 3D Simulators
- Maintenance Training Devices
UAV, Defense and Space Systems Applications

**Military Mission Avionics**
- Mission Computers
- Helmet-Mounted Displays
- Navigation, Guidance and Inertial Units
- Military Flight Management
- Load Management Systems
- C4ISR and Radar Displays

**UAV Systems**
- UAV Flight Controls
- UAV Mission Systems
- UAV Ground Stations

**Weapons Systems**
- Gun Turret Controls
- Missile Flight Software
- Weapons Stores Management

**Misc. Military Systems**
- Ejection Seat Controls
- Refueling
- Tanker Boom Controls
- Submarine Controls

**Space Control Systems**
- Launchers
- Satellites
- Cargo Systems
- Planetary Landers
SCADE Certification Track Record
# MBSE SCADE CERTIFICATIONS – Date, Authority, Level, Application

More than **100 DO-178B/C Equipment Certifications** achieved to date

<table>
<thead>
<tr>
<th>Qualification date</th>
<th>Certification Authority</th>
<th>Subsystem</th>
<th>Level</th>
<th>Qualification date</th>
<th>Certification Authority</th>
<th>Subsystem</th>
<th>Level</th>
<th>Qualification date</th>
<th>Certification Authority</th>
<th>Subsystem</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>EASA</td>
<td>Fire Detection</td>
<td>B</td>
<td>2006</td>
<td>EASA</td>
<td>Thrust Reverser</td>
<td>A</td>
<td>2010</td>
<td>EASA</td>
<td>Cockpit Display</td>
<td>A</td>
</tr>
<tr>
<td>2002</td>
<td>JAA</td>
<td>Flight Controls</td>
<td>A</td>
<td>2006</td>
<td>EASA</td>
<td>Electrical Load Management</td>
<td>A</td>
<td>2016</td>
<td>ARMAK</td>
<td>CDS</td>
<td>A</td>
</tr>
<tr>
<td>2014</td>
<td>FAA</td>
<td>Fuel Management</td>
<td>A</td>
<td>May 2012</td>
<td>EASA</td>
<td>IMA - Fuel Command Function</td>
<td>A/B/C</td>
<td>2015</td>
<td>FAA/UK CAA</td>
<td>HUD by wire</td>
<td>A</td>
</tr>
<tr>
<td>2014</td>
<td>FAA</td>
<td>Flight Controls</td>
<td>A</td>
<td>May 2012</td>
<td>EASA</td>
<td>IMA - Electrical System Functions</td>
<td>C</td>
<td>2015</td>
<td>FAA</td>
<td>Smoke detection</td>
<td>B</td>
</tr>
<tr>
<td>2014</td>
<td>FAA</td>
<td>Fuel Management</td>
<td>A</td>
<td>May 2012</td>
<td>EASA</td>
<td>Oxygen System Control Unit</td>
<td>B</td>
<td>2015</td>
<td>TC</td>
<td>Air Management</td>
<td>A</td>
</tr>
<tr>
<td>2014</td>
<td>FAA</td>
<td>Flight Controls</td>
<td>A</td>
<td>May 2012</td>
<td>EASA</td>
<td>Flight Controls</td>
<td>A</td>
<td>2016</td>
<td>TC/FAA</td>
<td>Electrical Brake Controls</td>
<td>A</td>
</tr>
<tr>
<td>2014</td>
<td>FAA</td>
<td>Flight Controls</td>
<td>A</td>
<td>May 2012</td>
<td>EASA</td>
<td>Loadmaster Logic</td>
<td>B</td>
<td>2016</td>
<td>TC</td>
<td>Cabin Pressure</td>
<td>A</td>
</tr>
<tr>
<td>2014</td>
<td>FAA</td>
<td>Cockpit Display</td>
<td>A</td>
<td>May 2012</td>
<td>EASA</td>
<td>Loadmaster isplay</td>
<td>B</td>
<td>2016</td>
<td>CAAC</td>
<td>CDS</td>
<td>A</td>
</tr>
<tr>
<td>2014</td>
<td>FAA</td>
<td>Head-Up Displays</td>
<td>A</td>
<td>May 2012</td>
<td>EASA</td>
<td>Fuel Control</td>
<td>A</td>
<td>2010</td>
<td>TC</td>
<td>Ruddler Control</td>
<td>A</td>
</tr>
<tr>
<td>2014</td>
<td>FAA</td>
<td>Air Data &amp; Inertial Reference Unit</td>
<td>A</td>
<td>May 2012</td>
<td>EASA</td>
<td>Anti-Icing Control</td>
<td>A</td>
<td>tbd</td>
<td>DGA</td>
<td>HUD</td>
<td>A</td>
</tr>
<tr>
<td>2005</td>
<td>EASA</td>
<td>Integrated Modular Avionics</td>
<td>C</td>
<td>May 2012</td>
<td>EASA</td>
<td>Navigation Unit</td>
<td>A</td>
<td>1999</td>
<td>JAA</td>
<td>Automatic Pilot</td>
<td>A</td>
</tr>
<tr>
<td>2009</td>
<td>EASA</td>
<td>Head-up Display</td>
<td>A</td>
<td>May 2012</td>
<td>EASA</td>
<td>Cockpit Display</td>
<td>A</td>
<td>2000</td>
<td>JAA</td>
<td>Automatic Pilot</td>
<td>A</td>
</tr>
<tr>
<td>2009</td>
<td>EASA</td>
<td>Flight Controls</td>
<td>A</td>
<td>May 2012</td>
<td>EASA</td>
<td>Cockpit Display</td>
<td>A</td>
<td>2004</td>
<td>JAA</td>
<td>Cockpit Display</td>
<td>A</td>
</tr>
<tr>
<td>2006</td>
<td>EASA</td>
<td>Flight Warning</td>
<td>A</td>
<td>2008</td>
<td>EASA</td>
<td>In-flight Refueling Controls</td>
<td>B</td>
<td>2004</td>
<td>JAA</td>
<td>Cockpit Display</td>
<td>A</td>
</tr>
<tr>
<td>2006</td>
<td>EASA</td>
<td>Data Concentrator</td>
<td>A</td>
<td>2010</td>
<td>CAAC</td>
<td>Braking</td>
<td>A</td>
<td>2016</td>
<td>ANAC</td>
<td>Active Side Stick</td>
<td>A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Qualification date</th>
<th>Certification Authority</th>
<th>Subsystem</th>
<th>Level</th>
<th>Qualification date</th>
<th>Certification Authority</th>
<th>Subsystem</th>
<th>Level</th>
<th>Qualification date</th>
<th>Certification Authority</th>
<th>Subsystem</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>ANAC</td>
<td>Braking</td>
<td>A</td>
<td>2016</td>
<td>ANAC</td>
<td>Cockpit Display</td>
<td>A</td>
<td>2008</td>
<td>Russia</td>
<td>Flight Controls</td>
<td>A</td>
</tr>
<tr>
<td>2016</td>
<td>ANAC</td>
<td>Slats Flaps</td>
<td>A</td>
<td>2012</td>
<td>EASA</td>
<td>Fuel Management</td>
<td>B</td>
<td>2016</td>
<td>FAA</td>
<td>Flight Controls</td>
<td>A</td>
</tr>
<tr>
<td>2016</td>
<td>ANAC</td>
<td>Cabin Pressure</td>
<td>A</td>
<td>2016</td>
<td>EASA</td>
<td>Fuel Management</td>
<td>B</td>
<td>2016</td>
<td>FAA</td>
<td>Environmental control</td>
<td>B</td>
</tr>
<tr>
<td>2014</td>
<td>ANAC</td>
<td>Cargo management GUI</td>
<td>C</td>
<td>May 2012</td>
<td>EASA</td>
<td>Navigation Unit</td>
<td>A</td>
<td>2012</td>
<td>FAA</td>
<td>Cockpit Display</td>
<td>A</td>
</tr>
<tr>
<td>2014</td>
<td>ANAC</td>
<td>HUD</td>
<td>A</td>
<td>2008</td>
<td>ANAC</td>
<td>Braking System</td>
<td>B</td>
<td>2010</td>
<td>FAA/UK CAA</td>
<td>HUD by wire</td>
<td>A</td>
</tr>
<tr>
<td>2006</td>
<td>EASA</td>
<td>Flight Controls</td>
<td>A</td>
<td>2007</td>
<td>TC</td>
<td>FADEC</td>
<td>A</td>
<td>2016</td>
<td>UK MoD</td>
<td>Flight Controls</td>
<td>A</td>
</tr>
<tr>
<td>2006</td>
<td>EASA</td>
<td>Braking</td>
<td>B</td>
<td>2007</td>
<td>TC</td>
<td>FADEC</td>
<td>A</td>
<td>2013</td>
<td>ARMAK</td>
<td>FADEC</td>
<td>A</td>
</tr>
<tr>
<td>2006</td>
<td>EASA</td>
<td>Flight Control</td>
<td>A</td>
<td>Dec 2011</td>
<td>TC</td>
<td>FADEC</td>
<td>A</td>
<td>2016</td>
<td>EASA</td>
<td>FADEC</td>
<td>A</td>
</tr>
<tr>
<td>2006</td>
<td>FAA</td>
<td>Fuel Management</td>
<td>B</td>
<td>plan 2014</td>
<td>TC</td>
<td>FADEC</td>
<td>A</td>
<td>2015</td>
<td>EASA</td>
<td>FADEC</td>
<td>A</td>
</tr>
<tr>
<td>2009</td>
<td>TC</td>
<td>Braking</td>
<td>A</td>
<td>2016</td>
<td>FAA</td>
<td>Cockpit Display</td>
<td>B</td>
<td>2015</td>
<td>EASA</td>
<td>FADEC</td>
<td>A</td>
</tr>
<tr>
<td>2009</td>
<td>FAA</td>
<td>Braking</td>
<td>A</td>
<td>2016</td>
<td>FAA</td>
<td>Cockpit Display</td>
<td>A</td>
<td>2015</td>
<td>EASA</td>
<td>FADEC</td>
<td>A</td>
</tr>
<tr>
<td>2017</td>
<td>FAA</td>
<td>Braking</td>
<td>A</td>
<td>2016</td>
<td>FAA</td>
<td>Cockpit Display</td>
<td>A</td>
<td>2015</td>
<td>EASA</td>
<td>FADEC</td>
<td>A</td>
</tr>
<tr>
<td>2015</td>
<td>FAA</td>
<td>Fuel Quantity Signal Conditioner</td>
<td>B</td>
<td>2008</td>
<td>TC</td>
<td>FADEC</td>
<td>A</td>
<td>2015</td>
<td>EASA</td>
<td>FADEC</td>
<td>A</td>
</tr>
<tr>
<td>2015</td>
<td>FAA</td>
<td>FADEC</td>
<td>A</td>
<td>2016</td>
<td>FAA</td>
<td>Fuel Management</td>
<td>B</td>
<td>2015</td>
<td>EASA</td>
<td>FADEC</td>
<td>A</td>
</tr>
</tbody>
</table>

© 2015 ANSYS, Inc.  September 27, 2017  ANSYS Confidential
SCADE Customers in A&D
SCADE @ Airbus

• Program/Application
  o Airbus A380, A400M, A350
  o Most embedded control and display systems

• Key Results
  o SCADE Suite and Display selected by Airbus and suppliers for all current commercial and military programs
  o **Compliance with ARINC 661** = standardization all Airbus cockpits Look and Feel across programs
  o ...enabling **maximum reuse** from one program to another
  o ... while meeting **stringent DO-178B safety certification requirements**

“Airbus never experienced any bug in flight in our Flight Control System software produced automatically.”

Jean-Charles DALBIN, Automatic Code Generation Tool Qualification Expert Avionics Software Airbus Operations SAS

⇒ Read “Dimensions” magazine
SCADE in the Airbus A380

8 Million Lines of Code Generated!

- Engine Interface
- Fuel Control
- Thrust Reverser
- Cooling System
- ATSU (Board / Ground communications)
- Cockpit Display System
- Flight Warning System
- Electrical Load Management System
- Flight Control System
- Braking and Steering System
- Anti-Icing System
SCADE in the Airbus A380 Cockpit
SCADE in the Airbus A400M

- Engine Interface Function (EIF)
- Fuel Control
- Air Data Reference, GPS, Hybrid Navigation
- Cockpit Display System
- Flight Warning System
- Electrical Load Management System
- Anti Icing System
- Flight Control System
- Loadmaster
- Fire Protection
- Braking and Steering System
SCADE in the Airbus A400M Cockpit
SCADE @ Northrop Grumman

• Program/Application
  o Black Hawk UH-60V
  o Cockpit Display System Digitalization

• Key Results
  o $1 Billion program win by Northrop Grummann on the BlackHawk Avionics Upgrade (800 helicopters)
  o FACE and DO-178C compliance, as mandated by US DoD
  o Automated translation of legacy IData and Simulink models into SCADE Display and SCADE Suite integrated environment

“SCADE allows us to take full advantage of model-based engineering, resulting in improved development and testing efficiencies and delivering an affordable software sustainment approach across the program life cycle.”

Simona Kelley
Director of US Army Avionics Programs, Northrop Grumman
Northrop Grumman is supplying a mission equipment package for a digital cockpit upgrade of the U.S. Army's UH-60L BLACK HAWK helicopters...which is designated UH-60V.

Key elements of the system that were assessed include the open, scalable design using model-based engineering and a fully partitioned software architecture; the technical data package with government purpose rights; navigation system performance; and portability of software applications.

The UH-60V digital cockpit solution is aligned with the Future Airborne Capability Environment (FACE™) standard and supports integration of off-the-shelf hardware and software, enabling rapid insertion of capabilities while reducing cost and risk for system integration and upgrades.

Additionally, the UH-60V's advanced cockpit solution meets the standards for safety-critical software development and is designed to comply with the Federal Aviation Administration and European Aviation Safety Agency's Global Air Traffic Management requirements, enabling the system to traverse military and civilian airspace worldwide.
DO-178C Overview
What is DO-178C?

• DO-178C defines the guidelines for the development of airborne software

• The objective of the guidelines is to ensure that software performs its intended function with a level of confidence in safety that complies with airworthiness requirements

• DO-178C guidelines specify:
  – Objectives for software life-cycle processes
  – Activities for achieving those objectives, according to the software level (A through D)
  – Description of the evidence indicating that the objectives have been satisfied
What is DO-178C?

Hence, it is key to be able to plan a safe, predictable and repeatable lifecycle of the software project that shall meet DO-178C objectives up to level A:

- Based on experience
- Taking into account the human factor
- Adaptable to the complexity of the application to be developed
- Well placed within the organization of the company

Why DO-178C?

- DO-178B was issued in 1992 (i.e. a loooong time ago for software)
- New technologies: Model-Based, Object Oriented, Formal Methods
- Skyrocketing software complexity
DO-178C Documentation Structure

- **Core (DO-178C)**
- **OOT/RT (DO-332)**
- **FM (DO-333)**
- **MBDV (DO-331)**
- **TOOLS (DO-330)**
- **FAQ, DP (DO-248C)**
DO-178C Core Document
DO-178C Core Document

• The **Structure** of the Core document did not change according to DO-178B
  o Same processes are considered (see next slides)

• **Only clarifications have been implemented**
  o Reminder: DO-178C complies with DO-178B
  o See details in next slides
Consistent Terminology

• **DO-178C avoids the use of “guidelines”**
  - Unclear use of “guidance” and “guidelines” in DO-178B
  - No glossary definition
  - Their meanings are just the opposite in US English and UK English
  - “guidance” is material that could be recognized by the authorities
  - “guidelines” are more supporting information

• **§1.4 clarifies the terms “Objectives” & “Activities”**
  - DO-178C is objective-oriented (as for DO-178B)
  - DO-178C describes activities for achieving those objectives
  - The applicant may plan and, subject to the approval of the certification authority, adopt alternative activities to those described in this document.
Traceability and Derived Requirements

• Traceability (§6.5, new)
  o Shall be bi-directional
  o May also be based on naming conventions
  o Also required now between test cases and test procedures

• Derived Requirements
  o Glossary: Requirements produced by the software development processes which
    • (a) are not directly traceable to higher level requirements, and/or
    • (b) specify behavior beyond that specified by the system requirements or
      the higher level software requirements.
  o Table A-2.2 objective: “Derived high-level requirements are defined and provided to the
    system processes, including the system safety assessment process”
Testing

• Robustness test cases should be requirements-based
  o A specific note has been added to §6.4.2
  o It is considered as a key point for an efficient robustness testing strategy

• Some clarifications related to Structural coverage
  o §6.4.4.1.d An analysis is now required to confirm that all test cases used to achieve structural coverage are traceable to requirements
  o 6.4.4.2.c Structural coverage analysis of data and control coupling should be achieved by assessing the results of the requirements-based tests
  o 6.4.4.2.d all tests added to achieve structural coverage are based on requirements

• Masking MC/DC is now officially allowed
  o DO-178B only defined “unique cause” MC/DC
  o CAST paper allowed Masking MC/DC
Dead Code & Deactivated Code

• 6.4.4.3.c Dead Code
  o “dead code” becomes “extraneous code including dead code”
  o Definition of “extraneous code” is given in DO-178C glossary
    • Code (or data) that is not traceable to any system or software requirement.
    • An example of extraneous code is legacy code that was incorrectly retained although its requirements and test cases were removed.
    • Another example of extraneous code is dead code.

• 6.4.4.3.d Deactivated Code
  o Some clarifications have been added in the glossary definition
  o 2 categories of “deactivated code” are considered and corresponding activities are given (depending on the category)
Data and Control Coupling

• §6.4.4: data/control coupling is explicitly identified as a software structure coverage analysis activity
DO-331 Model-Based Development and Verification
DO-331: Model-Based Development and Verification Supplement (MBDV)

• The MBDV Supplement is applicable for SCADE Projects

• It identifies additions, modifications and substitutions to DO-178C when SW models are used.

• It supplements the guidance given in DO-178C as follows:
  o DO-178C is still used for all aspects of the SW life cycle where model-based approach is not relevant.
  o Annex MB.A describes how the DO-178C objectives are revised/modified wrt a model-based approach.
DO-331 Key Concepts

• **Requirements from which the model was developed**
  - It is a relative concept.
  - They can be at software or system level.
  - They should be external to the model and should be a complete set of requirements and set of constraints.

• **Specification Model**
  - Is an abstract representation.
  - It supports an understanding of SW functionality and does not prescribe a specific SW implementation or architecture.

• **Design Model**
  - Should describe the internal details of software components: (LLR, architecture, data structures, data flow, control flow,…).
Specification Model vs Design Model

• A model can not be classified as both a specification model and a design model

• Both can be executable models but only design model is used to generate the Software

• From a practical point of view, the frontier between both is sometimes very difficult to identify
  o MB examples 2 and 3 (see Table MB.1-1) use Specification Models in their workflow
  o These 2 approaches are not recommended by Esterel because they may raise several sensible questions from Certification Authorities
SW Model Standard

• It defines **modeling techniques** for each type of Model (Specification Model, Design Model)

• It ensures that these techniques are **suitable** to the type of information expressed by the Model

• It provides **means to identify** the **requirements & derived requirements** contained in the model and to manage traceability

• It provides means to identify each **model element** that does **not** contribute to the representation of requirement or architecture
Role of Model Simulation in the Verification Process

- For low-level requirements verification (DO-331 MB 6.8)
  - Verify compliance of LLR to HLR A-4.1
  - Verify algorithms accuracy HLR A-4.7 (precision, convergence/stability)

- Simulation detects design errors in a much more effective way than design review and target testing
  - Every engineer has a PC
  - Model-level debugging
  - Real life experience on traditional processes shows that most errors have been introduced by design or hand-coding process
Simulator, Simulation Cases and Procedures

- **Simulator**
  - Is a tool
  - May need to be qualified
    (see DO-178C and DO-330 document, FAQ #5)

- **Simulation cases and procedures**
  - Are requirement-based
  - Shall be verified like test cases
    (see additional objectives of Table A-4: MB14, MB15, MB16)
Testing vs. Model Simulation

- **Testing (in a strict sense)**
  - Means exercising the real thing, i.e. the EOC (Executable Object Code) on the target
  - Allows emulation of the EOC on special hardware for some tests
  - Allows simulation of the EOC on host with a SW-based hardware simulator.

- **Model Simulation**
  - Is a way to demonstrate **compliance** of the model to its **higher level requirements**, in addition to Reviews and Analyses
  - Is **not** considered as **testing**
  - Usually **not accepted** for objectives of Table MB.A-6.
DO-178C Testing Process
Testing: Target Run Is Required

• M.B.6.8.2: several SW testing Objectives cannot be satisfied by means of simulation
  o In particular for the demonstration of compatibility to the target computer

• ANSYS recommendation is to run 100% of Test Procedures in the target environment (or with target emulator).
Model Coverage is required in DO-331

- Model Coverage analysis is explicitly specified in MB.6.7
  - as a way of **detection of unintended functions** in the Design Model

- Model coverage by HLR tests is required

- Coverage of derived LLR shall be achieved by Test Cases on their corresponding derived HLR
DO-330 Software Tool Qualification Considerations
DO-330: Tool Categorization

• There are 3 criteria:

  - **Criteria 1 tool**
    • A tool whose output is part of the airborne software and thus could insert an error (e.g. a code generator)

  - **Criteria 2 tool**
    • A tool that automates verification process(es) and thus could fail to detect an error, and whose output is used to justify the elimination or reduction of verification process(es) other than that automated by the tool, or development process(es) that could have an impact on the airborne software (e.g. a tool that checks for stack overflow)

  - **Criteria 3 tool**
    • A tool that, within the scope of its intended use, could fail to detect an error (e.g. a design reporter)
Why DO-330?

• Develop a qualification approach that addresses tool qualification issues without raising the bar

• Account for the proliferation of tools and emerging tool capabilities in development efforts that simply did not exist when DO-178B was published (1992)

• Better reflect how tools are actually used in airborne software development efforts

• Better define the responsibilities of the tool developer and the tool user to ease reuse and facilitate COTS tools development and usage
DO-330 – Similarities and Differences from Supplements

• **Similarities**
  
  o Objective-Activity/process structure

• **Differences**
  
  o Tool Qualification is a *stand-alone* document
  
  o Tools occupy their own domain
  
  o Guidance in the DO-330 document may be applicable to other domains, not just airborne software:
    
    • non-airborne (i.e. ground) software (DO-278A)
    
    • airborne electronic hardware (DO-254)
    
    • highly integrated or complex aircraft systems (ARP 4754A)
    
    • tools (recursive application of the STQC...)
    
    • etc.
Tool Qualification Needs

- Qualification of a tool is needed when processes are eliminated, reduced or automated by the use of a Software tool without its output being verified.

- **Objective** of the tool qualification process is to ensure that the tool provides confidence at least equivalent to that of processes that are eliminated, reduced or automated.

- Only deterministic tools may be qualified (same output for the same input data when operating in the same environment).
The tool may introduce errors into the embedded objects

- DO-178B development tool /DO-178C criteria 1 tool

- *Examples: code generator, IMA configuration data generator*
A tool may fail to detect an error (although it does not itself introduce an error into the embedded objects) [and another overlapping verification process exist]

- DO-178B verification tool / DO-178C criteria 3 tool
- Examples: code analyzer, test tool
If a tool performs verification and its output is used to justify the elimination or reduction of:

- Verification process(es) other than that automated by the tool,
- or Development process(es) that could have an impact on the airborne software.

⇒ DO-178C criteria 2 tool

⇒ *Example:* proof tool on source code + reduction in testing
Assigning the Tool Qualification Level

<table>
<thead>
<tr>
<th>(DO-178C) Software Level</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>TQL-1</td>
</tr>
<tr>
<td>B</td>
<td>TQL-2</td>
</tr>
<tr>
<td>C</td>
<td>TQL-3</td>
</tr>
<tr>
<td>D</td>
<td>TQL-4</td>
</tr>
</tbody>
</table>
DO-178C Qualification of SCADE Tools

<table>
<thead>
<tr>
<th>Software Level</th>
<th>Criteria 1</th>
<th>Criteria 2</th>
<th>Criteria 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>TQL-1</td>
<td>TQL-4</td>
<td>TQL-5</td>
</tr>
<tr>
<td>B</td>
<td>TQL-2</td>
<td>TQL-4</td>
<td>TQL-5</td>
</tr>
<tr>
<td>C</td>
<td>TQL-3</td>
<td>TQL-5</td>
<td>TQL-5</td>
</tr>
<tr>
<td>D</td>
<td>TQL-4</td>
<td>TQL-5</td>
<td>TQL-5</td>
</tr>
</tbody>
</table>

SCADE Suite KCG
SCADE Display KCG
SCADE Test Model Coverage
SCADE Test Execution
SCADE LifeCycle Reporter
DO-178C Qualification of SCADE Tools

SCADE Suite KCG Code Generator – C and Ada (P/N: SCS-MD-L-10)
SCADE Suite KCG is a C and Ada code generator from Scade models that has been qualified for DO-178C/DO-330 at TQL-1, certified for IEC 61508 at SIL 3, and for EN 50128 at SIL 3/4, and qualified for ISO 26262 software up to ASIL D. This code generator saves verification effort in the coding phase, such as code reviews and low-level testing on the SCADE Suite KCG generated code. This productivity improvement shortens certification and/or modification time and effort. SCADE Suite KCG has successfully passed the qualification procedure on several large programs and is currently used in production for many programs in Europe, Asia, and the Americas.

SCADE Display KCG (P/N: SCY-MD-L-20) SCADE Display KCG is a C code generator for SCADE Display that has been qualified for DO-178C/DO-330 at TQL-1, certified for IEC 61508 at SIL 3, and for EN 50128 at SIL 3/4, and qualified for ISO 26262 software up to ASIL D. It features compact and efficient code generation of readable, traceable and retargetable ANSI C code for embedded HMIs. It natively supports the OpenGL, OpenGL SC 1.0 and 2.0 (Safety Critical), OpenGL ES 1.1 and 2.0 (Embedded Systems) standards, through the SCADE Display OGLX (OpenGL eXtension to KCG) portable library of C code, delivered along with SCADE Display KCG. Generated code integrates out-of-the-box with COTS or proprietary, certified or not, OpenGL graphics libraries. SCADE Display KCG also enables targeting all proprietary embedded target platforms with minimal effort.

<table>
<thead>
<tr>
<th>(DO-178C) Software Level</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>TQL-1</td>
</tr>
<tr>
<td>B</td>
<td>TQL-2</td>
</tr>
<tr>
<td>C</td>
<td>TQL-3</td>
</tr>
<tr>
<td>D</td>
<td>TQL-4</td>
</tr>
</tbody>
</table>

SCADE Suite KCG
SCADE Display KCG
DO-178C Qualification of SCADE Tools

SCADE Test Model Coverage (P/N: SCS-MD-L-15)

is a coverage analysis tool that executes and reports coverage on requirements-based tests coverage for SCADE Suite both at the model level and at the generated code level (for both C and Ada). It tracks successful execution paths and percentages of each SCADE Suite function and operator that have been tested, and enables DC and MC/DC coverage criteria at the SCADE Suite model level and at the generated code level. SCADE Test Model Coverage has been qualified for DO-178C/DO-330 at TQL-5. SCADE Test Model Coverage certification data includes Tool Qualification Plan (TQP), Tool Operational Requirements (TOR), Tool Configuration Index (TCI), and Release Note (RN).

SCADE Test Target Execution (P/N: SLC-BD-L-02)

allows automatic generation of test harnesses from the same set of model-based test cases for COTS on-Target Test execution tools like IBM RTRT, LDRA TestBed and Vector Software VectorCast. It enables a complete verification workflow from high-level requirements-based testing on model down to integration testing on target, thus allowing significant time and cost savings over manual testing.

Model-based applications developed with SCADE Suite can be automatically tested with RTRT, TestBed or VectorCAST, which ensures that the embedded application is running as expected on the target. The same tests can automatically be reused on both host and target, significantly reducing the effort typically used to generate and prove tests during both phases of development and final verification on target.

SCADE Test Target Execution has been qualified for DO-178C/DO-330 at TQL-5.
DO-178C Qualification of SCADE Tools

**SCADE LifeCycle Reporter (P/N: SCS-MD-L-20)**

SCADE LifeCycle Reporter automates the time consuming job of creating detailed and complete reports from SCADE Architect, SCADE Suite, SCADE Display, and SCADE UA Page Creator designs. It includes generic templates that can be easily modified by the customer. The underlying scripting language for the Reporter is Tcl, a simple, non-proprietary open source scripting language (see [http://www.tcl.tk/scripting/](http://www.tcl.tk/scripting/)) that enables customers to produce any kind of custom documents that they require. SCADE LifeCycle Reporter eliminates the usual overhead of creating documentation on the design and the related code that is 100% accurate and always up-to-date.

The SCADE LifeCycle Reporter is qualified off-the-shelf for DO-178C/DO-330 at TQL-5 (for SCADE Suite, SCADE Display and SCADE UA Page Creator for ARINC 661). SCADE LifeCycle Reporter certification data includes Tool Operational Requirements (TOR), Tool Configuration Index (TCI), and Release Note (RN).

<table>
<thead>
<tr>
<th>(DO-178C) Software Level</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>TQL-1</td>
</tr>
<tr>
<td>B</td>
<td>TQL-2</td>
</tr>
<tr>
<td>C</td>
<td>TQL-3</td>
</tr>
<tr>
<td>D</td>
<td>TQL-4</td>
</tr>
</tbody>
</table>
Tool Stakeholders

• Tool Developer
  o Responsible for developing, verifying, documenting, and producing the tool
  o Satisfies development objectives for tool

• Tool User
  o Responsible for selecting, using, and qualifying the tool
  o Satisfies installation and use objectives for tool

• These roles were not identified as such in DO-178B
SCADE Code Generator  Qualification
Tool Qualification Needs

- Qualification of a tool is needed when processes are **eliminated**, **reduced** or **automated** by the use of a Software tool without its output being verified.

- **Objective** of the tool qualification process is to ensure that the tool provides **confidence** at least equivalent to that of processes that are eliminated, reduced or automated.

- Only **deterministic** tools may be qualified (same output for the same input data when operating in the same environment).
General considerations

• KCG qualification primarily impacts verification of outputs from the design and coding processes of the software developed with SCADE

• It only concerns part of the software developed with SCADE
  • For the rest of the software, the user shall perform the activities required by DO-178C

• Qualification of KCG does not eliminate any DO-178C objective but impacts the activities remaining to be done by the user
Impact of KCG qualification on the user MBDV process

- Static verification of the model (DO-331 Tables MB.A-4)
- Static verification of generated source code (DO-331 Table MB.A-5)
- Dynamic verification (Testing, DO-331 Tables MB.A-6 and A-7)
Impact of KCG qualification on the user MBDV process

• **Static verification of the model (DO-331 Tables MB.A-4)**

• **Static verification of generated source code (DO-331 Table MB.A-5)**

• **Dynamic verification (Testing, DO-331 Tables MB.A-6 and A-7)**
## KCG Impact on Design Output Verification Table (MB.A-4)

<table>
<thead>
<tr>
<th>A-4</th>
<th>Objective</th>
<th>Verification Method</th>
</tr>
</thead>
</table>
| 1   | Low level requirements comply with high level requirements. | **Review** SCADE LLRs  
- Simulate SCADE Model with **SCADE Test**  
- Analyze SCADE Model Coverage with **SCADE TMC** |
| 2   | Low level requirements are accurate and consistent. | **Scade language** formal definition and **consistency rules** guarantee accuracy and consistency  
- **Check** syntax/ semantic of SCADE Model with KCG |
| 3   | Low level requirements are compatible with target computer. | **Analyze** SCADE Model complexity with SCADE Lifecycle **Dashboard**  
- **Analyze** execution time and memory size with TSO/TSV  
- Run **CVK** and analyze results |

*Partial support* 
*Full support*
<table>
<thead>
<tr>
<th>A-4</th>
<th>Objective</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Low level requirements are verifiable.</td>
<td>- Scade language <strong>formal definition</strong> guarantees verifiability</td>
</tr>
</tbody>
</table>
| 5   | Low level requirements conform to standards.               | - **Check** compliance to predefined syntax/semantic rules on SCADE Model with KCG  
- [Verify](#) conformance to user defined rules (manual/scripted with SCADE Suite **API**)]                                                                 |
| 6   | Low level requirements are traceable to high level requirements. | - **Review trace** data (**RM Gateway** report) between Scade LLRs and HLRs                                                                                                                                       |
## KCG Impact on Design Output Verification Table (MB.A-4)

<table>
<thead>
<tr>
<th>A-4</th>
<th>Objective</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Algorithms are accurate.</td>
<td>- Review SCADE LLRs and/or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Simulate SCADE Model with SCADE Test-TEE</td>
</tr>
<tr>
<td>8</td>
<td>Software architecture is compatible with high level requirements.</td>
<td>- Review SCADE Architecture (incl. HLRs-SCADE Architecture Allocation Matrix)</td>
</tr>
<tr>
<td>9</td>
<td>Software architecture is consistent.</td>
<td>- Scade language <strong>formal</strong> definition and consistency rules guarantee <strong>accuracy</strong> and <strong>consistency</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Check</strong> syntax/ semantic of SCADE Model with KCG</td>
</tr>
</tbody>
</table>

*Partial support*  
*Full support*
<table>
<thead>
<tr>
<th>A-4</th>
<th>Objective</th>
<th>Verification Method</th>
</tr>
</thead>
</table>
| 10  | Software architecture is compatible with target computer. | - Review SCADE Architecture  
- Analyze SCADE Models **complexity** with SCADE Lifecycle **Dashboard**  
- Analyze execution time and memory size  
- Run **CVK** and analyze results |
| 11  | Software architecture is verifiable. | - Scade language **formal definition** guarantees verifiability  
- **Check** syntax/ semantic of SCADE Model with KCG |
| 12  | Software architecture conforms to standards. | - **Check** compliance to predefined syntax/ semantic rules on SCADE Model with KCG  
- [Verify conformance of SCADE Models to user design rules with SCADE **API**] |
# KCG Impact on Coding Output Verification Table (MB.A-5)

<table>
<thead>
<tr>
<th>Objective</th>
<th>Verification method</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Source Code complies with low-level requirements</td>
<td>SCADE KCG qualification</td>
</tr>
<tr>
<td>2  Source Code complies with software architecture</td>
<td>SCADE KCG qualification</td>
</tr>
<tr>
<td>3  Source Code is verifiable</td>
<td>SCADE KCG qualification</td>
</tr>
<tr>
<td>4  Source Code conforms to standards</td>
<td>SCADE KCG qualification</td>
</tr>
<tr>
<td>5  Source Code is traceable to low-level requirements</td>
<td>SCADE KCG qualification</td>
</tr>
<tr>
<td>6  Source Code is accurate and consistent</td>
<td>SCADE KCG qualification</td>
</tr>
<tr>
<td>7  Output of software integration process is complete and correct</td>
<td>Analysis of the build and loading data</td>
</tr>
</tbody>
</table>
Qualification of KCG on customer’s project

• Tools that should be qualified for DO-178B/C are audited by the certification authority in the context of a given aircraft project.
  o The tools part of the certification process is running in parallel with the certification of the application. It follows a very standard flow with typical SOI#1 to 4 audit meetings (as in the FAA classification)

  o Certification Authorities (EASA, FAA,...) run the audit of the tools. The applicant is also present and ANSYS Esterel (the Safety team together with the R&D team) presents its own tool certification flow, answers questions and takes action items as the results of the audits

  o ANSYS Esterel has successfully supported clients many times with various Certification Authorities over 18 years.
KCG Certification Kit (1/2)

• SCADE KCG Certification Kits contain material demonstrating to certification authorities that the SCADE Suite KCG C code generator was developed in compliance with the highest levels of Safety Standards

• These certification kits provide access to the documents that you need as part of your certification tasks

  • Compliance Analysis of SCADE Suite KCG with DO-178C/DO-330
  • Tool Qualification Plan (TQP)
  • Tool Operational Requirements (TOR)
  • Tool Accomplishment Summary (TAS)
  • Tool Installation Procedure (TIP)
  • Tool Configuration Index (TCI)
  • Tool Environment Configuration Index (TECI)
KCG Certification Kit (2/2)

• Other documents are available on premises at Esterel Technologies:
  • Tool Verification Records (for example test cases, procedures and results)
  • Tool Qualification Development Data (for example, requirements, design and code)

• Acquisition of the Certification Kit includes Esterel Technologies’ support for audits that may be requested by the certification authorities.
KCG Tool Accomplishment Summary

• **TAS**: the documented demonstration that the product complies with the specified safety requirements

• It shall contain:
  o Evidence of Quality Management
  o Evidence of Safety Management
  o Evidence of functional and technical safety
  o *Conditions of use*

• **SCADE Suite KCG Certification Kit** provides a large portion of evidence of Safety Management (software part of the system)
ANSYS Esterel Certification Support

• ANSYS Esterel helps customers in a number of ways in setting up the certification process of their application. This is the role of the **Safety team**, composed of experts that have followed all the certification activities of SCADE customers (more than 100) and that have largely participated to the creation of DO-178C guidelines.
  
  o In the first place, for the planning activities, customers can use the **Certification Plans templates**. They are generic plans for SCADE applications that can be tailored to the specific needs of the customer’s project. They are based on Esterel own experience with numerous customers and can save a lot of time in the planning phase.
  
  o Moreover, while developing the project, the Safety team will always be there to **answer the certification-related questions** that may arise. A point of contact will be assigned to the customer at the project start and interaction with him can be as deep as needed.
Qualification of the SCADE tools on customer’s project

• Tools that should be qualified for DO-178B/C are audited by the certification authority in the context of a given aircraft project.
  o The tools part of the certification process is running in parallel with the certification of the application. It follows a very standard flow with typical SOI#1 to 4 audit meetings (as in the FAA classification).
  o For the user qualification activities, customers can use the User TQP (Tool Qualification Plan) and User-TOR (Tool Operational Reqs) templates
  o EASA runs the audit of the tools (SCADE Suite and Display KCG, plus the SCADE verification tools). The applicant is also present and ANSYS Esterel (the Safety team together with the R&D team) presents its own tool certification flow, answers questions and takes action items as the results of the audits.
Planning
DO-178C Certification Plans

• Set of plans required for the certification of SCADE Suite software applications (DO-178C Level A & B):
  o **Generic plans developed from ANSYS experience** in supporting DO-178C certification process for applications developed with SCADE Suite
  o Help SCADE users to successfully achieve their DO-178C SOI#1 Milestone in a record time

- SOI#1 (a.k.a. « Planning Review ») is the milestone where the certification authority agrees on compliance of the user plans and standards with DO-178

<table>
<thead>
<tr>
<th>Project Plans &amp; Standard</th>
<th>SCS-SDP-DO178C-A-B</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCADE Suite® Application - Software Development Plan</td>
<td>SCS-SVP-DO178C-A-B</td>
</tr>
<tr>
<td>SCADE Suite® Application - Software Verification Plan</td>
<td></td>
</tr>
<tr>
<td>SCADE Suite® Application - Software Configuration Management Plan</td>
<td>SCS-SCMP-DO178C-A-B</td>
</tr>
<tr>
<td>SCADE Suite® Application - Software Quality Assurance Plan</td>
<td>SCS-SQAP-DO178C-A-B</td>
</tr>
<tr>
<td>SCADE Suite® Application - Software Development Standard</td>
<td>SCS-SDST-DO178C-A-B</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compliance Matrices</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SCADE Suite® Application – Compliance Matrix for DO-178C level A and B</td>
<td>SCS-CMTX-DO178C-A-B</td>
</tr>
</tbody>
</table>
DO-178B/C Methodology Handbooks

Efficient Development of Safe Avionics Software with DO-178B/C Objectives

• Contents:
  o Development and verification steps of DO-178B/C compliant software
    • Model-based development with SCADE Suite and SCADE Display
    • Simulation and Model Test Coverage
    • Formal verification
    • Automatic code generation with KCG
    • C compiler verification activities
  o Set of guidelines for developing efficient models, generating efficient code, etc.
  o Two versions available
    • Display centric applications
    • Control centric applications

Download the handbook from www.esterel-technologies.com
Software Plans (DO-178C, §4.3 and §11)

- The **Plan for Software Aspects of Certification** is the top-level plan and provides references to the other plans.

- The **Software Development Plan** defines the software life cycle(s), development strategy and the methods and tools used to support this development strategy.

- The **Software Verification Plan** defines the verification strategy and describes the methods and tools used to support this verification strategy.

- The **Software Configuration Management Plan** defines the list of configuration items, the configuration control and change control processes.

- The **Software Quality Assurance Plan** defines the SQA activities for each life cycle process including SQA methods (inspections, audits,...) and conformity review activity.
Software Standards (DO-178C, §4.5 and §11)

- **Software development standards** define the rules and constraints for the software development processes.
- **Software Requirements Standards** define the methods, rules, and tools to be used to develop the high-level requirements.
- **Software Design Standards** define the methods, rules, and tools to be used to develop the software architecture and low-level requirements.
- **Software Code Standards** define the programming languages, methods, rules, and tools to be used to code the software.
Goal of the ANSYS SBU Certification Plans

- Provide a methodological framework for the development of SCADE Model-Based software through detailed templates of plans and development standard that comply with DO-178C
- Support our customers in the transition from DO-178B to DO-178C
- Little effort for customization by the SCADE customer to adapt the plans and development standard to his project
- Help our SCADE customers to successfully achieve their DO-178C SOI#1 Milestone in a record time
  - SOI#1 Milestone (a.k.a. « Planning Review ») is the milestone where the certification authority agrees on compliance of the user plans and standards with DO-178
Content of the ANSYS SBU Package

- This package is dedicated to **SCADE Suite Applications for DO-178C Levels A and B software**

- This package includes detailed templates of:
  - Software Development Plan
  - Software Verification Plan
  - Software Configuration Management Plan
  - Software Quality Assurance Plan
  - Software Development Standard
  - Compliance Matrix with DO-331

- Based **on more than 10 years of experience**
  - from *customer* projects
  - From our *own products* qualification/certification
Software Development Plan
Software Development Plan (SDP)

• Main topics
  – Project organization
  – Software life cycle and specific activities for each phase
  – Software life cycle environment
  – Software life cycle data
  – Compliance analysis with respect to DO-331 MB.11.1 and MB.11.2

• The Software Life Cycle is adapted to the SCADE Development and is compliant with DO-178C/DO-331
Relation with Other Plans

- Application Software – Plan for Software Aspects of Certification [PSAC]
  - Application Software Development Plan [SDP]
    - SCADE Software Development Plan [SC_SDAP]
    - Supporting Tools’ Qualification Data
      - Supporting Tools’ Pre-Qualification Data
  - Application Software Verification Plan [SVP]
    - SCADE Software Verification Plan [SC_SVP]
  - Application Software Configuration Management Plan [SCMP]
    - SCADE Software Configuration Management Plan [SC_SCMP]
  - Application Software Quality Assurance Plan [SQAP]
    - SCADE Software Quality Assurance Plan [SC_SQAP]
MBD-Software LifeCycle

Legend
- Life Cycle
- Phase of a Life Cycle: Phases' details are informative, not exhaustive.
- Phases' sequence
- (H) Host – (T) Target
- Software Management Review
- Project Management Meeting

Application Software Life Cycle
- SCADE Libraries Life Cycle
- SCADE Import Life Cycle
- Build and Load Procedure

SCADE Architecture Design Phase
- SCADE Architecture Design Model
- SCADE Architectural Design Document
- SCADE-Allocated-HLRs to SCADE Architecture Allocation Matrix
- SCADE KCG Semantic Checker Results (H)
- SCADE OW Test Results (T)
- SCADE KCG Metrics (H)

SCADE Detailed Design Phase
- SCADE Detailed Design Models
- SCADE Detailed Design Document
- SCADE-Allocated-HLRs - SCADE LLRs Matrix
- SCADE KCG Semantic Checker Results (H)
- SCADE OW Test Results (T)
- SCADE KCG Metrics (H)
- SCADE QTE Simulation Results (H)
- SCADE MTC Model Coverage Analysis Results (H)
- SCADE TSO/TSV Results (H)

SCADE Verification Cases and Procedures Preparation Phase
- SCADE Verification Cases and Procedures
- SCADE-Allocated-HLRs - SCADE Verification Cases and Procedures Traceability Matrix

SCADE Coding and Integration Phase
- SCADE Generated Code
- SCADE Component EOC

SCADE Import Life Cycle
- SCADE Component and associated software data

SCADE Integration Testing Phase
- Target Test Harnesses
- SCADE Integration Test Results (T)
- SCADE MTC Code Coverage Analysis Results (H)
- SCADE Verification Procedures – SCADE Integration Test Results Traceability Matrix
- SCADE Integration Test Report
Software LifeCycle Terminology

• **Processes and Phases**
  – **Processes**: planning, development, verification,…
  – **Phases**: local organization over time of activities involving one or several processes

• **Phase Transition Criteria**
  – Phase Transition Criteria are split into entry criteria and exit criteria

• **Software Management Reviews**
  – It is associated to the release of software data and assessment of phases’ exit and entry criteria.
  – Assess that the development, verification, SQA and SCM activities have been performed according to the plans
Software Verification Plan
Independence Requirements

• The Verification Team is independent from the Development Team

• The verification of verification cases, procedures and results is not performed by the author of the verification cases, procedures and results (this information is tracked into the review report).

• The Software Quality Engineer is from another department than the Development and Verification Teams, and the Project Management

• Evidence of independence is managed with the software data.
## Compliance with DO-331 Verification Objectives

### Table 1: DO-178C Table MB.A-4

<table>
<thead>
<tr>
<th>Objective Description</th>
<th>Activity Ref</th>
<th>Verification Method</th>
<th>Verification Results</th>
</tr>
</thead>
</table>
| Low level requirements comply with high level requirements. | MB.6.3.2.a | Pre-requisite: Qualify SCADE Reporter, SCADE QTE, SCADE MTC  
- Review SCADE LLRs from SCADE Detailed Design Report  
- Simulate SCADE Detailed Design Models with SCADE QTE  
- Analyze Model Coverage with SCADE MTC | SCADE Detailed Design Verification Report incl.:  
- SCADE LLRs Review Results  
- SCADE QTE Simulation Results  
- SCADE MTC Model Coverage Results |
| Low level requirements are accurate and consistent. | MB.6.3.2.b | Pre-requisite: Qualify SCADE KCG  
- Verify syntax and semantic of SCADE Models with SCADE KCG | SCADE Detailed Design Verification Report incl.:  
- SCADE KCG Semantic Checker Results |
| Low level requirements are compatible with target computer. | MB.6.3.2.c | Pre-requisite: Qualify SCADE Reporter, SCADE KCG, Design Rule Checker Tool  
- Verify that SCADE CVK tests pass on target and that SCADE KCG Metrics are compatible with SCADE CVK Metrics  
- Analyze SCADE Detailed Design Models complexity, with respect to complexity management Design Rules  
- Analyze execution time and memory size with SCADE TSO/TSV | SCADE Detailed Design Verification Report incl.:  
- SCADE CVK Test Results  
- SCADE KCG Metrics  
- Design Rule Checker Results  
- Review results for non-automated User Design Rules  
- SCADE TSO/TSV Results |
Overall System/Software Architecture Design
System – Software Collaboration

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

Interfaces described in SCADE System model
Detailed Design
Traceability from Requirements to SCADE models with SCADE LifeCycle ALM Gateway (1/2)

- The SCADE Lifecycle ALM Gateway provides an **access to requirements and enables traceability** for the software development process
  - Enables traceability of all artifacts:
    - Requirements (from DOORS (OSLC), From Reqtify)
    - SCADE System, SCADE Suite & SCADE Display designs
    - SCADE Test procedures, etc.

- The SCADE Lifecycle ALM Gateway is integration to the SCADE System, SCADE Suite, SCADE Display and SCADE Test development environments
Traceability from Requirements to SCADE models with SCADE LifeCycle ALM Gateway (2/2)

- Requirements are **visible while designing** in a new Panel
- **Traceability** can be done during design with Drag & Drop
- Traceability Status (covered or not) is displayed
# KCG Impact on Coding Output Verification Table (MB.A-5)

<table>
<thead>
<tr>
<th>Objective</th>
<th>Verification method</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Source Code complies with low-level requirements</td>
<td>SCADE KCG qualification</td>
</tr>
<tr>
<td>2  Source Code complies with software architecture</td>
<td>SCADE KCG qualification</td>
</tr>
<tr>
<td>3  Source Code is verifiable</td>
<td>SCADE KCG qualification</td>
</tr>
<tr>
<td>4  Source Code conforms to standards</td>
<td>SCADE KCG qualification</td>
</tr>
<tr>
<td>5  Source Code is traceable to low-level requirements</td>
<td>SCADE KCG qualification</td>
</tr>
<tr>
<td>6  Source Code is accurate and consistent</td>
<td>SCADE KCG qualification</td>
</tr>
<tr>
<td>7  Output of software integration process is complete and correct</td>
<td>Analysis of the build and loading data</td>
</tr>
</tbody>
</table>
OGLX Library

• High-level graphics software library developed in C language by ANSYS
• Delivered in its source code format with SCADE Display KCG
• Documents required for the certification of this library are provided in the OGLX Certification Kit
Communication between Logic and Graphics (1/2)

- Data-Processing oriented application

![Diagram: Architecture for data processing-oriented applications](image-url)
Communication between Logic and Graphics (2/2)

• Display applications with Interactivity

Figure 4.28: Architecture for Display applications with interactivity
Benefits Summary

- SCADE System/Suite combined solutions efficiently support the design of DO-178C software
- The **best tool** for each activity
  - For overall system/software architecture
    - SCADE System with data management & ICDs, and automated synchronization of SW interfaces with SCADE Suite
  - For software design
    - SCADE Suite and SCADE Display rigorous (formal) notation
    - Intuitive, structured modeling technique, fit for complex software
  - Support efficiently iterative System/Software design processes as described in ARP 4754
## Benefits

<table>
<thead>
<tr>
<th>Standards</th>
<th>SCADE provides a common representation between systems and software teams sharing models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portability</td>
<td>SCADE generates portable C or Ada code which is RTOS, hardware &amp; bus platform independent</td>
</tr>
<tr>
<td>Support</td>
<td>ANSYS has worldwide training and support capabilities</td>
</tr>
<tr>
<td>Lifecycle</td>
<td>SCADE has been integrated to leading Requirements Management, Traceability, RTOSes, IDEs, Compilers, Testing and Code analysis tools</td>
</tr>
<tr>
<td>Results</td>
<td>SCADE users have experienced a 2X speed-up improvement in time-to-certification and a 40% reduction in project development costs!</td>
</tr>
</tbody>
</table>