SCADE User Group Conference, 15.10.2015

Developing Software for the A350 XWB Slat Flap Control Computer with SCADE

Paul Linder, Diehl Aerospace
1 Company Presentation
2 Introduction to the A350 XWB SFCC
3 Development Procedure
4 Modeling Guidelines and Verification Methods
5 Experiences
Diehl Aerospace (DAs)

Corporate Division

DIEHL Aerospace Systems

Sales: over € 1,010 m  |  Employees: ≈ 4,700  |  Headquarters: Laupheim, Germany

Operational Units

DIEHL Aerospace

Sales: ≈ € 300 m
Employees: ≈ 1,200
Headquarters: Überlingen, Germany
Shareholders: 51% Diehl, 49% Thales

joint venture with THALES

DIEHL Comfort Modules
AOA
DIEHL Aircabin
DIEHL Service Modules

Numbers are based on forecast 2015
System Expertise

Flight Control
- Slat Flap Control Computer
- Flaps Lever
- Position Pick-Off Unit

Doors & Slides Management System
- Doors & Slides Management Control Unit
- Local Door Controller
- Autonomous Standby Power Supply Unit
- Control Panels & Indicators
- Sensing
- Swivel Actuator

Integrated Modular Avionics
- Core Processing Input/Output Module (CPIOM)
- Standardized hardware module, I/O capabilities & mechanical packaging
- IMA Tool Suite

Lighting & Interior Functions
- Cabin Lighting Systems
- Cabin Mood Lighting Systems
- Emergency Lighting Systems
- Starlight Systems
- Noise Masking Systems
- Full Automatic Hat Rack Systems
### Major Customers and Platforms

#### Civil

- **AIRBUS**
  - A300/310 Family
  - A320 Family
  - A330/340 Family
  - A380 Family
  - A350 XWB Family

- **BOEING**
  - 737 Family
  - 747 Family
  - 767 Family
  - 777 Family
  - 787 Family

- **BOMBARDIER**
  - Bombardier Q400
  - Global 7000/8000

- **EMBRAER**
  - E170/190
  - E135/140
  - Legacy 600

#### Military

- **A400M**
- **Eurofighter**
- **KC-46A Tanker**
- **NH90**
- **Tiger**
- **Tornado**
1 Company Presentation
2 **Introduction to the A350 XWB SFCC**
3 Development Procedure
4 Modeling Guidelines and Verification Methods
5 Experiences
What is a Slat Flap Control Computer?

- Slat Flap Control Computer (SFCC)
  - Safety-related fly-by-wire system (secondary flight control)
  - Controls and monitors high lift system

- High lift system
  - Increases lift for take-off and landing

A320 High Lift Actuation System

A350 XWB High Lift System

- Technologies
  - Droop-nose device on inboard wing
  - Multifunctional trailing edge flap system: Adaptive Dropped Hinge Flap
  - Integrated use as high-lift device and for inflight adaptation of cruise wing shape

- Benefits
  - Fuel burn reduction through drag saving
  - Load alleviation functions and cruise efficiency enhancement

• **Functionality**
  - Determination and control of surface position including load alleviation functions
  - Monitoring of high lift system and components (e.g. power control unit)
  - Test functions and maintenance services (BITE)
  - AFDX data loading for SW update

• **Design**
  - 2 exchangeable SFCCs with 2 independent channels (slat/flap) per SFCC
  - Redundant and dissimilar design
  - Overall 16 micro controllers and several DSPs
  - Level A design assurance

*Note:* A350 XWB SFCC similar to depicted A380 SFCC.
Overview

1 Company Presentation
2 Introduction to the A350 XWB SFCC
3 Development Procedure
4 Modeling Guidelines and Verification Methods
5 Experiences
Project Context

- **Project context**
  - Equipment development project according to ARP-4754 / DO-254 / DO-178B level A
  - Schedule DAs: 07/2008 – ongoing (type certification on 30.09.2014)

- **SCADE involvement**
  - SCADE applied for level A development of SFCC application SW
    » Parallel to development of manually coded basic software (e.g. scheduling, driver, data loading)
    » ~150 application SW modules (e.g. high-lift system monitors, component monitors)
  - SCADE version 5.1 applied
    » Only data flow diagrams
    » No state-charts (due to tool qualification constraints), no higher-order functions
DAs SCADE Development Procedure

SW Design

- SW Architectural Description
- Low-level REQ (manual coding)
  - SCADE models (= low-level REQ)

SCADE models

- Specification of individual SW modules (cf. DO-178C/DO-331 “Design Model” level)
- Qualified code generation (joint generation)
- Manual source code

High-level REQ (HLR)

- HLR allocated to standard dev.
- HLR allocated to model-based dev.

Tool-aided SCADE model review

SCADE model tests

DAs SCADE standard

HW/SW integration tests

Manual object code
**High-level REQ**

SRD_OPS-REQ-2298

A Slat Cross Lane Output Monitor failure condition shall be detected if the signals indicated in the table below do not match within the associated **Threshold**:

<table>
<thead>
<tr>
<th>Signal</th>
<th>Description</th>
</tr>
</thead>
</table>

**Low-level REQ / SCADE model**

SDD_OPS-REQ The behaviour of the module is specified by the related SCADE model documented by W-CT-2912 in the SCADE project report SXLO_SlatXLaneOutputMon.rtf, ClearCase version 22.

SRD_OPS-REQ-2298 SRD_OPS-REQ-2300 SRD_OPS-REQ-2291 SRD_OPS-REQ-2292

Diagram:

```
<table>
<thead>
<tr>
<th>bool</th>
</tr>
</thead>
<tbody>
<tr>
<td>bbool</td>
</tr>
<tr>
<td>bbool</td>
</tr>
<tr>
<td>bbool</td>
</tr>
<tr>
<td>bbool</td>
</tr>
<tr>
<td>bbool</td>
</tr>
<tr>
<td>bbool</td>
</tr>
<tr>
<td>bbool</td>
</tr>
<tr>
<td>bbool</td>
</tr>
<tr>
<td>bbool</td>
</tr>
<tr>
<td>bbool</td>
</tr>
<tr>
<td>bbool</td>
</tr>
</tbody>
</table>
```

CrossFailureBool
• High-level REQ

SRD_OPS-REQ-2300

A Cross Lane Output Monitoring failure condition shall be validated if a cross lane failure condition is validated for five (5) validation cycles.

• Low-level REQ / SCADE model

The behaviour of the module is specified by the related SCADE model documented by the SCADE project report SXLO_SlatXLaneOutputMon.rtf, ClearCase version 22.

Call of library operator (non-expansion)
Overview

1. Company Presentation
2. Introduction to the A350 XWB SFCC
3. Development Procedure
4. Modeling Guidelines and Verification Methods
5. Experiences
• Guidance on following issues:
  – Tool settings and options to ensure conditions imposed by SCADE tool qualification
    » E.g. interdiction of unary minus operator to avoid SCADE 5.1 maintenance issue CR ID 5137
  – Modeling conventions to support DAs model verification procedures
    » E.g. naming and traceability conventions, complexity restrictions, algorithmic constraints

• Overview of rules
  – **16 mandatory rules** to avoid undefined and failure-prone features (cf. tool qualification)
  – **23 required rules** related to modeling conventions (cf. verification procedures) ➔ Justifications allowed
  – No optional or recommended rules applied
Model Review: DAs SCADE StyleChecker

- Automatic check of 26 rules of the DAs SCADE Development Standard
  - Checks generation options, modeling elements, complexity restrictions, naming conventions, model/report/autocode consistency
  - Remaining 13 rules subject to manual review (based on SCADE report)

- Developed with TCL and Python
  - TCL scripts using SCADE API
    - E.g. `MapRole $model node` 
    - `CountForbiddenModelOperators`
  - Python checking source/report generation and producing HTML report

- Qualified as verification tool
  - Qualified “batch mode”
  - Engineering “GUI mode” (see figure)
Model Review: DAs SCADE StyleChecker (cont’d)

• HTML report

Checking Run Overview
Checking Run: 01 Jun 2015 16:38:21

Summary
Total number of SCADE projects checked: 151
SCADE projects PASSED: 151
SCADE projects FAILED: 0
SCADE projects ERROR: 0

Total number of findings: 38
Number of mandatory rule findings: 0
Number of required rule findings: 38
Number of justifications for required rules: 0

Verdict: PASSED

Configuration
Reference: SCADE Development Standard (SCDSTD) for A350 XWB Slat Flap Control Computer and Sensors (A350 XWB SFCC), issue 000_07

Checking Objects:
"A350_SFCC_SW\model\scade_gen\scade_gen.bat"

Checking Protocol
Check Item 01-01: 0 violation(s)
Check Item 02-01: not checked (manual review required)
Check Item 02-02: 0 violation(s)
Check Item 03-01: 0 violation(s)
Check Item 03-02: 0 violation(s)
Check Item 04-01: 0 violation(s)
Check Item 07-01: 0 violation(s)
A Cross Lane Output Monitoring failure condition shall be validated if a cross lane failure condition is validated for five (5) validation cycles.

**Simulation with SCADE QMTC**

**SCADE model**

**Simulation cases**

**DAs Test Script Formatter**

**DAs Test Result Comparator**

**Coverage**

**PASS/FAIL**

**Qualified toolchain**

**High-level requirement**

*SRD_OPS-REQ-2300*
Overview

1 Company Presentation
2 Introduction to the A350 XWB SFCC
3 Development Procedure
4 Modeling Guidelines and Verification Methods
5 Experiences
Experiences

• Successful certification of level A software!
  – EASA type certification Airbus A350 XWB on 30.09.2014

• Estimated >2x higher efficiency for SW module development
  – Omission of source code verification due to qualified source code generation
  – Bypass of effort-consuming conventional LLR specification and module testing

• Automatic consistency checks proved very valuable
• Set model expansion options in conformance to testing approach
  – 100% structural coverage may not be achieved with full expansion of libraries
  – Advice: Non-trivial library operators should not be expanded

• Mind the configuration management
  – Not only SCADE model and higher level requirements but also traceability data and review results (findings) have to be subject to version control

• Be aware of your modeling semantics
  – Identical syntax may have different meaning on different specification levels (cf. DO-178C/DO-331 “Design Model” vs. “Specification Model”)
  – Do not disregard quality conditions and design constraints requirements
Contact

Diehl Aerospace GmbH
Alte Nussdorfer Str. 23
88662 Ueberlingen

Phone +49 7551 891 0
Fax +49 7551 891 4001

www.diehl.com/aerosystems

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.