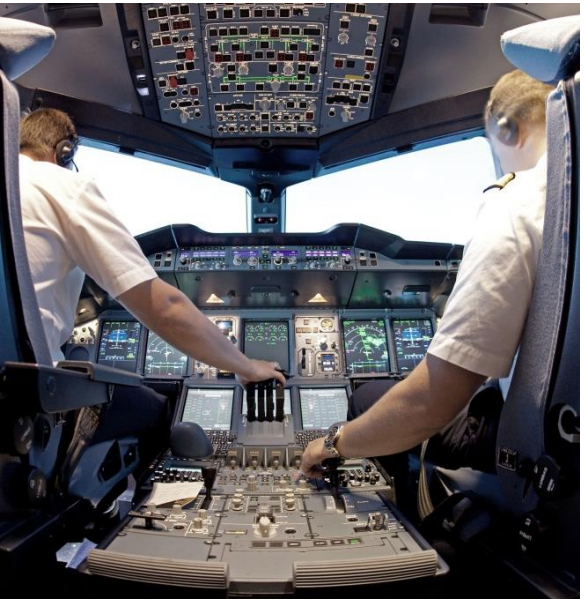
DIEHL
Aerospace

SCADE User Group Conference, 15.10.2015

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




Paul Linder, Diehl Aerospace

Overview

DIEHL
Aerospace

Diehl Aerospace (DAs)

Corporate Division

DIEHL Aerosystems

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

DIEHL Aerospace

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

DIEHL Aerospace

Civil

AIRBUS	BOEING	BOMBARDIER	EMBRAER
• A300/310 Family	• 737 Family	• Bombardier Q400	• E170/190
• A320 Family	• 747 Family	• Global 7000/8000	• E135/140
• A330/340 Family	• 767 Family		• Legacy 600
• A380 Family	• 777 Family		
• A350 XWB Family	• 787 Family		

Military

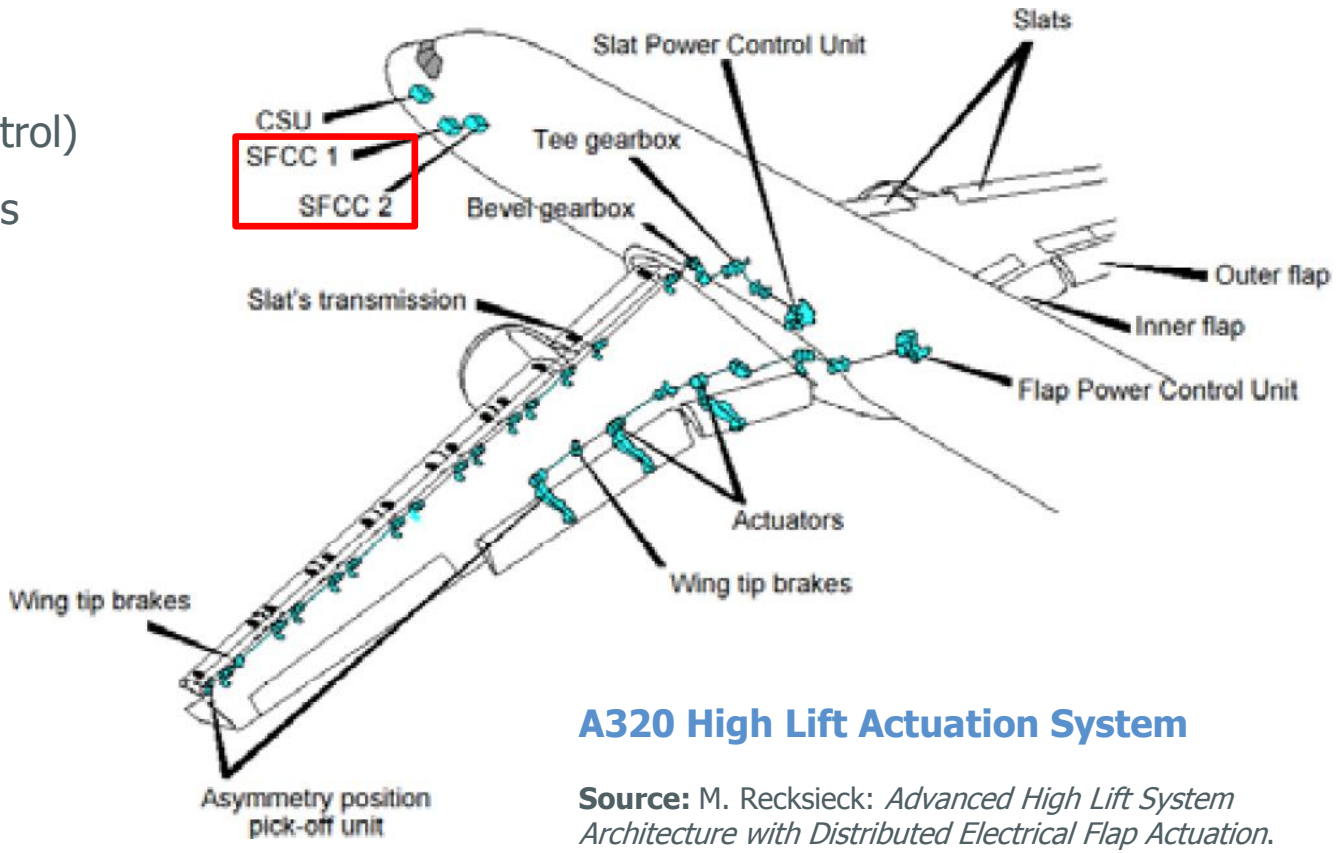
- A400M
- Eurofighter
- KC-46A Tanker
- NH90
- Tiger
- Tornado

Company Trailer

Overview

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

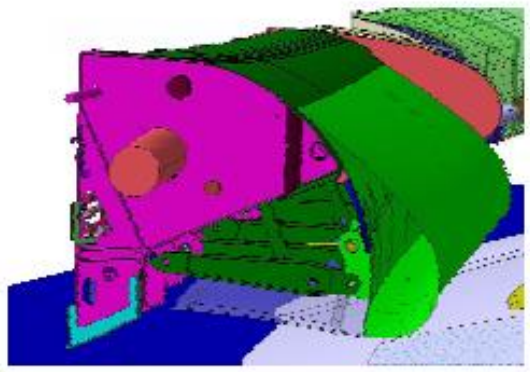


A320 High Lift Actuation System

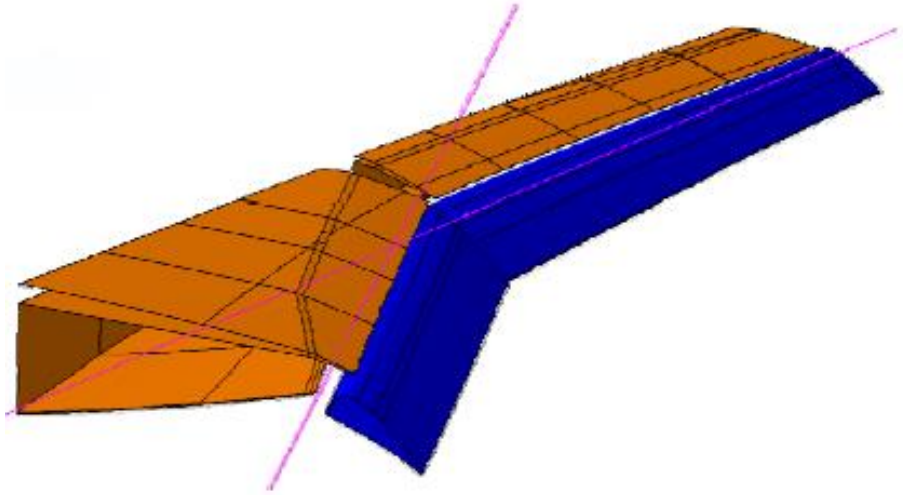
Source: M. Recksieck: *Advanced High Lift System Architecture with Distributed Electrical Flap Actuation*. Workshop on Aviation System Technology (AST) 2009.

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 in-flight adaptation of cruise wing shape



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



Source: D. Hills: *The Airbus Challenge* : EADS Engineering Europe, Budapest 9-10th May 08.

A350 XWB Slat Flap Control Computer

- 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.

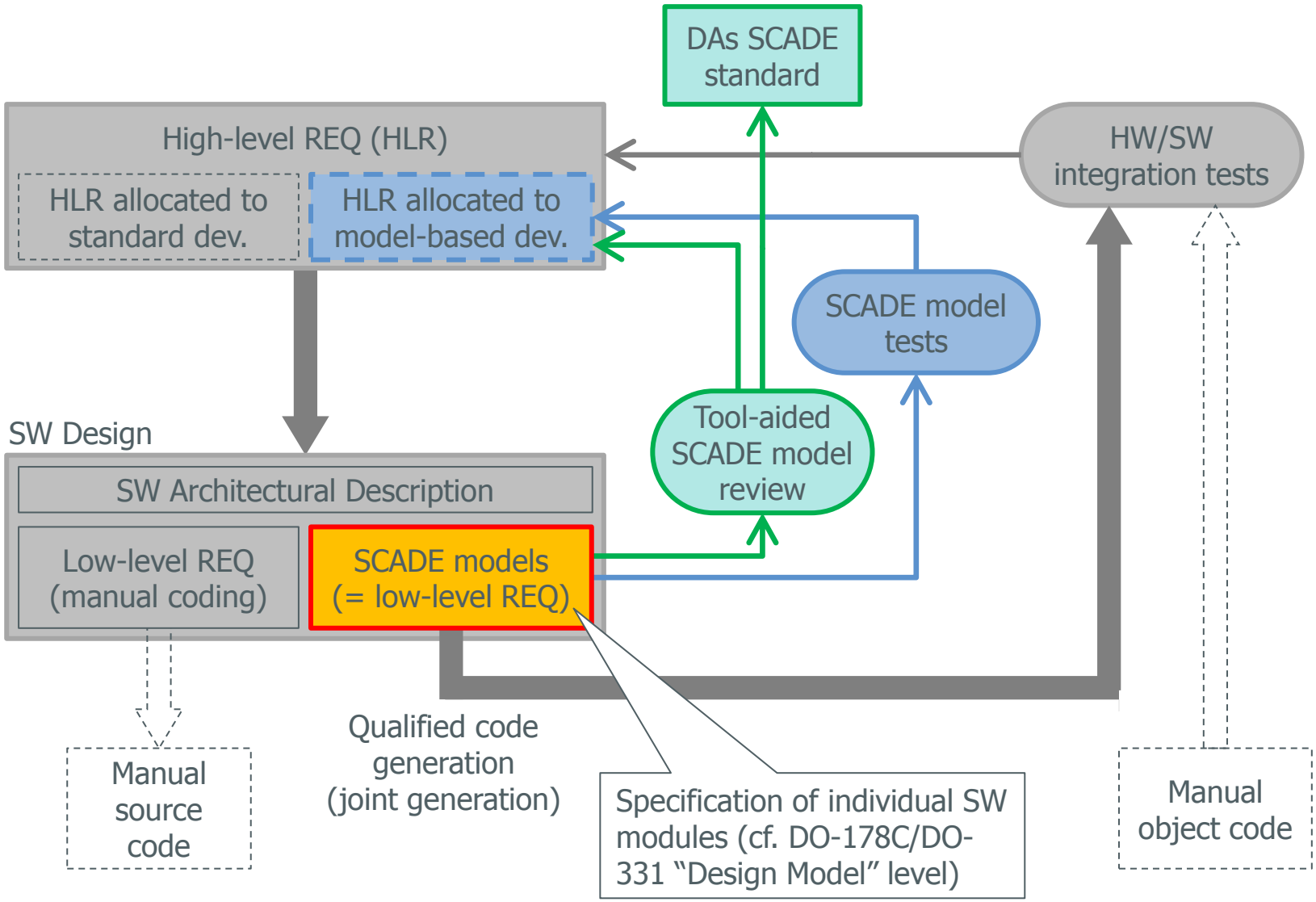
Overview

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



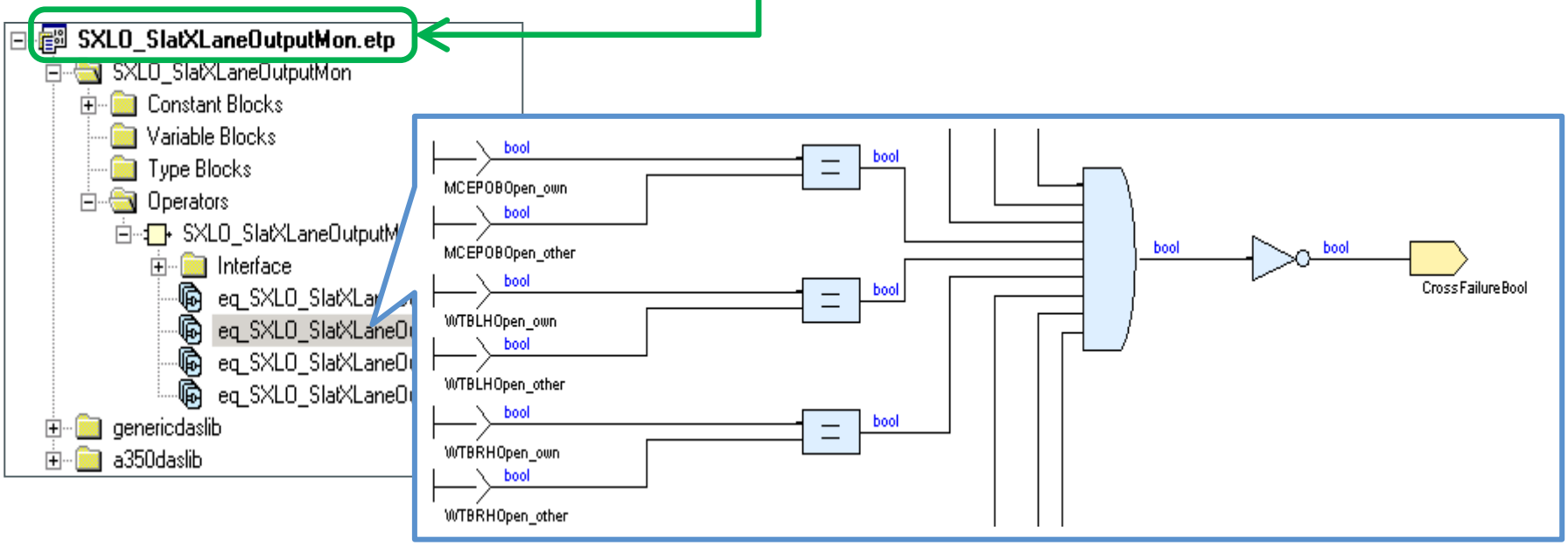
DAs SCADE Model Design

- 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**:	
	Signal	**Description**

- Low-level REQ / SCADE model

SDD_OPS W-CI-2912	The behaviour of the module is specified by the related SCADE model documented by the SCADE project report SXLO_SlatXLaneOutputMon.rtf, ClearCase version 22.	SRD_OPS-REQ-2298 SRD_OPS-REQ-2300;SRD_OPS-REQ-



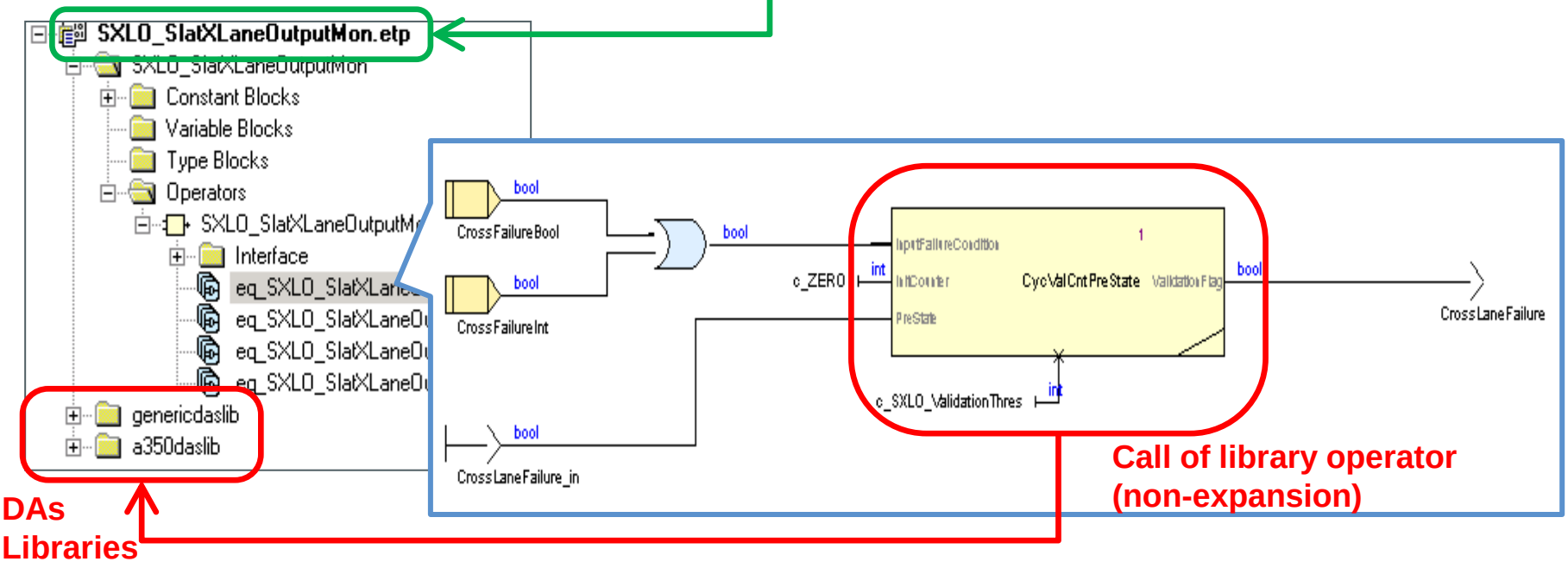
DAs SCADE Model Design (cont'd)

- 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

SDD_OPS W-CI-2912	The behaviour of the module is specified by the related SCADE model documented by the SCADE project report SXLO_SlatXLaneOutputMon.rtf, ClearCase version 22.	SRD_OPS-REQ-2298;SRD_OPS-REQ-2300;SRD_OPS-REQ-



Overview

Model Review: DAs SCADE Standard

- 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

COMPANY CONFIDENTIAL

DIEHL
Aerospace

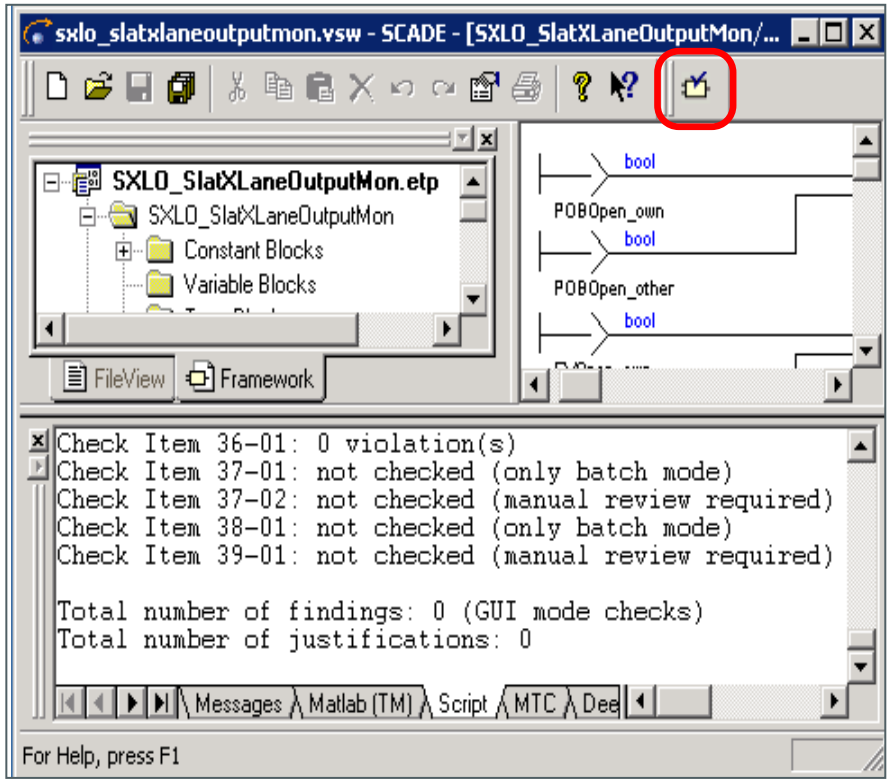
Dok. Nr./Pub. No.	PD1000006084
Ausgabe/Issue	000_07
Seite/Page	1/58
Datei/File Name	PD1000006084_000_07_SCDSTD.docx

SCADE Development Standard
(SCDSTD)
for
A350 XWB Slat Flap Control Computer
and Sensors (A350 XWB SFCC)
(ATA 27)
for the
Airbus A350XWB Program

	Name/Name Funktion/Function	Datum/Date	Unterschrift/Signature
Erstellt / Prepared	Paul Linder Software Engineer	15.8.2013	Paul Linder
Technisch verifiziert / Technical checked			
Freigabe Qualität / Quality approved			
Technisch Autorisiert / Technical Authorized			

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)

DIEHL Aerospace

- HTML report

Checking report

Overview

SCADE StyleChecker, Version 2.0, (c) Diehl Aerospace GmbH 2013

Checking Report:
Model sxlo_slatxlaneoutputmon

Checking Run: 01 Jun 2015 16:38:21

Summary

Total number of findings: 0
Number of mandatory rule findings: 0
Number of required rule findings: 0
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:
T:\A350_SFCC_SW\model\scade_gen\scade_gen.hat

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)

SCADE StyleChecker, Version 2.0, (c) Diehl Aerospace GmbH 2013

Checking Run Overview

Checking Run: 01 Jun 2015 16:58:25

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: 38

Configuration

Directories searched for SCADE projects:

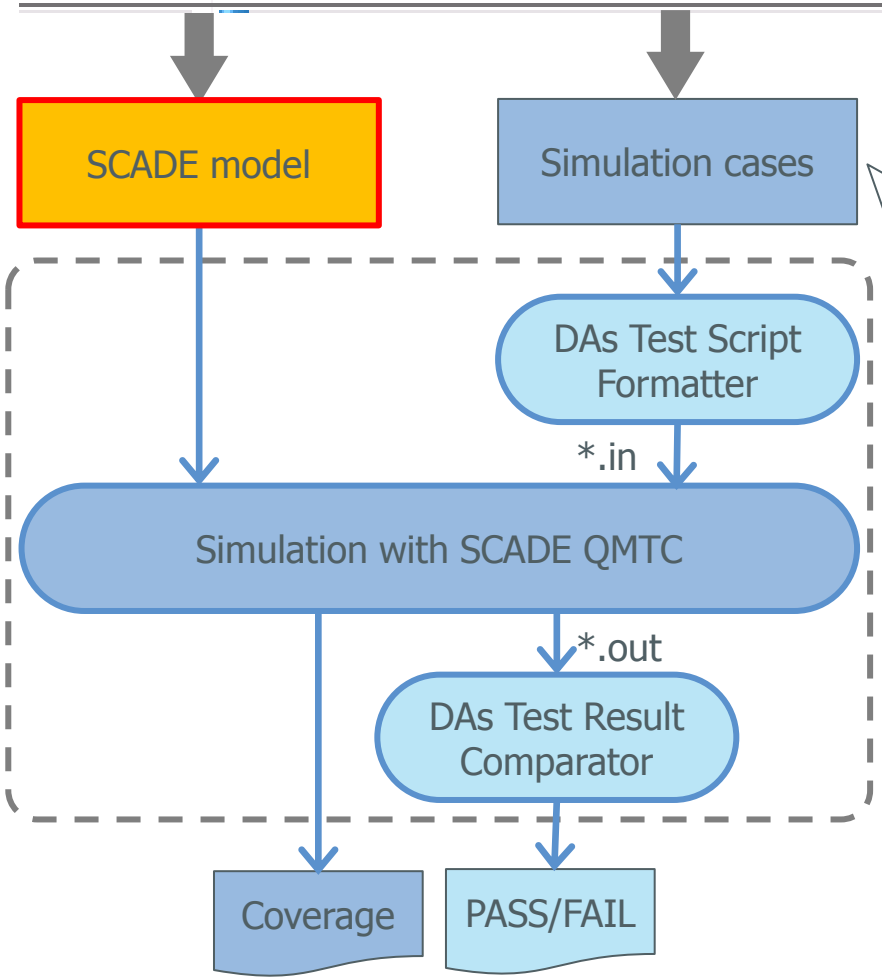
Overview

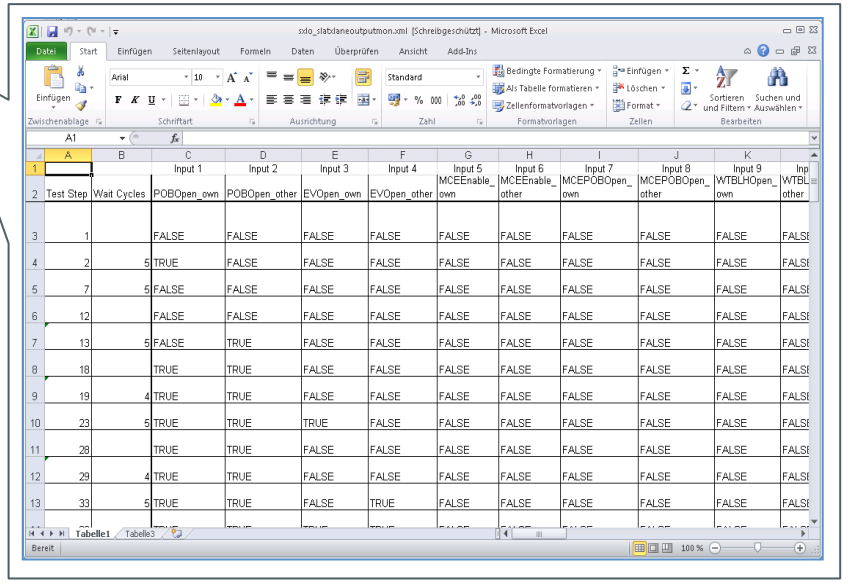
SCADE Project	Author	Verdict	Mandatory Findings	Required
fsam_fsysasymmonfailval		PASSED	0	1
ssam_ssysasymmonfailval		PASSED	0	0
fpal_fadgblhpwravailfail		PASSED	0	0
fpar_fadgbrhpwravailfail		PASSED	0	0
sxlo_slatxlaneoutputmon		PASSED	0	0

DAs Model Testing Procedure

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.

High-level requirement





	Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Input 7	Input 8	Input 9	Inp
Test Step	Wait Cycles	POBOpen_own	POBOpen_other	EVOpen_own	EVOpen_other	MCEEnable_own	MCEEnable_other	MCEPOBOpen_own	MCEPOBOpen_other	WTBLHOpen_own	WTBL other
1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	5	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
7	5	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
12		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
13	5	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
18		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
19	4	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
23	5	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
28		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
29	4	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
33	5	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Qualified toolchain

Overview

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

Some Remarks

- 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

DIEHL
Aerospace

Contact

Diehl Aerospace GmbH
Alte Nussdorfer Str. 23
88662 Ueberlingen

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

www.diehl.com/aerosystems

DIEHL
Aerospace