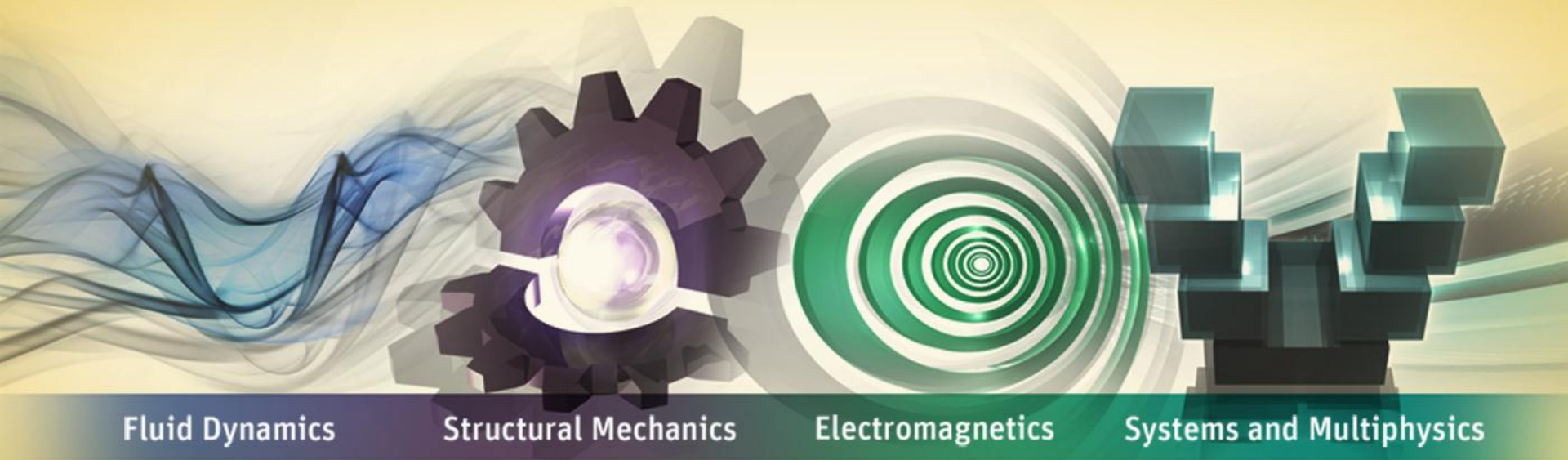


The SCADE Certification Kits



Fluid Dynamics

Structural Mechanics

Electromagnetics

Systems and Multiphysics

Dr. Bernard Dion, CTO, Esterel Technologies
bernard.dion@esterel-technologies.com

First Tool Qualification Symposium
Munich, April 9th 2013



- Esterel Technologies update
- SCADE product family overview
- Tool qualification and certification standards
- SCADE tools qualification
for DO-178, IEC 61508, EN 50128, and ISO 26262
- Return on Experience/Benefits

Esterel Technologies Update



Fluid Dynamics

Structural Mechanics

Electromagnetics

Systems and Multiphysics



Provide **critical system and software developers**
with **model-based development solutions**
that reduce **cost, risk and time-to-certification**

Business

Leading critical system and software model-based development solutions provider. Fully-owned subsidiary of ANSYS

HQ

Elancourt (near Paris, France)

End Markets

Aerospace & Defense, Turbomachines, Industrial machinery, Automotive, Rail & Transport, Energy & Nuclear

Certifications

DO-178B/C, EN 50128, ISO 26262 and IEC 61508 (and derived standards) - Software safety certifications

ISO 9001:2008 – Certified for design and sale of embedded software tools and services

World presence

Direct presence in 8 countries, customers in 29 countries

Customer Base: 250+



Aerospace & Defense



ADASI
Aeroprivor
Antonov
Airbus
Alenia
Astronics
AVIC
AVtech
Avionika
BAE SYSTEMS
Beriev
BOEING
Bosch Aerospace
Bundeswehr
(BWB)
CALT
CASC / CAST
CETC
CMC
COMAC
Crane Aerospace
DARE
Dassault Aviation
Defense
Singapore
Diehl Aerospace
DLR
EADS CASA
EADS Astrium
EADS Cassidian
ECICT
Elbit Systems
Elektroavtomatika
Embraer

EKRAN
ELTA
ELV
ESA
ESG
Eurocopter
FADACATEC
GE Aviation
GE IQ
Goodrich
GosNIIAS
HAL
Hamilton Sundstrand
Hispano-Suiza
Intecs Sistemi
Intertechnique
IRKUT
KAL/ADD
KEEVEN
KHI
L3
Liebherr
Aerospace
Lockheed Martin
Meggitt Safety
Systems
Meggitt Sensors
Meggitt Avionics

MIEA
NASA
NAUKA
NIIAO
NKBVS
Messier-Bugatti
OAK (UAC)
ONERA
Parker
Piaggio Aerospace
Poliot
Pratt & Whitney
Rheinmetall
Rolls Royce Aero
Saab Avionics
SAIC
Safran/ Sagem
Selex Galileo
Snecma
Star
Sukhoi
Turkish Aerospace Ind.
Tekhprivor
Thales Avionics
Thales Training & Sim.
Toshiba Aerospace
Turbomeca
Samsung Thales
Ultra Electronics
Ulyanovsk
US Army Redstone Ars.
VEGA
VNIIRA
Xian Aerospace
ZODIAC

Rail Transportation



Alcatel Shanghai Bell
Alstom Transportation
Ansaldo STS
AREVA TA
BJTU

CAF
CASCO
Deuta Werke
Dimetronic
EFACEC
Engineering AT
Hollysys
Hyundai Rotem
Ikerlan
INVENSYS Rail
Istanbul Ulasim
Kyosan

Mitsubishi Rail
NIIAS
NRIET
POSCON
PT LEN
RATP
Samsung SDS
Siemens Rail Transportation
Systemer
Thales Rail Signaling Systems

Industrial & Automotive



Bosch
DCNS
Fuji Heavy
GE Energy
IKV
Liebherr Construction
Mitsubishi
Johnson Controls
NIAT

Nihon Seiko
PSA
Schindler Elevators
Subaru
Terex Cranes
Toyota Automotive
Toyota Robotics
Volvo Trucks

Energy & Nuclear



AREVA NP
BARC
IGCAR Nuclear Research
Rolls-Royce Civil Nuclear
KAERI
KOPEC
NPCIL
NPIC

Rolls Royce Submarine
SNERDI
Techenergy
VESTAS
VNIIA /Rosatom

SCADE Product Family Overview



Fluid Dynamics

Structural Mechanics

Electromagnetics

Systems and Multiphysics

**Model-Based
System Engineering**

**SCADE
SYSTEM**

System Architecture,
System Verification

**Control
Software Design**

**SCADE
SUITE**

Prototyping, Design,
Verification, Qualified
Code Generation

**HMI
Software Design**

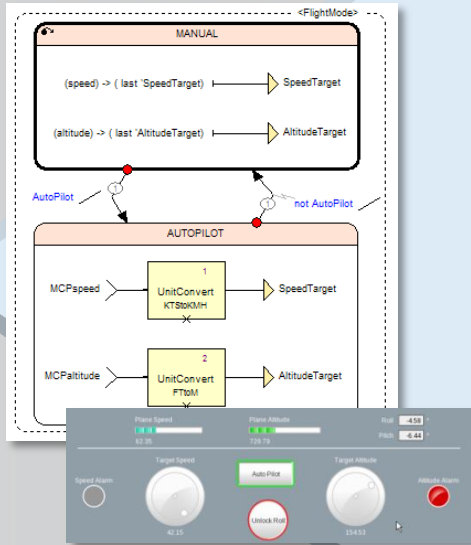
**SCADE
DISPLAY**

Prototyping, Design,
Verification, Qualified
Code Generation

**System & Software
Lifecycle Mgt**

**SCADE
LIFECYCLE**

Certification Plans, Metrics,
Requirements, Configuration
Management,
Documentation
Generation



**PROTOTYPE
& DESIGN**

Control Software Design



Model Checking



Formal Verification



Debug & Simulation



Rapid Prototyping & Executable Spec



Model Coverage Analysis



Time & Stack Analysis

VERIFY

**SCADE Suite
KCG
C & Ada**

**RTOS
Adaptors**



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

GENERATE



Object Code & Compiler Verification



HMI Software Design



**Model
Checking**



Simulation

**SCADE
Display KCG**

OpenGL|SC
Compliant

OpenGL|ES

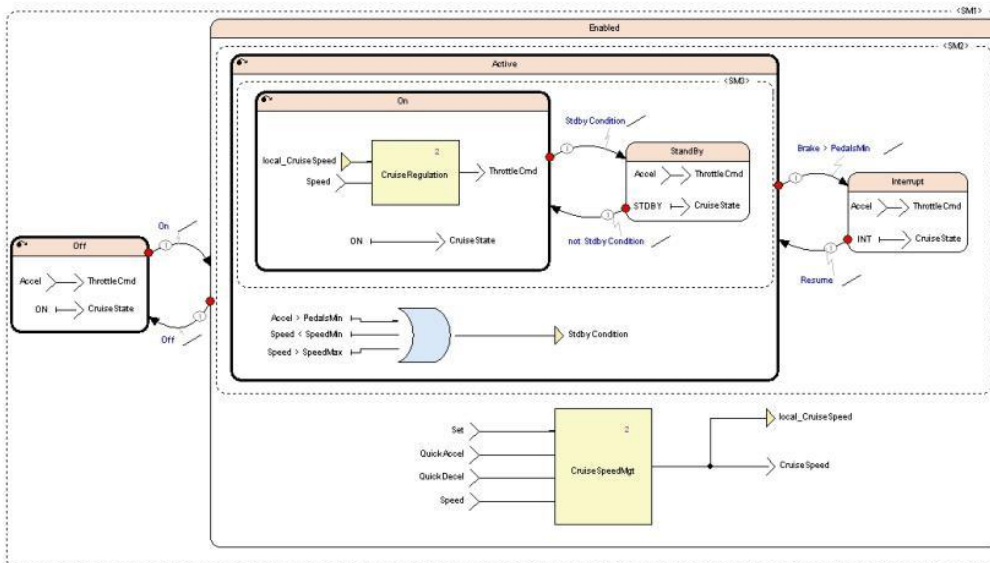


**DO-178B
DO-178C
IEC 61508
EN 50128
ISO 26262
Certification Kits**

**PROTOTYPE &
DESIGN**

VERIFY

GENERATE

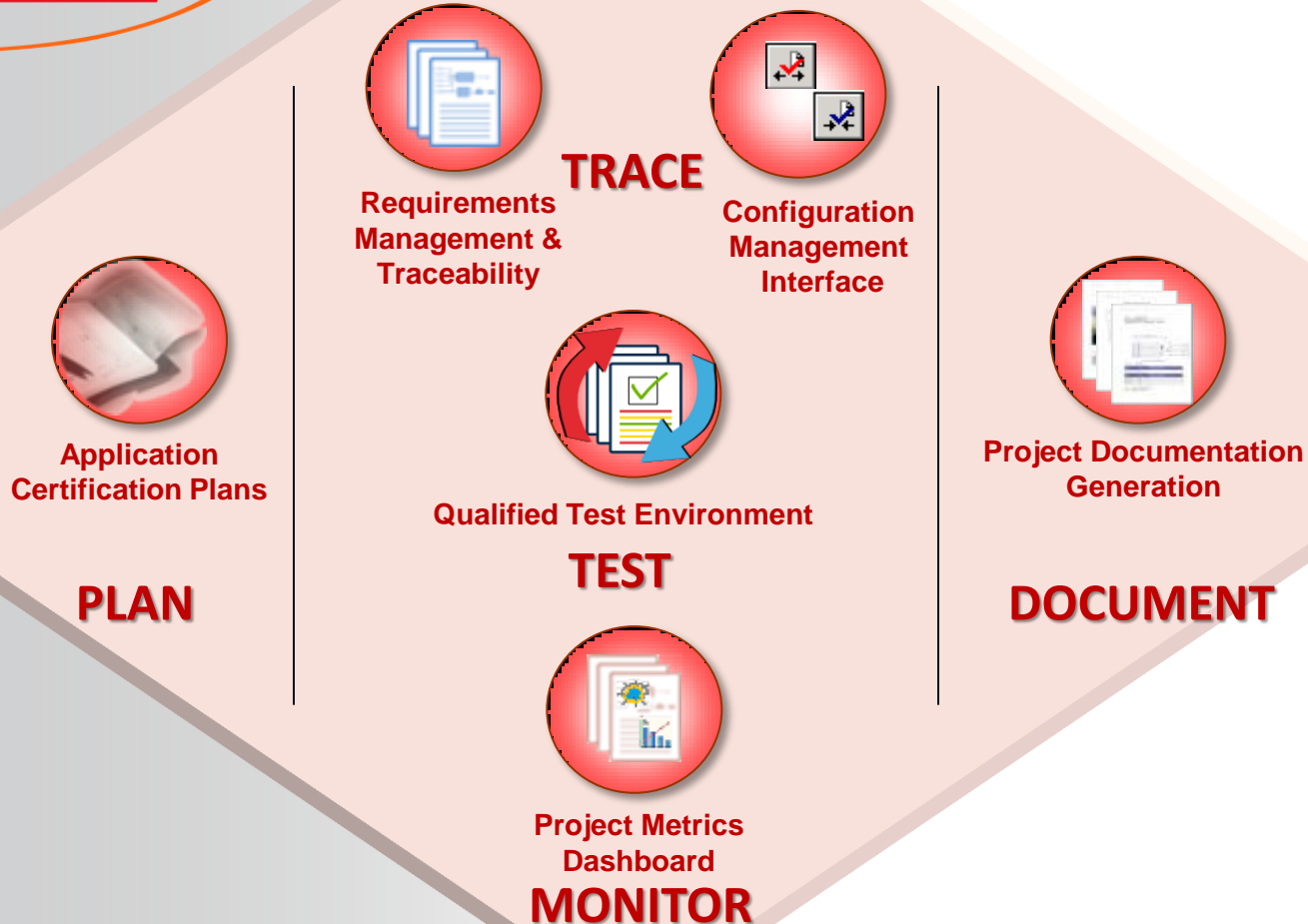


Top Level of the Cruise Control application

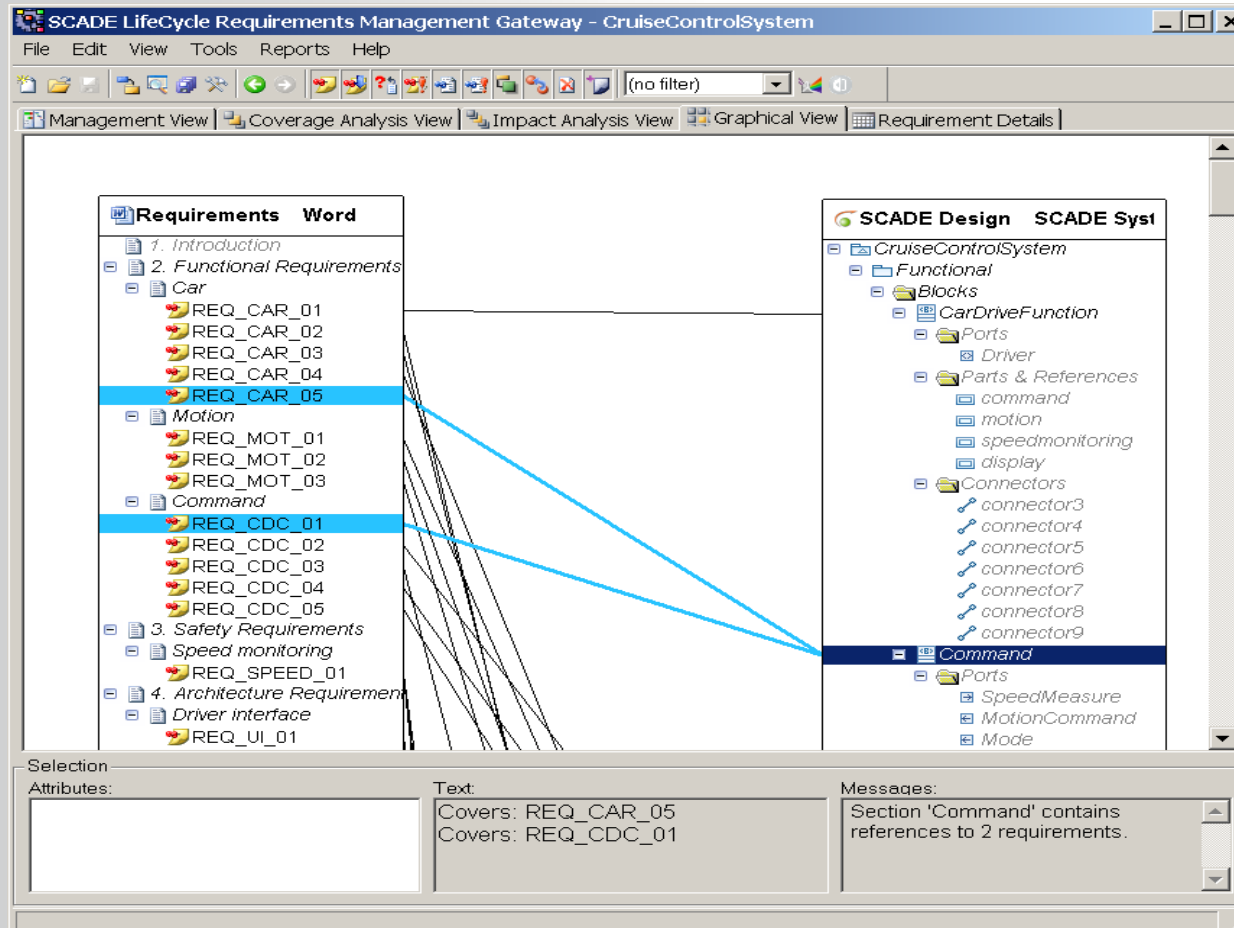




System & Software Lifecycle Management



SCADE LifeCycle Requirements Management Gateway



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:**
 - **DO-178B/C qualification up to Level A – Aeronautics**
 - **EN 50128 certification up to SIL 3/4 – Rail Transportation**
 - **IEC 61508 certification up to SIL 3 – Industrial & Energy**
 - **IEC 60880 full compliance – Nuclear I&C**
 - **ISO 26262 certification up to ASIL D – Automotive (2013)**
- **Same products qualified at the highest level of safety across 5 market segments by 10 safety authorities, worldwide**

Example SCADE Display in Airbus A380 Cockpit



- **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



Tool Qualification and Certification Standards



Fluid Dynamics

Structural Mechanics

Electromagnetics

Systems and Multiphysics

- Is tool qualification needed? (*e.g. in DO-178C*)
 - Yes, “when processes of this document are eliminated, reduced, or automated by the use of a software tool without its output being verified as specified in section 6.0”

- **There are 3 criteria for tools in DO-178C**
 - **Criteria 1 tool**
 - A tool whose output is part of the airborne software and thus could insert an error
 - **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
 - **Criteria 3 tool**
 - A tool that, within the scope of its intended use, could fail to detect an error

- **Tools are 3 classes of tools in EN 50128:2011**
 - **Class T1 tool**
 - generates no outputs which can directly or indirectly contribute to the executable code (an Editor)
 - **Class T2 tool**
 - supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create them (a Test harness generator)
 - **Class T3 tool**
 - generates outputs which can directly or indirectly contribute to the executable code (a Code generator)

TQL – Tool Qualification Level (DO-330)

(DO-178C) Software Level	Criteria		
	1	2	3
A	TQL-1	TQL-4	TQL-5
B	TQL-2	TQL-4	TQL-5
C	TQL-3	TQL-5	TQL-5
D	TQL-4	TQL-5	TQL-5

- **For each tool that has to be qualified at TQL-1 (Criteria 1 tool used to develop Level A software), evidence shall be available that the tool output conform to its specification**
- **Evidence will be based on compliance with the objectives of DO-330 at TQL-1**


Tool Qualification with EN 50128 Class T3

- **For each tool in Class T3, evidence shall be available that the tool output conform to its specification**
- **Evidence may be based on compliance with the safety integrity levels derived from the risk analysis of the process and procedures including the tool**

SCADE Tools Qualification for DO-178, IEC 61508, EN 50128 and ISO 26262

A visualization of fluid flow, showing blue and white wavy lines representing the movement of a fluid.

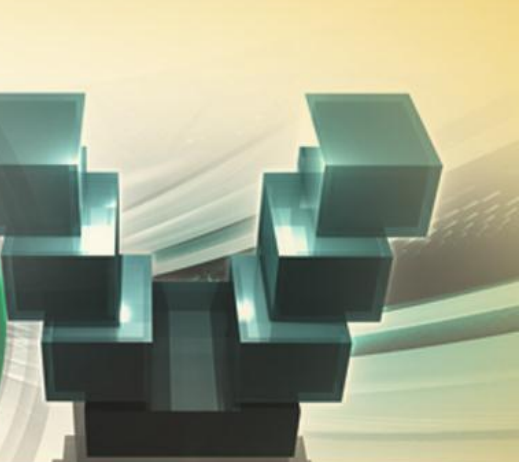
Fluid Dynamics

A 3D rendering of a dark purple gear with a glowing white and purple center, set against a background of other gears.

Structural Mechanics

A 3D rendering of a green target with concentric circles, set against a background of a glowing green sphere.

Electromagnetics

A 3D rendering of several blue and black rectangular blocks stacked together, set against a background of a glowing blue sphere.

Systems and Multiphysics

SCADE Suite
and Display
KCG

SCADE Suite
MTC

SCADE LifeCycle
Reporter & QTE

(DO-178C) Software Level	Criteria		
	1	2	3
A	TQL-1	TQL-4	TQL-5
B	TQL-2	TQL-4	TQL-5
C	TQL-3	TQL-5	TQL-5
D	TQL-4	TQL-5	TQL-5

- **SCADE Suite KCG Certification Kits (one per standard) contain material demonstrating to certification authorities that the SCADE Suite KCG code generator was developed in compliance with the highest levels of Safety Standards.**
- **These Certification Kits provide access to the documents that are needed by the various stakeholders, including tool user and certification authority**

SCADE Suite KCG Certification Kits Contents (1/2)

- **Compliance Analysis of SCADE Suite KCG at the Safety Level identified in the Certification Kit**
- **Safety Plan (*EN 50128, IEC 61508, and ISO 26262*)**
- **Tool Qualification Plan (TQP)**
- **Tool Operational Requirements (TOR)**
- **Tool Requirements (TR)**
- **Tool Accomplishment Summary (TAS) (*DO-178B or C*)**
- **Safety Case (SC) (*EN 50128, IEC 61508, and ISO 26262*)**
- **Test Report (TR)**

SCADE Suite KCG Certification Kits Contents (2/2)

- Tool Installation Procedure (TIP)
- Tool Configuration Index (TCI)
- Tool Life Cycle Environment Configuration Index (TLCECI)
- *Other documents are available on premises at Esterel Technologies:*
 - *Tool Verification Records (for example test cases, procedures and results)*
 - *Tool Qualification Development Data (requirements, design, code, etc.)*

Tool Qualification Plan (TQP) (1/2)

- **The TQP presents the provisions taken by Esterel Technologies for the qualification of KCG as a development tool that fulfills the requirements of DO-330 objectives up to TQL 1, IEC 61508 up to SIL 3 and EN 50128 up to SIL 3-4, ISO 26262 up to ASIL-D.**
- **This document is directed to**
 - The project team
 - KCG users
 - Certification authorities

- **The TQP includes**
 - Tool overview
 - Project organization and schedule
 - Tool development lifecycle
 - (Qualified) tools to develop KCG
 - Certification credits sought for the tool user

SCADE Suite Compliance Matrix

Example: DO-330/Table T0 extract for DO-178C

TABLE T-0: TOOL OPERATIONAL PROCESSES

	Objective		Activity DO330 Ref.	Applicability by TQL					Review Items	Status	Problem ID	Problem Closure	
	Description	DO330 Ref.		1	2	3	4	5				Baseline N°	Status
1	The tool qualification need is established.	4.1	[Note 1]	○	○	○	○	○	[KCG_SDP] 2.2 [KCG_TQP] 1.2, 2.2, 7	OK			
2	Tool Operational Requirements are defined.	5.1.1.a	5.1.2.a 5.1.2.b 5.1.2.c	○	○	○	○	○	[KCG_SDP] 2.1 [KCG_SDP] 4.4.6 [KCG_SVP] 4.4 [KCG_SQAP] 3.3	OK			
3	Tool Executable Object Code is installed in the tool operational environment.	5.3.1.a	5.3.2.a 5.3.2.b 5.3.2.c	○	○	○	○	○	[KCG_TQP] 10.9.3 [KCG_SDP] 4.4.11 [KCG_SVP] 5.4.6 [KCG_SQAP] 3.7 (installation)	OK			
4	Tool Operational Requirements are complete, accurate, verifiable, and consistent.	6.2.1.a	6.2.2.a	●	●	○	○		[KCG_SVP] 4.4 [KCG_SCMP] 6, 7 [KCG_SQAP] 3.3 [KCG_TQP] 3.6 (independence)	OK			

SCADE Suite KCG Tool Accomplishment Summary (TAS) – DO-178B/C

- The TAS presents the status of activities carried out for the development of the SCADE Suite KCG code generator (qualifiable version as defined in the TQP), in compliance with DO-330 TQL-1
- It includes:
 - Project status
 - Tool installation considerations
 - Conditions of use
 - Open problems and limitations

SCADE Suite KCG Safety Case – IEC 61508, EN 50128, ISO 26262

- **The Safety Case of KCG provides the evidence that KCG was developed with the appropriate level of safety lists the Conditions of Use that shall be obeyed by the KCG users so that they may claim the certification credits of the tool.**
- **It includes:**
 - Project organization
 - Quality status
 - Risks analysis related to the development of KCG
 - Risks analysis related to the use of KCG

SCADE Suite KCG – Safety Status Report

- **This KCG Safety Status Report presents the status of defects remaining in KCG and additional considerations to be taken into account by KCG users in their qualification process since the publication of the Tool Accomplishment Summary**
- **It provides means for managing related safety risks**
- **Its is distributed on a regular basis to all users**

SCADE Methodology Handbooks

DO-178, IEC 61508, EN 50128, ISO 26262

- **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.



Download the handbook from
www.esterel-technologies.com

Return on Experience Benefits



Fluid Dynamics

Structural Mechanics

Electromagnetics

Systems and Multiphysics

- **53 DO-178B Program Certifications in aeronautics**
 - 30 already achieved
 - 23 undergoing certification
- **For more than 98 systems**
 - Ranging from level A to D (mostly level A)
- **By multiple certification authorities**
 - FAA, EASA, Transport Canada, ANAC, CAAC, etc.
- **DO-178C ready**

- **Similar experiences in rail and nuclear**
- **ISO 26262 qualification in 2013 for automotive**

- **Reduces development and verification costs**
 - Low-level testing effort is drastically reduced due to code generation qualification credits
- **Reduces risk, time and cost certification**

Thank you! Questions



Fluid Dynamics

Structural Mechanics

Electromagnetics

Systems and Multiphysics