Braunschweiger Verkehrskolloquium 3. Februar 2004

Advanced Methodologies for Aerospace, Automotive and Transportation software development

ESTEREL Technologies GmbH

Jakob Gärtner & Wolfgang Klinge

Esterel Technologies Confidential

Esterel Technologies - Corporate Profile (1)

- Headquarters in Mountain View, California and Elancourt, France (founded in 2000)
- Esterel Technologies GmbH in Germany
- Certified Services Partner in Transportation ICS AG

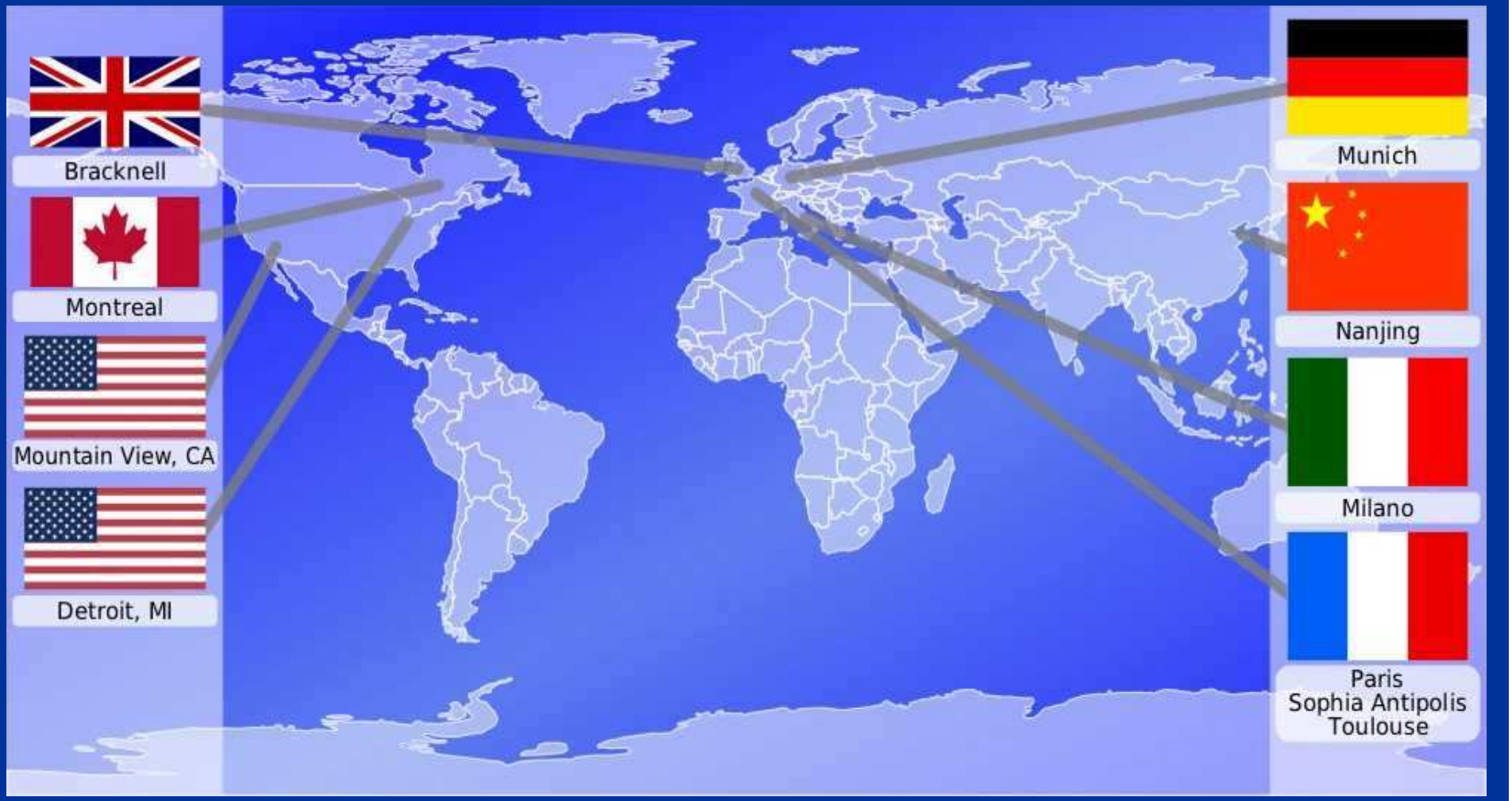
Esterel Technologies Confidential

Esterel Technologies - Corporate Profile (2)

- R&D centres in Toulouse and Nice, France
- 120 employees in 7 countries
- 50+ large corporate customers
- 50+ universities worldwide teaching the use of Esterel Technologies solutions

Esterel Technologies Confidential

World-Wide Presence



Esterel Technologies Confidential

SCADE Suite™ & SCADE Drive™

Safety Critical Application Development Environment

Photo courtesy of AIRBUS

Falcon 7X by Dassault Aviation

Aeroengines by Snecma
©Snecma/Studio Pons

Rooted in 10 Years of Successful Industrial Application and More Than 20 Years of Research

- Optimized for:
  - *Aerospace & Defense SCADE Suite*
    - DO178B Level A qualified → **100% certification success rate**
  - *Transportation & Energy SCADE Suite*
    - IEC 61508 certified (for all SIL levels)
  - *Automotive SCADE Drive*
    - MISRA compliant & IEC 61508 certified (for all SIL levels)

Esterel Technologies Confidential

Critical Embedded Software Applications

- Aerospace & Defence
  - *Flight control systems*
  - *Autopilots*
  - *Engine control systems*
  - *Braking systems*
  - *Cockpit display and alarm management*
  - *Fuel management*
  - *Power management*
  - *Reconfiguration management*
- Automotive
  - *Engine regulation*
  - *Airbags*
  - *Display management*
  - *Chassis Systems*
  - *Driver Assistance Systems*
  - *Restraining systems*
  - *Entertainment systems*
  - *X-By-Wire applications*
- Transportation & Energy
  - *Interlocking systems control*
  - *Nuclear systems control & command*

Photo: FRAMATOME

Esterel Technologies Confidential

SCADE Suite
Current Customer Base

Civilian Avionics

- *Aircraft Braking Systems*
- *Airbus*
- *Dassault Aviation*
- *Diehl Avionik Systeme*
- *Elbit Systems*
- *Eurocopter*
- *Liebherr-Aerospace*
- *Messier-Bugatti*
- *Nanjing Aerospace Inst.*
- *Pratt & Whitney*
- *Rockwell Collins*
- *Snecma*
- *Thales Avionics*

Defense & Space

- *Dassault Aviation*
- *EADS Military*
- *EADS Space Transport*
- *Elbit Systems*
- *ESA*
- *Eurocopter*
- *Flight Dynamics*
- *Hispano-Suiza*
- *Lockheed- Martin*
- *NASA*
- *Rockwell Collins*
- *Sagem*
- *Thales Airborne Systems*

Energy & Transportation

- *Ansaldo Signal*
- *Framatome*
- *Schneider Electric*
- *DS&S*

SCADE Suite

Esterel Technologies Confidential

SCADE Drive
Current Customer Base

Automotive

- *AWA*
- *Audi*
- *FTE*
- *General Motors*
- *Johnson Controls*
- *PSA Peugeot Citroen*
- *Visteon*

SCADE Drive

Esterel Technologies is a member of

FlexRay™

and

tta Group

Esterel Technologies Confidential

ESTEREL Technologies

Airbus A380

- After the objective metrics from the A340, Airbus made SCADE the corporate standard for all new airplane development. It is using SCADE on the following systems in the A380:
  - *Flight Control System*
  - *Flight Warning System*
  - *Electrical Load Management System*
  - *Anti Icing system*
  - *Braking and Steering system*
  - *Cockpit Display system*
  - *Part of ATSU (board / Ground communications)*
  - *FADEC (Engine Control)*
  - *EIS2 : Specification GUI Cockpit (4 functions DU (Display Unit)) :*
  - *PFD : Primary Flight Display*
  - *ND : Navigation Display*
  - *EWD : Engine Warning Display*
  - *SD : System Display*

Esterel Technologies Confidential

PSA Success

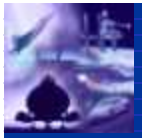
PSA PEUGEOT CITROËN

- SCADE Drive has been operated to develop the next generation of Control Suspension System (CSS) that will go to production on high end Citroen cars

- Achievements
  - *30 000 lines of codes generated by SCADE*
  - *Overall productivity increased by 33%*
  - *Generated code fits strong code optimization constraints*

Esterel Technologies Confidential

ESTEREL Technologies



SCADE & IEC 61508

- Very important for the understanding is to know that the statements presented with the following slides have been assessed and approved by the TÜV.

Esterel Technologies Confidential

IEC 61508: history

- 1980: German ministry for science & technology (BMFT) financed TÜV study “microcomputers in safety technology” which becomes foundation for further work
- Until 1995: creation of a German standard (E DIN 65A)
- pan- European standard IEC 61508 is built on E DIN 65 A and
- 2001 ratified by CENELEC as IEC 61508
- 1.8.2004: IEC 61508 officially replaces older standards in Europe

Esterel Technologies Confidential

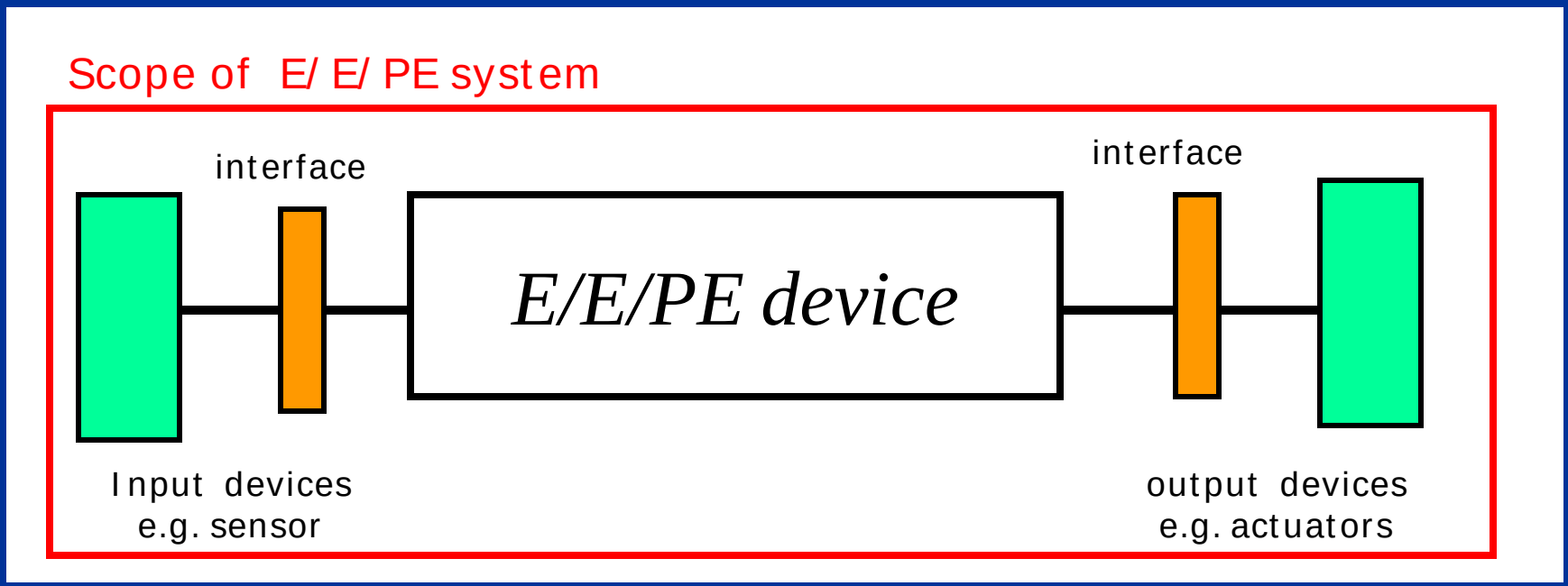
IEC 61508: concepts

- Introduces the notion of the “safety life cycle” which monitors the safety relevant aspects over the full life cycle of an EUC
- Introduces a phase model
- Manages all phases of the safety life cycle, including concept, requirements, design, use, maintenance, modification, etc.
- Aims in establishing a “safety- culture” of continuous improvement
- Aims in developing safety relevant skills
- Focus on quality assurance and safety assurance
- Defines requirements on documentation of the entire process

- Bottom line: all aspects that directly or indirectly have an effect on the correct function of a safety relevant product

Esterel Technologies Confidential

IEC 61508: definitions (1/4)



E/E/PES: electrical, electronic, programmable electronic systems

Esterel Technologies Confidential

IEC 61508: definitions (2/4)

- EUC: equipment under control:
  - *In IEC 61508, the EUC is subject to the certification project*
  - *Definition of EUC depends on scope of the certification*
  - *EUC can be:*
    - A complete car with dozens of subsystems
    - Any of these subsystems
    - Any distinct component of any of those subsystems
  - *The required safety integrity level for an EUC has to be determined using methods like FMEA, FTA, hazard and risk analysis*

Esterel Technologies Confidential

IEC 61508: Definitions (3/4)

- Validation "Are we doing the right thing?"
  - *we have to give evidence that our product is working correctly and will fulfill its defined purpose. Validation is the evaluation of the results of a process to ensure correctness and consistency with respect to the inputs and standards provided to that process.*
- Verification "Are we doing the thing right?"
  - *The evaluation of the results of a process to ensure correctness and consistency with respect to the inputs and standards provided to that process. This can be done through analysis or tests that show that under all checked circumstances the system behaves as expected. Usually, the result of this verification will only give a certain level of confidence that the design is correct with respect to the requirements.*
- Proof "Can we prove that we are doing it right?"
  - *the result of a proof is binary. It can be "true" or "false" that a certain property (binary expression) is valid. A proof is the strongest form of verification and assures 100% that a certain requirement is met*

Esterel Technologies Confidential

IEC 61508: Definitions (4/4)

- Safety integrity: probability, that an EUC will execute all functions that are relevant to safety requirements under all defined conditions over a given period of time
- The required safety integrity level for an EUC has to be determined using methods like FMEA, FTA, hazard- and risk analysis
- According to the required SIL level, the standard requires specific measures and actions to be taken

Esterel Technologies Confidential

IEC 61508

SIL level: quantitative approach

Table 3 – Safety integrity levels: target failure measures for a safety function operating in high demand or continuous mode of operation

Safety Integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$
NOTE – See notes 3 to 9 below for details on interpreting this table.	

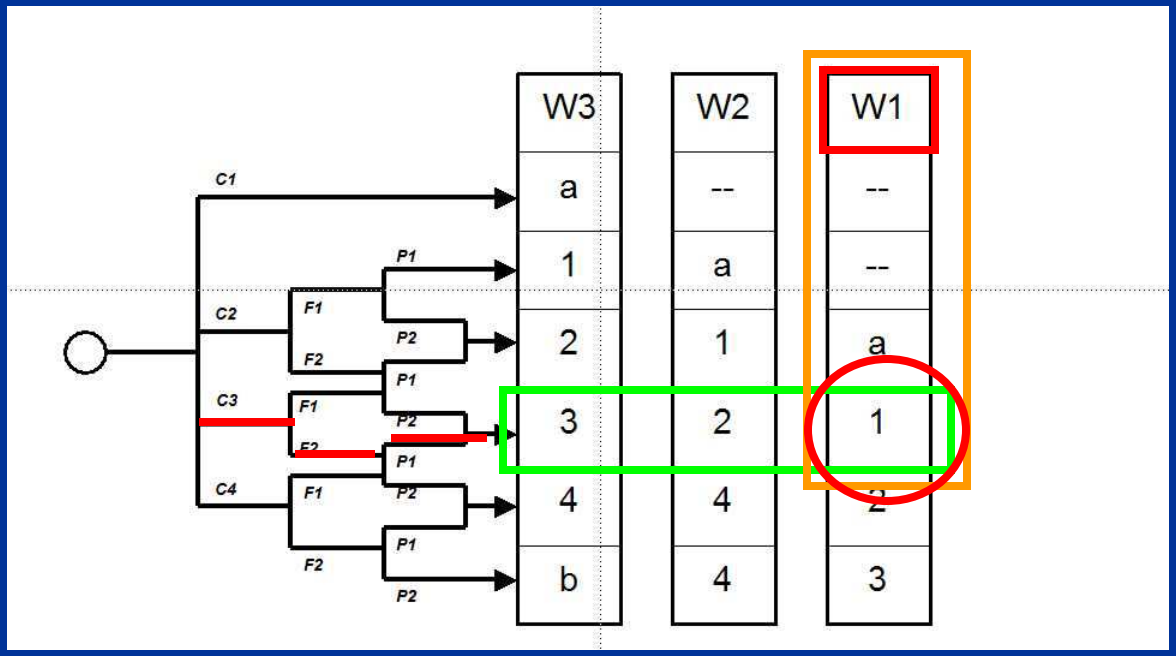
[risk] = [frequency or probability of failure] * [cost of failure]

Esterel Technologies Confidential

IEC 61508: SIL levels

Qualitative approach: example

SEAT MEMORY: risk for unintended movement while driving with accident as result



C3: death of several persons

F2: the persons are permanently in the car

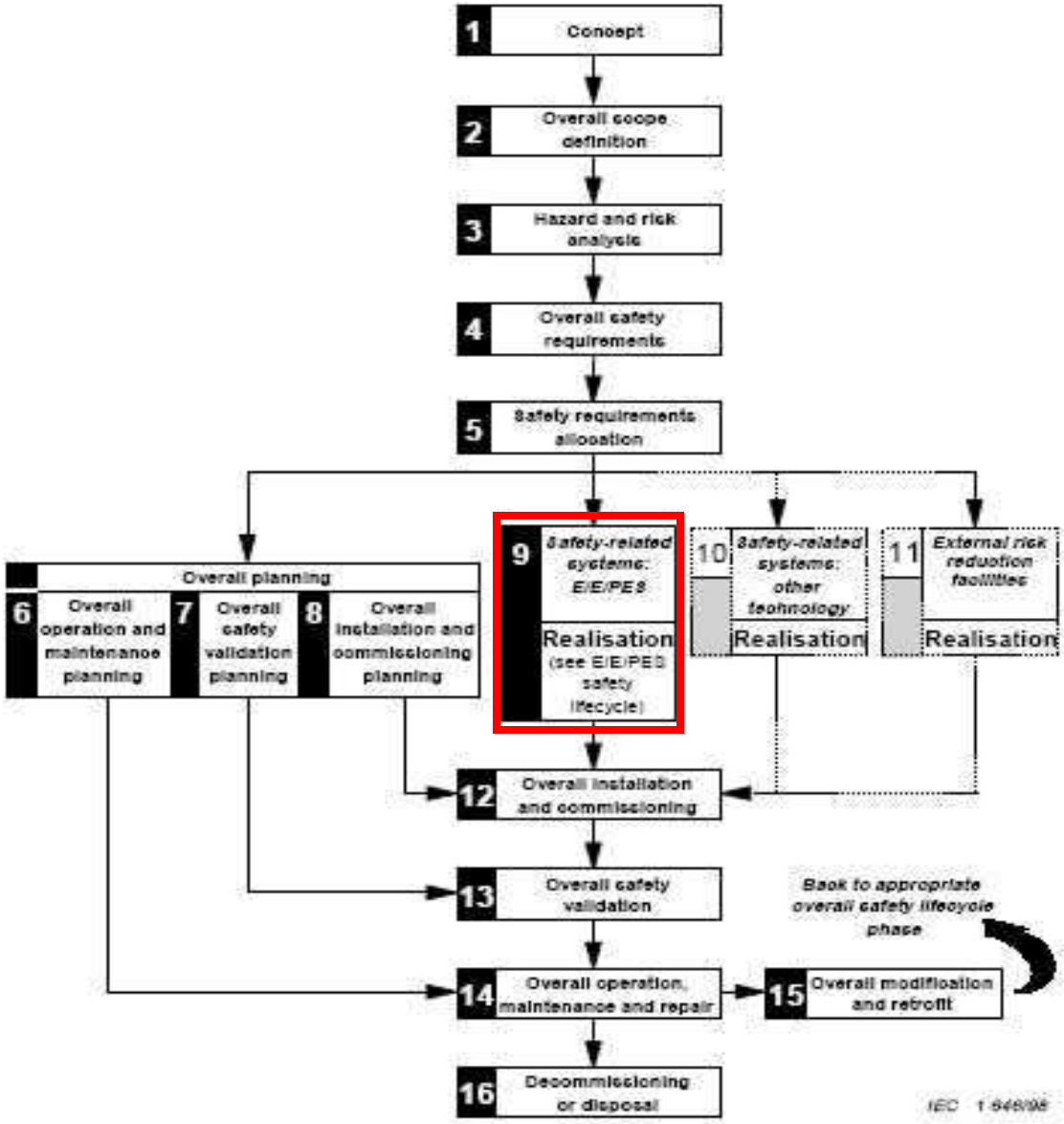
P1: the driver can possibly find a way to safely stop the car even if seat moves during ride

W1: the existing system is known to be very reliable

the system is classified SIL 1

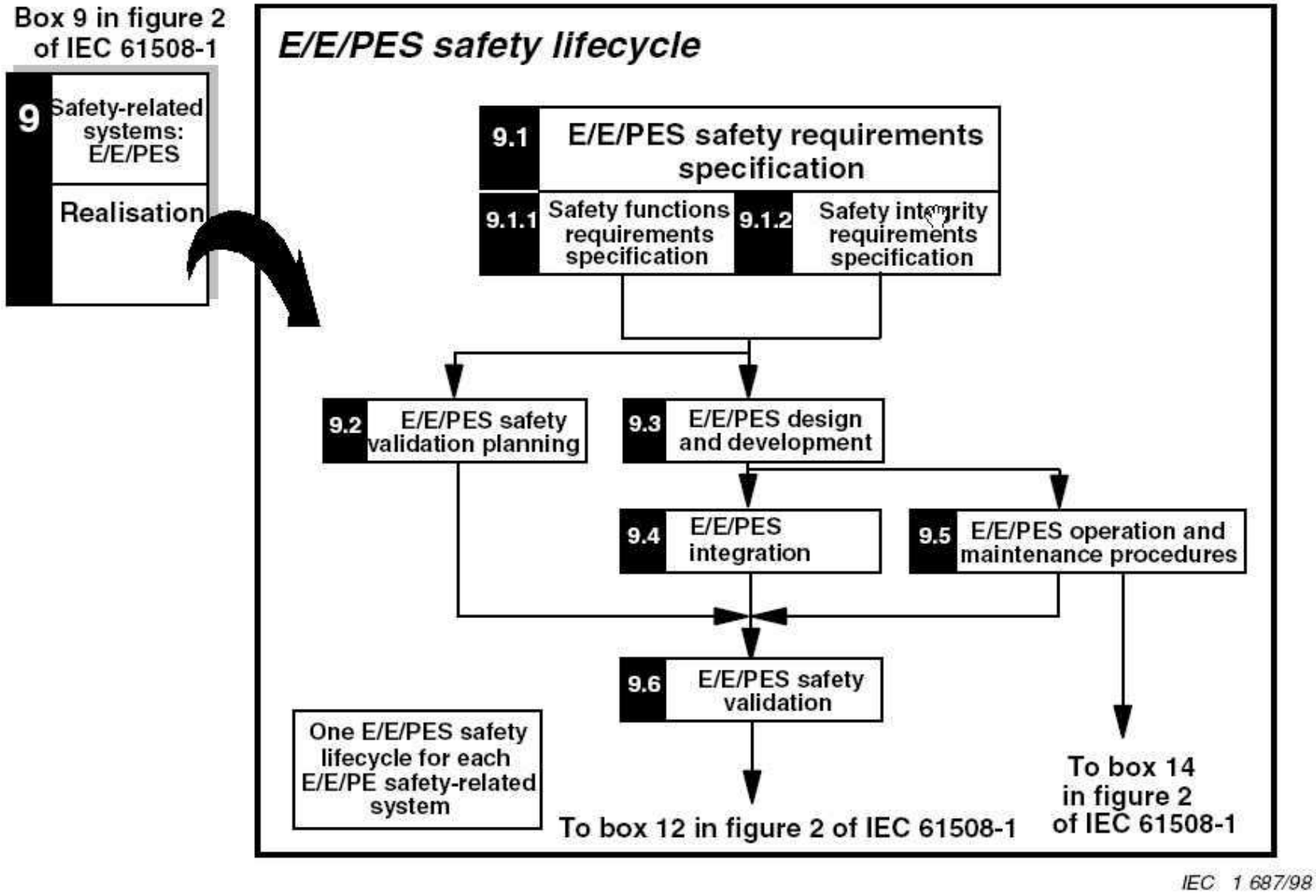
Esterel Technologies Confidential

IEC 61508: Overview



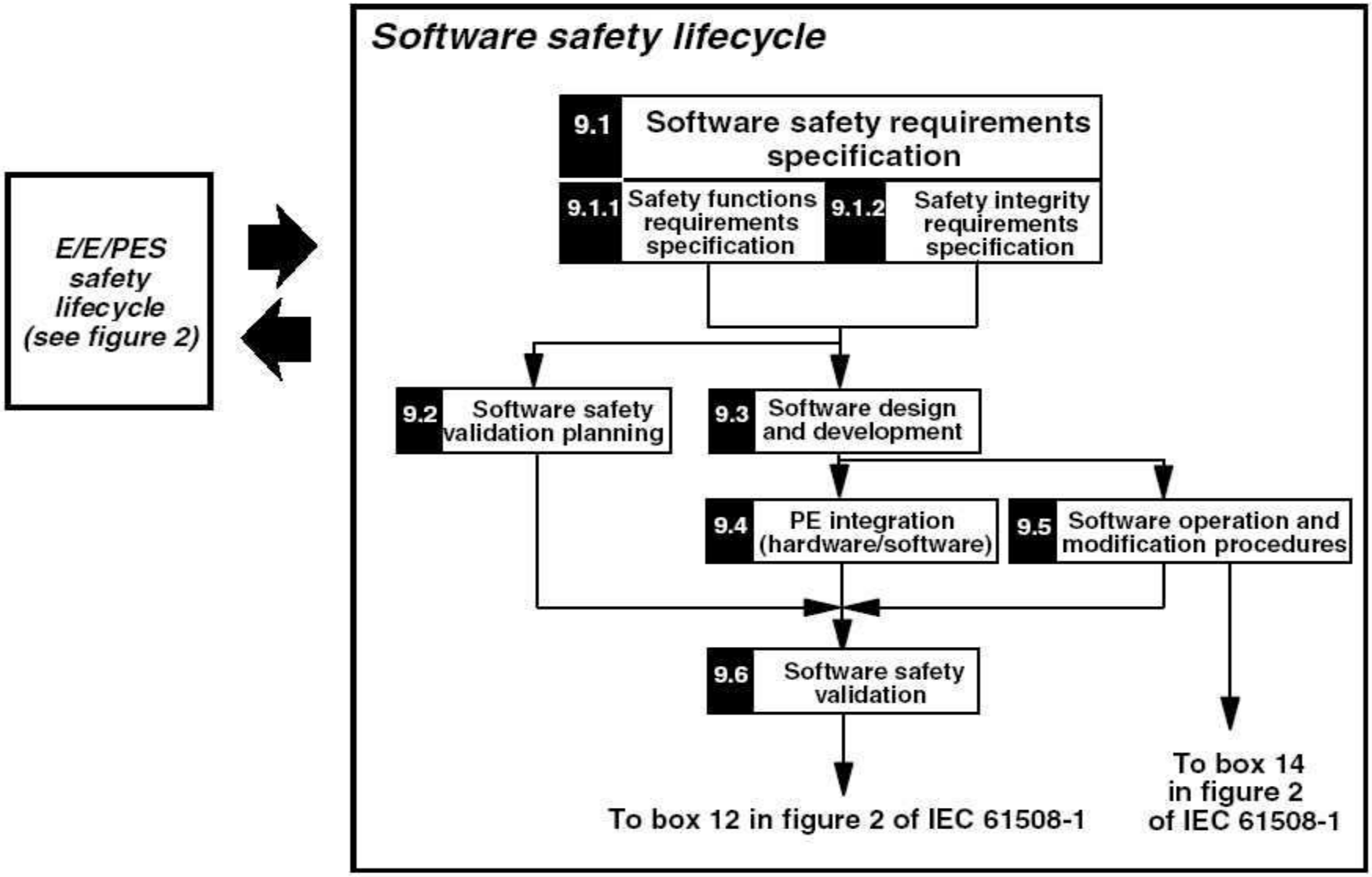
Esterel Technologies Confidential

IEC 61508: safety lifecycle



Esterel Technologies Confidential

IEC 61508: software safety lifecycle

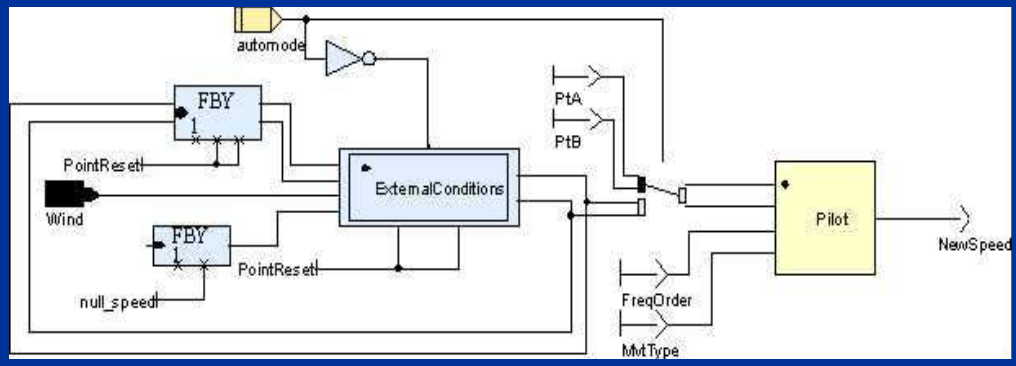


Esterel Technologies Confidential

This watermark does not appear in the registered version - http://www.clicktoconvert.com

Introduction

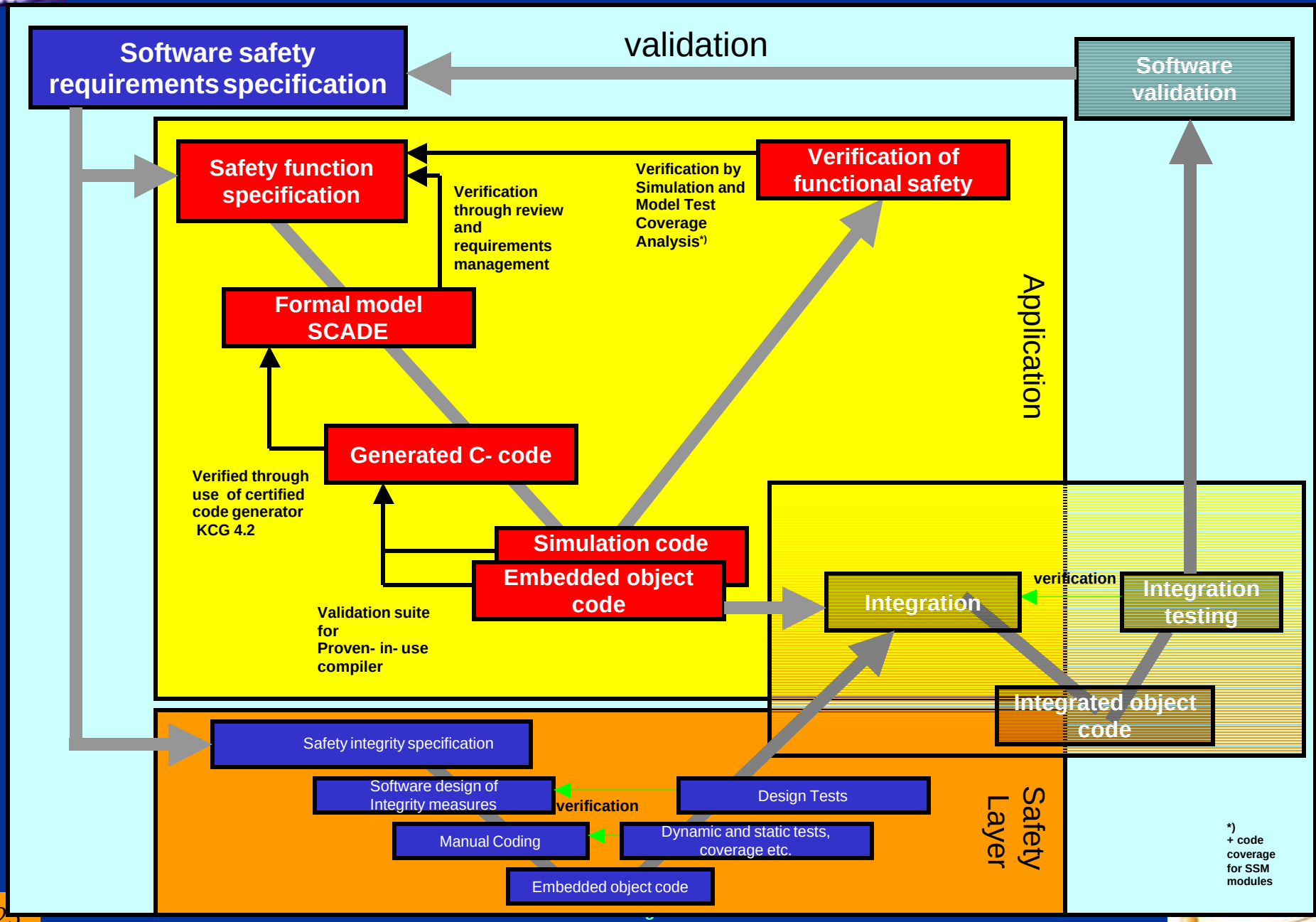
- SCADE Model-based development recognized as an efficient and cost effective way to develop critical embedded software
  - *relies on classical graphical notations for modeling: block diagrams & state machines*
  - *is used for airborne software with DO-178B level A objectives and in transport/ automotive with IEC 61508 functional safety objectives*



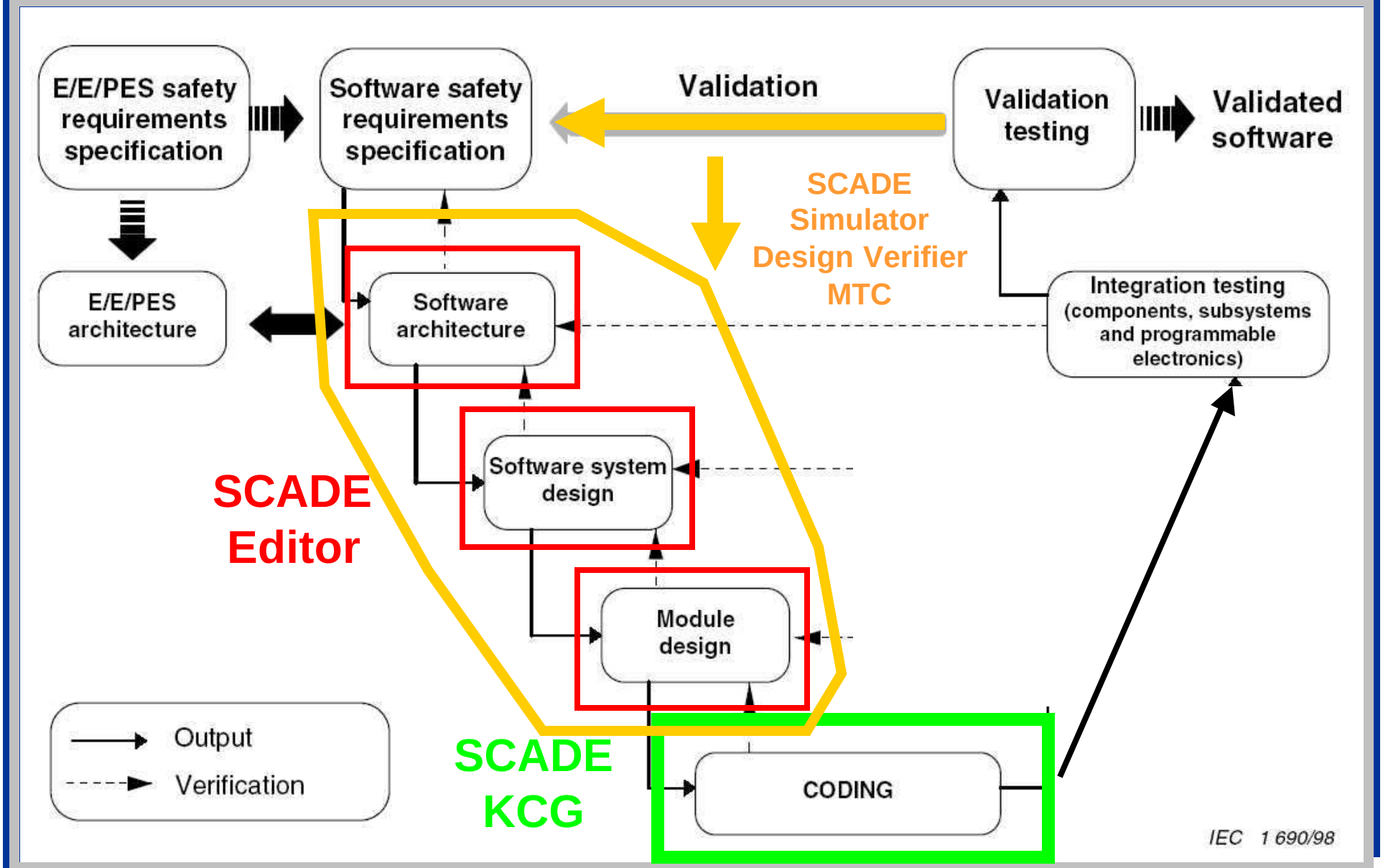
- In this paradigm, the model is the detailed specification
- In order to fully benefit from this approach, a certified automatic code generation (KCG) is used to generate C code from the model

Esterel Technologies Confidential

IEC 61508: V- model for certified code generation of application layer
Process overview



IEC 61508: V- model

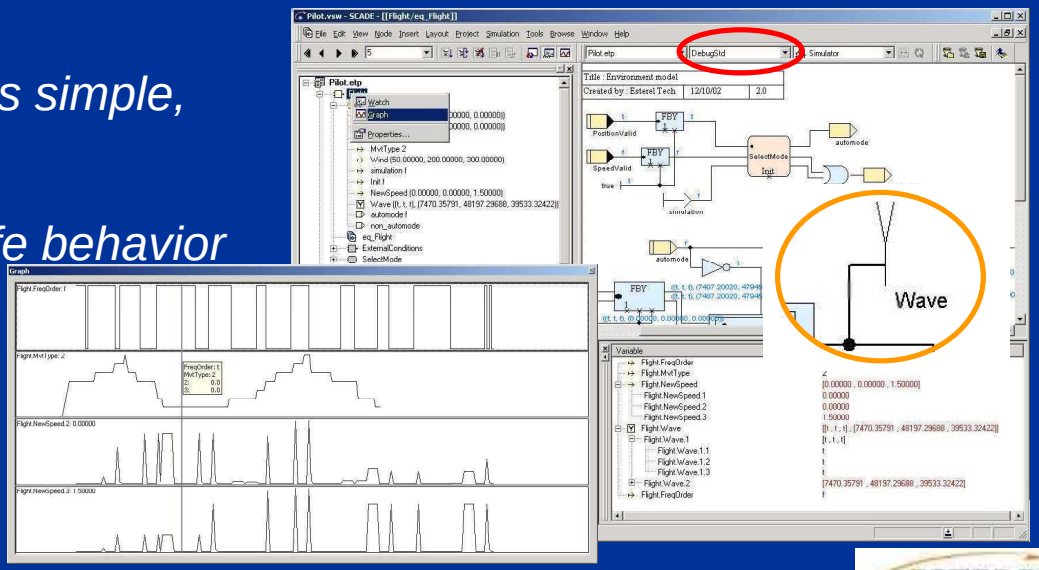


Esterel Technologies Confidential

This watermark does not appear in the registered version - http://www.clicktoconvert.com

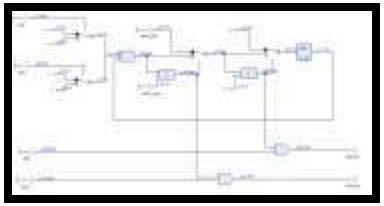
SCADE

- SCADE uses a very familiar domain dependent graphical notation with block diagrams & state machines that is rigorously defined and fully deterministic
- The SCADE toolset includes a graphical editor that performs semantics verification and a simulator
- SCADE automatically generates Source C Code from this graphical notation with a certified Code Generator (SCADE/KCG);
- that ensures
  - *the generated Source C Code is simple, verifiable and traceable*
  - *the generated code exhibits safe behavior*
    - deterministic
    - safe memory management
    - predictable execution time



Esterel Technologies Confidential

SCADE KCG: coding process



SCADE KCG

code that has to be traditionally verified

user code

certified/ validated SCADE OS_config tool

generated code

SCADE library code

Certified Safety Layer

code that is certified

Esterel Technologies Confidential

Software Verification with SCADE

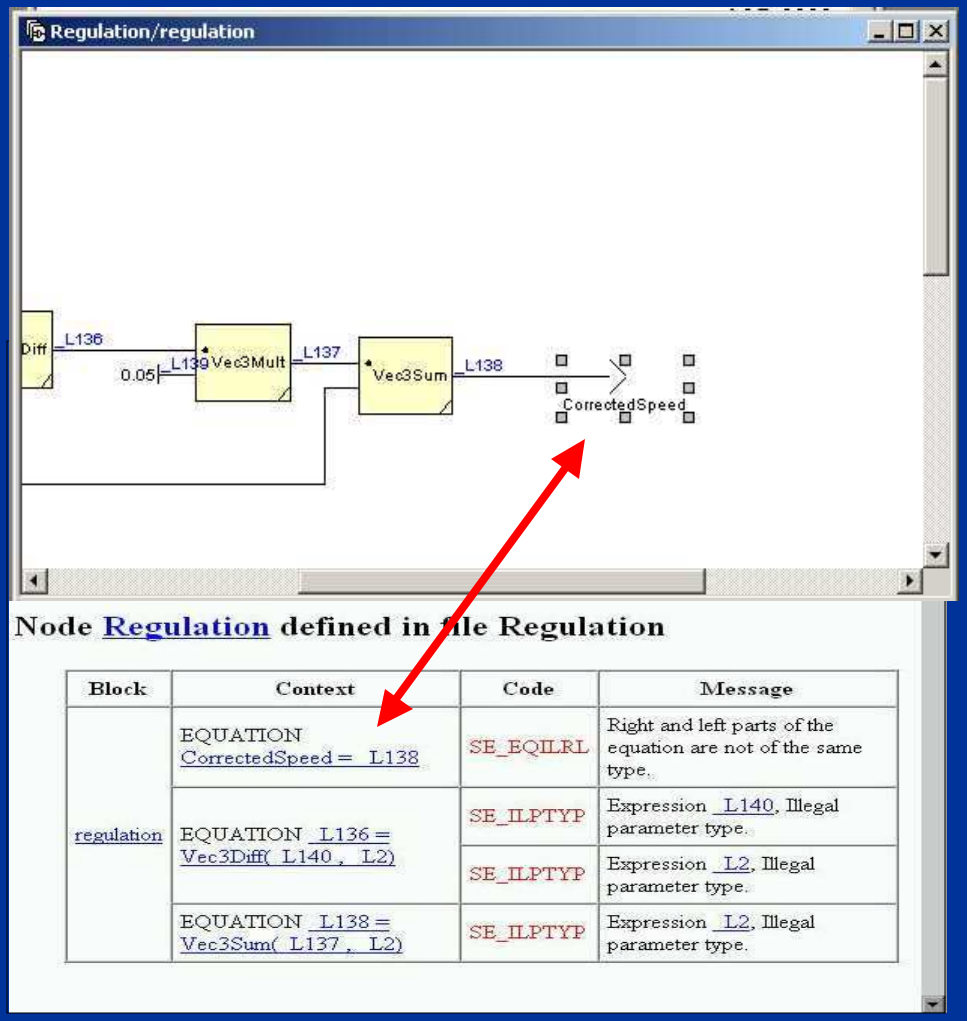
- Verification activities pulled up onto the model level
- Static semantical checks on the model
- Formal proof applied directly on the model to directly verify safety relevant functionality with respect to safety requirements
- Software- in the loop simulation, can be tailored to various test requirements in order to execute a variety of dynamic tests
- Model- level test coverage measurement and analysis

- Trusted and certified translation to C- code by SCADE KCG

Esterel Technologies Confidential

Software Verification/ Validation with SCADE/ Editor

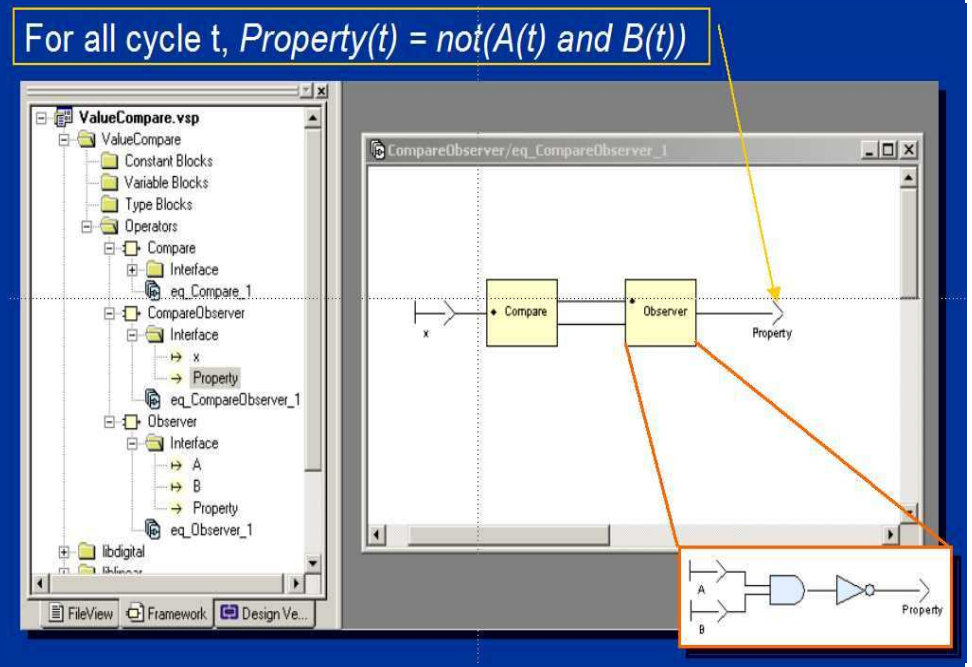
- well established block diagram/ state machine notation
- Direct editing of formal model
- Semantic checks on standard or user rules
- Extensible MMI and API
- Support of software- engineering standards (structure, hierarchy, encapsulation, modularization, configuration/ change management…



Esterel Technologies Confidential

Software Verification/ Validation with SCADE/ Design Verifier

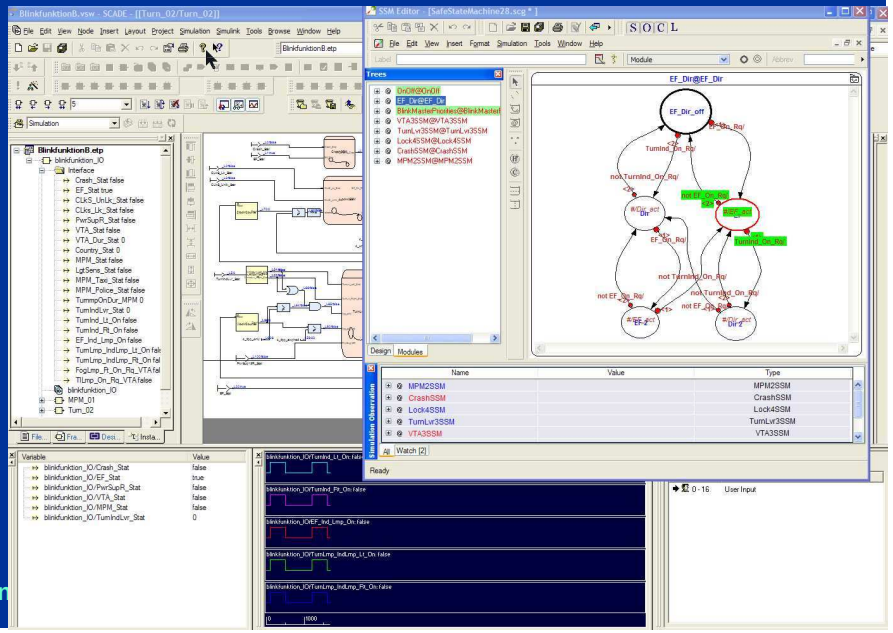
- Model Checking
  The design can be checked for functional safety requirements compliance
- A specification or implementation can be formally checked to always fulfill a given safety relevant requirement
- If the requirement can be proven to be falsifiable, a counter-example is produced and a simulation scenario generated for further analysis



Esterel Technologies Confidential

Software Verification/ Validation with SCADE/ Simulator

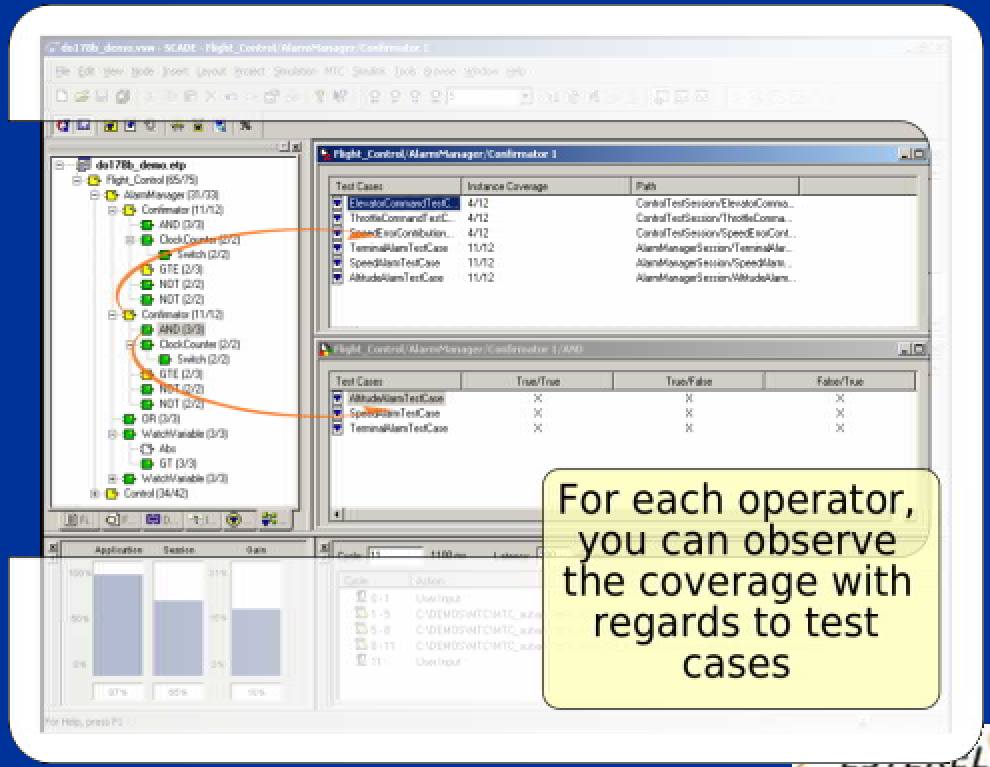
- Validation of Requirements
- Verification of Design
- White box or Black box simulation
- Software- in the loop
- Co simulation of non- SCADE libraries
- Scenario driven simulation with comparison with expected results (requirements based testing)
- Batch mode simulation
- Open API for integration in custom process



Software Verification/ Validation with SCADE/ MTC

- Extension of SCADE/Simulator
- Framework to systematically execute predefined test cases relevant to functional safety requirements
- Provides detailed, tunable coverage measurement capabilities
- Powerful tools to analyze the cumulated coverage data
- Powerful reporting, ensuring validation of tests and verification of model

- Input:
  - Model
  - Requirements based test scenarios (SCADE format, can be linked to DOORS)
- Output:
  - Detailed test and coverage report, mapping functional safety requirements to coverage data



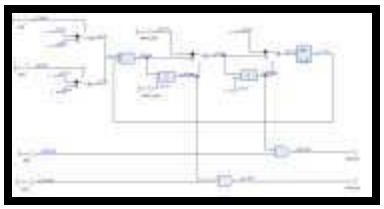
Esterel Technologies Confidential

Automatic Code Generation with SCADE/KCG

- The SCADE/KCG Automatic C Code Generator is about to be certified as a software development tool by TÜV for safety relevant applications according to IEC 61508
- When a code generator is certified
  - *The conformance of the code to the input model is trusted*
  - *The verification activities related to the coding phase can be eliminated*
- Certification requires that the tool has been developed with the same safety objectives as the code it generates
  - *For SCADE KCG, it is SIL4*
- A Certification Kit is available in order to facilitate the certification process on customer's projects

Esterel Technologies Confidential

Software Verification/ Validation with a certified OS



SCADE
KCG

code that has to be traditionally verified

user code

certified/
validated
SCADE
OS_config
tool

generated code

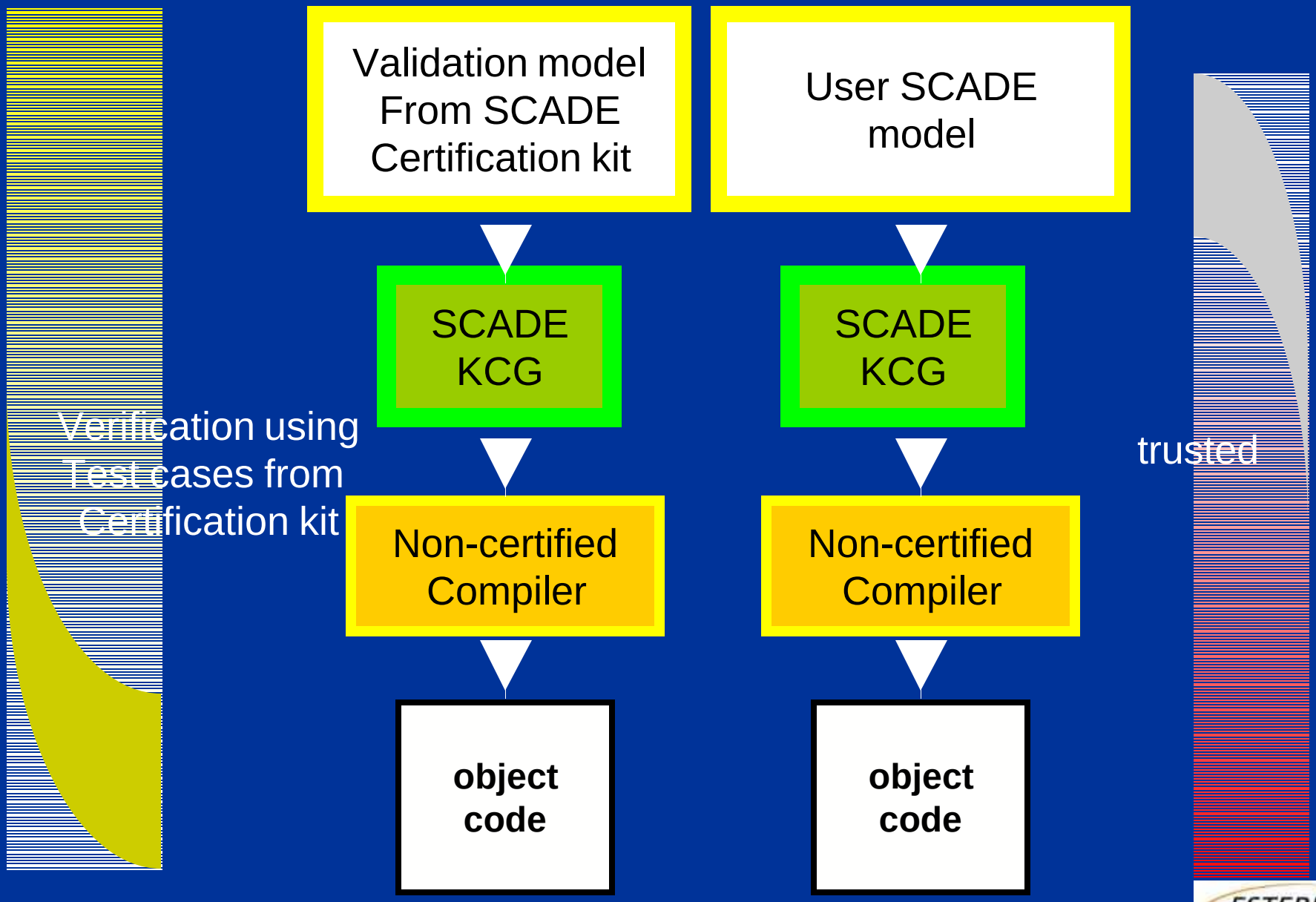
SCADE library code

Safety layer

code that is certified

Esterel Technologies Confidential

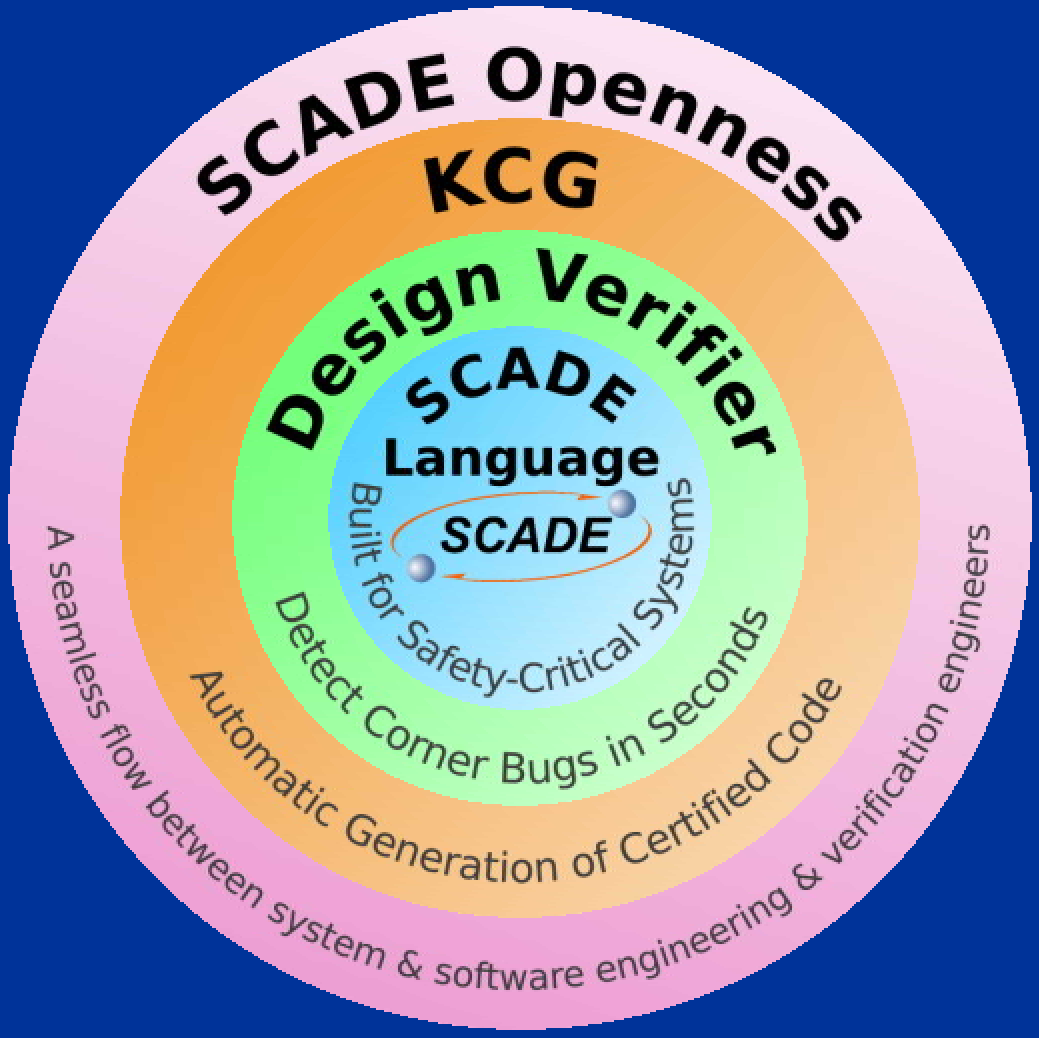
Software Verification/ Validation source code to object code



Esterel Technologies Confidential

This watermark does not appear in the registered version - http://www.clicktoconvert.com

SCADE Properties: Agenda



Central place in the Software Development Cycle

Esterel Technologies Confidential

SCADE Language: Built for Safety-Critical Systems

Graphical Formal Language

- The interpretation of a SCADE model does not depend on the reader or on a tool
- Definition was achieved in close connection with its early industrial users and certification authorities in the aeronautics & nuclear energy domains: Airbus & Schneider Electric

Esterel Technologies Confidential

SCADE Language: Built for Safety-Critical Systems

Graphical Formal Language

Language Modularity

- A SCADE node is modular (readable, maintainable, reusable).
- A SCADE node is a functional module, defined by
  - A formal interface
  - A set of local variable declarations
  - A set of equations to describe the behaviour
- The behaviour of a node does not depend on its context.

Esterel Technologies Confidential

SCADE Language: Built for Safety-Critical Systems

Graphical Formal Language

Language Modularity

Strong Typing

- The SCADE language is strongly typed, which is a mandatory constraint for safe SW development
  - Predefined types
  - Enumerated types
  - Structured types
  - Imported C/ADA types
- Type consistency is verified by the SCADE tools

Esterel Technologies Confidential

SCADE Language: Built for Safety-Critical Systems

Graphical Formal Language

Language Modularity

Strong Typing

Safety Checks

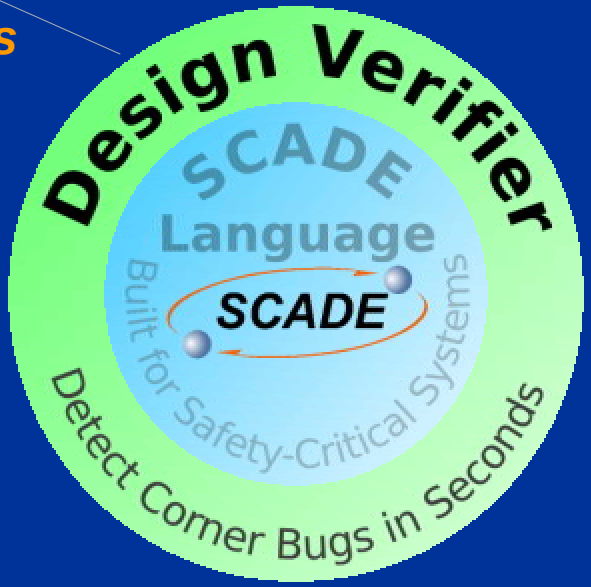
- SCADE is a modelling language that enforces safety rules
  - Strong typing
  - No recursion in data flows
  - No recursion in node calls
  - Consistency of clock propagation
- These rules are exhaustively verified by the different Check functions of the Editor
- Syntactic check
  - Completeness (no unconnected wire)
- Semantics check
  - Type-checking (eg, not adding a Boolean and an integer)
  - Cycle detection (no immediate recursion)

Esterel Technologies Confidential

Design Verifier: Detect Corner Bugs in Seconds

Checks high and low level safety property requirements

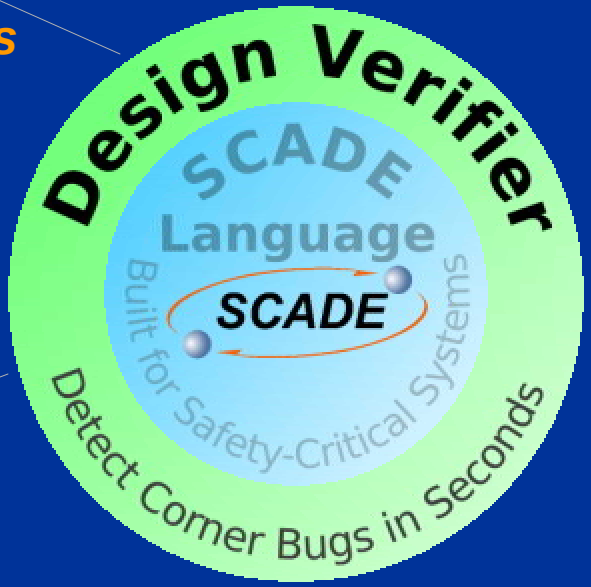
- 100% exhaustive & automatic analysis
- Very simple property definition



Esterel Technologies Confidential

Design Verifier: Detect Corner Bugs in Seconds

Checks high and low level safety property requirements



Detect Corner Bugs in Seconds

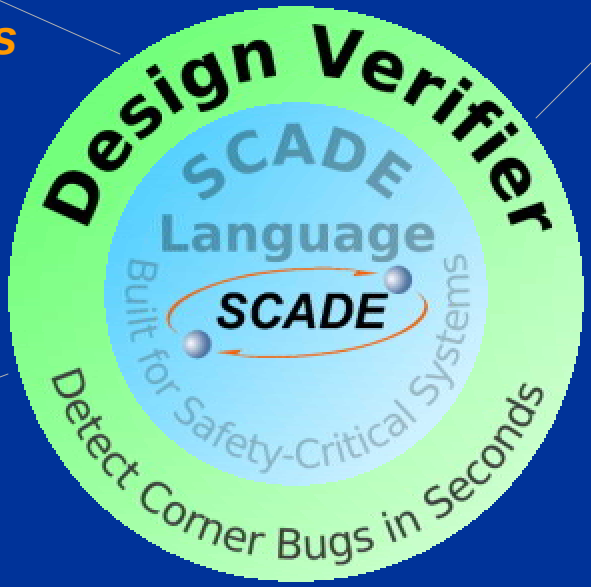
- Early detection of bugs without writing any verification tests
- Counter-example test generation for detected bugs

Esterel Technologies Confidential

Design Verifier: Detect Corner Bugs in Seconds

Checks high and low level safety property requirements

Detect Corner Bugs in Seconds



Properties proved on several real industrial projects

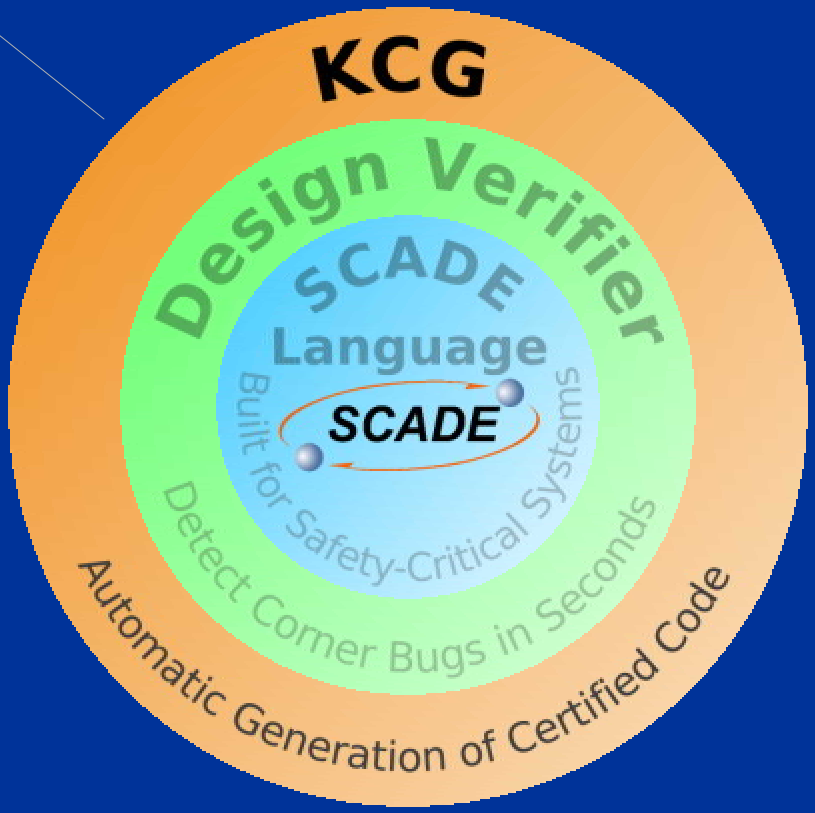
- Aerospace & Defence
  - flight control application, sensor voter algorithms (Airbus, HCL India, Dassault Aviation, Honeywell)
- Automotive embedded applications
  - AUDI, PSA, Johnson Controls, Delphi

Esterel Technologies Confidential

KCG: Qualified/ Certified C Code Generator

DO-178B Qualified/ IEC61508 certified C Code Generator

- Only model-based code generator in the world qualified for DO-178B Level A
- Only model-based code generator in the world certified accordingly to IEC 6 1508 for all SIL levels



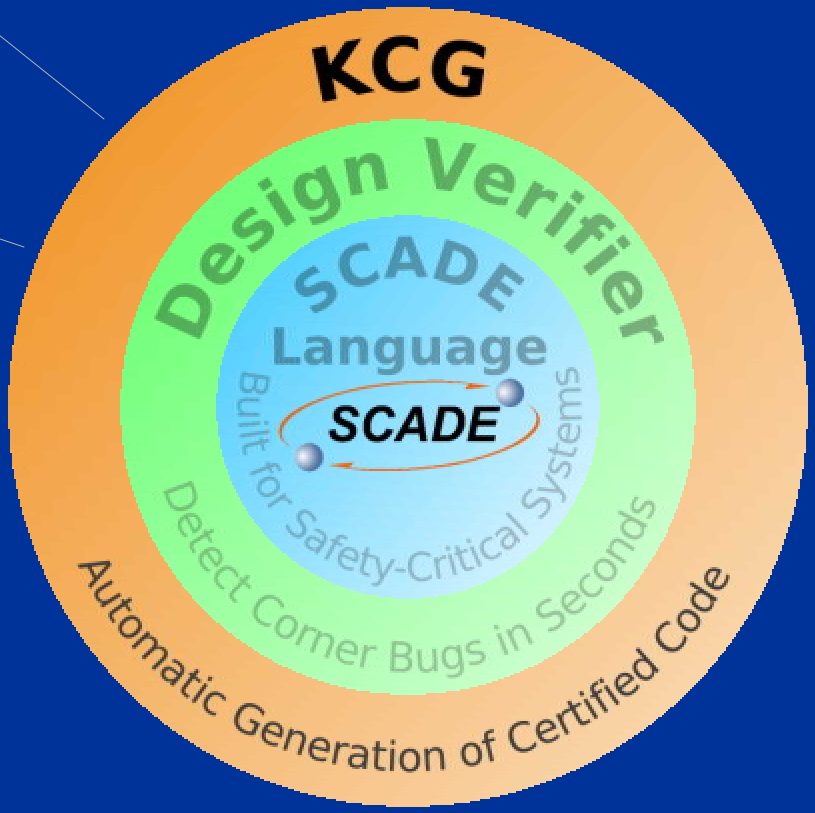
Esterel Technologies Confidential

KCG: Qualified/ Certified C Code Generator

DO-178B Qualified/ IEC61508 certified C Code Generator

Predictable Execution Time

- Safe control structures
- Linear control sequences
- No loops, no recursion, no jumps



Esterel Technologies Confidential

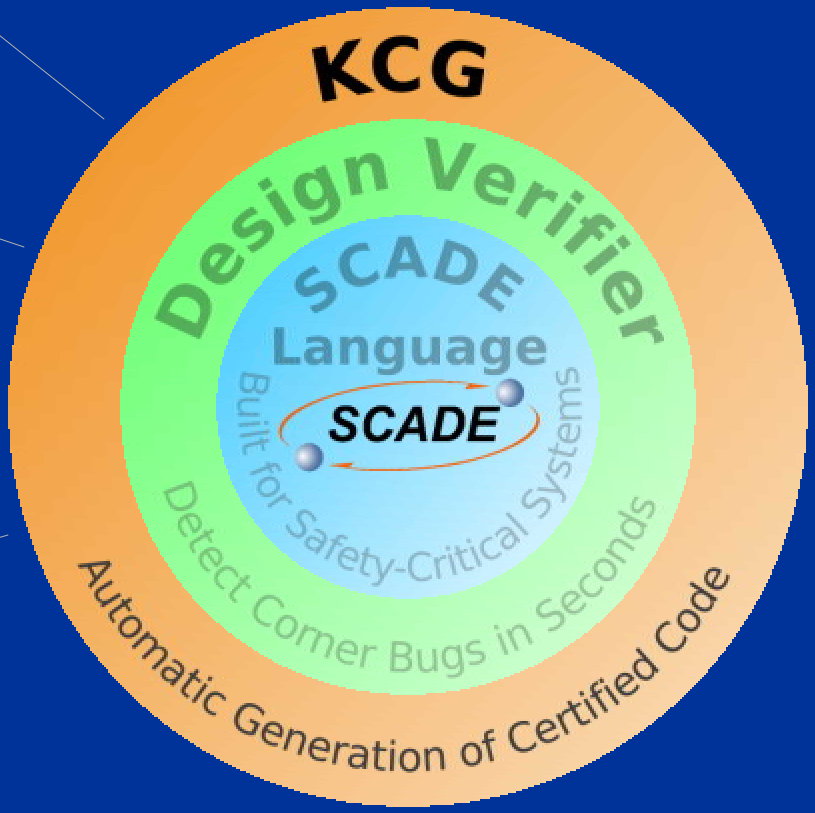
KCG: Qualified/ Certified C Code Generator

DO-178B Qualified/ IEC61508 certified C Code Generator

Predictable Execution Time

Data Integrity Guaranteed

- Safe data structures
- No dynamic variables
- Fully static memory allocation



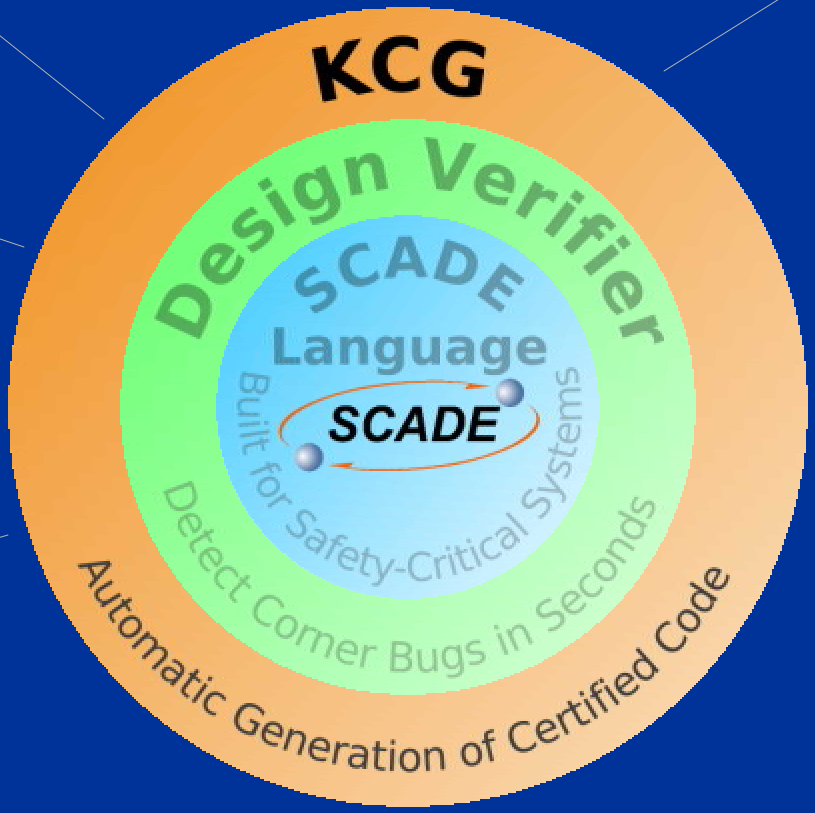
Esterel Technologies Confidential

KCG: Qualified/ Certified C Code Generator

DO-178B Qualified/ IEC61508 certified C Code Generator

Predictable Execution Time

Data Integrity Guaranteed



Traceability

- The source C code generated by KCG is fully traceable with respect to the corresponding SCADE model

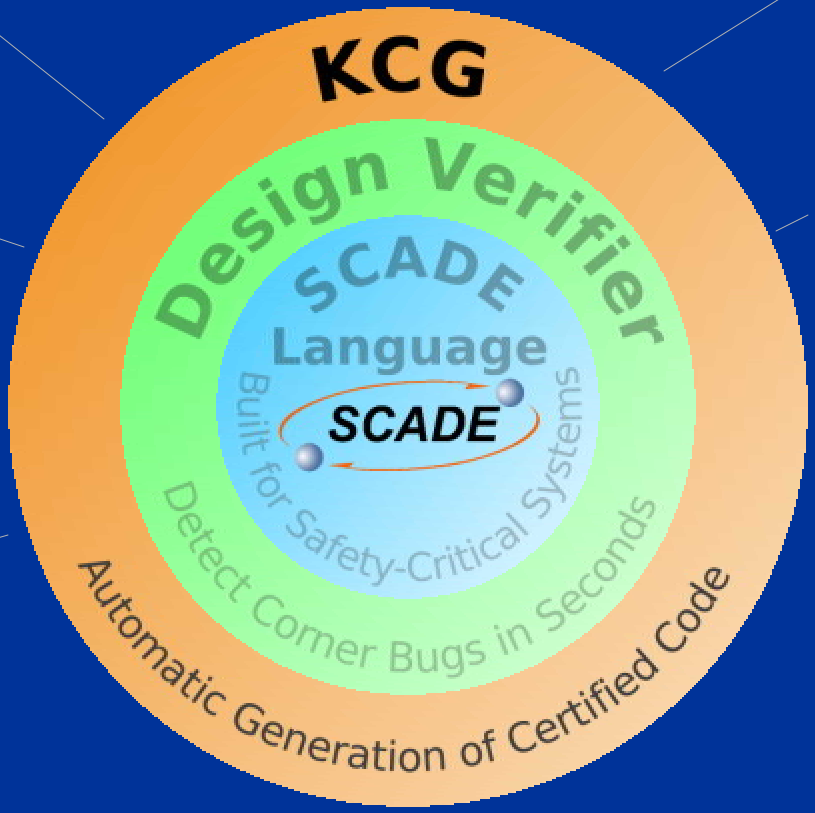
Esterel Technologies Confidential

KCG: Qualified/ Certified C Code Generator

DO-178B Qualified/ IEC61508 certified C Code Generator

Predictable Execution Time

Data Integrity Guaranteed



Traceability

Costs Dramatically Reduced

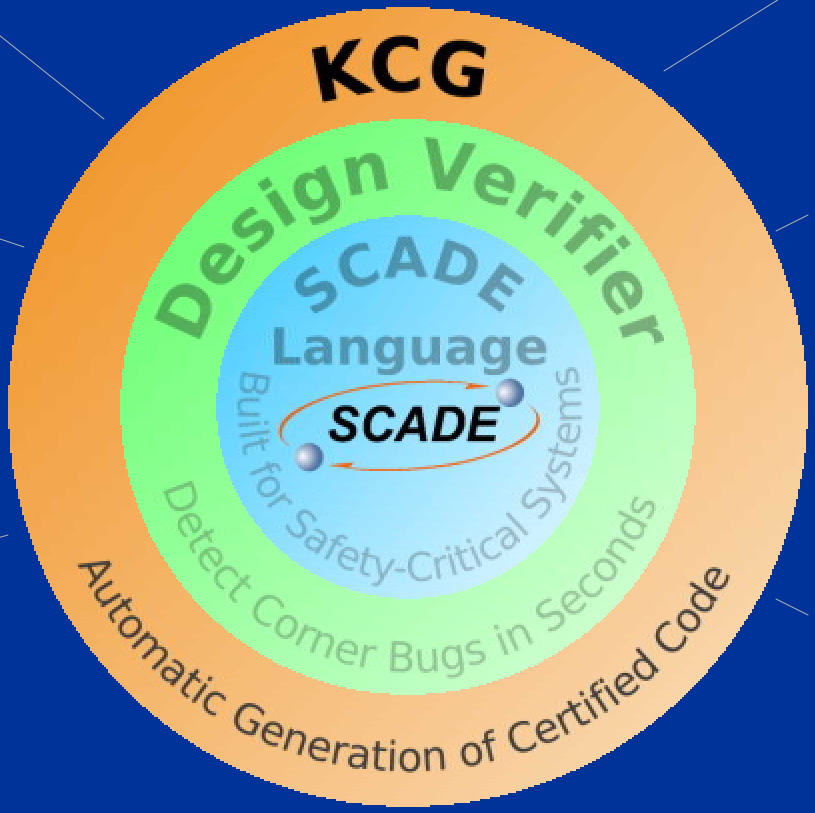
- Reduces up to 50% of the coding and testing phase costs
- *"With SCADE, integrating modifications in a new version has now become possible in 24 to 48 hours."* (source Eurocopter)
- KCG Qualification Kit saves much of the testing and re-reading effort required by DO-178B certification programs

Esterel Technologies Confidential

KCG: Qualified/ Certified C Code Generator

DO-178B Qualified/ IEC61508 certified C Code Generator

Traceability



Predictable Execution Time

Costs Dramatically Reduced

Data Integrity Guaranteed

Rooted in 10 Years of Successful Industrial Applications

- Efficiency has been proven on many production projects in all relevant industries
- No coding error ever found in code generated with SCADE

Esterel Technologies Confidential

Central Place in the Software Development Cycle

DOORS Link

- Requirements Management
- Traceability

Simulink Gateway

- Algorithm Design Capture

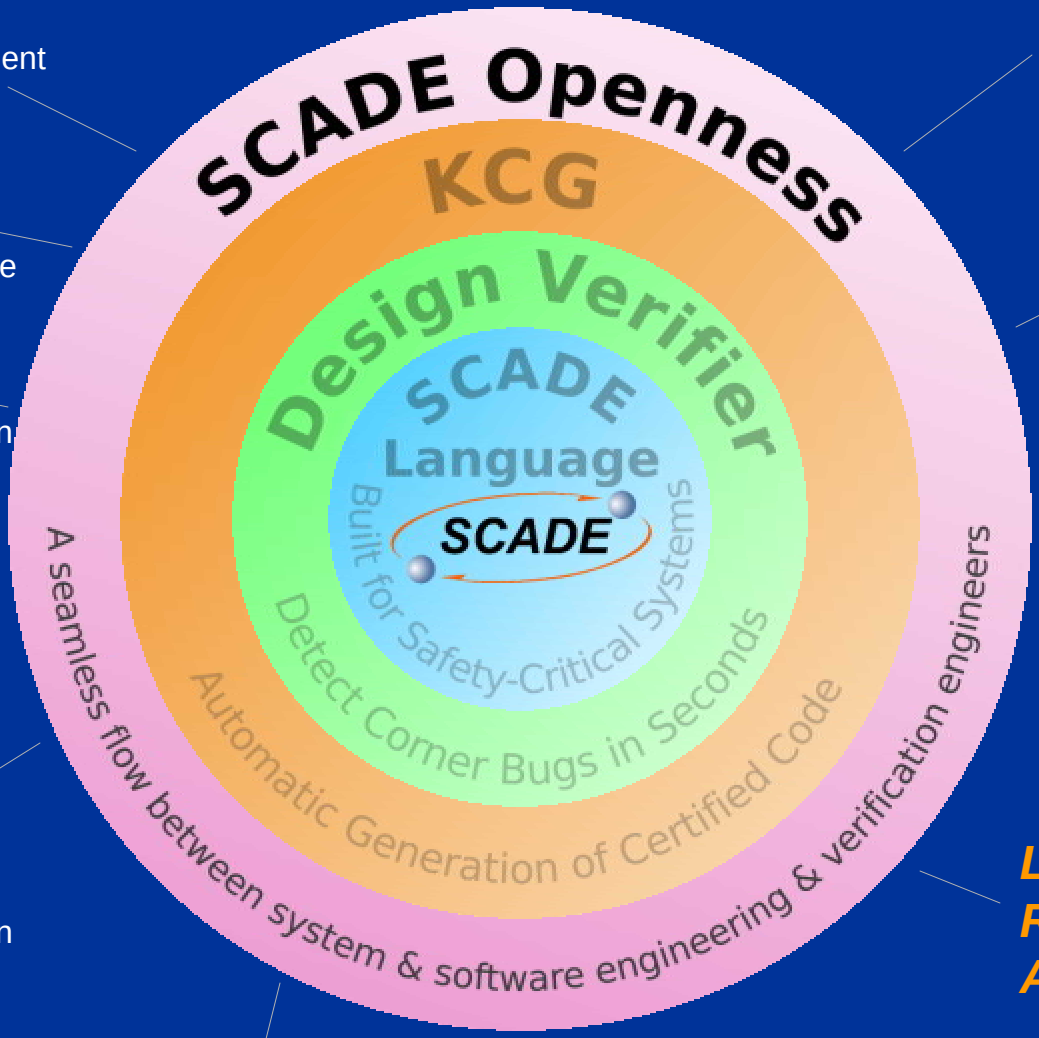
SCCI Gateway

- Interface to Configuration Management tools

UML Gateway

SCADE Editor

- Model based Application SW Specification, Design Editor & Documentation Generator with Completeness & Consistency Checking



KCG

- Automatic Qualified C Code Generation

SCADE Simulator

- Functional Simulation
- Visual Debugging

Design Verifier

- Formal Validation of System Properties

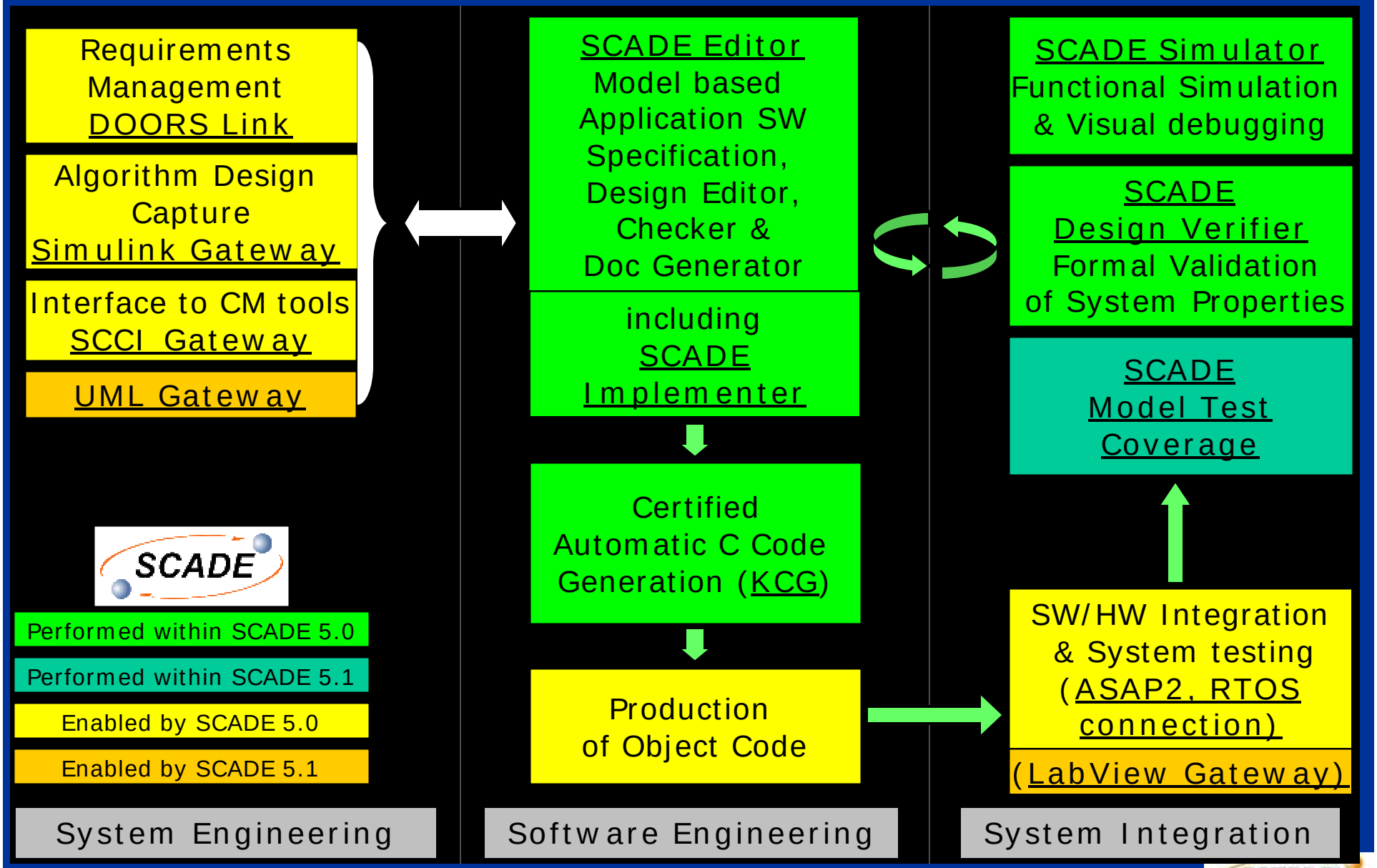
SCADE Model Test Coverage

LabVIEW Gateway, RTOS connection, ASAP2

- SW/HW Integration & System testing

Esterel Technologies Confidential

Central Place in the Software Development Cycle



Esterel Technologies Confidential

Thank You For Your Attention

Info.de@esterel-technologies.com

Esterel Technologies Confidential

Glossary of Terms

E/E/PES	Electric/ Electronic/Programmable Electronic System
EUC	Equipment under control
DV	Design Verifier
HR	Technique or measure is Highly Recommended for given SIL
KCG	SCADE Certified Code Generator at IEC 61508 SIL 4
M	Mandatory according to EN requirements for railway applications
NR	Technique or measure specifically Not Recommended for SIL
OSEK/VDX	Offene Systeme für Elektronik im Kraftfahrzeug/ Vehicle Distributed Electronics
R	Technique or measure is Recommended for given SIL
SIL	Safety Integrity Level
SCADE	Safety Critical Application Development Environment
SSM	Safe State Machines: SCADE implementation of finite state machine notion
WCET	Worst Case Execution Time Analysis

Esterel Technologies Confidential

AIRBUS Success

Photo courtesy of AIRBUS

- Since the 1990's a pioneer in automated code generation
- SCADE Suite™ KCG Code Generator used for the A340/600 secondary flight control system
- Measured Results
  - *SCADE Suite™ → 70% of the code*
  - *No coding error ever found in the code embedded from SCADE Suite™*
  - *Development costs reduced by 50%*
  - *Specifications changes & modified code were more quickly available. A repeatable reduction by a factor of 3x to 4x of the code modification cycle*

DO 178 B
level A
CERTIFIED

Esterel Technologies Confidential

EUROCOPTER Success

- World leader in civilian helicopters
- Introduced SCADE Suite™ for the development of the EC135 and EC155 autopilots

Photos courtesy of EUROCOPTER

- Results
  - *SCADE Suite™ → 90% of the code*
  - *Development time reduced by 50%*
  - *JAA certified the equipment at level A (8 certifications performed for: EC155, EC135, EC145; EC225 on-going)*

DO 178 B level A CERTIFIED

Esterel Technologies Confidential