Powering Innovation That Drives Human Advancement

Model-Based Solution for Embedded Controls of the Future

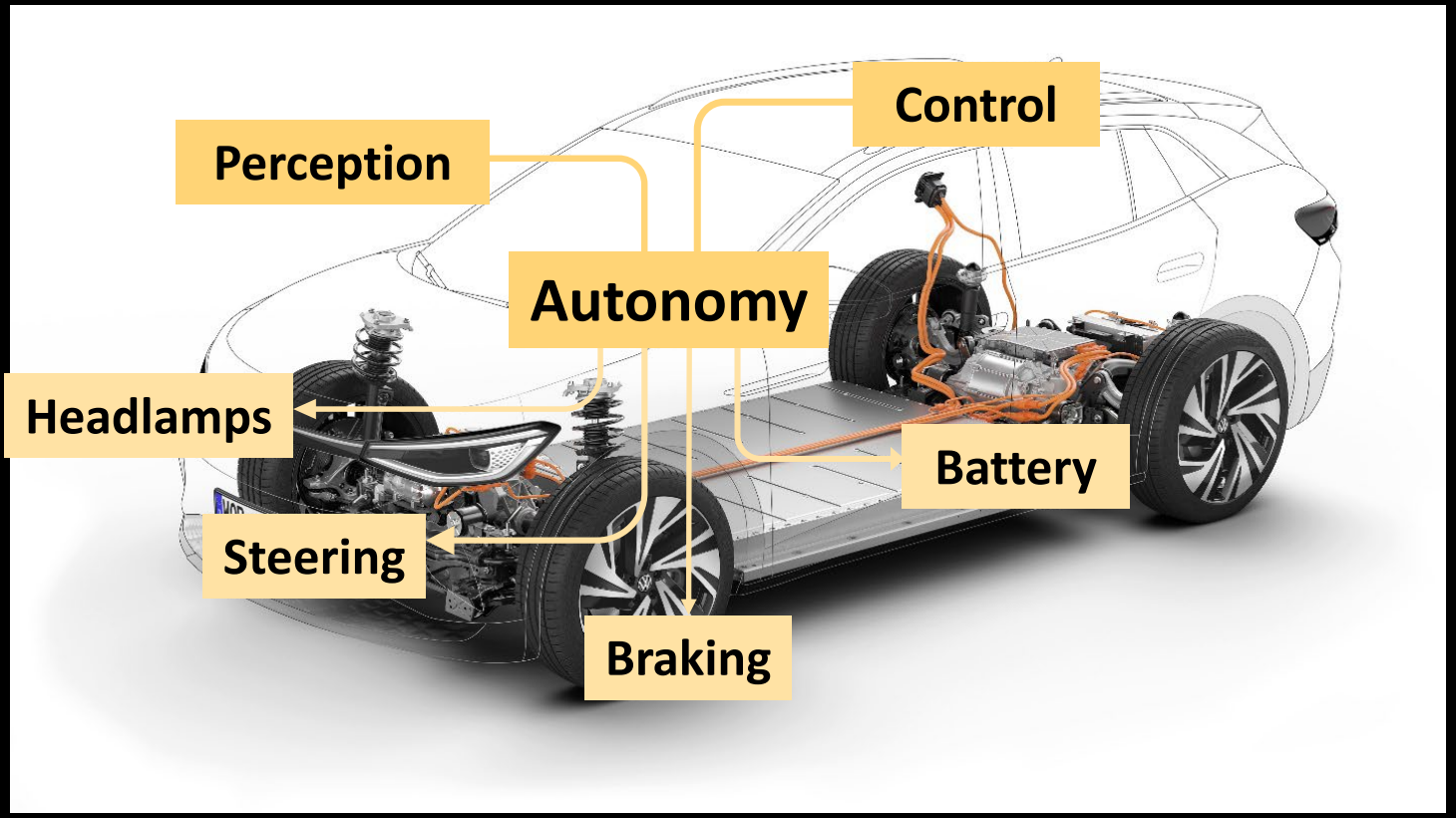
Christian Schrader
Global Technical Lead Automotive

Oct 16, 2024

From Fail-Safe to Fail-Operational Systems: Challenges

Fail-operational demands driven by **automotive autonomy (SAE 3+)**

Autonomy & Electrification as drivers towards higher ASIL (HW and SW)



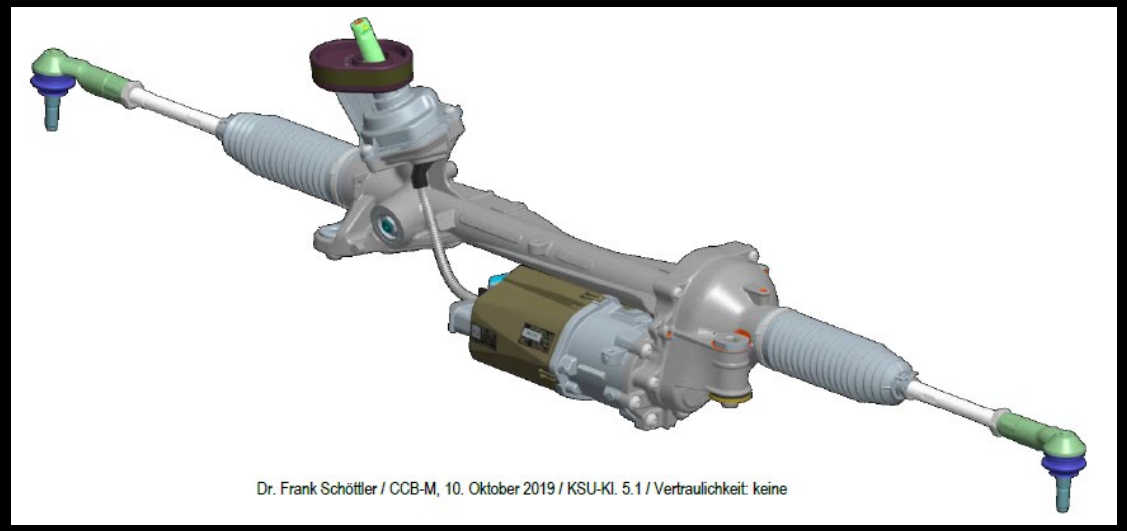
Fail-operational demands driven by **automotive autonomy (SAE 3+)**

"A **fail-safe system** relies on the human as part of the safety concept to maintain a degraded level of control to be able to stop the vehicle in the event of a failure."

"A **fail-operational system** is designed to maintain normal operation, even in the event of a system fault."

	Previous Gen		Current Gen		Next Gen	
	FAIL SAFE		**SAFETY AND AVAILABILITY**		**FAIL OPERATIONAL**	
	Detect fault Indicate fault to safe state system		Detect fault Indicate fault to safe state system and recover		Detect fault Indicate fault to safe state system	
	Stop operation		Continue operation Continue degraded Stop operation		Continue full operation	
SAE Levels of Driving Automation	**0** – No Adas	**1** – Feet off	**2** – Hands off	**3** – Eyes off	**4** – Mind off	**5** – No driver
	Human driver is driving			Upon system request Human driver is driving	System is driving	
	Driver support features			Automated driving features		

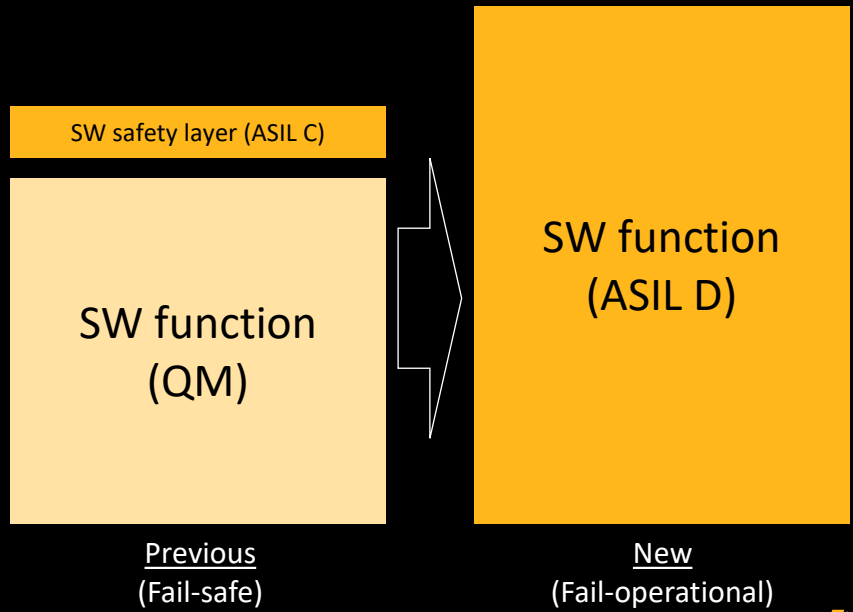
Transition to **fail-operational automotive** systems



Volkswagen

Customer challenges

- **VW** is developing a **new Electrical Power Steering Platform**
  - SAE **Level 3+** (SAE **Level 2** in previous steering generation)
  - ASIL D fail operational (no ASIL + fail safe in previous steering generation)
- New approaches required to cope with **increased complexity**
  - **Change** in strategy from developing a system with **cut-off mechanism** towards a system **that guarantees availability** demanded by autonomous driving functions
  - Towards full model-based toolchain **from systems to SW level**

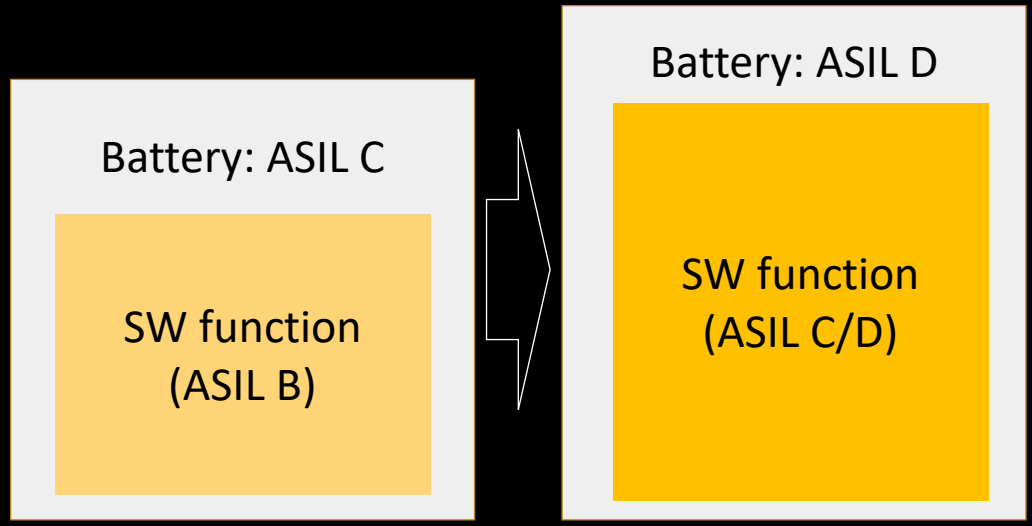


Transition to **fail-operational automotive** systems

Volkswagen

Customer challenges

- **VW** is developing **Battery Management System** (BMS) for next generation electric and ADAS/autonomous vehicles
- Toolchain maintenance consumes a significant amount of **engineering bandwidth** every year
  - Version stability, checks on model level and code level for safety violations etc.
- **Autonomous Driving** requirements at the vehicle level trigger a shift from ASIL B to ASIL C and D for the BMS Software
  - Combined with **fail-operational availability** demands
- These requirements trigger increase of **workload in verification and validation, reviews, compliance to A-Spice etc.**



From Fail-Safe to Fail-Operational Systems: Solution

A solution rooted in **commercial aerospace and defense** (A&D)

Eurocopter – EC 135/155 Autopilot DO-178B DAL A Certification (1999)

Flight Control Systems

- Autopilots
- Air Data and Inertial Reference
- Flight Control / High Lift / Slat&Flaps
- High Lift Hydraulic Control System
- Activ

Cockpit & Avionics

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

Thales Aerospace – Airbus A350 Cockpit Display System (1st flight 2013)

All of these systems are **fail-operational!**

GE Aviation – LEAP engine FADEC for Airbus A320 Neo, Boeing 737 Max, COMAC C919 (1st flight 2016)

Engine Control Systems

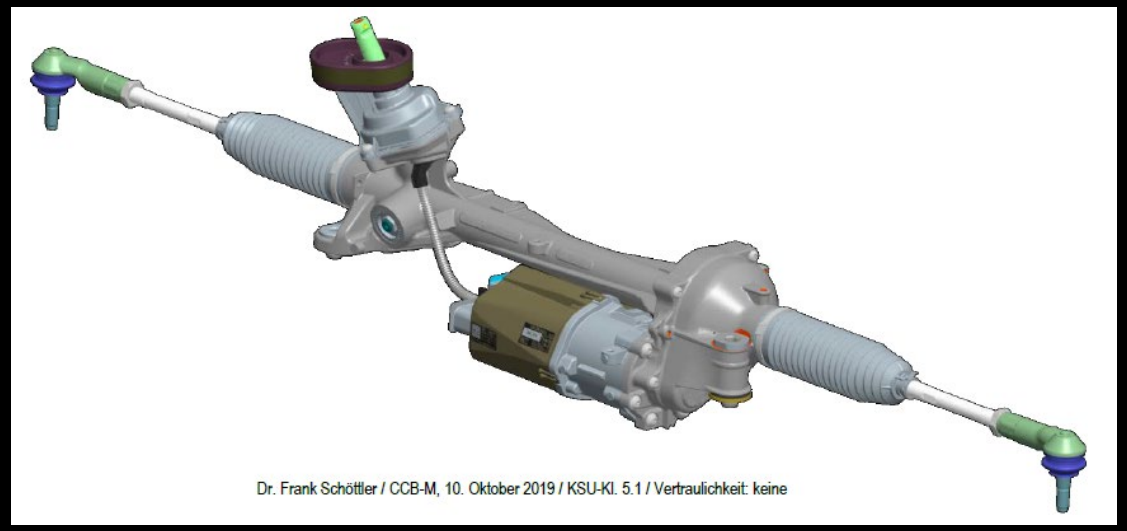
- Engine Control (FADEC)
- Nacelle Controls
- Thrust Reversers
- Electric Engines
- Hydrogen Engines

Control Systems

- Fuel Management
- Power Management
- Auxiliary Power Units (APU)
- Anti-Icing
- Braking and Landing Gear
- Hydraulic Controls
- Air & Cabin Controls

Meggitt – Brake Control System for Dassault Aviation Falcon 7X and Embraer Phenom 100

… supporting transition to **fail-operational automotive** systems



Volkswagen

"Integration time going down from 6 weeks to 2 days. Testing time going down from 16 weeks to 4 weeks. System is completely ASIL-D certifiable."

Learn More

Customer challenges

- **VW** is developing PPE - a **new Electrical Power Steering Platform**
  - SAE **Level 3+** (SAE **Level 2** in previous steering generation)
  - ASIL D fail operational (no ASIL + fail safe in previous steering generation)
- New approaches required to cope with **increased complexity**
  - **Change** in strategy from developing a system with **cut-off mechanism** towards a system **that guarantees availability** demanded by autonomous driving functions
  - Towards full model-based toolchain **from systems to SW level**

Key Results with Ansys

- System is completely **ASIL-D certifiable**
  - With fully **ASIL D qualified end-to-end** toolchain: code generation, testing, reporting, Autosar integration
- Testing and review activities **on model level**
  - No **back-to-back** testing, source **code reviews**
  - Integration time going down **from 6 weeks to 2 days**
  - Testing time going down **from 16 weeks to 4 weeks**
- Smooth **integration** between requirements management, architecture and functional SW design

... supporting transition to **fail-operational automotive** systems

Volkswagen

Fast and safe transition from fail-safe and ASIL B battery management SW to fail-operational and ASIL C

Learn More

Customer challenges

- **VW** is developing **Battery Management System** (BMS) for next generation electric and ADAS/autonomous vehicles
- Toolchain maintenance consumes a significant amount of **engineering bandwidth** every year
  - Version stability, checks on model level and code level for safety violations etc.
- **Autonomous Driving** requirements at the vehicle level trigger a shift from ASIL B to ASIL C for the BMS Software
  - Combined with **fail-operational availability** demands
- These requirements trigger increase of **workload in verification and validation, reviews, compliance to A-Spice etc.**

Key Results with Ansys

- **Suppression of need for in-house verification tools** thanks to trustable ISO 26262-qualified generated code
- Guaranteeing **version stability** in models and code
- Improved validation activities through **fast test execution (x100), including model coverage**
- **In production (ID.3 & ID.4). 20 different projects use SCADE**. 100% of BMS SW developed using SCADE.

SCADE / The reference for Safety-Critical Embedded Software

System & Software Requirements

System & SW Architecture

Embedded Systems & Software Architecture

System Architecture

System Safety Analysis

Ansys MEDINI

System Simulation & Digital Twins

Ansys AVXCELERATE & driving simulators

Ansys TWIN BUILDER

Auto

Auto

SW Design

Prototyping & control laws

Critical Embedded Control Software

Ansys SCADE SUITE

Auto

Critical Embedded HMI Software

Ansys SCADE DISPLAY

SW Components / MiL / PiL / HiL

Simulation

Test / MiL

Auto

Auto

AUTOSAR

ASAM MEMBER

ISO 26262

MISRA

Certified Automatic Code Generation

EN 50716 SIL 3/4

DO-178C DAL A

ISO 26262 ASIL D

IEC 61508 SIL 4

C code

Auto

Embedded Control & HMI Software Testing

Ansys SCADE TEST

Platform Integration
RTOS & HW
Multi-rate / Multi-core

System Level

Application

Task Management

System Services

Micro-kernel

HW

Core 0

Core 1

Core *n*

MultiCore™

Test / PiL / HiL

Qualification level of SCADE Tools

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATE

No. Z10 055460 0027 Rev. 00

Holder of Certificate: ANSYS France SAS
15 Place Georges Pompidou
78180 Montigny-le-Bretonneux
FRANCE

Certification Mark:

Product: Software Tool for Safety Related Development

Model(s): Code Generator SCADE Suite KCG 6.6.4

Parameters: The code generator - classified as T3 offline support tool according to IEC 61508-4 / EN 50128 and TCL 3 according to ISO 26262-8 - is qualified for the use in safety-related software development according to IEC 61508, EN 50128 and ISO 26262.

The report AM101878C is a mandatory part of this certificate.

Tested according to:
IEC 61508-1:2010 (SIL 3)
IEC 61508-3:2010 (SIL 3)
EN 50128:2011 (SIL 3/4)
EN 50128:2011/A1:2020 (SIL 3/4)
EN 50128:2011/A2:2020 (SIL 3/4)
ISO 26262-8:2018 (ASIL D)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. This certificate is valid until the listed date, unless it is cancelled earlier. All applicable requirements of the testing and certification regulations of TÜV SÜD Group have to be complied. For details see: www.tuvsud.com/ps-cert

Test report no.: AM101878C
Valid until: 2028-12-07

Date, 2023-12-13

(Peter Weiß)

Page 1 of 1
TÜV SÜD Product Service GmbH · Certification Body · Ridlerstraße 65 · 80339 Munich · Germany

Everyone has something similar to this <u>at first glance</u>!

Multiple SCADE Suite and Display KCG Tool certifications by TÜV

SCADE code generator has been developed according to the highest levels of safety standards

5.3 Conclusion

Safety of **Scade-language** means that the language is scientifically proven to be completely accurate and formally defined. Safe State Machines, formerly expressed by Esterel-language, and Block Diagrams were merged into SCADE 6 language by the extension of LUSTRE-language.

Safety of **generated C/Ada code** means that unsafe C/Ada language constructs are explicitly excluded. It contains no dynamic memory allocation, no pointer arithmetic, and the only loops are bounded loops over delay buffers and over bounded arrays. It also means that the generated code behaviour complies with the model semantics.

Safety of **Code generator KCG** means that the behaviour of the generated C/Ada Code complies with the model semantics of the SCADE model. To avoid deviations between SCADE model and generated C/Ada Code, the development process of ANSYS France underlies the requirements of safety related software standards with respect to fault avoidance.

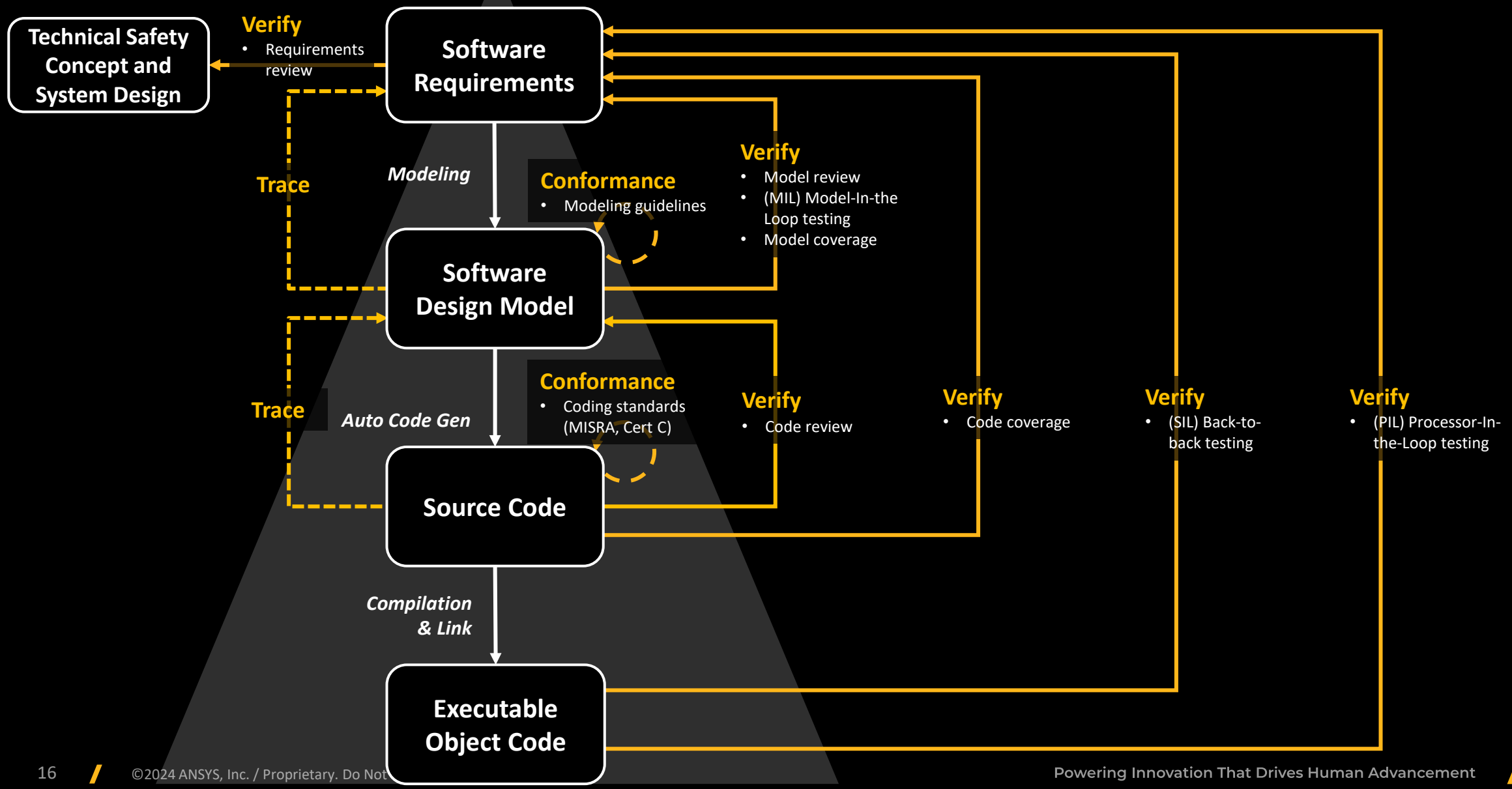
Safety of **implementation** means that the development tools used for KCG are reliable. The use of ML language and compiler has been assessed according to IEC 61508 SIL3 and EN 50128 SIL3/4. The assessment summary, provided in the technical report, concludes that the ML language and compiler with their restrictions of use are fit for the purpose of developing KCG.

Ansys SCADE is the only tool with this type of certification.

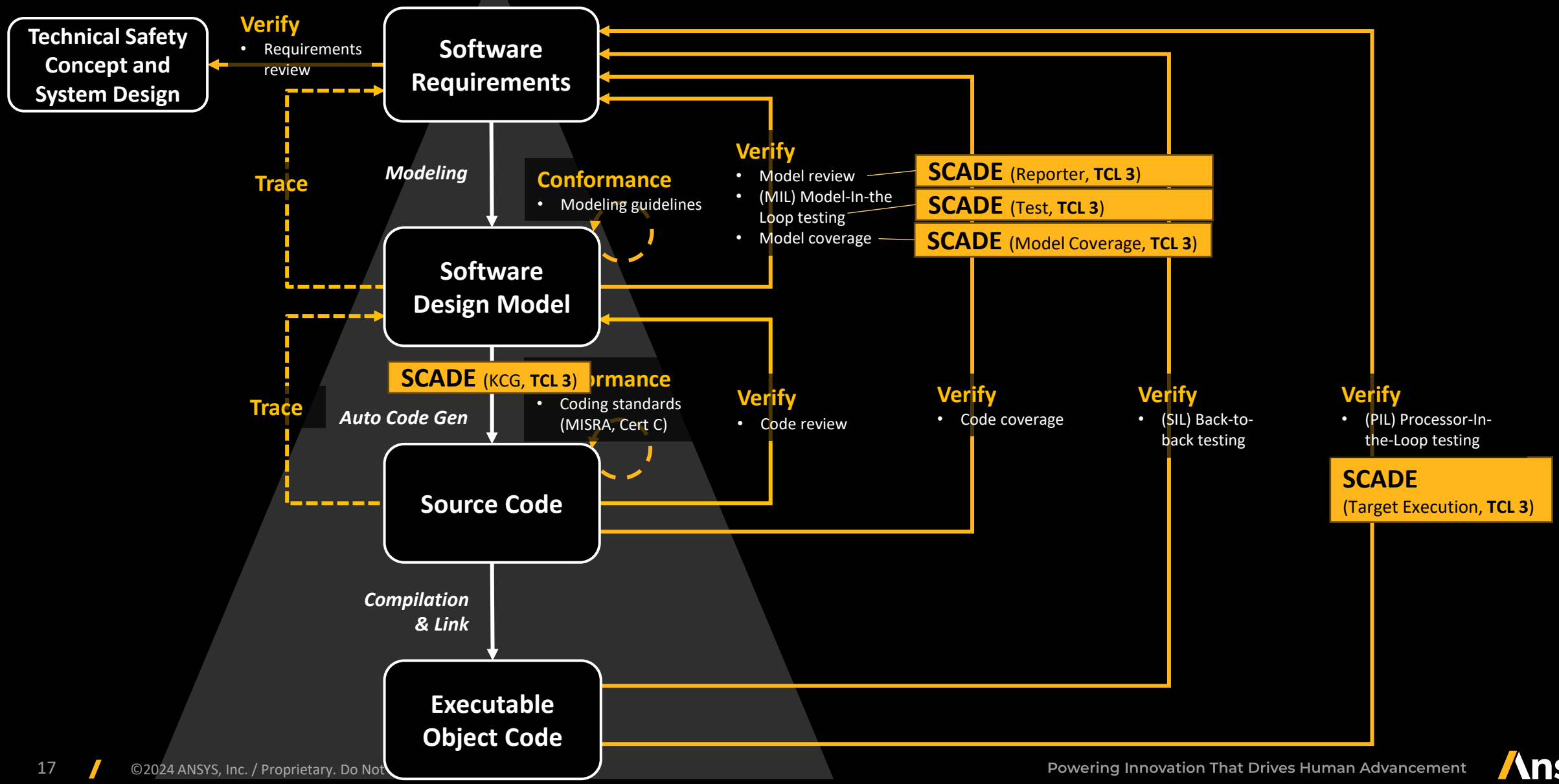
Only **full TCL3 certification** on the market (**code generator** + testing and reporting)

Benefits for the ISO 26262 process with Ansys SCADE

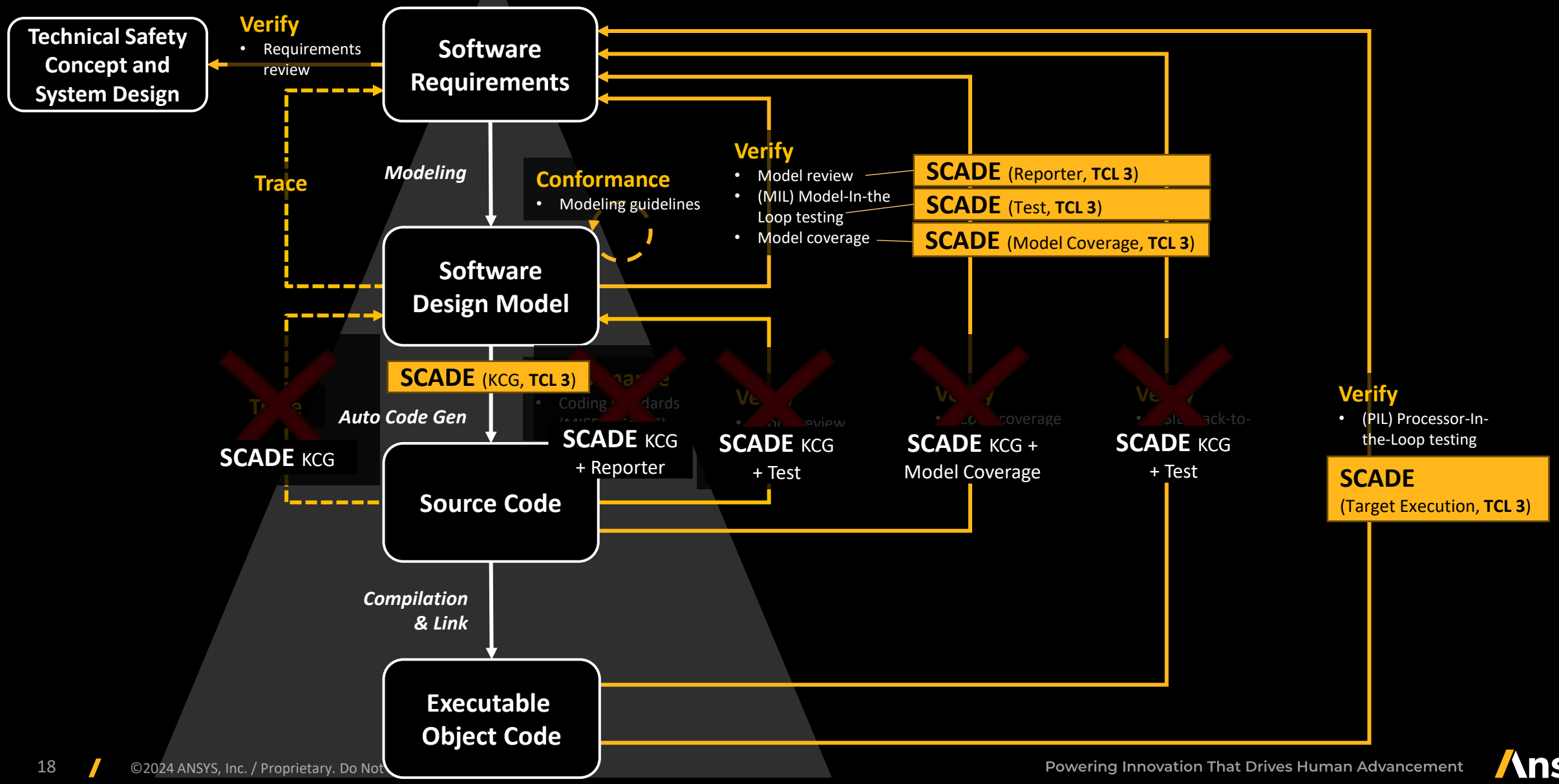
ISO 26262-6 Model-Based Software Design Workflow (Generic)



ISO 26262-6 Model-Based Software Design Workflow (with **SCADE**)



ISO 26262-6 Model-Based Software Design Workflow (with **SCADE**)



ISO 26262-6 Model-Based Software Design Workflow (with **SCADE**)

Technical Safety Concept and System Design

Verify
- Requirements review

Software Requirements

Trace

Modeling

Conformance
- Modeling guidelines

Verify
- Model review
- (MIL) Model-In-the Loop testing
- Model coverage

SCADE (Reporter, **TCL 3**)
SCADE (Test, **TCL 3**)
SCADE (Model Coverage, **TCL 3**)

Software Design Model

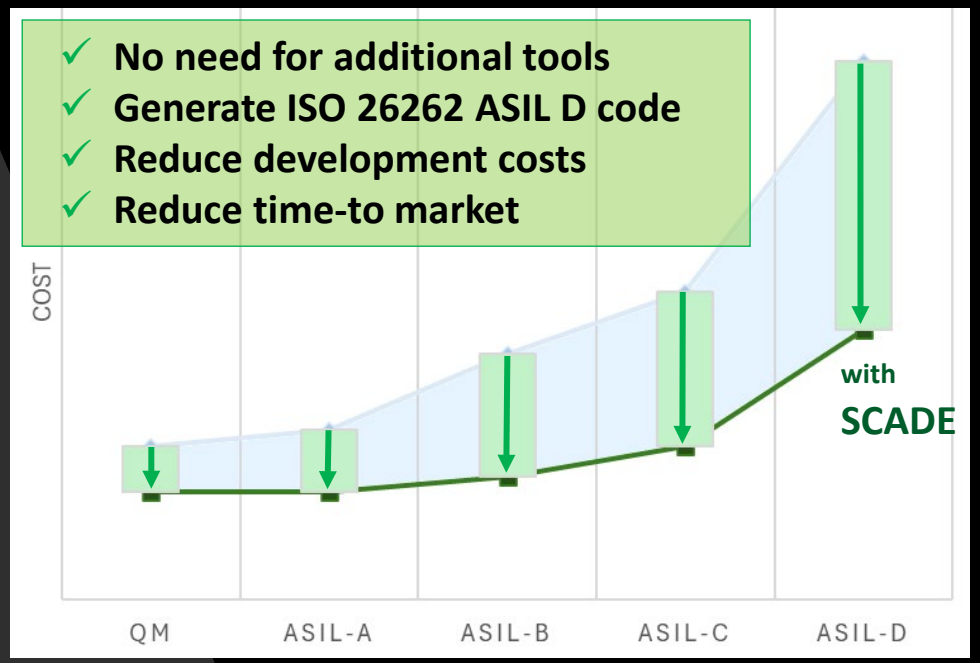
SCADE (KCG, **TCL 3**)

Auto Code Gen

Source Code

Compilation & Link

Executable Object Code

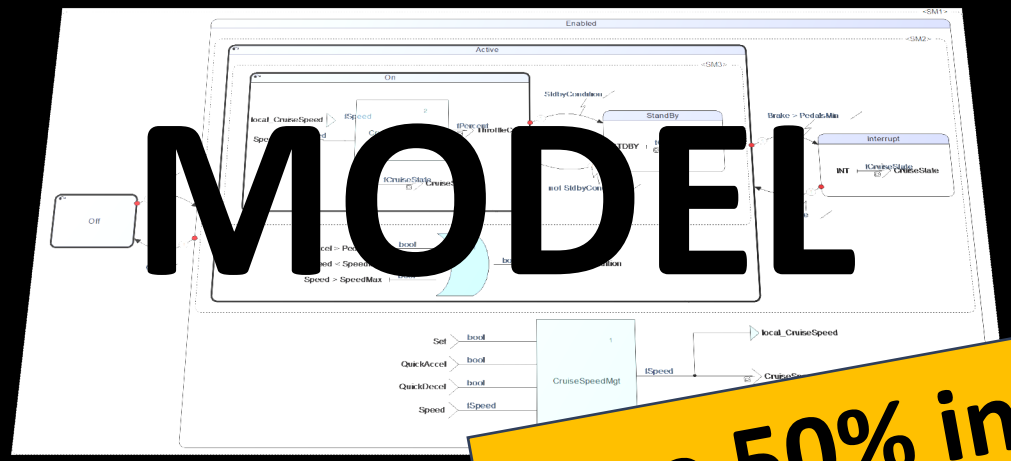


Verify
- (PIL) Processor-In-the-Loop testing

SCADE (Target Execution, **TCL 3**)

Summary

With Ansys SCADE



MODEL = CODE

```
/* Architecture::Regulation/ */
void Regulation_Architecture(
 /* ECU_Command/ */
 tECU_cmd_Architecture *ECU_Command,
 /* AccelPedal/ */
 tPercent_Architecture AccelPedal,
 /* Speed/ */
 tVehicleSpeed_Architecture Speed,
 outC_Regulation_Architecture *outC)
{
 kcg_float3
 /* SM1:Re      L3/ *
 kcg_float      L3_Re      l_SM1
 /* SM1: *
 SSM_ST_S      SM1_
 /* SM1: *
 kcg_
                                    nxt) {
                                    M1 :
                                    Command).Status == ON_Architecture;
                                    te_act = SSM_st_Regul_SM1;
 else {
  SM1_state_act = SSM_st_NotRegul_SM1;
 }
 break;
```

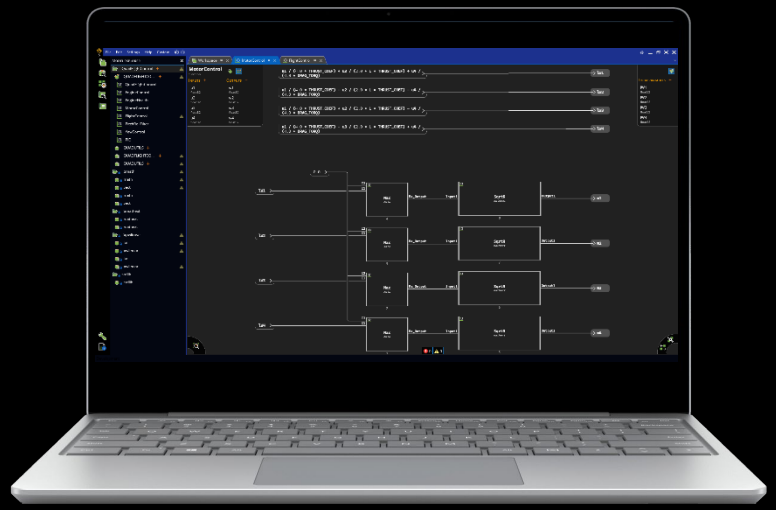
Save 50% in time and effort

- **NO NEED FOR SAFE SUBSET**
- **NO CODE REVIEWS**
- **NO SIL BACK-TO-BACK TESTING**
- **NO CODE COVERAGE**

Coming up next…

Scade One / The next generation of SCADE

Ansys
SCADE ONE



- A unified environment, for all activities
  Design | Debug | Generate | Test | Integrate
- A visual coding experience
  Efficient modeling | Auto-layout | On-the-fly-checks | User assistance
- Improved modeling and testing capabilities
  Better scalability | Simpler handling of array/matrices | Tests as models
- Democratizing model-based development
  Scade One Essential , a dedicated offering for non-certified embedded software

A Wider Scope of Applications!

In Every Mission / Safety / Cost Critical Embedded System

… and many more innovations to come
Collaboration | Full V&V workflow | Qualification | Unified HMI/Logic