Safety Critical Application and Safety Analysis in Railway Systems

ANADOLU RAYLI ULAŞIM SİSTEMLERİ KÜMELENMESİ

ARUS

numesys

NUMERICAL SYSTEMS

Systems Business Unit

Business Development Director

Tahsin ÖZTÜRK

tahsin.ozturk@numesys.com.tr

Ansys CERTIFIED ELITE CHANNEL PARTNER

Ansys is the Best Partner to Help you Achieve Your Goals in Product Development

And Numesys is the 3rd Biggest Channel Partner of Ansys in Europe, located in Turkey.

About Ansys and Numesys

anova
'Yarın için bugünden Ar-Ge'

Since 2003
+100 Engineer

numesys
NUMERICAL SYSTEMS

Since 2018
+40 Engineer

molekulas
İleri Mühendislik Hizmetleri

Since 2019
+15 Engineer

FİGES
engineering

Since 1990
+25 Engineer

Employee **65+**

Approx. Engineering Experience **8+**

5 Locations in Turkey

750+ Customer

1000+ Supported Project

Ankara
Hacettepe Teknokent

İstanbul
Turkuaz Plaza Ataşehir

İzmir
Tepekule İş Merkezi Bayraklı

Konya
Teknoloji Geliştirme Bölgesi
Innopark Selçuklu

Bursa
Green White Plaza

Agenda

- ✓ System Analysis, Simulation and Embedded Software Development
- ✓ Systems & Embedded Software Customer Testimonials
- ✓ Model-Based System Safety Analysis with medini™
- ✓ Model-Based Embedded Systems & Software Development with SCADE®

numesys
NUMERICAL SYSTEMS

System Analysis, Simulation and Embedded Software Development

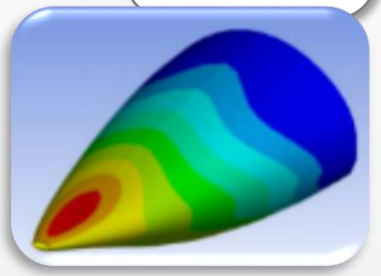
Ansys CERTIFIED ELITE CHANNEL PARTNER

ANSYS Simulation Platform Overview

- From Comprehensive Component-Level Design & Simulation …

FLUIDS

STRUCTURES



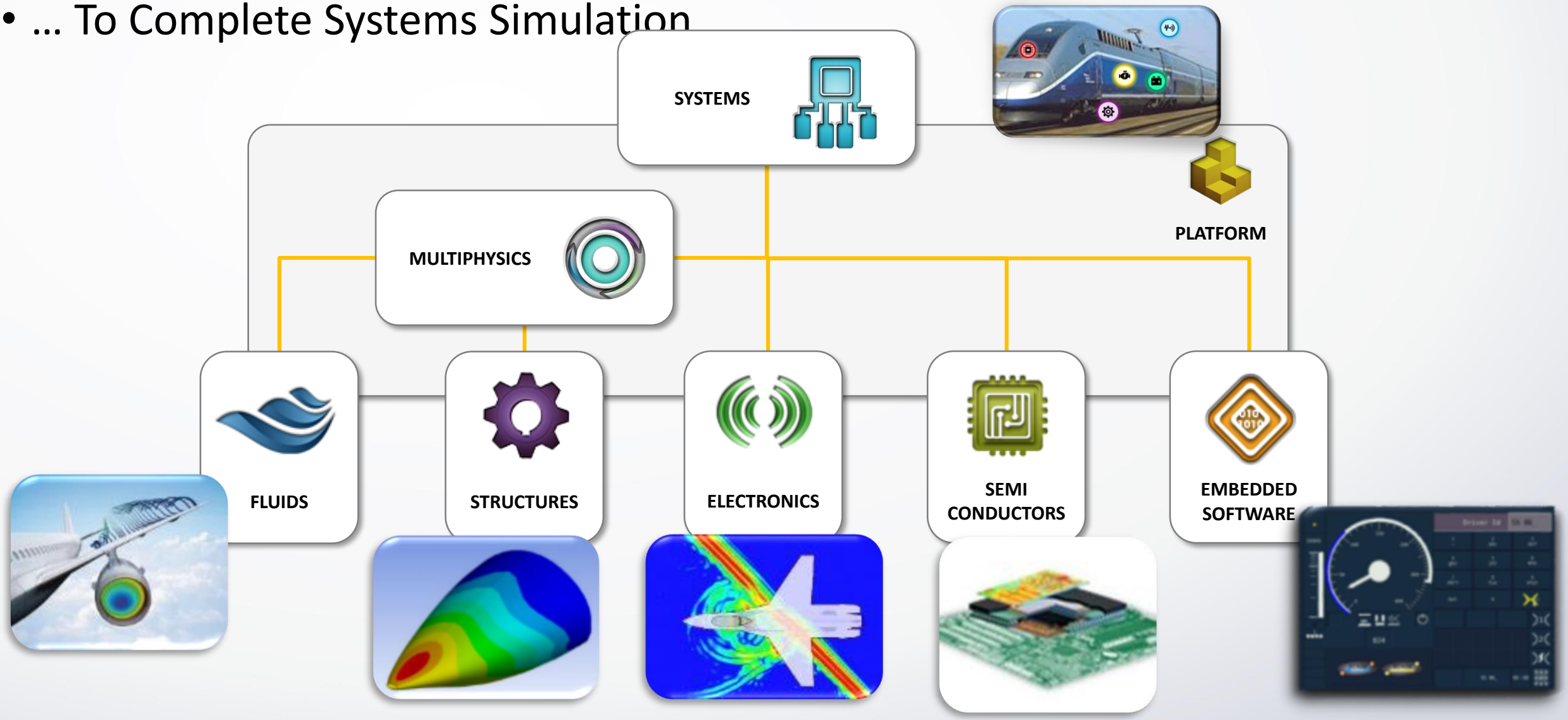
ELECTRONICS

SEMI CONDUCTORS

EMBEDDED SOFTWARE

ANSYS Simulation Platform Overview

- … To Complete Systems Simulation



Systems & Software Development Challenges

Assuring Functional Safety and Security

Managing Design Complexity

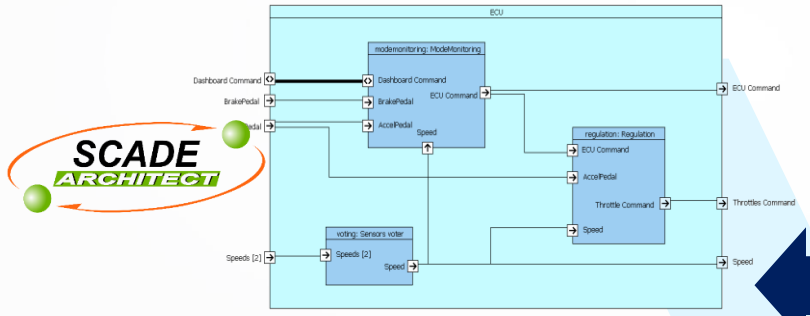
Optimizing Overall System Performance

Reducing Embedded Software Costs

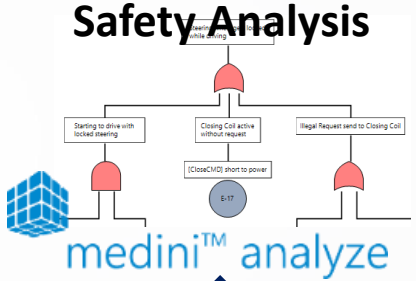
Reducing Physical Validation Costs

ANSYS Systems & Embedded Software Capabilities

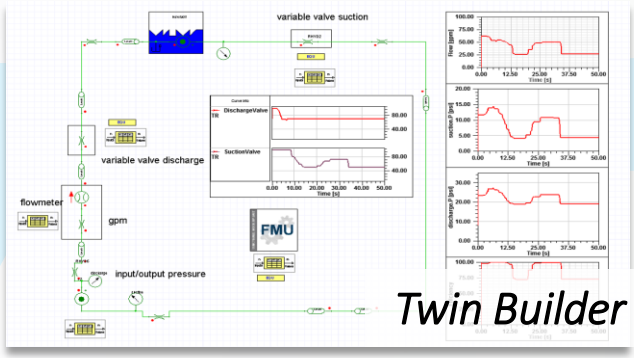
Model-Based Systems Engineering



Model-Based System Safety Analysis

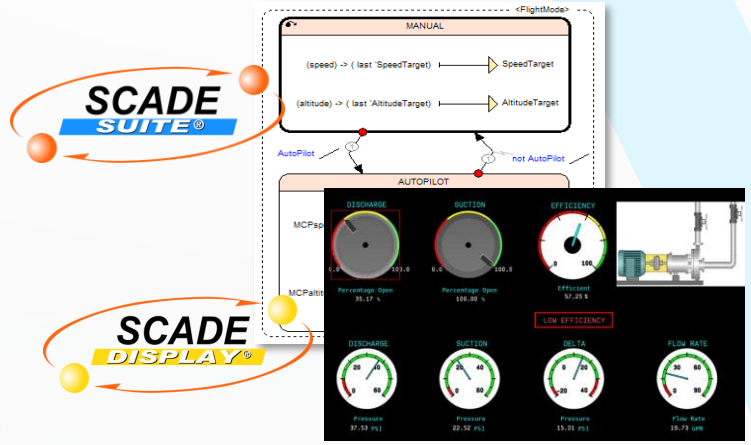


System Simulation & Digital Twins



System Architecture

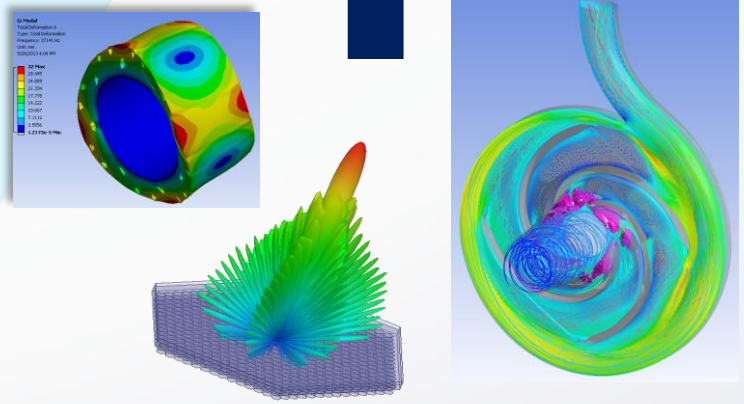
System/SW Architecture



Model-Based Software Engineering

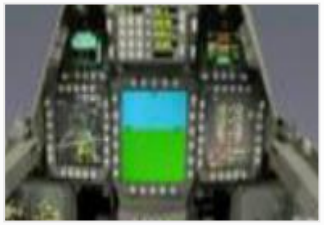
SW Components (FMI)

ROM



3D Physics Simulation

Vertical Market Focus



Aerospace & Defense

500% increase in software lines of code (SLOC) in aerospace in 10 years

Automotive

100Mi software lines of code (SLOC) in modern vehicles

Railways

Ever increasing certification costs and project delays/costs overrun

Industrial Equipment

More than 380K software and system engineers work in the oil and gas industry

Energy & Nuclear

Software-based Instrumentation and Controls have become State of the art

Healthcare

Software Failures are Responsible for 24% of all Medical Device recalls

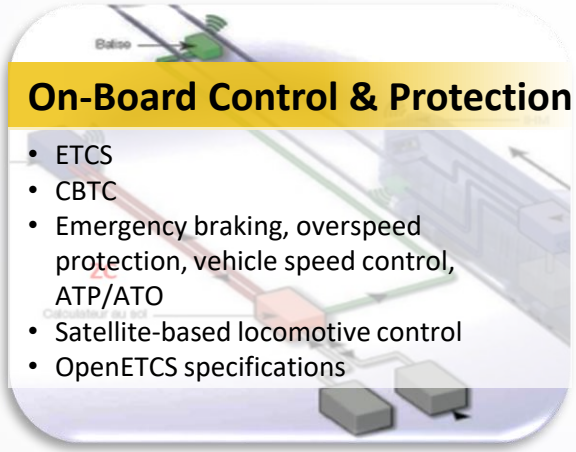
Our Customers in A&D

numesys
NUMERICAL SYSTEMS

Systems & Embedded Software Customer Testimonials

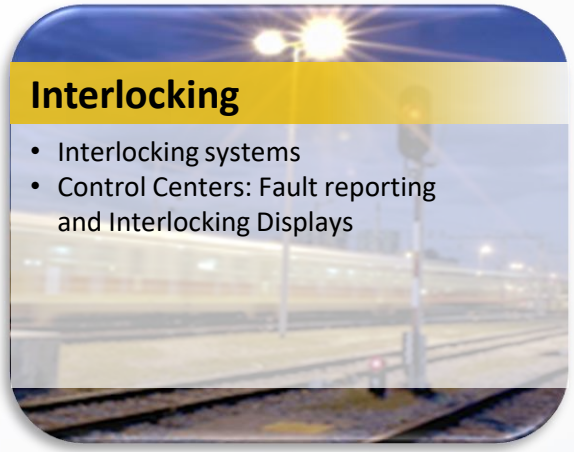
Ansys CERTIFIED ELITE CHANNEL PARTNER

Rail Transportation Systems Applications



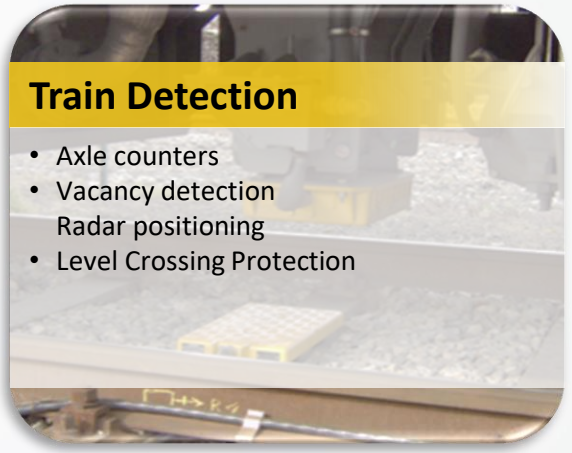
On-Board Control & Protection

- ETCS
- CBTC
- Emergency braking, overspeed protection, vehicle speed control, ATP/ATO
- Satellite-based locomotive control
- OpenETCS specifications



Interlocking

- Interlocking systems
- Control Centers: Fault reporting and Interlocking Displays



Train Detection

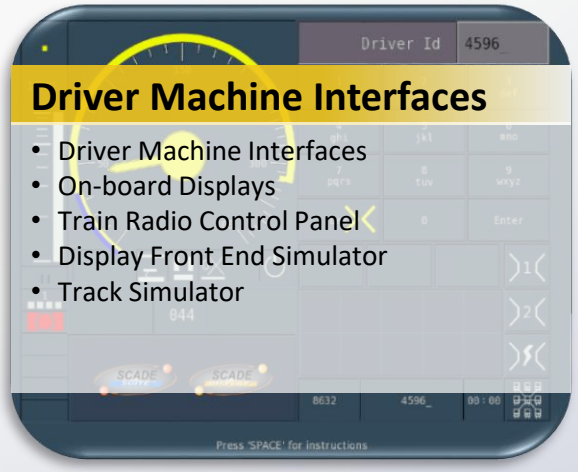
- Axle counters
- Vacancy detection
  Radar positioning
- Level Crossing Protection

Platform - Cabin

- Doors opening
- Departure interlocks

Mechatronic Control Systems

- Train Traction and Braking



Driver Machine Interfaces

- Driver Machine Interfaces
- On-board Displays
- Train Radio Control Panel
- Display Front End Simulator
- Track Simulator

SCADE @ ALSTOM

- Program/Application:
  - Paris Subway Lines 5 & 9
  - CBTC (Ouragan ATP/ATO System)

By kaffeeeinstein - Creative Commons

- Key Results:
  - PEGASUS 301™ product line developed on time
  - SIL3 certification achieved

"We are confident that SCADE Suite is a vital part of the infrastructure… [T]he benefits that we can achieve with the unique SCADE certified code generator save many man-hours that would, without SCADE, be spent performing unit testing activities"

Bruno Dubois
Safe Transport & Equipment Product Line Manager,
ALSTOM

SCADE @ Samsung SDS

- Program/Application:
  - Korean Railway System
  - **Korean Radio-based Train Control System**

- Key Results:
  - SCADE as **communication language between system designers and developers**
  - **50%** Cost & Time Reduction through **certified automated code generation**
  - **60%** Cost & Time Reduction through **documentation generation**
  - **60%** Cost & Time Reduction with **Graphical Simulation Environment for testing**

SCADE @ Ansaldo STS / Hitachi Rail

- Program/Application:
  - Hong Kong Subway
  - **Signalling System Refurbishing**

- Key Results:
  - 16 subway stations, **1,5 Mio lines of generated C code**
  - **15X productivity** increase per line of code (300 lines/day)

SCADE @ Siemens

SIEMENS

- Program/Application:
  - Cottbus Bahnhof Interlocking
  - **Train Vacancy Detection System**
- Key Results:
  - SIL 4 application
  - **In Operation**

SCADE @ POSCO ICT

- Program/Application:
  - Sao Paolo Subway
  - **Doors Opening and Departure Interlocks, Platform Screen Doors**

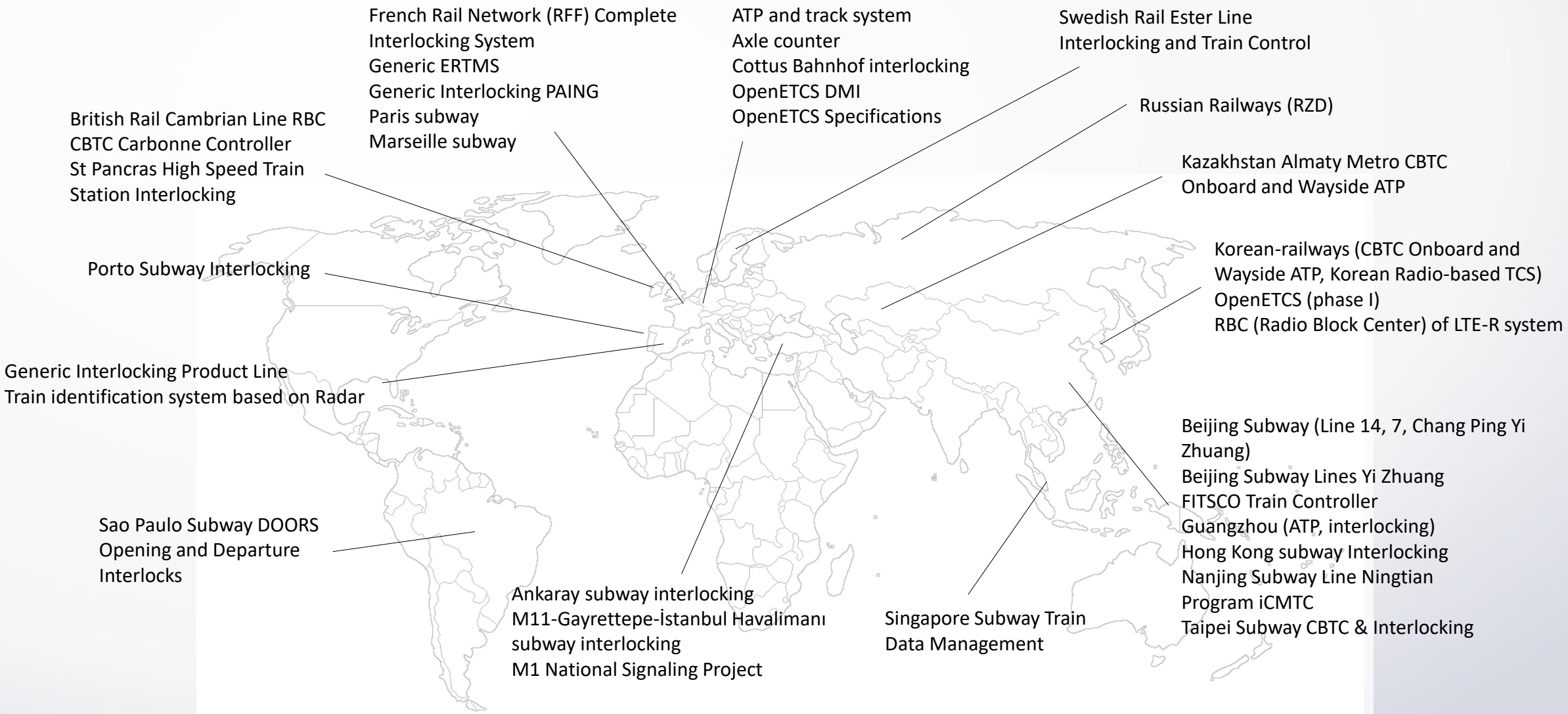
- Key Results:
  - **In Operation**
  - **Complete design** of platform screen doors
  - **SCADE Suite was easy to learn** (modeling started after just one week of training)
  - **High quality generated embeddable code**
  - **Significant** verification savings
  - **Fast close loop** between specification changes and updated software

HUNTER TECHNOLOGY

SCADE @ Hunter Technology

- Program/Application:
  - TRCP (Train Radio Control Panel) System and Driver Machine Interface

SCADE Usage Overview by Country in Rail Transportation



numesys
NUMERICAL SYSTEMS

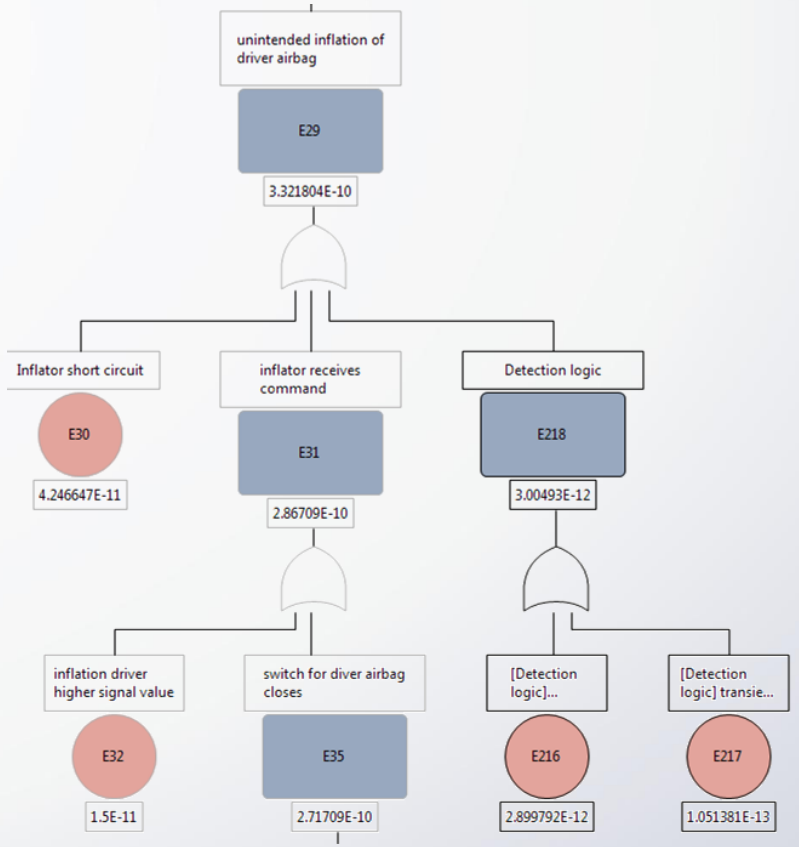
Model-Based System Safety Analysis with medini™

numesys.com.tr

Ansys CERTIFIED ELITE CHANNEL PARTNER

ANSYS medini analyze: the Integrated Solution for Safety Analysis

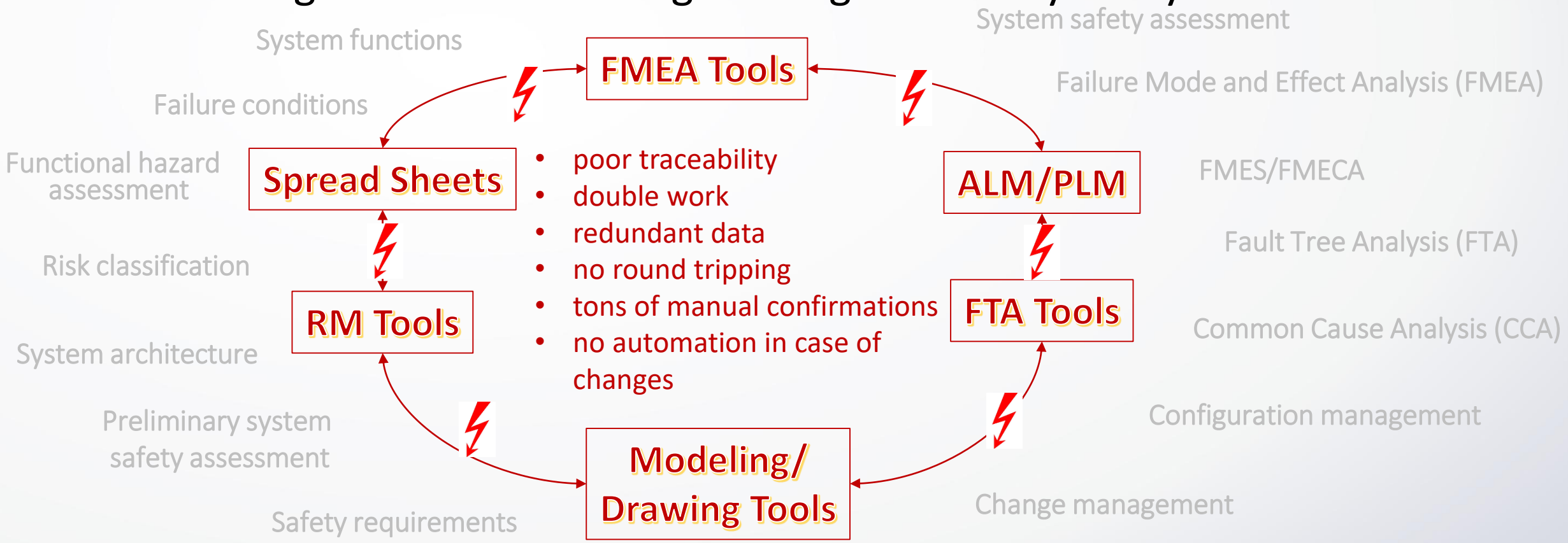
- Integrated solution for functional safety and reliability engineering
- Compliant to state-of-the-art standards: ARP4754A and ARP4761, IEC 61508, ISO 26262, VDA-Band 4, SAE J1739, SN 29500, IEC 62380, MIL HDBK 217, FIDES, EN 50126
- Efficient application of safety and reliability engineering methods at concept, system, software and hardware level
- Reduce up to 50% of effort and time-to-market for safety and reliability assurance



Fault Tree Analysis

Traditional approach: Point Tools for individual Tasks

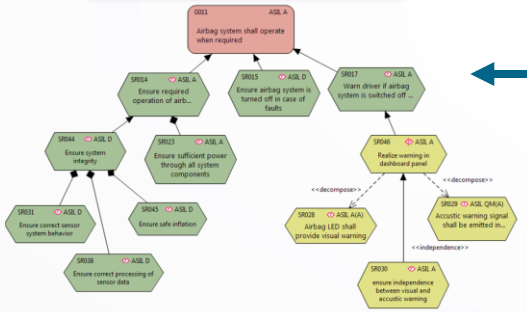
- Poor integration between Engineering and Safety Analysis



The traditional approach with point tools is error-prone, time consuming and a waste of efforts

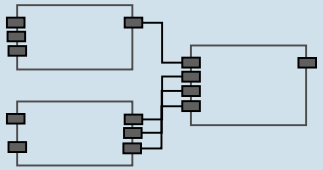
medini analyze – a Model-based and System-oriented Solution

Safety Requirements



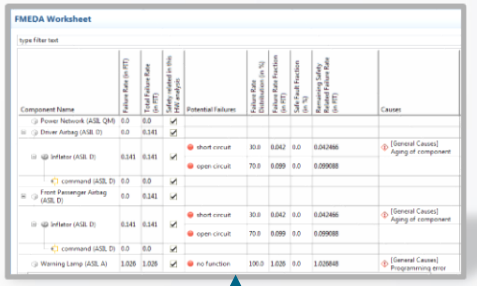
System Models

Functional, Architecture, Hardware, PCB, Software, IP Design (RTL/NL), etc.

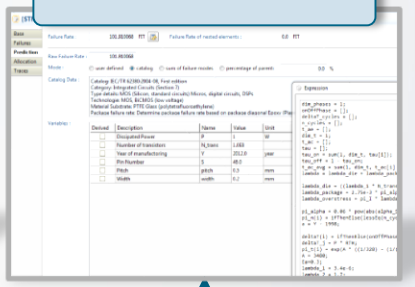


SysML extended with safety analysis related properties

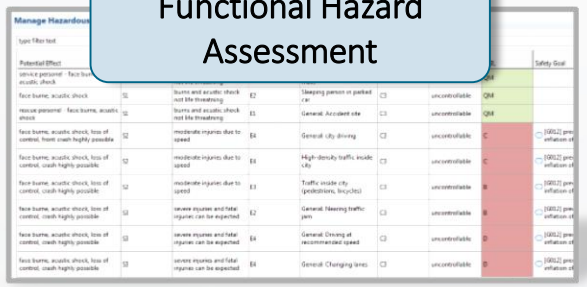
FMEA



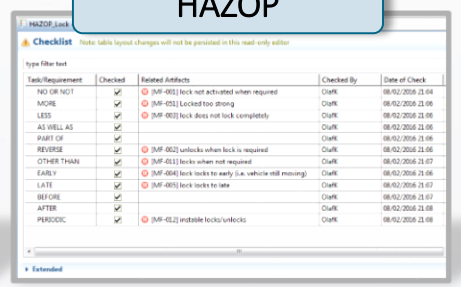
Reliability Prediction



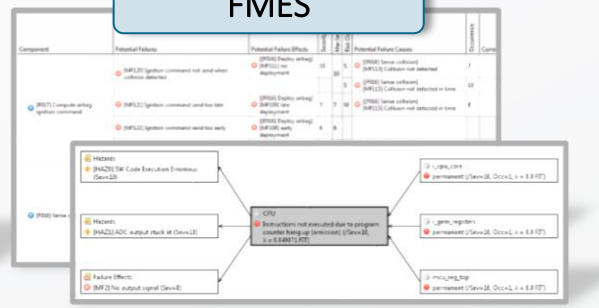
Functional Hazard Assessment



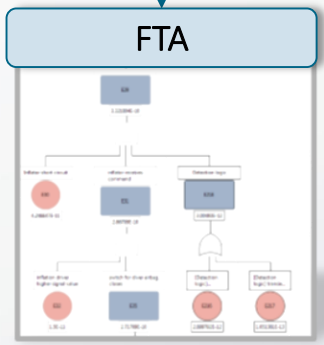
HAZOP



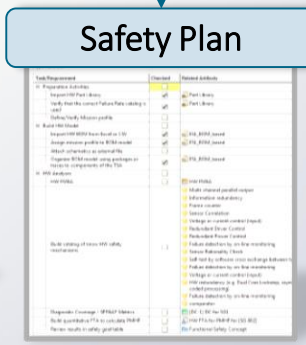
FMES



FTA



Safety Plan



Model-based approach ensures unrivalled level of consistency, traceability and efficiency

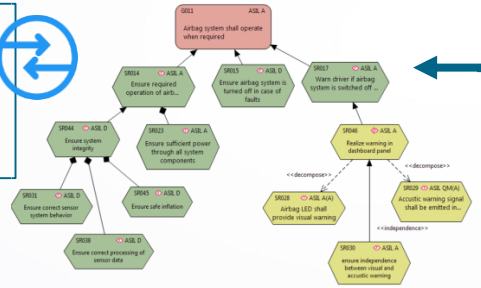
Integration is Key

- … in a Complex World

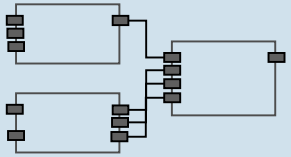
SCADE Architect
IBM Rhapsody
Enterprise Architect
MATLAB Simulink

Safety Requirements

JAMA
DOORS
PTC Integrity
ReqIF



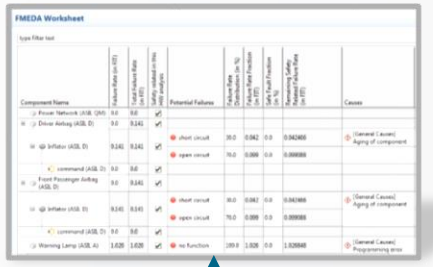
System Models
Functional, Architecture, Hardware, PCB, Software, IP Design (RTL/NL), etc.



Extended with analysis related properties

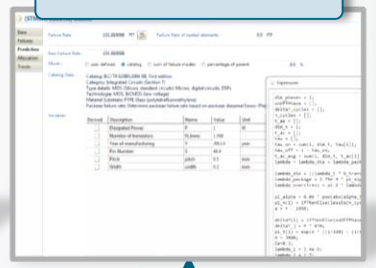
Excel

FMEA

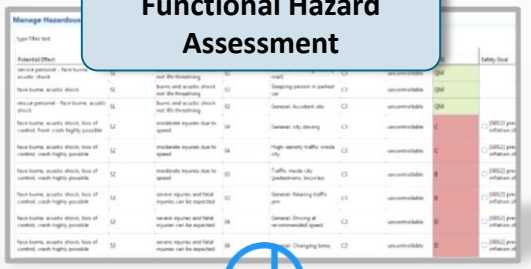


Excel

Reliability Prediction

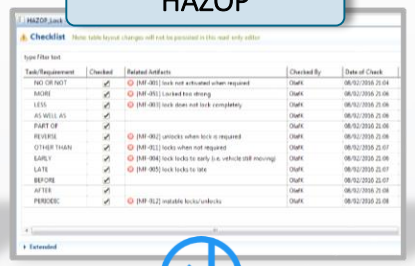


Functional Hazard Assessment



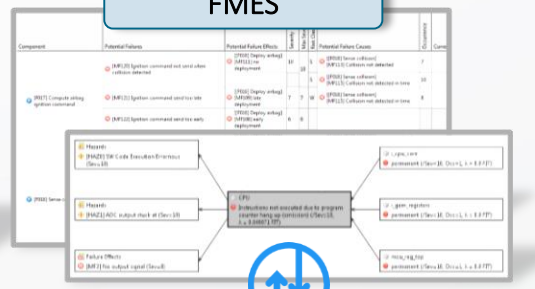
Excel
Word/PDF/HTML

HAZOP



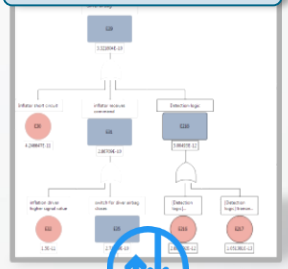
Excel
Word/PDF/HTML

FMES



MSR-XML
Task Management
Excel

FTA



FaultTree+
OpenPSA
Excel
Word/PDF/HTML

Safety Plan

Task Management

Integration with engineering tools and support of open standards

ANSYS medini analyze

Model-based Safety Analysis

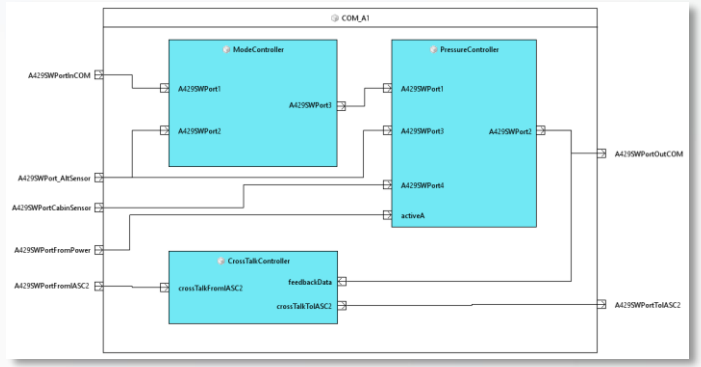
Efficient analysis of functional safety based on architectural design on system, software and hardware levels

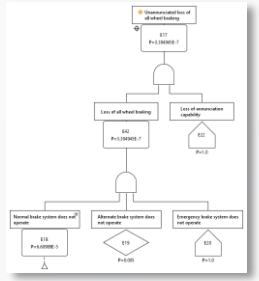
Integrated Suite supporting multiple Safety Analysis Methods

Consistent application of (inductive and deductive) safety analysis methods including FHA, FTA, FMEA, FMES, CCA

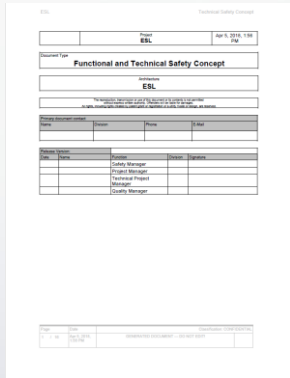
Safety Case Document Generation

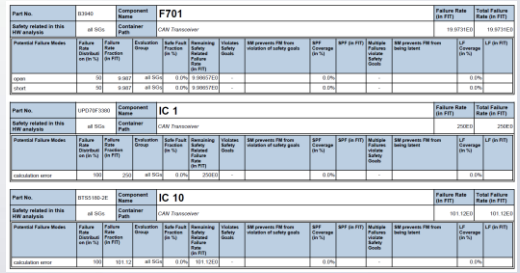
Customizable report generation enables the generation of documents that are required for certification





ID	Function	HAZOP Guide Word	Operational /Environmental condition	Phase	Failure Condition (Hazard description)	Effect of failure condition on Aircraft/Crew	Failure Condition Classification	DAL	Safety Objective
IPS-1-02	[F001] Provide cabin pressure and air exchange	NOT	Cruise altitude	In Flight	[IPS-1-02] Unannunciated loss of cabin pressure	Significant reduction of oxygen flow and pressure inside cabin decreases. Significant increase on crew workload.	Hazardous	B	[SO_01] The EICAS has to be available.
IPS-1-04	[F001] Provide cabin pressure and air exchange	NOT	Take off	In Flight	[IPS-1-03] Annunciated loss of cabin pressure	Significant reduction of oxygen flow and pressure inside cabin decreases. Significant increase on crew workload.	Major	C	[SO_01] The EICAS has to be available.

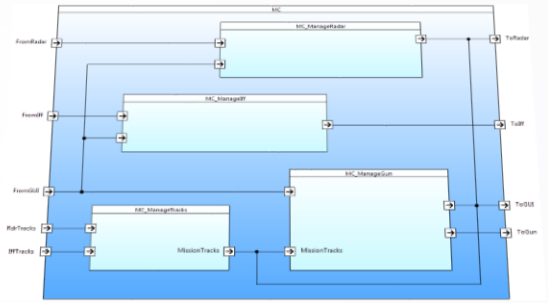




SCADE/medini Integration for Model-Based Safety Analysis

SCADE ARCHITECT

System/SW Architecture



Iterative approach

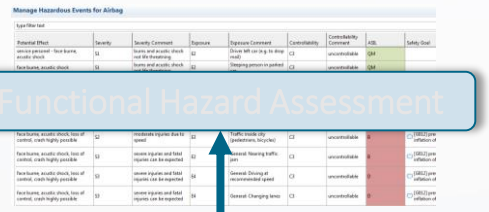
Safety process seamlessly integrated with system development

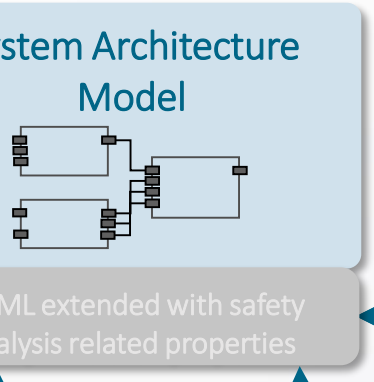
Safety analysis results always consistent

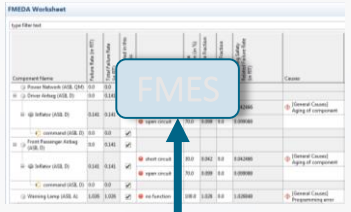
Safety requirements discovered and considered early in the design process

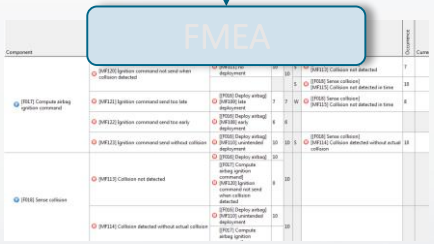
medini™ analyze

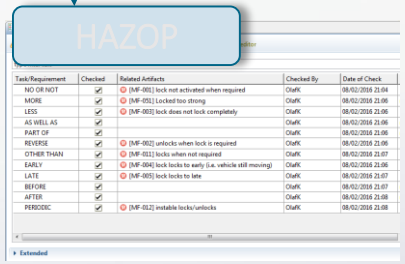
Functional Safety Analysis and Design

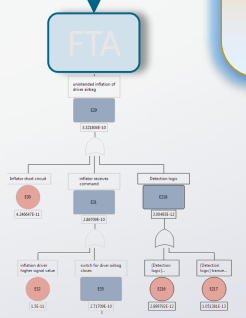






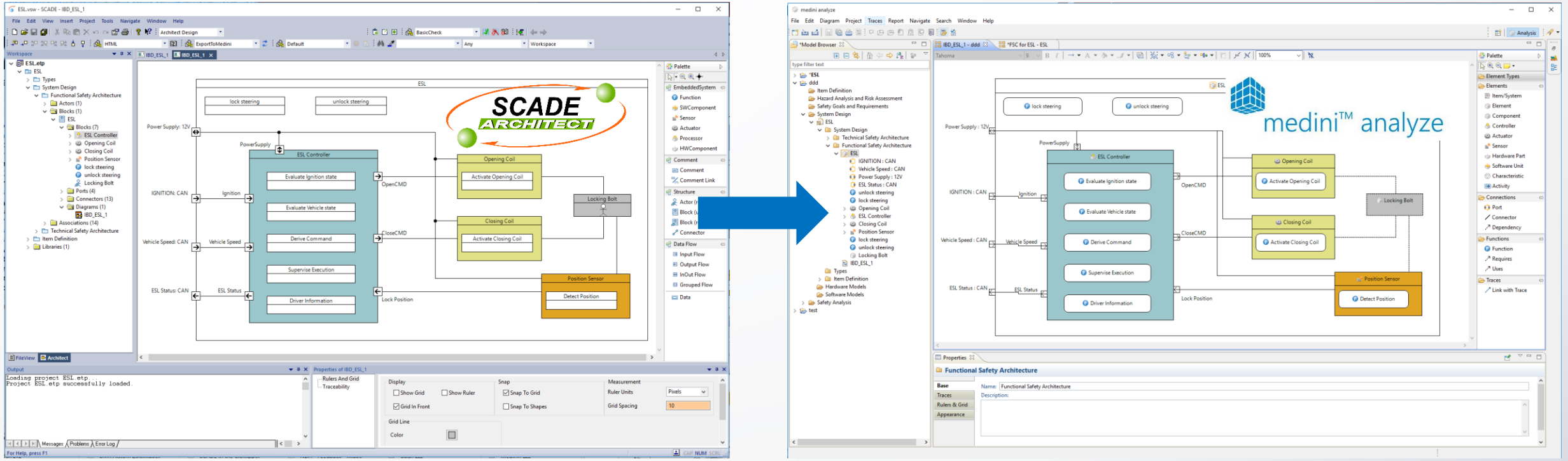






SCADE/medini Integration for Model-Based Safety Analysis

- SCADE Architect is bundled with medini analyze Enterprise



SCADE Architect to medini analyze: example of automatic functional architecture import

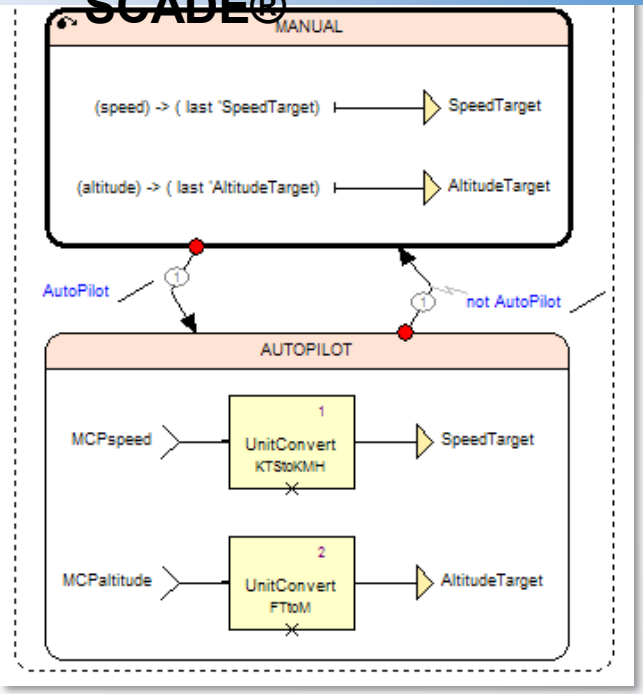
numesys
NUMERICAL SYSTEMS

Embedded Systems & Software Development with SCADE®

numesys.com.tr

Ansys CERTIFIED ELITE CHANNEL PARTNER

What is ANSYS SCADE used for ?

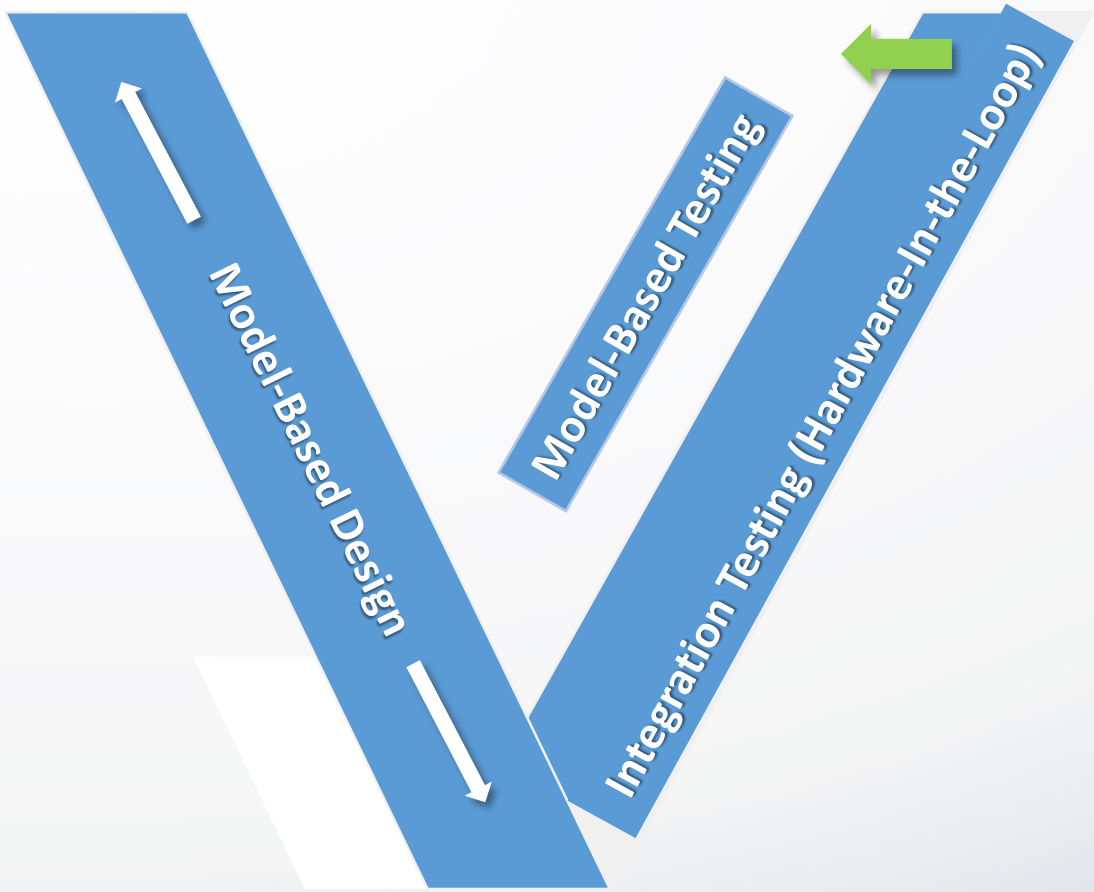


Embedded Software Application Development

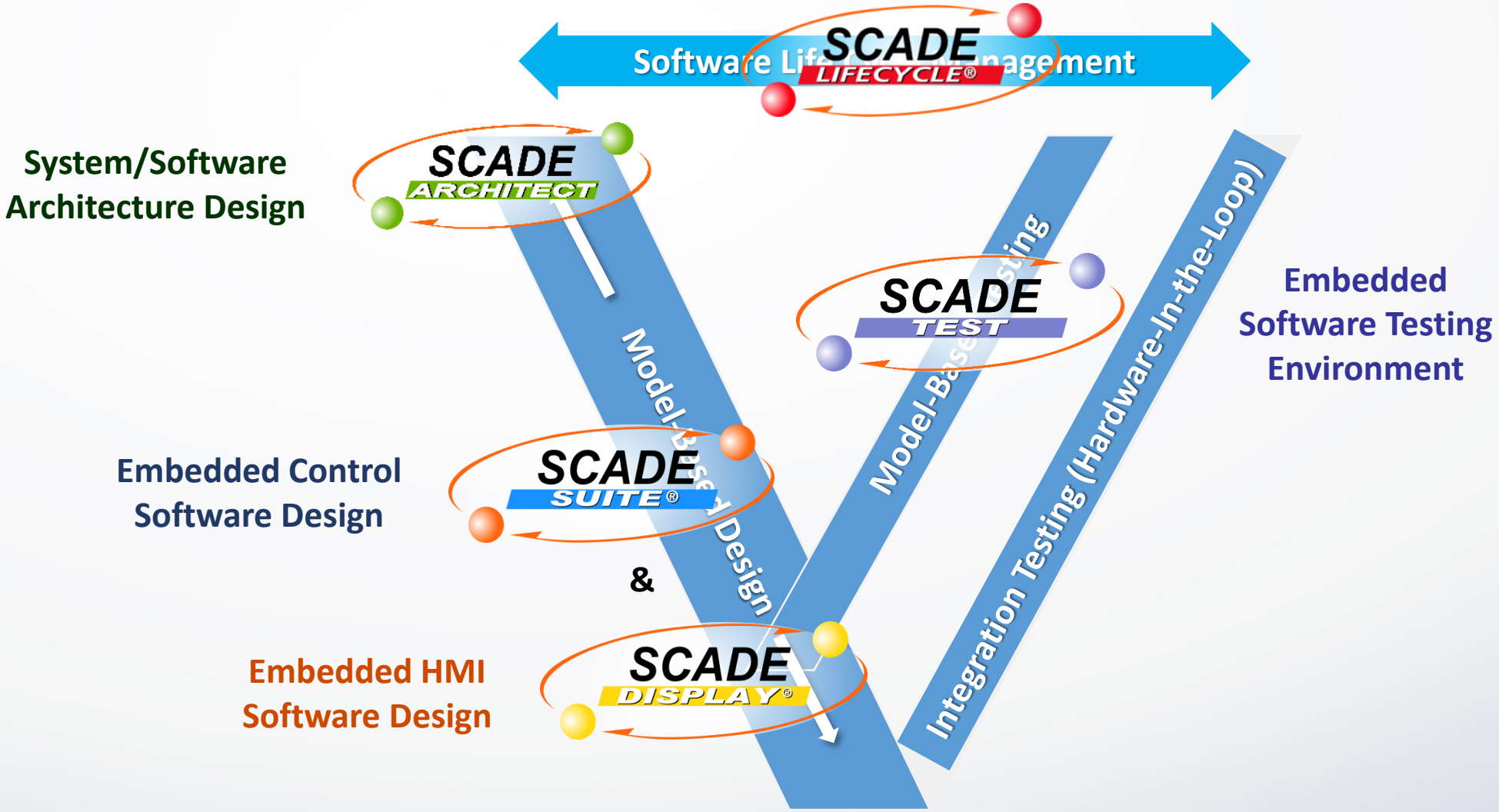
Embedded Controls and Displays

High Quality, High Dependability Mission or Safety Critical Applications (with or without software certification requirements)

ANSYS SCADE Products in the Software V-Cycle



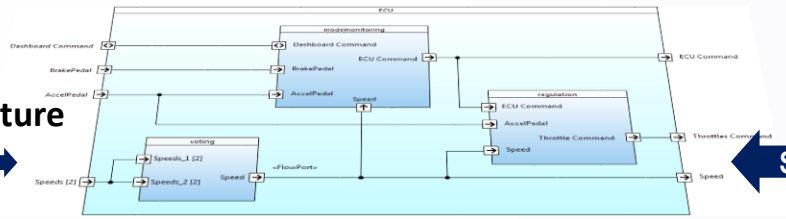
ANSYS SCADE Products in the Software V-Cycle



Unique Integration of Systems & Embedded Software Solutions

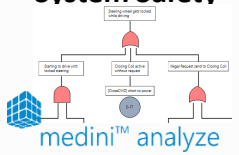
SCADE ARCHITECT

System & SW Architecture



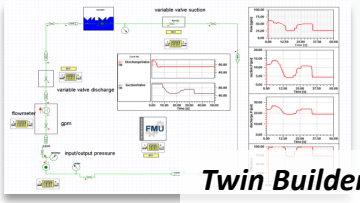
System Requirements

System Safety



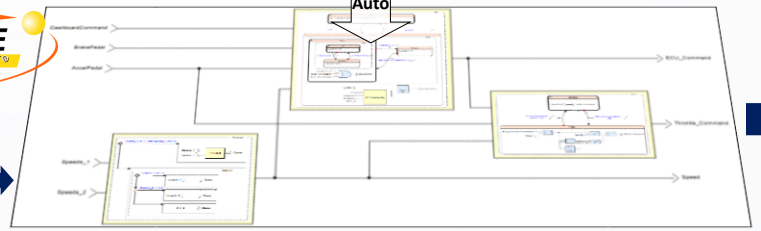
System Architecture

System Simulation & Digital Twin Builder



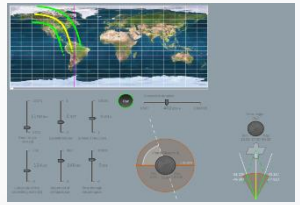
SCADE SUITE® SCADE DISPLAY®

SW Design



Software Requirements

Simulation

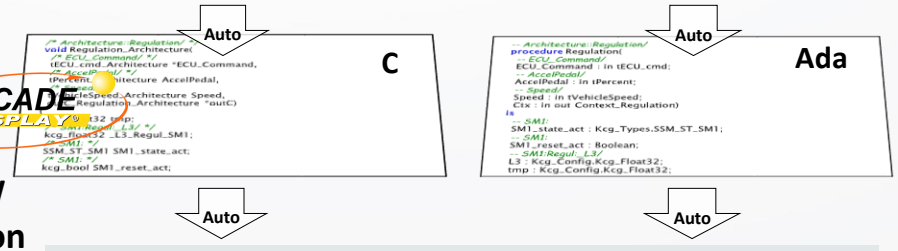


Test

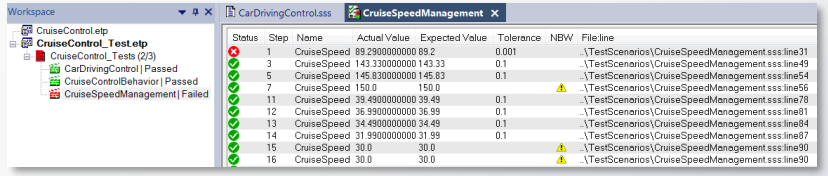
SCADE TEST

SCADE SUITE® SCADE DISPLAY®

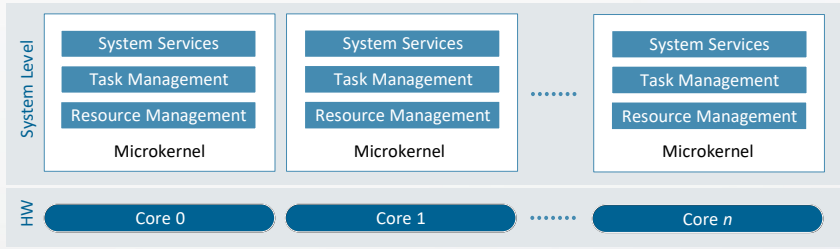
Automatic SW Code Generation

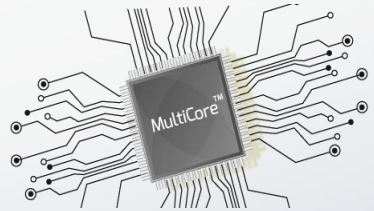


Test



RTOS & HW platforms
Multi-rate / Multi-core





SCADE Benefits and Value Proposition for Rail Transportation

STRATEGIC

- **Compliance with Software Safety Certification** and **Risks Mitigation**
- Improved **Communication & Collaboration** among system and software teams, customers, suppliers and certification authorities
- Improved **Long-term Maintainability** of applications

TECHNICAL

- **Automated Production** of readable, portable, high performance and high quality **Code**
- **Documentation Quality** and **Accuracy**
- **Early Detection of Design Flaws**

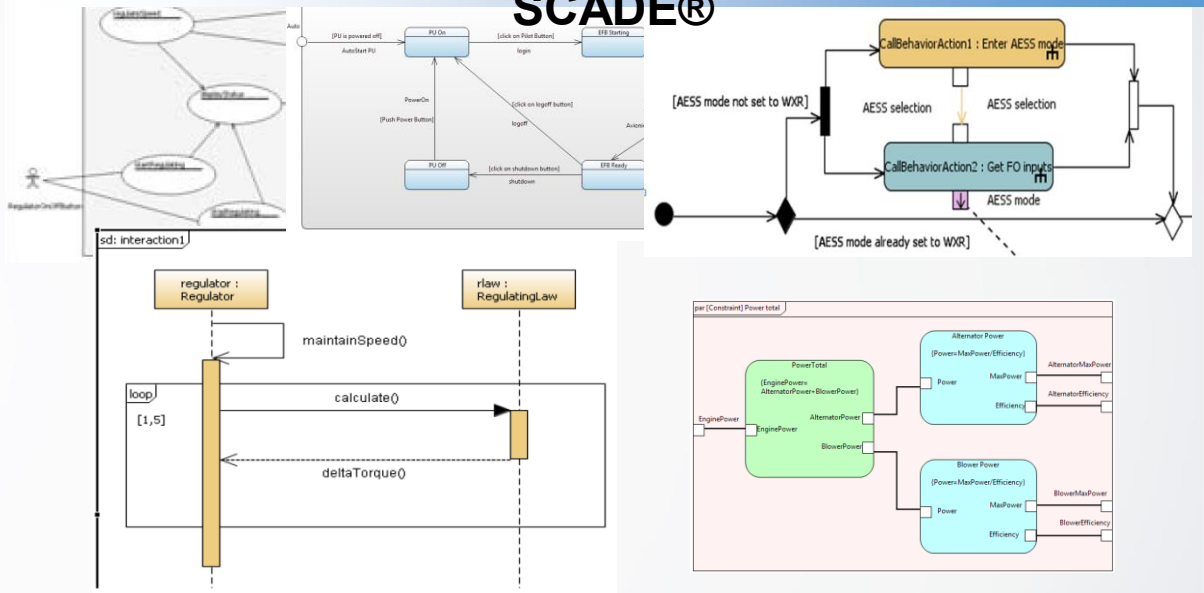
ECONOMICAL

- **50% Development and V&V Costs Reduction** overall

ANSYS SCADE Architect

Model-Based embedded systems architecture design

SysML standard based, focus on ease of use,
Data dictionaries and data propagation in architecture.



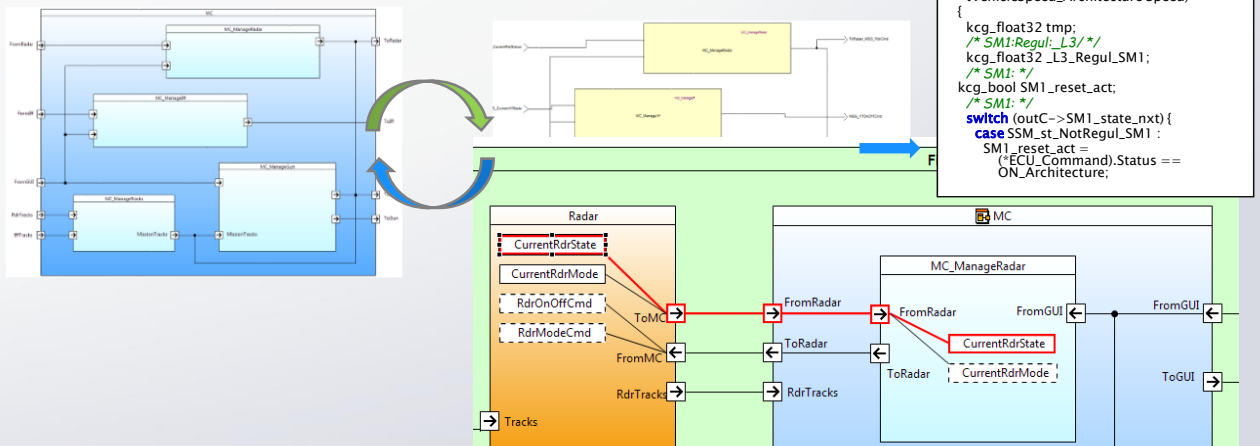
		A	B	C	D	E
		Name	DS_ID	Address	Length	Message Type
1	CP_FW_LG	CP_FW_LG				NonProtocol
3	Res	Res		0	4	
4	FS1	FS1		4	1	
5	FS2	FS2		5	1	
6	FS3	FS3		6	1	
7	FS4	FS4		7	1	
9	DISP_LG	DISP_LG	813	8	12	
10	DS_RES1	DS_RES1	814	20	12	
11	DS_RES2	DS_RES2	823	32	16	
12	MSG_ADIRU_COM_C10	MSG_ADIRU_COM_C10				NonProtocol
14	Res	Res		0	4	
15	FS1	FS1		4	1	
16	FS2	FS2		5	1	
17	FS3	FS3		6	1	
19	DS_ADIRU_AC_GND_SPEED	DS_ADIRU_AC_GND_SPEED	1	8	4	
20	DS_ADIRU_AC_ACCEL	DS_ADIRU_AC_ACCEL	2	12	4	
21	DS_ADIRU_AC_PITCH_ANGLE	DS_ADIRU_AC_PITCH_ANGLE	3	16	4	
22	MSG_COCKPIT_COM_C10	MSG_COCKPIT_COM_C10				NonProtocol
24	Res	Res		0	4	
25	FS1	FS1		4	1	
26	FS2	FS2		5	1	
27	FS3	FS3		6	1	
28	FS4	FS4		7	1	
30	DS_I_U_LBP	DS_I_U_LBP	1	8	4	
31	DS_I_U_RBP	DS_I_U_RBP	2	12	4	
32	DS_I_U_BPPS	DS_I_U_BPPS	3	16	4	
33	DS_DISCRETE_COCKPIT_COM	DS_DISCRETE_COCKPIT_COM	4	20	4	
34	MSG_COM_ACMS_C10	MSG_COM_ACMS_C10				NonProtocol

Interface Control Documents (ICD) production

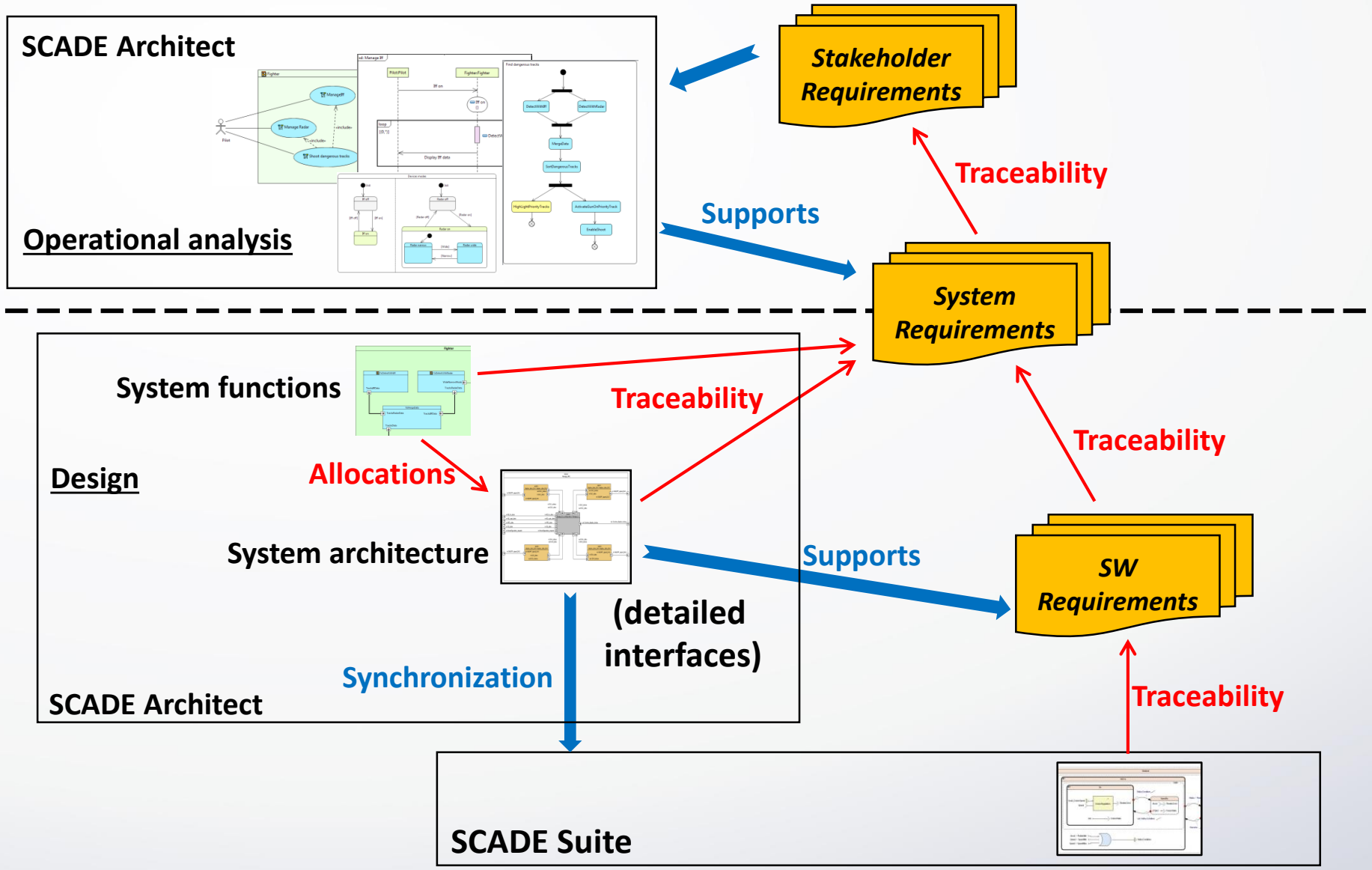
Support of Domain Specific Language and hierarchical table with MS Excel import/export demonstrated through ready to use industry specific packages

Integrated workflow for software intensive systems design

Synchronization with SCADE Suite designs for certified software development;
Supports industry engineering standards such as AUTOSAR, AADL, FACE



What is Requirement Traceability?

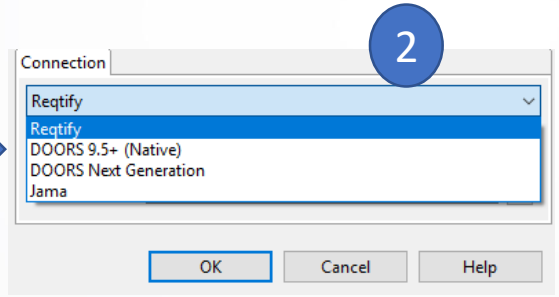


What is Requirement Traceability?

1

System or Software Requirements

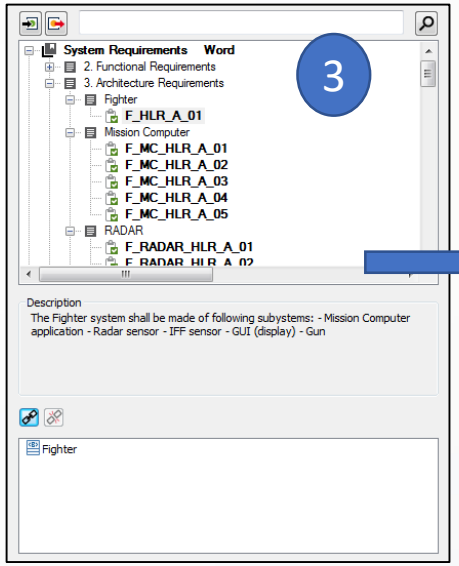
2



SCADE SUITE®

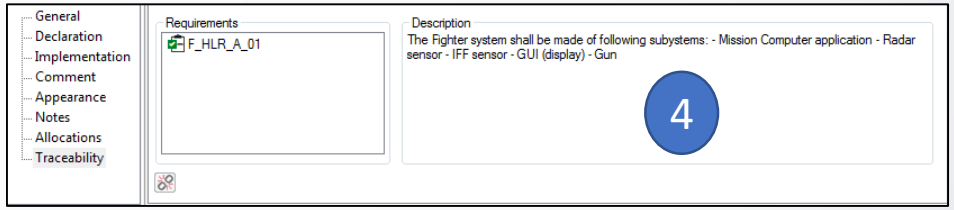
SCADE ARCHITECT

3



SCADE SUITE®

SCADE ARCHITECT



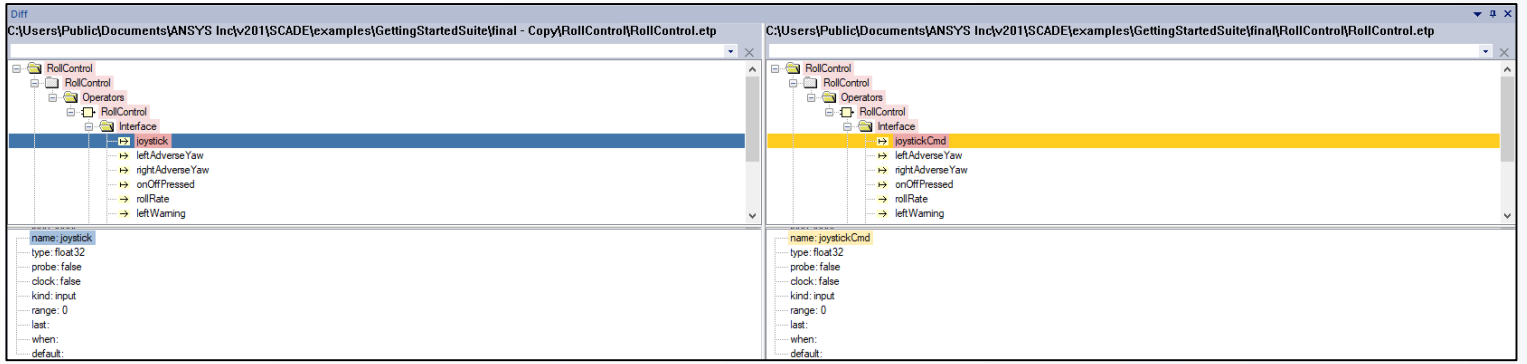
4

SCADE SUITE®

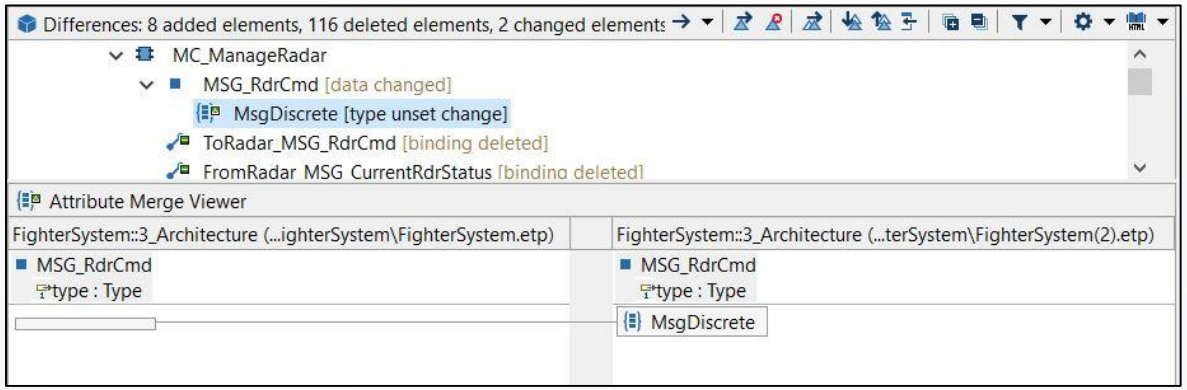
SCADE ARCHITECT

Model Diff-Merge and Difference Report

1



2



3

Diff/merge report between (1) [Package] 3_Architecture and (2) [Package] 3_Architecture

(1) [Package] 3_Architecture : C:\SCADE Training Kit\trunk\Basic\Introduction to ANSYS SCADE Architect\For Customer\Lesson 2\Labs\Solutions\Lab 4\FighterSystem\FighterSystem.etp
(2) [Package] 3_Architecture : C:\SCADE Training Kit\trunk\Basic\Introduction to ANSYS SCADE Architect\For Customer\Lesson 2\Labs\Solutions\Lab 2\FighterSystem\FighterSystem.etp

Table of contents

I. Initial differences

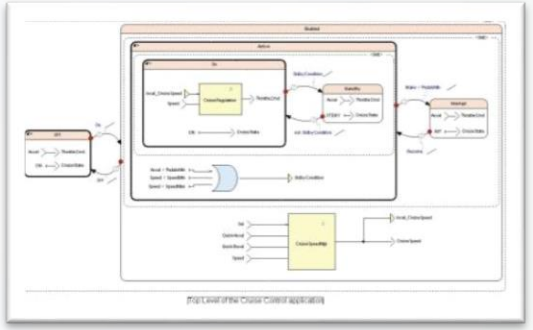
I.1 [Package] 3_Architecture

(1) FighterSystem::3_Architecture
(2) FighterSystem::3_Architecture

ANSYS SCADE Suite

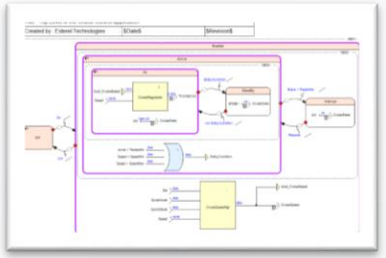
Embedded Control Software Design

Efficient modeling of controls, logic and algorithm designs within a single environment



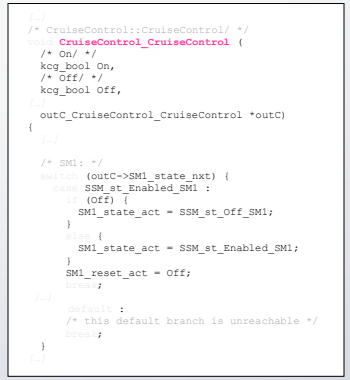
Integrated Suite for Prototyping, Modeling, Simulation, Verification, and Optimization

Efficient debugging and optimization of software models and code size, speed and performance



Certified Code Generation

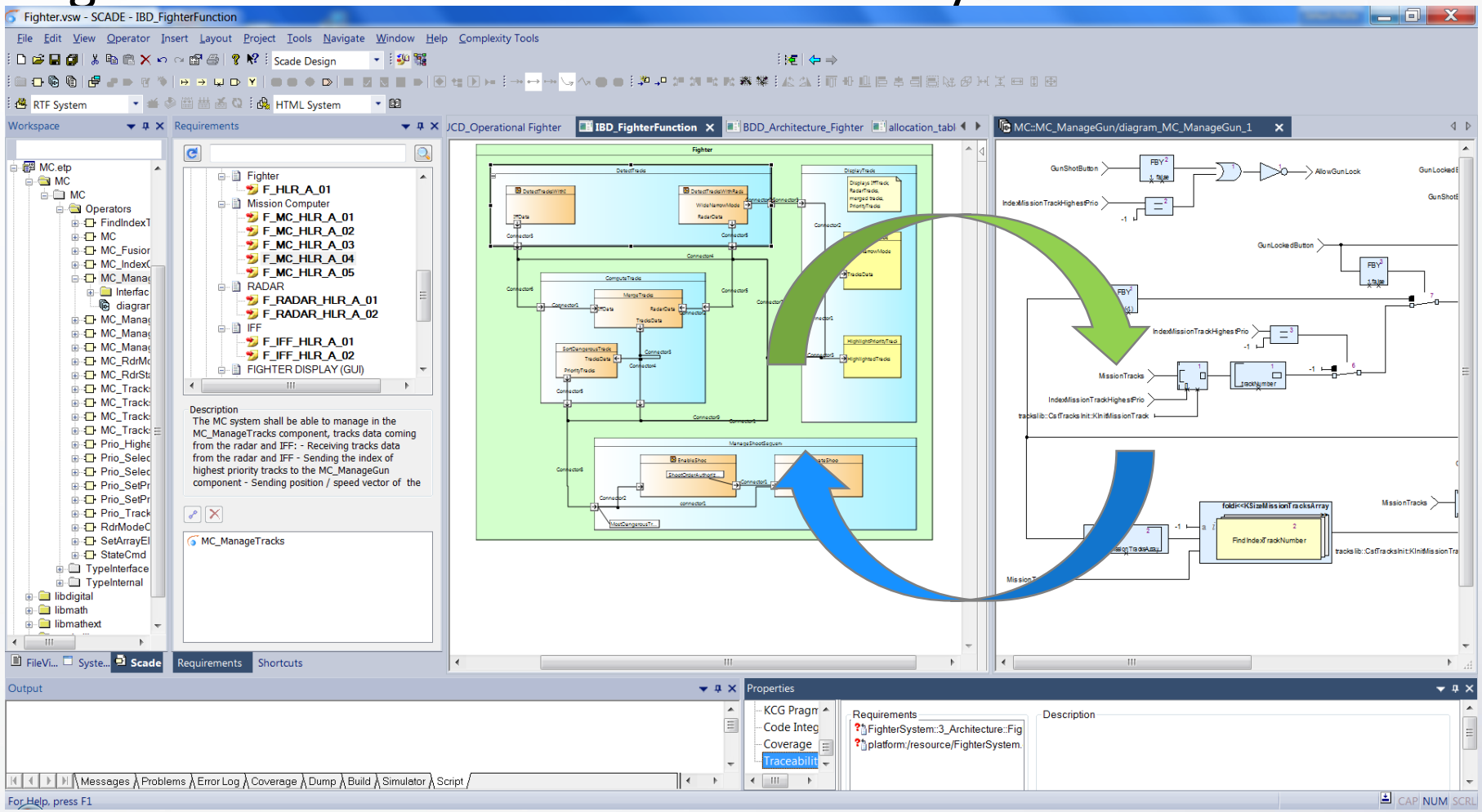
Automatic C and Ada certified code generators (DO-178C, EN 50128, ISO 26262, IEC 61508)
Enables 80% embedded code production and testing cost reduction



```
/* CruiseControl::CruiseControl/ */
void CruiseControl_CruiseControl (
  /* On/ */
  kcg_bool On,
  /* Off/ */
  kcg_bool Off,
  outC_CruiseControl_CruiseControl *outC)
{
  /* SM1: */
  switch (outC->SM1_state_nxt) {
    case SSM_st_Enabled_SM1 :
      if (Off) {
        SM1_state_act = SSM_st_Off_SM1;
      }
      else {
        SM1_state_act = SSM_st_Enabled_SM1;
      }
      SM1_reset_act = Off;
      break;
    default :
      /* this default branch is unreachable */
      break;
  }
}
```

SCADE Architect Synchronization with SCADE Suite

- An Integrated Workflow for SW-intensive Systems



Integrated Workflow for Software Intensive Systems

SCADE ARCHITECT

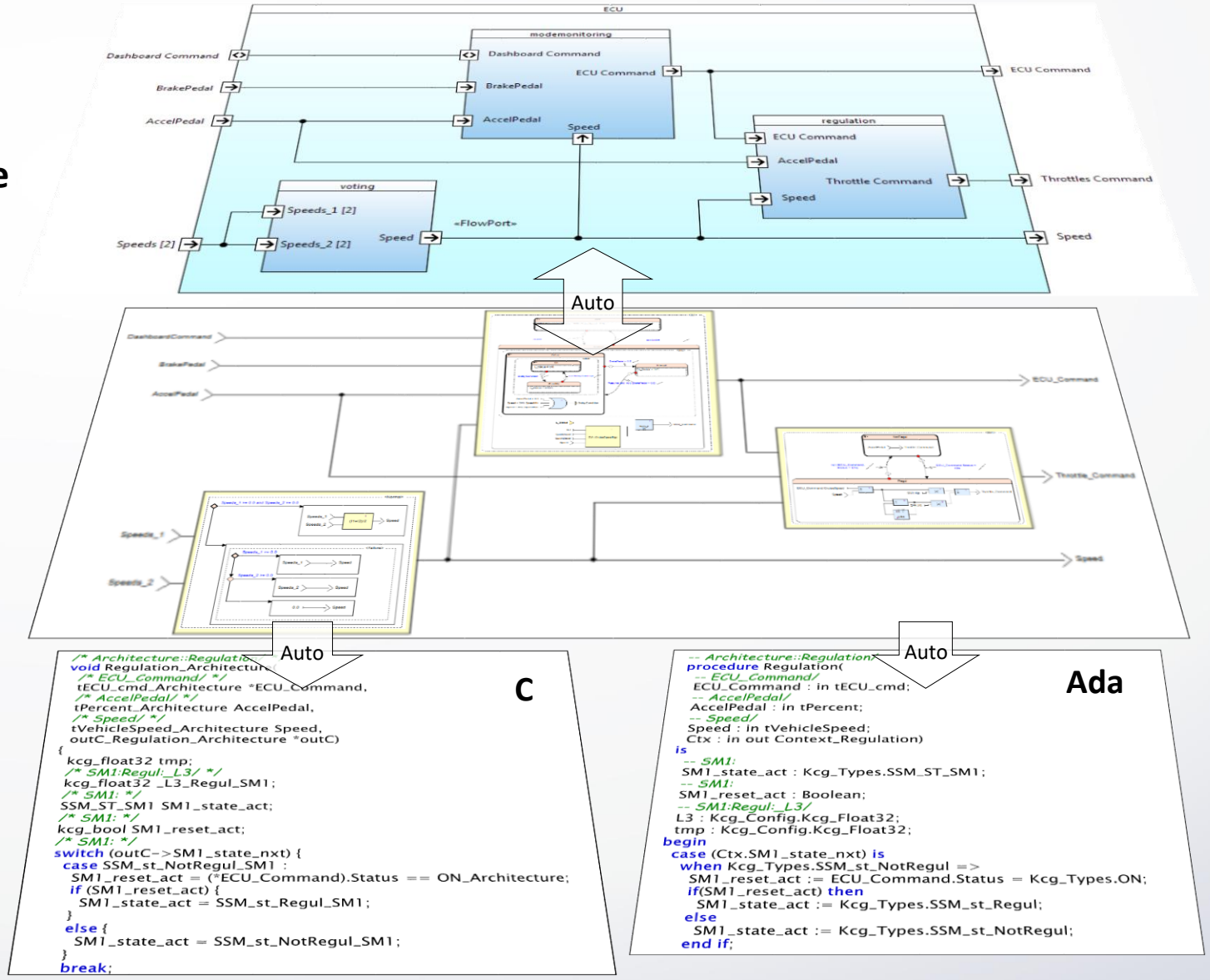
SW Architecture

SCADE SUITE®

SW Design

SCADE SUITE®

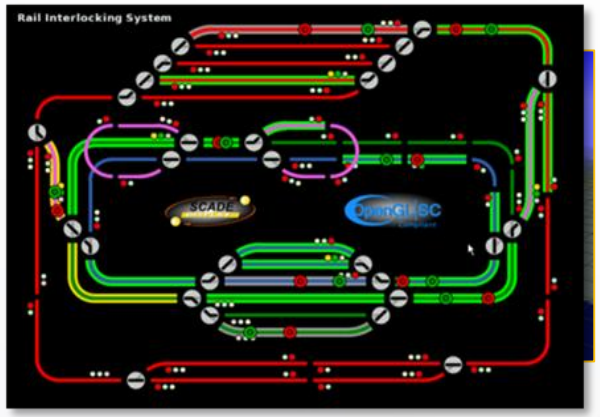
SW Coding



ANSYS SCADE Display

HMI Software Design

Efficient modeling of HMI designs
featuring an integrated environment with logic design



Complete GUI Prototyping, Modeling, Simulation, Verification, and Optimization

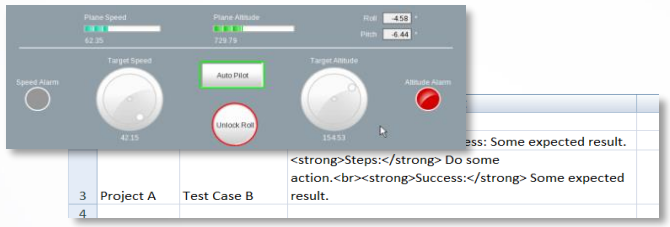
Rapid prototyping, model checking and debugging, simulation, integration with graphics platforms and human factors optimization

Certified Code Generation

Automatic certified code generator
(DO-178C, EN 50128, ISO 26262, IEC 61508)
Enables 80% embedded code production and testing cost reduction

PC, Android, Apple iOS and critical/rugged embedded graphics platforms

ANSYS SCADE Test

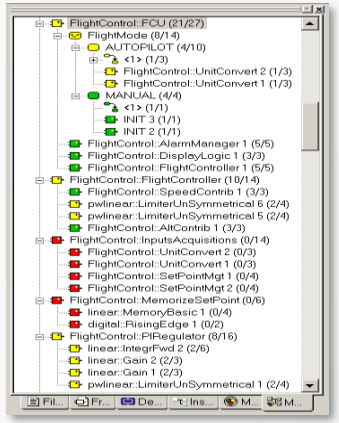


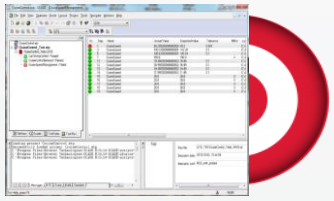
Interactive Test Creation and Rapid Prototyping

Efficient environment to create requirements-based test suites and run interactive software simulation

Automated Tests Execution of Software Models on development platform with Automated Model Coverage acquisition

Ensures 100% confidence in software test suites

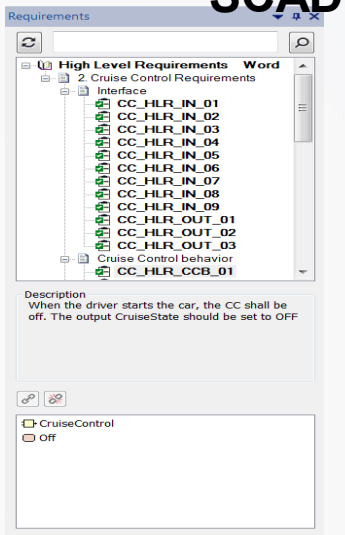




Automated Tests Execution of Generated Software Code on any Hardware Target

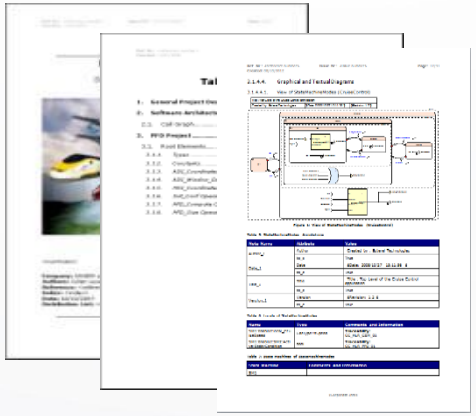
Fully automated reuse of validated software test suites on processor target (includes drivers for LDRA, RTRT & VectorCAST)

ANSYS SCADE LifeCycle



Requirements Traceability

Direct traceability between System and Software requirements (in DOORS, Word, Excel, etc..) and SCADE Architect, SCADE Suite & SCADE Display models and SCADE Test suites



Automatic Documentation Generation

Ensures that System, Software, Tests & Code documentation are automatically produced …and up to date with the design

Multi-Vendor ALM Support

Seamless integration with Application Lifecycle Management, version and configuration management tools, and automated production of design metrics

Unique Benefits for Certification

- SCADE products and solutions are developed specifically to address critical system and software applications
- SCADE Suite and Display code generators are certifiable according to the following international safety standards:
  - **EN 50128 certification up to SIL 3/4 – Rail Transportation**
  - **IEC 61508** certification up to SIL 3 – Industrial & Energy
    - IEC 60880 full compliance – Nuclear Instrumentation & Control
    - IEC 62304 full compliance – Medical Systems
    - EN 13849 full compliance – Industrial Machines Safety
  - DO-178C qualification up to Level A – A&D
  - **ISO 26262** certification up to ASIL D – Automotive
- Same products qualified at the highest level of safety across 6 market segments by 10 safety authorities, worldwide

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE

No. Z10 16 11 55460 008

Holder of Certificate: **Esterel Technologies**
14 & 15, Place Georges Pompidou
78180 Montigny-le-Bretonneux
FRANCE

Factory(ies): 55460

Certification Mark:

Product: **Software Tool for Safety Related Development**

Model(s): **Code Generator SCADE Suite KCG 6.6**

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

The report EM90205C 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)
ISO 26262-8:2011 (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. See also notes overleaf.

Test report no.: EM90205C

Valid until: 2021-11-14

Date, 2016-11-18 (Peter Weiss)

Page 1 of 1

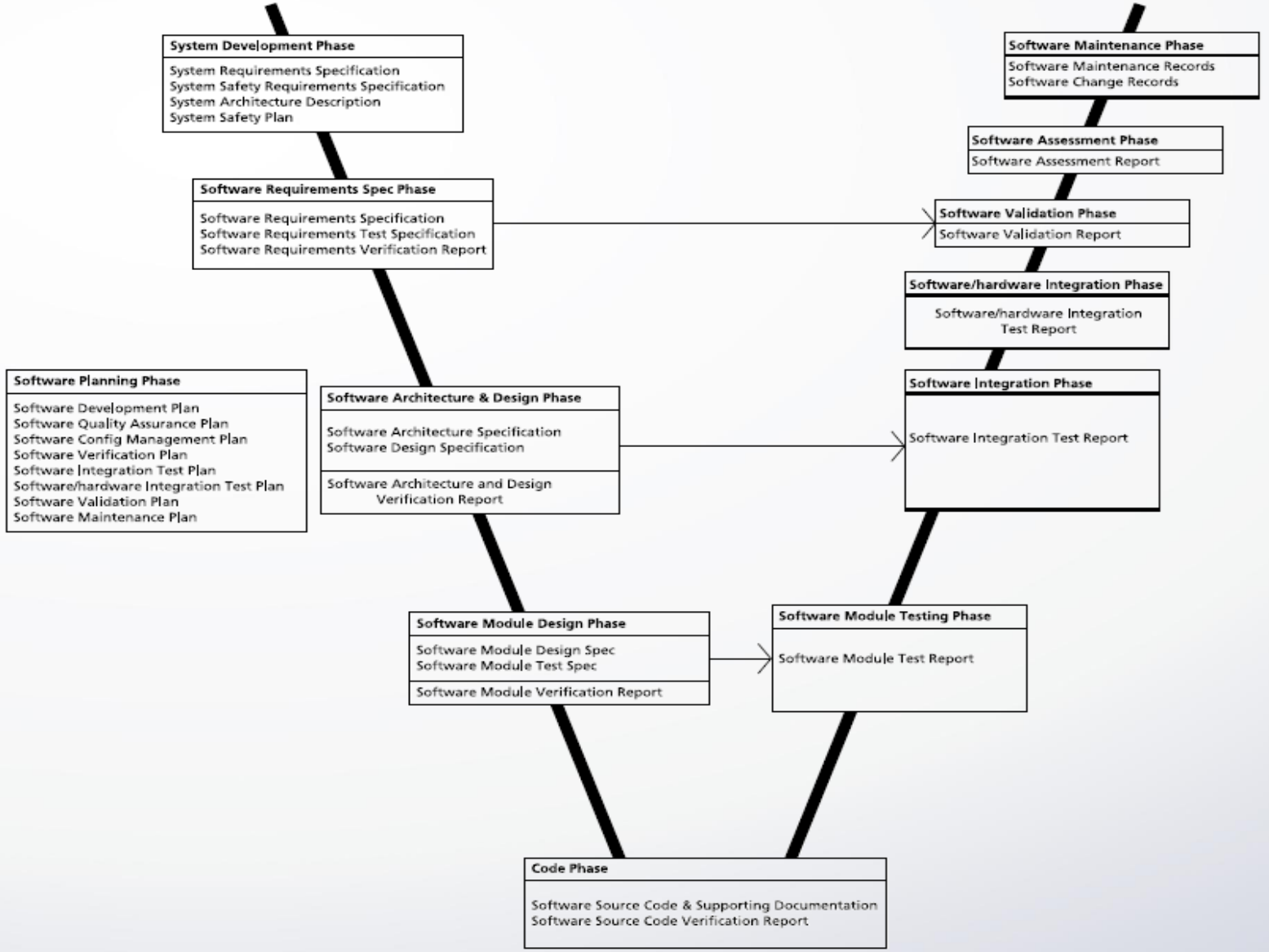
TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

TÜV®

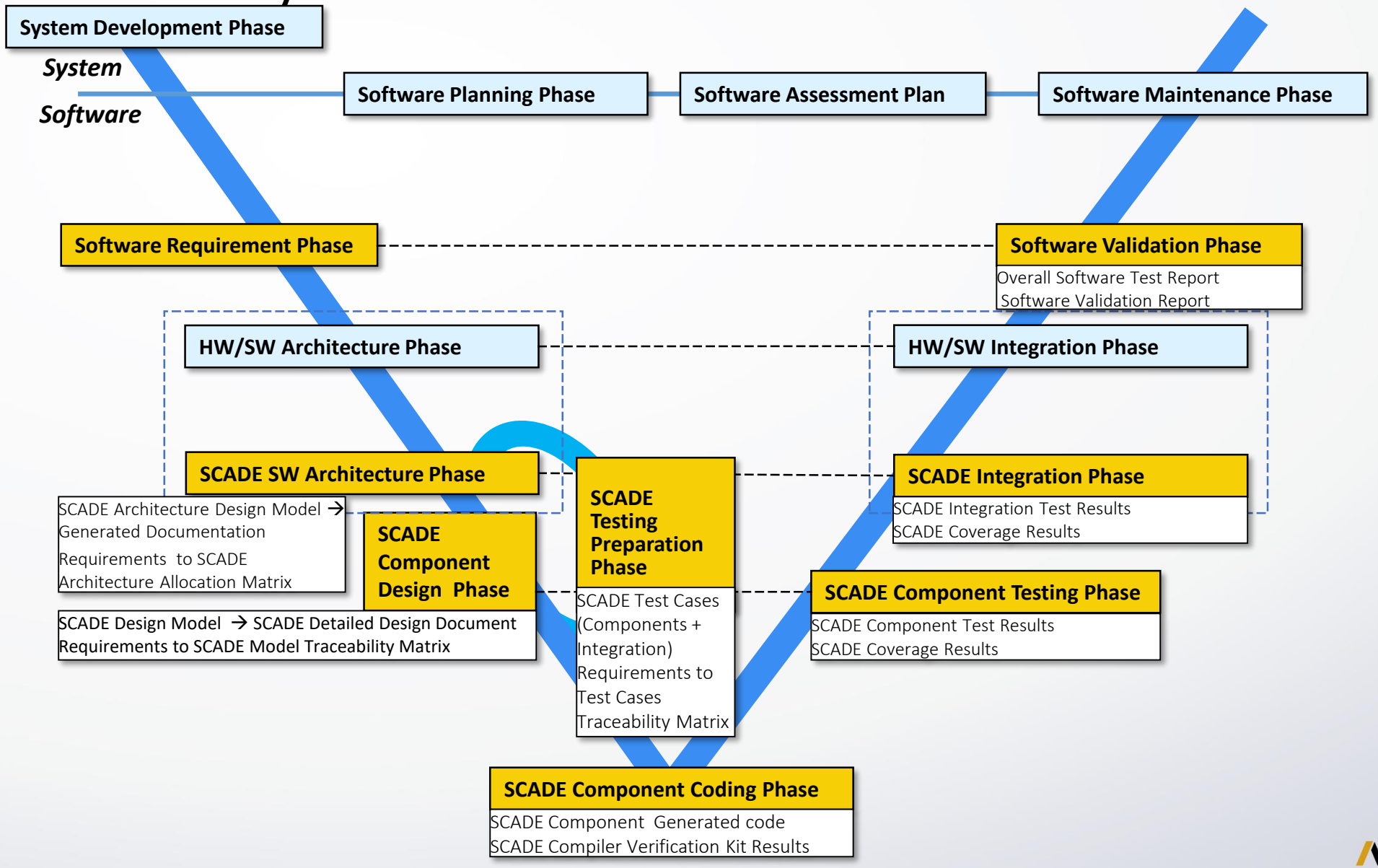
A1 / 04.11

Multiple EN 50128 SCADE Suite and Display KCG Tool certifications by TÜV

The System and Software V-Model (EN 50128)



SCADE V-Cycle



Software Development Cost Savings with SCADE

Level	Non-Safety Related Cost	SIL 1 Cost	SIL 2 Cost	SIL 3 Cost	SIL 4 Cost
Comparative Cost*	Baseline	Base +10%	SIL 1 +36%	SIL 2 +80%	SIL 3 +30%
Cost	100	110	150	270	350+
Cost with SCADE	100	100	120	160	175
Savings with SCADE	-	10%	20%	40%	50%

(*): Comparative Software Development Cost per SIL Level, including Testing / Empirical data

Example Of Rail Project: a CBTC component

- Initial project uses Train Position Determination Module, which uses complex data structure ➔ success
- Project extended to ATP and ATO
- End of project: SCADE generated code ratio is 97%
- Around 60% manpower and 40% time saving (first project ever with SCADE !)

- Katılımız için çok teşekkürler.
- Detaylı bilgi ve toplantı talepleri için; Tahsin.ozturk@numesys.com.tr veya www.numesys.com.tr