Systems & Embedded Software Solutions

MBSE, MBSA for Safety Critical Embedded & HMI Applications in A&D, Rail, Auto and Energy
ANSYS Simulation Platform Overview

... To Complete Systems Simulation

MULTIPHYSICS

SYSTEMS

PLATFORM

FLUIDS

STRUCTURES

ELECTRONICS

SEMI CONDUCTORS

EMBEDDED SOFTWARE
A bit of Background

• We all know and use Computers...........
A bit of Background

• In the Industry (Aeronautic, Automotive, etc...), On Board computers, also referred to as Embedded Computer Systems look like this...
A bit of Background

• When the software on your computer fails, it is **bad**, it is **annoying**, it is **tiring**.........
A bit of Background

- When an On-Board computer fails, it can be more **serious or catastrophic**!
A bit of Background

• As a result, **Safety Critical Software** development has to comply to **Certifications**…

• ... And **even more with Nuclear, Military, Medical etc.**
At ANSYS we enable SYSTEMS

- ...To Complete Systems Analysis and Simulation

VIRTUAL SYSTEM PROTOTYPES

... And Embedded SW is a Critical Component
Systems Development Challenges

- Managing Design Complexity
- Assuring Functional Safety and Security
- Optimizing Overall System Performance
- Providing Reliable Systems
- Reducing Embedded Software Costs
- Reducing Physical Validation Costs
State-of-the-Art Engineering Practices

- Managing Design Complexity
- Model-Based Systems Engineering
- Optimizing Overall System Performance
- Multi-Physics and System Simulation

- Reducing Embedded Software Costs
- Model-Based Software Engineering
- Assuring Functional Safety and Security
- Model-Based Safety and Security Analysis

- Reducing Physical Validation Costs
- 3D Physics Simulation
- Providing Reliable Systems
- Model-based Reliability Evaluation
ANSYS Systems & Embedded Software Capabilities

Model-Based Systems Engineering

Model-Based System Safety Analysis

System Simulation & Digital Twins

System Architecture

System/SW Architecture

SW Components (FMI)

ROM

Model-Based Software Engineering

3D Physics Simulation

ANSYS Innovation Conference - Bologna - June 13, 2018
Automotive Systems Applications

Powertrain/Drivetrain
- Transmission
- Gear Shift
- Engine Control

Body Control
- Front-Light, Back-Light
- Tailgate
- Indicator
- Brake Light
- Wipers
- Door Control
- Climate Control

Chassis
- Electric Power Steering
- Suspension
- Electric Steering Lock
- Braking

ADAS
- Intelligent Speed Assist
- Lane Departure Warning
- Adaptive Cruise Control
- Forward Collision Warning
- Automatic Emergency Braking
- Blind Spot Warning

Electric Drivetrain
- Electric Vehicle (EV) / Hybrid Electric Vehicle (HEV) Engine Controls
- Vehicle energy consumption
- Battery Management
- Driveline (eAxle)

Active & Passive Safety
- Multi-Collision Breaking
- Airbag
- Anti-Lock-Braking
- Electronic Stability Control
- Slip+Traction Control

Autonomous Driving
- Next Generation Electric Power Steering
- Car Driving Simulators
- Machine Learning Algorithms

Displays
- Instrument Clusters
- Head-up Displays
- Infotainment
- Car Driving Simulators
Aerospace Systems Applications

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

Flight Control Systems
- Autopilots
- Air Data and Inertial Reference
- Flight Control / High Lift / Slat&Flaps
- High Lift Hydraulic Control System
- Active Control Side Stick

Engine Control Systems
- Engine Control (FADEC)
- Nacelle Controls
- Thrust Reversers

Mechatronic Control Systems
- Anti-Icing
- Braking and Landing Gear
- Doors and Slides
- Hydraulic Controls

Air & Cabin Control Systems
- Cabin Pressure and Climate Control
- Oxygen Control
- Water & Waste Controls
- Environmental Control Systems
- Fire Protection & Control Systems

Power Control Systems
- Fuel Management
- Power Management, Electrical Load Management
- Auxiliary Power Units (APU)
- Power Conversion Systems
- Starter Generators

Maintenance Systems
- Health Monitoring & Utility
- On-Board Maintenance

Training & Simulators
- 2D simulators
- 3D Simulators
- Maintenance Training Devices

ANSYS Innovation Conference - Bologna - June 13, 2018
UAV, Defense and Space Systems Applications

**Military Mission Avionics**
- Mission Computers
- Helmet-Mounted Displays
- Navigation, Guidance and Inertial Units
- Military Flight Management
- Load Management Systems
- C4ISR and Radar Displays

**UAV Systems**
- UAV Flight Controls
- UAV Mission Systems
- UAV Ground Stations

**Weapons Systems**
- Gun Turret Controls
- Missile Flight Software
- Weapons Stores Management

**Misc. Military Systems**
- Ejection Seat Controls
- Refueling
- Tanker Boom Controls
- Submarine Controls

**Space Control Systems**
- Launchers
- Satellites
- Cargo Systems
- Planetary Landers
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

ANSYS Innovation Conference - Bologna - June 13, 2018
Energy Systems Applications

**Wind Energy**
- Power Electronic Inverters
- Electric Generators
- Drive Train
- Startup/Generator/Pitch Controls
- Grid-side Controls

**Solar Power**
- Power Electronic Inverters
- Positioning Actuation & Controls
- Protection
- Grid-side Controls

**Oil & Gas**
- Power Conversion
- Motor Drives & Controls
- Cables & Umbilicals
- Undersea Robot Controls

**Nuclear Energy**
- Nuclear Instrumentation & Control Systems
- Reactor/Plant Protection Systems
- Reactor Monitoring Displays
- Rod control systems

**Primary & Aux. Power Gen.**
- Gas Turbines
- Electronic Engine Controls
- Uninterruptable Power Supplies
- UPS Controls
- Micro-Turbine Generation

ANSYS Innovation Conference - Bologna - June 13, 2018
Industrial Machinery Systems Applications

**Industrial Drives**
- Machine Drive Systems
- Power Supplies & Conversion
- Controls & Software

**Construction & Heavy Equip.**
- Motor Drives & Controls
- Power Supplies & Conversion
- Control Systems
- Human-Machine Interfaces
- Boom Movement & Anti-Tipping
- Traction Control
- Safety & Surveillance

**Material Handling & Elevators**
- Motor Drives & Controls
- Power Supplies & Conversion
- Human-Machine Interfaces
- Safety & Surveillance

**Manufacturing & Production**
- Power Supplies & Conversion
- Motor Drives & Controls
- Actuators
- Motion Control Systems
- Induction Heating
- Plasma Generation
- Human-Machine Interfaces
ANSYS Systems & Embedded Software Expertise addressing Safety Problematic with the state-of-art portfolio

Model-Based Software Engineering

Model-Based Systems Engineering

Model-Based System Safety Analysis

System Simulation & Digital Twins

SCADE Suite®

SCADE Display®

medini™ analyze

Twin Builder
SCADE
Safety Critical Application Development Environment For Embedded Systems
SCADE MBSE: overcome challenges for Safety Critical Software Development

- Avoid multiple descriptions of the software
- Prevent ambiguity and lack of accuracy in specifications
- Avoid design and coding errors
- Allow efficient implementation of code on target
- Find specification and design errors as early as possible
- Lower complexity of updates
- Improve verification efficiency
- Provide efficient way to store Intellectual Property (IP)
- Drive and map SW Development process to CERTIFICATION goals
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)
# Where Time Goes in Embedded Software Projects?

<table>
<thead>
<tr>
<th>Phase</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept Definition</td>
<td>5%</td>
</tr>
<tr>
<td>System Design (Requirements, Functions and System Architecture)</td>
<td>12%</td>
</tr>
<tr>
<td>System Requirements allocated to Software (HLRs)</td>
<td>14%</td>
</tr>
<tr>
<td>Software Design (LLRs)</td>
<td>15%</td>
</tr>
<tr>
<td>Coding</td>
<td>10%</td>
</tr>
<tr>
<td>Software Unit Testing (Low Level testing)</td>
<td>10%</td>
</tr>
<tr>
<td>Software / Software Integration &amp; Testing</td>
<td>7%</td>
</tr>
<tr>
<td>Hardware/Software Integration &amp; Testing</td>
<td>10%</td>
</tr>
<tr>
<td>Documentation &amp; Reviews</td>
<td>7%</td>
</tr>
<tr>
<td>Project Management</td>
<td>10%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>100%</td>
</tr>
</tbody>
</table>

*Source: AGARD (USA)*
## Where Does SCADE Cut Costs?

<table>
<thead>
<tr>
<th>Phase</th>
<th>Comments</th>
<th>Reference Cost Breakdown (Manual process)</th>
<th>Cost Breakdown (SCADE-based process)</th>
<th>SCADE Gain</th>
<th>Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept Definition</td>
<td></td>
<td>5</td>
<td>5</td>
<td>0%</td>
<td>Out of the scope of SCADE</td>
</tr>
<tr>
<td>System Design (Requirements, Functions and System Architecture)</td>
<td>Functional &amp; Architectural Definition, System Safety Analysis</td>
<td>12</td>
<td>8</td>
<td>35%</td>
<td>Usage of SCADE System to model functions and architecture</td>
</tr>
<tr>
<td>System Requirements allocated to Software (HLRs)</td>
<td>Control Laws, Logic definition, HLRs (text, equations...)</td>
<td>14</td>
<td>9</td>
<td>35%</td>
<td>Reuse of functional and architectural definitions done in SCADE System</td>
</tr>
<tr>
<td>Software Design (LLRs)</td>
<td>Detailed SW architecture, Functional design, Requirements-based tests creation</td>
<td>15</td>
<td>18</td>
<td>-20%</td>
<td>Detailed SW architecture, Functional design (if not using SCADE for Control laws). Additional formalisation of Software detailed specifications, requirements traceability</td>
</tr>
<tr>
<td>Coding</td>
<td>Detailed Coding</td>
<td>10</td>
<td>2</td>
<td>85%</td>
<td>Percentage of code automatically generated with SCADE</td>
</tr>
<tr>
<td>Software Unit Testing (Low Level testing)</td>
<td>Functional Unit testing</td>
<td>10</td>
<td>2</td>
<td>85%</td>
<td>Qualification of the Code Generator suppresses low-level testing against the code generated with SCADE</td>
</tr>
<tr>
<td>Software / Software Integration &amp; Testing</td>
<td>Testing of the above</td>
<td>7</td>
<td>1</td>
<td>85%</td>
<td>SW/SW Integration testing fully automated by SCADE for the SW application part</td>
</tr>
<tr>
<td>Hardware/Software Integration &amp; Testing</td>
<td>Incl. On target debugging</td>
<td>10</td>
<td>5</td>
<td>50%</td>
<td>Model already debugged - Very short late changes cycles, Compiler Verification Kit automates User Context verification and SCADE LifeCycle QTE automates application testing on target</td>
</tr>
<tr>
<td>Documentation &amp; Reviews</td>
<td>Design documentation and Quality reviews</td>
<td>7</td>
<td>1</td>
<td>85%</td>
<td>Doc for project and for authorities is automatically generated by SCADE LifeCycle</td>
</tr>
<tr>
<td>Project Management</td>
<td></td>
<td>10</td>
<td>5</td>
<td>50%</td>
<td>Automation of connection with Config Management Tools, Shortening of project duration, better requirements traceability thanks to SCADE LifeCycle</td>
</tr>
<tr>
<td><strong>TOTAL:</strong></td>
<td></td>
<td><strong>100</strong></td>
<td><strong>50</strong></td>
<td><strong>50%</strong></td>
<td></td>
</tr>
</tbody>
</table>
Safety-Critical Embedded Systems: The Need for an Integrated Toolkit

System/Software Architecture Design
Embedded Control Software Design
Embedded HMI Software Design
Embedded Software Testing

System & Software
Lifecycle Management

ANSYS Innovation Conference - Bologna - June 13, 2018
ANSYS SCADE Products in the Software V-Cycle
ANSYS SCADE Products in the Software V-Cycle

Embedded System & Software Lifecycle Management

System/Software Architecture Design

Embedded Control Software Design

Embedded HMI Software Design

Integration Testing (Hardware-In-the-Loop)

Model-Based Design & Model-Based Testing

Embedded Software Testing Environment

ANSYS Innovation Conference - Bologna - June 13, 2018
ANSYS SCADE Architect

Model-Based embedded systems architecture design

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

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, and US DoD FACE
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-178B/C, EN 50128, ISO 26262, IEC 61508)
Enables 80% embedded code production and testing cost reduction

/* CruiseControl */

void CruiseControl_CruiseControl(
    /* On/ */
    kcg_bool On,
    /* Off/ */
    kcg_bool Off,
    /* SM1: */
    switch(outC_CruiseControl_CruiseControl outC)
        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;
    }

ANSYS Innovation Conference - Bologna - June 13, 2018
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-178B/C, 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 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
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 Innovation Conference - Bologna - June 13, 2018
What is Unique About SCADE?

• SCADE Architect enables **system & software architecture design** with a seamless path to embedded software development process

• SCADE Test enables **full testing environment** from rapid prototyping on host to on-target execution with coverage measures and qualified reports

• SCADE LifeCycle supports **integrated lifecycle** of system and software development processes
Unique Integration of Systems & Embedded Software Solutions

System & SW Architecture

System Requirements

SW Design

Software Requirements

Automatic SW Code Generation

RTOS & HW platforms
Multi-rate / Multi-core

System Safety

System Simulation & Digital

Simulation

Test

ANSYS Innovation Conference - Bologna - June 13, 2018
What is Unique with SCADE?

• 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:
  • DO-178C qualification up to Level A – A&D
  • 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
  • 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
## Comparative Software Development Cost per Safety Level, including Testing

### DO-178C

<table>
<thead>
<tr>
<th>DO-178C Level</th>
<th>Level E Cost</th>
<th>Level D Cost</th>
<th>Level C Cost</th>
<th>Level B Cost</th>
<th>Level A Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comparative Cost*</td>
<td>Baseline</td>
<td>Level E +10%</td>
<td>Level D +36%</td>
<td>Level C +80%</td>
<td>Level B +30%</td>
</tr>
<tr>
<td>Cost</td>
<td>100</td>
<td>110</td>
<td>150</td>
<td>270</td>
<td>350+</td>
</tr>
<tr>
<td>Cost with SCADE</td>
<td>100</td>
<td>100</td>
<td>120</td>
<td>160</td>
<td>175</td>
</tr>
<tr>
<td>Savings with SCADE</td>
<td>-</td>
<td>10%</td>
<td>20%</td>
<td>40%</td>
<td>50%</td>
</tr>
</tbody>
</table>

### EN-50128

<table>
<thead>
<tr>
<th>Level</th>
<th>Non-Safety Related Cost</th>
<th>SIL 1 Cost</th>
<th>SIL 2 Cost</th>
<th>SIL 3 Cost</th>
<th>SIL 4 Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost without SCADE</td>
<td>100</td>
<td>110</td>
<td>150</td>
<td>270</td>
<td>350+</td>
</tr>
<tr>
<td>Cost with SCADE</td>
<td>100</td>
<td>100</td>
<td>120</td>
<td>160</td>
<td>175</td>
</tr>
<tr>
<td>Savings with SCADE</td>
<td>-</td>
<td>10%</td>
<td>20%</td>
<td>40%</td>
<td>50%</td>
</tr>
</tbody>
</table>

### IEC-61508

### ISO-26262

<table>
<thead>
<tr>
<th>Level</th>
<th>Non-Safety Related Cost</th>
<th>ASIL A Cost</th>
<th>ASIL B Cost</th>
<th>ASIL C Cost</th>
<th>ASIL D Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comparative Cost*</td>
<td>Baseline</td>
<td>Base +10%</td>
<td>SIL 1 +36%</td>
<td>SIL 2 +80%</td>
<td>SIL 3 +30%</td>
</tr>
<tr>
<td>Cost</td>
<td>100</td>
<td>110</td>
<td>150</td>
<td>270</td>
<td>350+</td>
</tr>
<tr>
<td>Cost with SCADE</td>
<td>100</td>
<td>100</td>
<td>120</td>
<td>160</td>
<td>175</td>
</tr>
<tr>
<td>Savings with SCADE</td>
<td>-</td>
<td>10%</td>
<td>20%</td>
<td>40%</td>
<td>50%</td>
</tr>
</tbody>
</table>
SCADE Benefits and Value Proposition for Safety Critical Applications

**STRATEGIC**
- Compliance with Software Safety Certification and Quality requirements at lowest cost
- Improved Communication & Collaboration among system and software teams, customers, suppliers and certification authorities
- Product Line Development support

**TECHNICAL**
- Automated Production of readable, portable, high performance and high quality Code
- Documentation Quality and Accuracy
- Early Detection of Design Flaws
- Improved Long-term Maintainability of applications

**ECONOMICAL**
- 50% Development and V&V Costs Reduction overall
medini analyze
MBSA
Model Based Safety Assessment
Safety terminology

• **Safety** is the **absence of (unreasonable) risk** to cause **physical injury** or damage to the **health of persons**.

• In automotive there are a variety of different safety terms:
  – Active Safety
  – Passive Safety
  – Product Safety / Safety Of The Intended Function (SOTIF)
  – Functional Safety

• ... and besides that we also have the requirements on Security
Functional Safety Analysis Across Industries

- IEC-61800-5-2: Electrical Drives
- IEC-61513: Nuclear
- IEC-61508: Generic E/E/PE
- IEC-61511: Process
- IEC-60601: Medical Devices
- ISO-13849-1: Machinery
- ARP4754, DO-178B/C, DO-254: Aerospace
- ISO-26262: Automotive
- ISO-13849: Control Systems
- ISO-25119: IFE
- EN-50128: Railway Application

ANSYS Innovation Conference - Bologna - June 13, 2018
Product Safety and Functional Safety

- Product Safety/SOTIF addresses the nominal performance of such functions in order to avoid the risk of harm by normal operation
  - Typical topics are reaction times, torque limits, environmental conditions, driver actions, ...

- Functional Safety addresses faults/malfunctions of such functions and targets to avoid or detect them in case they have the potential to cause harm to humans
  - Faults result in behavior outside of specified limits, no functionality when required, functionality when not required ...
Functional Safety Standards

Safety Process
– In general based on the classic V-Model for development & engineering
– Terminology

Risk assessment methods
– SIL, ASIL, PL, AgPL ...

Risk mitigation methods
– Process measures
  • mostly based on V-Model
  • some standards cover also hydraulics, mechanics ...
– Architecture measures
  • from wide selection of options to predefined architecture patterns
– HW/SW design guidelines
  • different degree of specification formality
  • coding rules, architecture patterns ...

Validation and Verification measures

Metrics
SPF/LMF/PMHF, MTBF, SFF, MTTF, ...

Tests
varying types and coverage criteria

Safety analyses
FTA, FMEA, ETA, Markov Chains, RBD ...

ANSYS Innovation Conference - Bologna - June 13, 2018
Comparing Different Safety Domains

ISO 26262
- Risk Graph (HARA): S/E/C -> ASIL
- Requirements: SGs, ASIL, decomposition
- SysML: ASIL, independence
- FMEDA: SPF/LF Metrics
- FTA: PMHF

ARP 4754/4761
- Risk Graph (FHA): Sev/Prob -> DAL
- Requirements: DAL
- SysML: FDAL (functions), IDAL (items)
- FMEDA: FMECA/individual risks
- FTA: Avg. P per flight hour

IEC61508, ISO 13849
- Risk Graph (PHA): S/F/P -> PL/SIL
- Requirements: SIL
- SysML: SIL, Safety functions
- FMEDA: SFF, MTTF
- FTA: PFD, PFH
ISO 26262 Safety Activities throughout the Development Process
Purpose of tool support for functional safety

• Help to create **Safe Systems** and to avoid hazards
• Create and relate all work products required by Safety Standards
• Speed up the required safety analysis
• Help to pass Safety Assessments/Certification efficiently
• Help in later liability cases by well-structured information
medini analyze – a Model based and System oriented Solution

Model-based approach ensures unrivalled level of consistency, traceability and efficiency
medini analyze – one solution for all safety activities

- Allocation between Architectures
- System and Functional Modeling based on SysML 1.4
- Reliability and Prediction Data
- Failure Connection Model
- Failure Rate Catalogs
- Mission Profiles
- Element Library
- Activity Diagrams

- Functional-, Technical-, HW-, and SW-Requirements Management
- Traceability
- Allocation to Architectures
- Safety Goals
- ASIL Propagation
- ASIL Decomposition
- Safety Measures & Safety Mechanisms
- Graphical Editor & Table Editor

- Safety Plan
- Task Management
- CMS Integration
- Workflow Management
- Process Management Support
- customization features
- Project Validation/Verification
- review/assessment support
- reusable knowledge libraries
- ALM/PLM
medini analyze – state-of-the-art safety and reliability analysis

HARA
- HAZOP
- Operational Situations Catalog
- ASIL Determination
- Severity, Exposure, and Controllability Values
- Hazards
- Safety Goals

FTA
- Qualitative FTA
- Quantitative FTA
- PMHF, PFD, ...
- Connected to Elements, Failure Modes, and Failure Rates

FMEA
- System FMEA
- Design FMEA
- Component FMEA
- Process FMEA
- Function FMEA
- VDA, SAE, ...
- Always synchronized with the system model

FMEDA
- Hardware Libraries
- BOM Import
- SPFM, LFM, Totals, ...
- Always synchronized with the system model and the Failure Rates

ANSYS Innovation Conference - Bologna - June 13, 2018
Seamless integration with the engineering toolchain

System Models
- SCADE Architect
- Rational Rhapsody
- Enterprise Architect
- ARTOP
- MATLAB Simulink
- BOM Import
- Export
- Cadence IP Design Data (Behaviour, NL, RTL)

Safety Requirements
- Jama
- Doors
- PTC Integrity
- Polarion
- ReqIF
- Excel

Task Management
- Jira
- TRAC
- Bugzilla
- Redmine
- Mantis
- PTC Integrity

Import
- Excel
- MSR-XML
- FaultTree+

Export
- standard Reports
- custom Reports
- OpenPSA
- MS Word & Excel
- PDF
- HTML
Integration is Key in this complex World

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

Extended with analysis related properties

Safety Requirements
- JAMA
- DOORS
- PTC Integrity
- ReqIF

PHA / Hazard Analysis & Risk Assessment
- Excel
- Word/PDF/HTML

HAZOP
- Excel
- Word/PDF/HTML

FMEA
- MSR-XML
- Task Management
- Excel

FMEADA
- SPF/LF Metrics

Reliability Prediction
- FaultTree+
- OpenPSA
- Excel
- Word/PDF/HTML

FTA
- Excel

Safety Plan
- Task Management

Task Management
- Excel

ANSYS Innovation Conference - Bologna - June 13, 2018
Automotive: ISO 26262

- is an international standard dedicated to product development processes for safety-related electrical and/or electronic systems.
- safety standards like ISO 26262 require to perform multiple analysis methods in a consistent, thoroughly manner.
ISO 26262 2nd Edition is expected soon, this year, 2018

Revision of the international standard dedicated to product development processes for safety-related electrical and/or electronic systems (E/E system) comes with new challenges for Semiconductors.

Safety Requirements

- Failure Mode and Effects Analysis (FMEA)
- Hardware Diagnostic Coverage Metrics (FMEDA)
- Safety Mechanism Design/Evaluation
- Fault Injection & Simulation
- Fault Tree Analysis (FTA)
- Dependent Failure Analysis
- Change Management & Impact Analysis

Extended Scope:
- Heavy Trucks
- Buses
- Motorcycles

NEW!
Complete FMEDA Workflow for Semiconductors

1. Export design data including die area/gate counts
2. Import design and map it to high level block descriptions
3. Predict failure rates: distribution over blocks is automated from mapping!
4. Perform FMEDA to compute SPF/LF metrics, safe fault fractions, etc.
5. Generate fault lists from FMEDA for fault injection simulation
6. Perform fault injection and simulation to determine coverage of safety mechanisms
7. Update Diagnostic Coverage for Safety Mechanisms and safe faults fractions from fault injection

Safety and Reliability Analysis (medini analyze)

Chip Design

Behavior

Register Transfer Level (RTL)

Netlist (NL)

Hardware Design Tooling (e.g. CADENCE, ANSYS RedHawk)
Aerospace: ARP4754A and ARP4761
international standards dedicated to development/safety assessment of civil aircraft and systems

system functions
- failure conditions
- functional hazard assessment
- risk classification
- system architecture

preliminary system safety assessment
safety requirements

system safety assessment
- Failure Mode and Effect Analysis (FMEA)
- FMES/FMECA
- Fault Tree Analysis (FTA)
- Common Cause Analysis (CCA)
- configuration management
- change management

safety standards require to perform multiple analysis methods in a consistent, thoroughly manner
medini Cyber Security Package

• Support Cyber Security analysis **early** in system design

• Provide Threat Identification Methods
  – Attack Trees with Attack Paths
  – Customer-specific methods

• Allow Customizable Threat Assessment
  – EVITA/Common Criteria
  – CVSS/CRSS
  – Customer-specific methods

• Further analysis methods
  – Co-Engineering Safety/Security: Interference Analysis

*If it’s not secure it’s not safe*
### Systems & Embedded Software Solutions

<table>
<thead>
<tr>
<th>Product Development Process Improvements</th>
<th>Best Practices for:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Model-Based Systems Engineering</td>
</tr>
<tr>
<td></td>
<td>• System Safety Analysis</td>
</tr>
<tr>
<td></td>
<td>• Integrated Multi-physics and Software Simulation</td>
</tr>
<tr>
<td></td>
<td>• Embedded Controls development</td>
</tr>
<tr>
<td></td>
<td>• Interactive Displays development</td>
</tr>
</tbody>
</table>

#### Key Benefits:

- **50%** Development Costs Reduction
- **2X** Time-to-Market Speed up
THANK YOU!