Design und Verifizierung nach Sicherheitsstandards

Simon Zubler
03.09.2019, Embedded Computing Conference, Winterthur
Electronic Trends Continue in 2019

<table>
<thead>
<tr>
<th>Trend</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smaller</td>
<td>3D mCAD integration, embedded components, rigid-flex, test, fine pitch, HDI</td>
</tr>
<tr>
<td>Faster</td>
<td>Signal integrity, shielding</td>
</tr>
<tr>
<td>Cheaper</td>
<td>Shorter component lifetime, EOL, alternate parts</td>
</tr>
<tr>
<td>Complexer</td>
<td>Higher integration, EMI, thermal</td>
</tr>
<tr>
<td>Higher Frequencies</td>
<td>Signal integrity, EMI</td>
</tr>
<tr>
<td>Low Power</td>
<td>Lower voltages, higher currents, thermal, power integrity</td>
</tr>
<tr>
<td>Connected</td>
<td>Standard interfaces, WLAN, SI-verification</td>
</tr>
<tr>
<td>Reliability</td>
<td>Thermal, stress, MTBF, ISO 26262</td>
</tr>
</tbody>
</table>

All trends lead to more design constraints and early issue recognition.
Solutions for Developers and Designers

- PCB Layout
- PSpice - Simulation
- SI- and PI-Simulation
- EMI and Antenna Simulation
- Magnetics Simulation
- Timing Analysis
- Thermal Simulation
- 3D mCAD-eCAD Integration
- CAM Verification
- Functional Safety / Reliability
- Model Based Design
- Boundary Scan Test
- CAD-Flow Management
- PLM and ERP-Connection
Focus on Customer Satisfaction

Sales
• Fair, competent advice
• Long term solutions

Support
• Hotline, Fastviewer
• Survey

Service
• PCB Design Services (Layout, Simulation, Migration)

Training
• Trainings center, on-site
• Workshops
Funktionale Sicherheit
Product Safety and Functional Safety

Warum Funktionale Sicherheit?

- zunehmend komplexere technische Systeme
  - Steuerung und Regelung von sicherheitskritischen Prozessen
  - Ablösung von mechanischen Systemen durch elektronische oder mechatronische
  - Verflochtene Systemverbünde
- Anforderungen werden vielfältiger
  - Kosten, Wettbewerb, Leistungsfähigkeit, Umwelt, Sicherheit und Zuverlässigkeit spielen eine hierbei eine grosse Rolle
  - Fast nur durch Einsatz von Elektronik & Software machbar

Sicherheitskritische Aufgaben:
- Überwachung von Fahrzeugzuständen und Fahrsituationen
- Steuerung von Zügen
- Regelung von Prozessen in chemischen Anlagen
- Roboter-Operationssysteme im medizinischen Bereich
Historie

- Auslöser war eine unkontrollierte Überhitzungsreaktion, die durch Überdruck eine Sicherung zerstörte
- Automatische Kühlsysteme für den Reaktor fehlten
- zum Zeitpunkt des Störfalls befand sich kein Chemiefachpersonal im Werk

EU: Seveso I-Richtlinie, Seveso II-Richtlinie (96/82/EU)
D: DIN Normen…..DIN61508/511 → IEC61508/511
IEC – 61508 und daraus entstandene Ableitungen

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

• Untersuchung der Umstände und Situationen, in denen ein System Menschen verletzen oder töten könnte

• HARA – Hazard Analysis and Risk Assessment

• Ermittlung Sicherheitsintegritätslevel
  – SIL/ASIL

• Ableiten von Sicherheitszielen („Safety Goals“), die das ungewollte Verhalten beschreiben

• Ableitung Safety Concept
  – Functional/Technical

• Product Development

• Safety Validation
Safety Activities in the Development Process

Additional Requirements to Architecture and Design

Additional Requirements to Verification and Test
Normen Nomenklatura

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

Risk assessment methods
- SIL, ASIL

Risk mitigation methods
- Process measures eg V-Model
- Architecture measures
- **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 ...

Einteilung Geräte in Klassen

SFF (Safe Failure Fraction/Anteil ungefährlicher Ausfälle)
HFT Hardware Failure Tolerance

<table>
<thead>
<tr>
<th>SFF</th>
<th>HFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 60%</td>
<td>-</td>
</tr>
<tr>
<td>60-90%</td>
<td>SIL1</td>
</tr>
<tr>
<td>90-99%</td>
<td>SIL2</td>
</tr>
<tr>
<td>&gt; 99%</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

„90%“ - 90 von hundert sind unbedenklich

PFD (Probability of Failure on Demand/gefährliche Versagenswahrscheinlichkeit)

<table>
<thead>
<tr>
<th>PFDaverage</th>
<th>SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥ 10⁻²</td>
<td>SIL1</td>
</tr>
<tr>
<td>≥ 10⁻³</td>
<td>SIL2</td>
</tr>
<tr>
<td>≥ 10⁻⁴</td>
<td>SIL3</td>
</tr>
<tr>
<td>≥ 10⁻⁵</td>
<td>SIL4</td>
</tr>
</tbody>
</table>
Implementation of Functional Safety Standards

- an international standard dedicated to product development processes for safety-related electrical and/or electronic systems (E/E system)

- controllability analysis
- driving situation analysis
- hazard analysis
- risk assessment
- safety goals
- safety requirements
- functional and technical safety concept
- safety validation
- FMEA and FMEDA
- hardware diagnostic coverage metrics (SPF, LF)
- fault tree analysis
- configuration management
- change management
- dependent failure analysis (DFA)
- safety architecture and safety mechanisms design

Safety standards require to perform multiple analysis methods in a consistent, thorough manner
Traditional Approach

- Example from our customer AUDI at medini User Conference 2018
- Document driven processes are error prone and inefficient
- Traceability cannot be demonstrated
- Impact analysis in case of change is hard to implement
Traditional Approach – Point Tools

→ Low Efficiency (as tool does automate typical tasks...)
→ Much double work
→ Inconsistencies within safety and between safety and normal development
→ Reuse performed unsystematically (further inconsistencies, no effective work reduction)
→ Difficult to present (especially, when original analysts have gone...)
ANSYS Systems & Embedded Software Capabilities

Model-Based Systems Engineering

System Safety Analysis

System Simulation & Digital

Twin Builder

Model-Based Software Engineering

3D Physics Simulation
Model based and System oriented Solution

System Models
Functional, Architecture, Hardware, PCB, Software, IP Design, RTL/NL

Extended with analysis related properties

PHA / Hazard Analysis and Risk Assessment
Diagnostic Coverage Metrics / FMEDA
Failure Rate Prediction

Safety Requirements
FMEA
HAZOP
FTA
Safety Plan

Model-based approach ensures unrivalled level of consistency, traceability and efficiency
Integration is Key in this complex World

Safety Requirements

PH-DOORS

PTC Integrity

ReqIF

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

Extended with analysis related properties

SCADE Architect
IBM Rhapsody
Enterprise Architect
MATLAB Simulink

PHA / Hazard Analysis & Risk Assessment

HAZOP

FMEA

FMEET

Metrics

Reliability Prediction

Excel

Task Management

FaultTree+
OpenPSA

Excel

Word/PDF/HTML

Excel

Word/PDF/HTML

MSR-XML

Task Management

Excel

Word/PDF/HTML

Safety Plan
Safety Lifecycle – Example

Determination of a suitable tool
Instance links in Medini analyze

Tool Selection Criteria
- Solid data handling
- Links between artefacts
- Optimisation of the consistency of safety concepts due to OCL Constraints
- Visualization through failure nets, dependency graph and matrices
- Increasing of efficiency
Customer Examples from User Conferences

Dr. Wolfgang Freese: „Applying FMEDA and FTA on E/E systems The advantage of a single tool solution“, 2016 medini analyze user conference, Troy, MI

Fujiyama Koji: „Efficient ISO 26262-based development using medini analyze“, 2017 medini analyze User Day, Tokyo, Japan
# medini™ analyze – 2016/17 Customer Stories

<table>
<thead>
<tr>
<th>Company</th>
<th>Description</th>
</tr>
</thead>
</table>
| **DAIMLER**   | • DAIMLER runs functional safety concept related activities using medini  
• high consistency in the safety work products throughout the business units  
• **almost all manual review work is now automated by medini**  
| **ZF, TRW**   | • medini analyze in integrated engineering environment from concept and system all the way down to hardware and software safety  
• application domains braking, steering and ADAS with 55% effort reduction  
• **integrated chain with requirements, engineering, analysis and ALM tools**  
| **Audi**      | • medini analyze is used from HARA all the way down to function development  
• application domain powertrain – engine development  
• **Audi is managing their 1200+ safety case variants using medini analyze**  
| **ADI**       | • ADI applies medini analyze mainly for conducting FTA and FMEDA for their ICs used in their radar solutions  
• efficient and consistent approach to functional safety is key  
• **50% effort/time reduction through medini compared to their earlier approach**  
| **Allegro**   | • medini analyze is used for IC design safety analysis  
• standardization of safety analysis for a global company with remote design centers  
• **Unification of safety analysis in one tool: Medini Analyze**  

---

[FlowCAD Confidential]
ANSYS Medini Analyze
medini™ analyze – User Interface
# Checklist

<table>
<thead>
<tr>
<th>Task/Requirement</th>
<th>Checked</th>
<th>Related Artifacts</th>
<th>Checked By</th>
<th>Date of Check</th>
<th>Note</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add known hazards</td>
<td>✅</td>
<td>[HZ 1] Steering blocked</td>
<td>eholz</td>
<td>04.02.19 19:36</td>
<td></td>
<td>Use “Hazards and Top-Level Effects” in the Hazard analysis and Risk Assessment Folder to capture all known hazards or other unwanted effects related to the item. Organize in “Additional Material” folder: Create and use sub-folders if necessary.</td>
</tr>
<tr>
<td>Additional documents</td>
<td>✅</td>
<td>Wikipedia</td>
<td>eholz</td>
<td>04.02.19 19:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hazard Analysis and Risk Assessment</td>
<td>✅</td>
<td></td>
<td>eholz</td>
<td>04.02.19 21:26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification of malfunctions</td>
<td>✅</td>
<td></td>
<td>eholz</td>
<td>04.02.19 21:26</td>
<td></td>
<td>A systematic approach shall be applied to identify the malfunctioning behavior for all functions of the item.</td>
</tr>
<tr>
<td>Perform HAZOP for all Item Functions</td>
<td>✅</td>
<td></td>
<td>eholz</td>
<td>04.02.19 21:25</td>
<td></td>
<td>Perform an HAZOP to systematically investigate the potential for malfunctioning behavior.</td>
</tr>
<tr>
<td>Option A: Using HAZOP Table</td>
<td>✅</td>
<td></td>
<td>eholz</td>
<td>04.02.19 19:47</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure traceability for Malfunctions</td>
<td>✅</td>
<td></td>
<td>eholz</td>
<td>04.02.19 19:48</td>
<td></td>
<td>Create traces between the HAZOP Analysis/Checklists and the related functions as well as between the HAZOP entries and the related Malfunctions as required.</td>
</tr>
<tr>
<td>Perform FMEA (optional)</td>
<td>✅</td>
<td></td>
<td>eholz</td>
<td>04.02.19 19:57</td>
<td>Malfunctions of Supporting functions may cause malfunctions of other Supporting functions and/or of Vehicle Level Functions. Malfunctions of “Vehicle Level” functions may cause Hazards. The cause-effect relations shall be investigated using a (simplified) function FMEA (derived from the “Item Functions” model) or using individual Failure Mode for the Malfunctions. Create new malfunctions/hazards if necessary.</td>
<td></td>
</tr>
<tr>
<td>Perform HAR</td>
<td>✅</td>
<td></td>
<td>eholz</td>
<td>04.02.19 21:25</td>
<td>At least for all malfunctions which directly cause hazards the HAR should be performed by combining them with all relevant operational situations. Start with situations from catalog and add further situations when required. Use the HAR table and/or the HAR matrix view as it is convenient.</td>
<td></td>
</tr>
<tr>
<td>Organize HAR tables</td>
<td>✅</td>
<td>HAR for LOCK Malfunctions, HAR for UNLOCK Malfunctions</td>
<td>eholz</td>
<td>04.02.19 21:25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organize Malfunctions</td>
<td>✅</td>
<td>Hazards and Top-Level Effects</td>
<td>eholz</td>
<td>04.02.19 21:25</td>
<td></td>
<td>Organize all Hazards detected during HAR in the collection “Hazards and Top-Level Effects”</td>
</tr>
<tr>
<td>Organize Safety Goals</td>
<td>✅</td>
<td>Functional Safety Requirements</td>
<td>eholz</td>
<td>04.02.19 21:25</td>
<td>The Functional Safety Concept consists of the Safety Goals, the Functional Safety Requirements, the Functional Safety Architecture and the relations between</td>
<td></td>
</tr>
</tbody>
</table>
HAZOP – Hazard and Operability

<table>
<thead>
<tr>
<th>Element</th>
<th>NO OR NOT</th>
<th>MORE</th>
<th>LESS</th>
<th>AS WELL AS</th>
<th>PART OF</th>
<th>REVERSE</th>
<th>OTHER THAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>[F-001]</td>
<td>Lock not activated when required</td>
<td>[MF-001]</td>
<td>Locked too strong</td>
<td>[MF-002]</td>
<td>Lock does not lock completely</td>
<td>[MF-006]</td>
<td>Unlock not activated when required</td>
</tr>
<tr>
<td>[F-002]</td>
<td>Unlock not activated when requested</td>
<td>[MF-003]</td>
<td>Ignition not detected</td>
<td>[MF-005]</td>
<td>Unlock does not unlock completely</td>
<td>[MF-007]</td>
<td>Ignition not detected when ignition is on</td>
</tr>
<tr>
<td>[F-001]</td>
<td>No status detected</td>
<td>[MF-017]</td>
<td>Ignition not detected when ignition is off</td>
<td>[MF-010]</td>
<td>Ignition not detected when ignition is on</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Additional Material
- Hazard Analysis and Risk Assessment
- Hazards and Top-Level Effects
- HARA for LOCK Malfunctions
- HARA for UNLOCK Malfunctions
- HAZOP Analysis
- Safety Goals and Requirements
- Safety Analysis
- Assessment and Audit Checklists
- S18_Aircraft Level
- S15_Complied
- S15_System Level
**HARA – Hazard Analysis & Risk Assessment**

<table>
<thead>
<tr>
<th>Potential Effect</th>
<th>Severity</th>
<th>Vulnerability</th>
<th>Exposure</th>
<th>Exposure Comment</th>
<th>Controllability</th>
<th>Controllability Comment</th>
<th>ASL</th>
<th>Safety Goal</th>
<th>Safe State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crash into obstacle, leaving road</td>
<td>S3</td>
<td>High speed</td>
<td>E4</td>
<td>General Driving at recommended speed</td>
<td>C3</td>
<td>distance to other vehicles; small road, braking not sufficient</td>
<td>D</td>
<td>SG-002</td>
<td>Prevent activation of steering lock while driving (ASS)</td>
</tr>
<tr>
<td>Crash into other vehicle, leaving road</td>
<td>S3</td>
<td>High speed</td>
<td>E4</td>
<td>General Changing lanes</td>
<td>C3</td>
<td>distance to other vehicles; small road, braking not sufficient</td>
<td>D</td>
<td>SG-002</td>
<td>Prevent activation of steering lock while driving (ASS)</td>
</tr>
<tr>
<td>Crash into other vehicles</td>
<td>S2</td>
<td>Medium speed</td>
<td>E4</td>
<td>Changing lanes in city traffic</td>
<td>C3</td>
<td>distance to other vehicles</td>
<td>C</td>
<td>SG-002</td>
<td>Prevent activation of steering lock while driving (ASS)</td>
</tr>
<tr>
<td>Crash into other vehicles or leaving road</td>
<td>S3</td>
<td>High speed</td>
<td>E3</td>
<td>General driving on country road with narrow curves</td>
<td>C3</td>
<td>distance to other vehicles; small road, braking not sufficient</td>
<td>C</td>
<td>SG-002</td>
<td>Prevent activation of steering lock while driving (ASS)</td>
</tr>
<tr>
<td>Crash into other vehicles or leaving road</td>
<td>S3</td>
<td>High speed</td>
<td>E3</td>
<td>General overtaking on country road</td>
<td>C3</td>
<td>distance to other vehicles; small road, braking not sufficient</td>
<td>C</td>
<td>SG-002</td>
<td>Prevent activation of steering lock while driving (ASS)</td>
</tr>
<tr>
<td>Crash into construction worker</td>
<td>S3</td>
<td>High speed</td>
<td>E3</td>
<td>Stopping at traffic lights in cities</td>
<td>C3</td>
<td>distance to other vehicles; small road, braking not sufficient</td>
<td>C</td>
<td>SG-002</td>
<td>Prevent activation of steering lock while driving (ASS)</td>
</tr>
<tr>
<td>Crash into obstacle, leaving road</td>
<td>S3</td>
<td>Very high speed</td>
<td>E3</td>
<td>General High-speed driving</td>
<td>C3</td>
<td>distance to other vehicles; small road, braking not sufficient</td>
<td>C</td>
<td>SG-002</td>
<td>Prevent activation of steering lock while driving (ASS)</td>
</tr>
<tr>
<td>Crash into other vehicles or leaving road</td>
<td>S2</td>
<td>Medium speed</td>
<td>E4</td>
<td>Stopping at traffic lights in cities</td>
<td>C2</td>
<td>distance to other vehicles; small road, braking not sufficient</td>
<td>B</td>
<td>SG-002</td>
<td>Prevent activation of steering lock if IGN is ON (ASS)</td>
</tr>
<tr>
<td>Crash into other vehicles or pedestrians</td>
<td>S2</td>
<td>Medium speed</td>
<td>E4</td>
<td>Stopping at traffic lights in cities</td>
<td>C2</td>
<td>distance to other vehicles; small road, braking not sufficient</td>
<td>B</td>
<td>SG-002</td>
<td>Prevent activation of steering lock if IGN is ON (ASS)</td>
</tr>
<tr>
<td>Crash into other vehicles or pedestrians</td>
<td>S2</td>
<td>Medium speed</td>
<td>E4</td>
<td>Stopping at traffic lights in cities</td>
<td>C2</td>
<td>distance to other vehicles; small road, braking not sufficient</td>
<td>B</td>
<td>SG-002</td>
<td>Prevent activation of steering lock if IGN is ON (ASS)</td>
</tr>
<tr>
<td>Crash into structure</td>
<td>S1</td>
<td>Low speed</td>
<td>E2</td>
<td>Stopped at entrance/exit of parking structure</td>
<td>C2</td>
<td>distance to structure</td>
<td>QM</td>
<td>SG-002</td>
<td>Prevent activation of steering lock if IGN is ON (ASS)</td>
</tr>
<tr>
<td>Crash into structure or other vehicles</td>
<td>S1</td>
<td>Low speed</td>
<td>E2</td>
<td>Backing up in city traffic</td>
<td>C1</td>
<td>distance to structure</td>
<td>QM</td>
<td>SG-002</td>
<td>Prevent activation of steering lock if IGN is ON (ASS)</td>
</tr>
<tr>
<td>Crash into structure or other vehicles</td>
<td>S1</td>
<td>Low speed</td>
<td>E2</td>
<td>Stopped at entrance/exit of parking structure</td>
<td>C2</td>
<td>distance to structure</td>
<td>QM</td>
<td>SG-002</td>
<td>Prevent activation of steering lock if IGN is ON (ASS)</td>
</tr>
<tr>
<td>Crash into structure</td>
<td>S1</td>
<td>Low speed</td>
<td>E2</td>
<td>Stopped at entrance/exit of parking structure</td>
<td>C2</td>
<td>distance to structure</td>
<td>QM</td>
<td>SG-002</td>
<td>Prevent activation of steering lock if IGN is ON (ASS)</td>
</tr>
</tbody>
</table>
Functional Safety Architecture
Software Safety Architecture
# Software FMEA

![Software FMEA Diagram](image)

<table>
<thead>
<tr>
<th>Component/Function</th>
<th>Comment/Remark/Justification</th>
<th>Potential Failures</th>
<th>Comment</th>
<th>Top Level Effect</th>
<th>Related FTA event</th>
<th>Potential Failure Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>VehicleSpeed CAN</td>
<td></td>
<td>Computed</td>
<td>Loss/Moorder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGNITION CAN</td>
<td></td>
<td>Computed</td>
<td>Loss/Moorder</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![System FMEA Worksheet](image)
### FMEDA Table

<table>
<thead>
<tr>
<th>Power/Bus</th>
<th>Failure Rate (FIT)</th>
<th>Failure Rate (FIT) Non-Failed</th>
<th>Failure Rate (FIT) Failed</th>
<th>Failure Rate (FIT) Failed w/ Safety</th>
<th>Failure Rate (FIT) Failed w/ Safety Non-Failed</th>
<th>Top Level Effect</th>
<th>Related FTA event(s)</th>
<th>SM prevents FM from violation of Safety Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>75.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>2.00</td>
<td>(Power Supply)</td>
<td>No effect</td>
</tr>
<tr>
<td>Functional</td>
<td>75.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>2.00</td>
<td>(Power Supply)</td>
<td>No effect</td>
</tr>
</tbody>
</table>

### Metrics

- **Total Failures:**
  - Single Point Faults: 119,151.14 FIT
  - Total Failure Rate: 43,240.51 FIT
- **Latent Failures:**
  - Total Failure Rate: 14,270.75 FIT

### Diagram Description

The diagram shows a detailed analysis of the FMEDA process, including failure modes, effects, and safety goals. It integrates various system components such as power supplies, controls, and network architectures, illustrating how each component contributes to the overall system reliability and safety.
ANSYS SCADE
ANSYS SCADE in the Software V-Cycle

Embedded System & Software Lifecycle Management

System/Software Architecture Design

Embedded Control Software Design

Embedded HMI Software Design

Embedded Software Testing Environment
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, AADL, 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-178C, EN 50128, ISO 26262, IEC 61508)*
Enables 80% embedded code production and testing cost reduction
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)
ANYS 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
CERTIFICATE

No. Z10 16 11 S5460 008

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

Factory(ies): S5460

Certification Mark: TÜV

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
role in safety-related software development according to
IEC 61508, EN 50128 and ISO 26262.

The report EM0205C is a mandatory part of this certificate.

Tested according to:
IEC 61508-1:2010 (SA, 2)
IEC 61508-2:2010 (SA, 2)
EN 50128:2011 (SA, 3/4)
ISO 26262-9:2011 (ASIL, 2)

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.: EM0205C

Valid until: 2021-11-14

Date: 2016-11-18

Page 1 of 1

TÜV SÜD Product Service GmbH - Zertifikatstelle - Rebstockäkle 89 - 80299 München - Germany

Multiple EN 50128 SCADE Suite and Display KCG Tool certifications by TÜV
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
ANSYS SCADE State Machine
ANSYS SCADE Simulation
ANSYS TWINBUILDER
What is a Simulation Based Digital Twin?

Connected, virtual *replica* of an in-service physical asset, in the form of an integrated multi-domain system simulation, that *mirrors* the *life and experience of the asset*.

Enables *system design and optimization*, *predictive maintenance* and optimize industrial *asset management*. 
Multi-Domain System Simulation: Integrate, Validate and Optimize multi-domain systems
Kontakt zu FlowCAD / Contact us

Für weitere Fragen und Informationen stehen wir gerne zur Verfügung. Please don't hesitate to contact us.

FlowCAD Deutschland
Mozartstr. 2
85622 Feldkirchen bei München
T +49 89 4563-7770
F +49 89 4563-7790
info@FlowCAD.de

FlowCAD Schweiz
Hintermättlistr. 1
5506 Mägenwil
T +41 56 485 91 91
F +41 56 485 91 95
info@FlowCAD.ch

FlowCAD Poland
ulica Sasiedzka 2A
80-298 Gdansk
T +48 58 732 74 77
F +48 58 732 72 37
info@FlowCAD.pl