Functional Safety Work Products

Adaptive Control Solution is ISO 26262 certified and ready for critical safe applications









ACU T222

ISO 26262 ASIL-D Ready from SGS-TÜV Saar

AC Composer & AC Lib

ISO 26262 Compliant Certified for the design of safe systems up to ASIL-D from SGS-TÜV Saar

AC App Inverter

ISO 26262 ASIL-D Compliant from SGS-TÜV Saar

Silicon Mobility, an intel company offers a full stack automotive solution that provides a control chip, application software and development environment all certified ISO 26262 for critical safe systems. Safety work products are available for most component describing the Safety Element out of Context (SEooC) methodology used, the safety mechanisms available and usage, and the certification report.

ACU - functional safety features with HISIL technology

ACU automotive semiconductor solution is designed to process critical information faster with 100% predictability and accuracy. HISIL is a patented hardware technology embedded into ACU. HISIL integrates a safety architecture that goes beyond ASIL-D SEooC objectives.

Benefits:

- Safety at application level with H/W acceleration
- **Enables ASIL-D designs**
- Saves CPU processing
- Enables software code simplification
- Shortens the fault reaction handling time interval
- Supports system scalability and reuse
- Saves development efforts from specification to assessment

HISII Infrastructure

- On-chip memory
 RAM with SECDED ECC
- Flash with SECDED ECC

Interconnect

- Multi-layer MPU
- ECC on data
- Parity on Address and Cmd
- · Programming monitoring
- Clocks
 Safe clock (IRC)

Clock monitoring Analog Comparators Registers Integrity

- Inputs/Outputs Safe I/O (Safe state restore)
- I/O monitoring with loopback

Supply

I/O supply LVD Core supply HVD & LVD

Temperature monitoring

2 x Temperature sensors

Execution Unit protections 2 clock delay Lock Step MPU Cache with ECC Events Sequence Control **ACU T222**

HISII Core

HISIL Sanity Checker

Complete Self Test

- Logic BIST
- Memory BIST ADC self test

HISIL Fault Manager

Faults Signaling and Diagnostic

- Fault collection
- Fault signaling
- Fault diagnostic
- Custom fault reactions
- FLU reprogramming
- Long/short reset
- Reset by group Safe clock switch
- I/O safe state
- Interrupt generation External Sate Signaling
- 1-2 pin signaling
- Bi-stable mode
- Switched mode
- Fault injection autotest

Methodology:

The FuSa analysis has been established upon four assumptions:

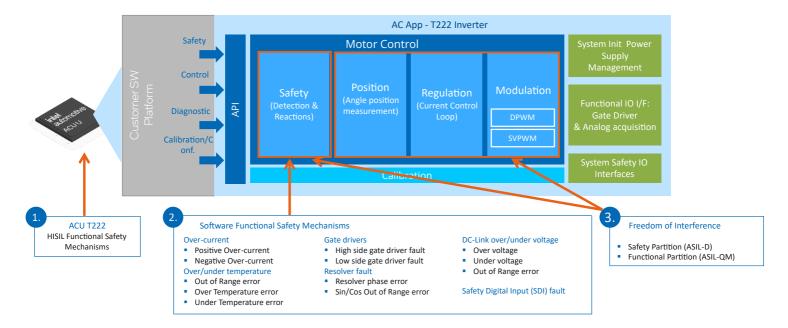
- Automotive traction inverter/e-motor control, DC-DC & OBC
- Safety goals
- Safe states
- External measures

Deliverables:

- Certificate and certification report
- Safety Manual
- FMEDA calculation sheet
- Frrata

AC App - T222 Inverter functional safety features

AC App - T222 Inverter is an **application software for ACU enabling best in class control of electrified powertrains.** Its functional safety is built upon 3 key elements: the hardware resources of the ACU, the software safety mechanisms and the software architecture.



Deliverables:

- Certificate and certification report
- Safety Manual

- FMEDA calculation sheet
- Errata

AC Composer & AC Lib - functional safety scope

AC Composer and AC Lib are software tools to develop safety-related software and applications up to ASIL-D. The scope of qualification to ISO 26262 includes:

- Our products:
 - AC Lib T222 Target
 - AC Lib T222 MATH
 - AC Composer T222 Target Framework
 - ARM CC compiler
- AGILIS Precision RTL

- MathWorks
 - MATLAB
 - Simulink
 - · Embedded Coder
 - HDL Coder

Safety Manual reports:

- The Tool Confidence Level (TCL)
- The qualification test protocols for TCL > TCL1
- The behavior under anomalous operating conditions and associated safety measures
- The assumptions of use

Deliverables:

- Certificate and certification report
- Safety Manual
- Tool Criteria Evaluation report (TI, TD, TCL)
- Tool Qualification Plan
- Anomalous conditions analysis reports
- Defect Reports

Safety work products records - available for audit

Silicon Mobility keeps records of comprehensive functional safety related documentations. Among them includes:

- Development process design rules
- Verification specification
- Report verification

- Functional requirement
- Safety requirement
- Dependent Failure Analysis report
- Traceability Matrix

