
The all-in-one tool suite to analyse and manage the impact of hardware random faults according to ISO 26262 and IEC 61508

The Safety Designer is a Tool Suite that automates the safety analysis of IPs, Integrated Circuits (MCUs, ASICs and Systems-On-Chip), FPGA and electronic units (ECUs) according to major functional safety standards.

YOGITECH frTools Suites, including the Safety Designer and the Safety Verifier, are derived from YOGITECH’s internal tools, used for years to perform functional safety analysis and the verification of many IPs, ICs and Electronic Control Units, and which successfully satisfy functional safety standards such as IEC 61508 and ISO 26262.

Today YOGITECH faultRobust Tools are a licensable Tool Suite which allows customers to independently perform the safety activity of their devices in their own environment, maintaining full control of their intellectual property.

HOW the SAFETY DESIGNER supports you:

• It analyses the IP, Integrated Circuits, MCU, ASI, SoC, FPGA or ECU at different levels of abstraction, starting from the functional safety concept down to the detailed hardware design
• It partitions a (detailed) design into its elementary parts
• It computes failure rates according to current standards (e.g. IEC 62380 and SN29500) or allows the user to associate custom failure rate values
• It provides the user with an extensive library of failure modes and safety mechanisms to be readily used in the analysis
• It performs the FMEA/FMEDA/FTA process, associating the failure modes to functional blocks and elementary parts, computing the safety metrics and estimating safeness and diagnostic coverage
• It prepares the safety verification plan at the appropriate level of abstraction
• It imports from the Safety Verifier the measured data from the safety verification activities, allowing the user to switch between estimated and measured views
• It exports the safety analyses and the resulting safety requirements for the creation of safety cases

The Safety Designer is the only safety tool on the market that can read the IP or IC design database (e.g. RTL or netlist) and automatically calculate safety properties, such as the failure mode distribution.
HOW it works:
The Safety Designer is a multiplatform tool: both Windows and Unix systems are supported, and its projects can be exchanged between them, guaranteeing all the flexibility you need. The tool has dedicated features to support database import/export, reuse, sub-designs and circuit derivatives. It has a special interface (SDAF) to allow further automation, e.g. direct RTL-to-FMEA flows. The Safety Designer Tool Suite implements YOGITECH’s fRMethodology, the patented white-box approach to performing functional safety analysis and safety-oriented design exploration of electronic circuits according to functional safety standards.

YOGITECH, founded in 2000, is a leading provider of services and solutions to silicon vendors and system integrators to help them meet their functional safety challenges. The faultRobust technology includes different product lines - fRMethodology, fRTools, fRTrainings, fR IPs and fRSTL - coherently with a mission to be the one-stop shop for functional safety. YOGITECH is a member of the ISO 26262 Working Group; it was the lead of the Part 10 – Annex A “ISO26262 and microcontrollers” and is now the lead of the new Part 11 “Application of ISO26262 to semiconductors”.

TARGETED APPLICATIONS

- Automotive
- Industrial automation
- Railways
- Medical
- Avionics

CUSTOMERS

- Silicon vendors
- System Integrators

YOGITECH’s fRTools are developed according to ASILD TCL2 of ISO 26262 and SIL3 T2 of IEC 61508. fRTools also take into account the recent guidelines of ISO 19451, the application of ISO 26262 to semiconductors.

fRTools are the only Tools Suites on the market that offer a unified flow from the functional safety concept to the detailed hardware design (Safety Designer) up to the hardware safety verification (the Safety Verifier). The Safety Designer takes the analysis from the qualitative FMEA at the functional concept level through more detailed levels of abstraction to the quantitative FMEDA conducted on the detailed design database, where the fRMethodology white-box approach offers a more accurate estimation of the safety metrics.