

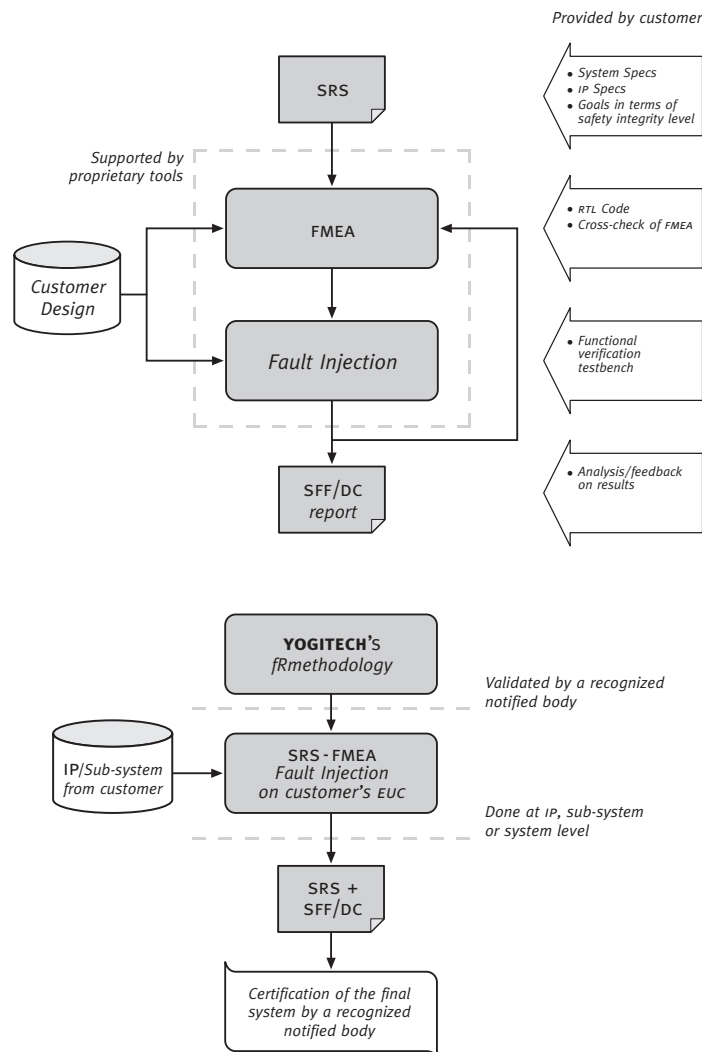
fR methodology

The IEC 61508 norm for functional safety of electronic safety-related systems introduces a deterministic approach to evaluate the robustness of a given Equipment Under Control or EUC since it also rules the documentation to be delivered with the safety system concerning the implementation and the validation flow of both HW and SW. For system sub-components such ASICs or IPs, to follow this norm means a complex analysis and evaluation procedure.

fR methodology is a systematic procedure offered by YOGITECH to address IEC 61508 requirements. Starting with the Safety Requirements Specification [SRS], a Failure Mode and Effect Analysis [FMEA] is performed, extracting information with proprietary tools from the RTL of the target design. Precise reports about Diagnostic Coverage and Safe Failure Fractions are delivered. fR methodology uses fault injection at all the different stages of the validation procedure: to validate the FMEA, to assess the safe failure fraction of the EUC including diagnostic, and at the end of the implementation stage. fR methodology can be used at block/IP, sub-system and system level.

YOGITECH's faultRobust is the technology for addressing and achieving fault robustness in Integrated Circuits. It provides a set of IPs, tools and methodologies for the detection and correction of faults affecting the different parts of the electronic equipment or soc. Each fRIP can be stand-alone, protecting a particular component such as CPU, memory system and peripherals, or it can be combined with other fRIPs for a complete solution.

YOGITECH's faultRobust technology optimizes costs by minimizing gate count, software overhead and power consumption; it reduces the common mode effects by adding diversity; it minimizes performance impact; offering a platform-based modular and reusable approach; it increases diagnostic capability; and it addresses the emerging norm IEC 61508, thus providing guidelines and a methodology for a system to be IEC 61508 adherent.



•fRmethodology

SRS

The Safety Requirements Specification [SRS] is a document containing all the requirements of the safety functions that have to be performed by the safety-related systems. It includes the Safety Functions [SFRS] and the Safety Integrity Requirements Specifications [SIRS]. The IEC61508 norm specifies in detail the contents of this document.

fRmethodology combines the information provided by the customer with that extracted from FMEA and fault injection and delivers a complete SRS in adherence with the IEC norm.

FMEA

FMEA is carried out through a systematic approach supported by a proprietary FMEA working sheet. In a first step, a set of *sensible zones* are identified from the RTL description. Then, a set of *observation points* are selected where the *main effect* of a fault is evaluated. Failure modes are defined for each sensible zone and each failure mode is weighted with accurate statistics. Particular attention is paid to failure modes specified in IEC61508-2. Then, following the IEC61508 guidelines, safe and dangerous failure rates are assigned to each failure mode. Diagnostic Coverage [DC] and Safe/dangerous failure fractions [SFF] are finally computed. In this way, it is possible to precisely position the component or sub-system under analysis in the SIL table of IEC61508-2.

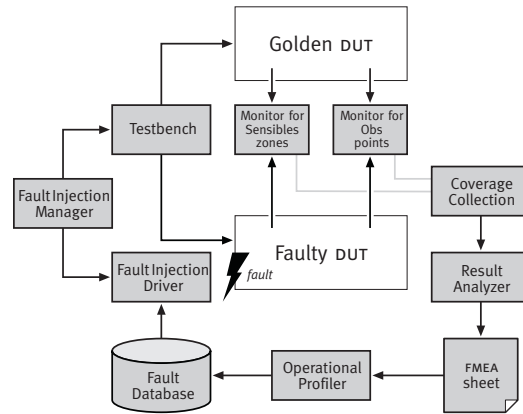
FAULT INJECTOR

State-of-the-art fault injectors mainly operate at gate level or only at highest level (*e.g. sw*), and they typically suffer from unacceptable simulation time for large circuits. fRmethodology uses a proprietary fault injector tool that works at all the abstraction layers. With an automatic flow, the FMEA results and the EUC workload are used for fault list generation, drastically reducing the simulation time. At the end of the fault injection campaign, the results assess and improve the quality of the FMEA. Fault Injector also works with fault-lists provided by the customer or randomly generated. Different fault models can be injected, from the lowest (*e.g. stuck-at, transient-error*) to the highest level (*such as bus errors, register mismatches and so on*), facilitating the mapping of failure modes specified by IEC61508-2 in real injected faults. Precise coverage metrics are delivered in order to get the highest level of confidence of the fault injection results.

For information: fr@yogitech.com

The product described in this document is subject to continuous development and improvement. YOGITECH reserves the right to make any changes to this document and related product at any time without prior notice. No responsibility is accepted for errors or omissions.

FAULT INJECTOR



DELIVERABLES

- SRS of the IP or sub-system including diagnostic, with all the required information by IEC61508.
- FMEA Work Sheet mainly including:
 - Collection of results such as Safe and Dangerous Failure rates, Safe Failure Fractions, Diagnostic Coverage and so on.
 - A list of sensible zones taken from the RTL.
 - A list of failure modes with conditions.
 - A list of sensible zones ranked based on their criticality.
 - A list of observation points.
 - A table of main and secondary effects for each failure mode and for each selected observation point.
 - A list of usage frequencies to be applied to each sensible zone.
- Files from the execution of YOGITECH's proprietary tool to extract the information from the RTL for the FMEA, and log files.
- Block diagram of the EUC with a direct graph showing the interaction between sensible zones.
- Files from the execution of YOGITECH's Fault Injector, including operational profile, result analyzer and coverage log files.