ENSURING FUNCTIONAL-SAFETY & ROBUSTNESS THROUGH SYSTEM TESTING ACCORDING TO ISO 26262
AUTOMOTIVE EMBEDDED SYSTEM TESTING

MAKING YOUR AUTOMOTIVE EMBEDDED SYSTEMS SAFE, RELIABLE AND ROBUST

The increasing complexity and safety integrity requirements of embedded components and systems are a real challenge for the automotive industry. With up to 70 Electronic Control Units (ECUs), some controlling highly-critical functions, 30% of a car’s total development cost is due to embedded systems.

To guarantee the necessary level of safety, the ISO-26262 (Functional Safety) standard addresses the planning and development of safety-critical systems for automotive ECUs. The higher the (Automotive) Safety Integrity Level (ASIL) of a specific system, the higher the Verification & Validation (V&V) requirements. For the highest level, ASIL-D, up to 40% of the development effort easily goes into V&V and safety management activities.

Every year, car recalls increase manufacturer’s operational costs and cause significant brand damage. Getting embedded software systems right first time is crucial. The quality and safety of the end product, the car, is of the highest importance. The time-to-market is critical.

How to guarantee an efficient and safe ECU integration?
How to improve the overall robustness, reliability and safety of systems?
How to deal with increasing complexity in a structured and systematic manner?
How to improve the time-to-market, while meeting all robustness goals?
How to improve efficiency and optimize resource usage?
How to reduce development and production costs, significantly improving overall competitiveness?

OUR EXPERTISE

Our engineers are experts in Hardware-in-the-loop (HIL), and Software-in-the-loop (SIL) V&V techniques, compliant with the ISO 26262 standard. Our capabilities include:

- Architecture, design and formal code reviews, with a particular focus on the optimization of code structure and maintenance, memory and CPU budgets, functional safety and correct-by-design;
- Validation activities through HIL and SIL techniques, including open and closed-loop testing, using simulated target environments and/or the actual target hardware;
- Independent validation activities, focusing on stress-testing and robustness-testing using Fault Injection and our state-of-the-art in-house csXception tool.

When conducting system safety and reliability assessments, activities are tailored to the specific criticality level of the system. These usually include hardware, software and system-level formal analysis techniques aimed at mitigating risk. Commonly referred to as ‘RAMS’, these include:

- Reliability Block Diagrams (RBDs);
- Fault Tree Analysis (FTAs);
- Failure Mode Effects and Criticality Analysis (FMECAs);
- Hazard Analysis (HA), and Hazard & Operability Studies (HAZOP);
- Hardware Software Interaction Analysis (HSIA).

With a strong culture and extensive hands-on experience of safety-critical projects, our engineers are knowledgeable in typical automotive low-level embedded architectures and micro controllers.

OUR OFFER

1) Design and deploy qualified validation solutions, tailored to the needs of our clients;
2) Provide testing, verification & validation of complete embedded systems;
3) Provide independent reliability functional safety assessments, and independent verification and validation of systems, including robustness testing and Fault Injection.

CRITICAL Software is able to:

How to guarantee an efficient and safe ECU integration?
How to improve the overall robustness, reliability and safety of systems?
How to deal with increasing complexity in a structured and systematic manner?
How to improve the time-to-market, while meeting all robustness goals?
How to improve efficiency and optimize resource usage?
How to reduce development and production costs, significantly improving overall competitiveness?
CHALLENGE | COST EFFICIENT FORMAL VALIDATION

Developing safety-critical software is costly, mainly due to the multiple levels of specification and the corresponding levels of verification. In addition, records of all activities must be duly produced and stored, ensuring the whole process is auditable. In the most demanding safety standards, the formal verification and validation activities account for more than 40% of the total project effort. When done manually, verification is time consuming and prone to errors.

SOLUTION | AUTOMATED HARDWARE IN THE LOOP VALIDATION FACILITY

CRITICAL Software has developed an automated Hardware in the Loop System Validation Facility (SVF), supporting fully-automated execution of test scripts and fully-automated checks, ensuring completely automated test campaigns, resulting in high productivity levels.

To address the various needs of the system under test, CRITICAL Software’s SVF is based on a highly configurable and extensible base solution, providing the following interfaces out of the box:

- Analog IO – dozens of AC, DC and discrete inputs and outputs are available for testing, with variable ranges of voltages, currents and wave types;

CRITICAL Software’s SVF also supports fault injection directly into the microprocessor of the system under test, allowing the stimulation of built-in tests without using instrumented software builds. By automatically coordinating the complete set of inputs and outputs, the SVF is able to verify timing requirements in the order of up to 10ms.

RESULTS | PRODUCTIVE VALIDATION CAMPAIGNS FOR HIGH CRITICALITY LEVELS

CRITICAL Software’s SVF enables easy implementation and fast execution of test campaigns. Regression testing becomes much more efficient, allowing more aggressive and extensive regression test policies. This provides higher levels of confidence on the system under test. Regression testing effort and schedule demands are dramatically reduced when compared to manual or semi-automated testing.

In addition, since tests are automated they are not prone to manual execution errors, are deterministic and follow a pre-planned execution time. Automation allows the execution of larger test campaigns without extending testing effort and provides more accurate inputs for effort estimation.

TECHNOLOGIES:

- Certification on the highest criticality level;
- Automated Hardware in the Loop testing;
- Fault injection for safety integrity testing;
- Highly-configurable reports.
REAL ADDED VALUE

CRITICAL Software can help your company build more robust embedded automotive systems, faster. Either by offloading V&V tasks, as well as RAMS related activities, or by increasing your development team’s capacity.

We offer fixed-price projects, and tailored solutions, while maintaining flexibility. Our highly-specialized engineering team can integrate with client teams, or work standalone in our offices, located throughout Europe, in Portuguese-speaking countries, and elsewhere in the world, also allowing us to connect directly to end-client locations, if required.

We are at the forefront of technological innovation in embedded systems. Our commitment allows us to go beyond our client’s initial expectations. We add value to our clients’ products by focusing on our core V&V and RAMS capabilities, using our unique Fault Injection techniques and tools. We help by significantly increasing robustness and significantly decreasing the number of defects at delivery.

Simultaneously, we possess detailed knowledge about embedded systems from the developing point of view; this allows us an independent view.

We enable the development of more efficient end-products, reducing production and evolution costs, helping our clients to gain a sustainable competitive advantage.

ABOUT CRITICAL SOFTWARE

Since 1998 CRITICAL Software has developed capabilities to deliver high-integrity systems for safety and mission-critical oriented solutions. Having the opportunity to work on applications in different domains has allowed the company to leverage its knowledge and experience across different markets. This cross-industry capability is recognised by CRITICAL Software’s customers as a strong competitive advantage.