Application of Functional Safety in accordance with ISO 26262

The problem

With the advent of Advanced Driver Assistance Systems (ADAS) and Autonomous Driving (AD), an automobile today can contain up to 200M lines of code (+500M by 2025) with interactions between over 150 control units. This considerable number of interactions combined with the complexity of the functionality being implemented significantly raises safety concerns. To address these concerns ISO 26262 was developed for the automotive industry, and it defines a framework of development through the specification of safety requirements.

This standard defines new ways of developing, validating, and verifying software systems within the automotive industry, and systems and subsystem makers will require external support in order to embark efficiently and very rapidly into these new platforms.

Our offering

The CS group owns the know how to perform system and software development, Validation & Verification (V&V) and integration of safety critical system through the application of ISO 26262.

- Perform the Functional Safety development – ISO 26262 Part 3
    - Hazard identification, risk assessment and ASIL determination
    - Development of the functional safety concept
    - Specification of the Functional Safety Requirements (FSR)
- Perform the System Level development – ISO 26262 Part 4
    - Refinement of the functional safety concept into the technical safety concept
    - Safety Validation
    - Specification of the Technical Safety Requirements (TSR)
- Perform the Software Level development – ISO 26262 Part 6
    - Disciplined specification, design, implementation and verification of real-time embedded software
    - Temporal/spatial partitioning (freedom from inference)
    - Specification of the Software Safety Requirements (SSR)
- Efficiently setup & perform Management of Functional Safety activities – ISO 26262 Part 2
    - Organization definition of the required safety roles (safety managers and engineers) and processes
    - Clear definition of responsibilities and interfaces along the life-cycle
    - Development of the Safety Plan

1-203-258-2401
info@c-s-inc.us
www.c-s-inc.us
East Hartford, CT, USA

- Establish the necessary Supporting Processes – ISO 26262 Part 8
    - Change and Configuration management tools
    - Development of verification plan and automation of verification tasks
    - Qualification and use of qualified tools
- Adapted proven methods and techniques from the verification of critical aerospace software for use in development of high ASIL automotive systems
    - Interaction with safety authorities and efficient means of compliance
    - Implementation of an organization structure to ensure independence
    - Requirement traceability and safety rationale justification (ARP-4754A)

Benefits

Our customers within the automotive industry can implement ISO 26262 rapidly and efficiently, thanks to our support, and therefore ensure that their systems will be safe, and that people's life within and around cars will be safeguarded.

Why CS?

To meet ISO 26262 challenges, The CS group has assembled a highly skilled team with substantial experience in critical real-time software development and V&V. This team has:

- Provided system/safety expertise to automotive industry in the development of advanced driver assistance functionality for 7+ years
- Adapted proven methods and techniques from the verification of critical aerospace software for use in development of high ASIL automotive systems
- A capability to use advanced methods and tools (e.g., formal methods) to meet the challenges of increasingly complex software in automotive applications
- Extensive experience with DO-178 certification of more than 30 airborne software programs