Railway Systems SIL-3 Safety Compliance

Success Story - March 2019

Customer

Our customer has assembled the most comprehensive collection of Radio Remote Control brands for locomotives, cranes, material handling equipment, mining machinery, mobile equipment and virtually any equipment where the operator can be moved to a safer, more efficient location.

With nearly 10,000 rail-related applications installed worldwide, this company offers the most comprehensive combination of experience, product quality and technical support.

This client entrusted us with the project of getting safety certifications for their products.

Challenges

The big challenge of the project was to comply with different safety standards i.e. CENELEC EN 50126, EN 50128 and EN 50129 and achieve the SIL-3 certification from TUV and EBA.

The software of this project was based on a complex RTOS (Real Time Operating System) and a complier without any formal safety certification. Additionally, code coverage analysis was also a key challenge in the product life cycle. The evaluation and approval criteria from the third party assessor were the key tasks in the project.

Solution

We met all the challenges inherent in the project with the help of our expertise in the relevant tools.

For compiler and assembler we collected known problems from the vendor company with historical data of tools. These tools were used in the safety industry since last 10 years and no hazardous situation was observed in this duration. Additionally, we did boundary tests with the compiler and assembler. Our RTOS library was not safety certified and we did not have the historical data. To overcome this challenge, we decided to work with RTOS development company during our maintenance contract. We analyzed the safety violations in the library along with boundary test on our target CPUs. These evidences were enough to satisfy the safety requirements.

We created a translation table in which each requirement of the relevant rail standards was listed and then realized a gap in our activity list.

We conducted different review sessions with CENELEC committee members and modified our processes and deliverables according to these standard requirements.

Another barrier in our product life cycle was dynamic code coverage analysis of the complete source code. The code consisted of nearly 50,000+ lines and our standard requirement was to execute each line, branch, and decision from an external tool. Without any dynamic analysis tool this challenge was impossible to overcome. We consulted many software tool vendors and took many demonstrations on different tools. After this thorough tool analysis, we finalized a software tool from the company LDRA as their tool was reputed to be the

best in the safety certification field. We started LDRA tool training sessions with the LDRA company and within one week we finalized the workflow of the dynamic analysis on our target CPUs. We delivered our product on time along with the required static and dynamic analysis reports for product safety assessment.

Achievements

We successfully completed the project with the following key achievements:

- Rail Safety Standards Analysis
- Gap Analysis (Standard Requirements Vs. Product Specification)
- Safety Processes and Management Compliance
- Design SIL-3 Documentation Structure
- LDRA Tool (Code Coverage)
- Safety Risk Assessment
- FEMA (Failure Effect Mode Analysis)
- Fault Tolerance Analysis
- RAMS (Reliability Availability Maintainability and Safety) Compliance
- Target SIL Level Evaluation
- Functional Safety Tests
- SIL-3 Certification from TUV and EBA

Business Result

Our customer vended this product to rail industry and, as a result, became one of the market leaders in rail control system domain.

Contact Us

Explore ways to use our expertise in growing your business while establishing a valuable partnership with us.

Contact our consultants at:

Phone: +1.412.533.1700 (Ext: 585)
E-mail: info@sqaconsultant.com
Website: www.sqaconsultant.com