

# Case Study: Full Lifecycle Safety Critical Software

## Synopsis

Resource Engineering Projects developed and verified a suite of operating system level software services to EN 50128 SIL 4.

The development process used UML and Ada, whilst the verification testing activities used AdaTEST and bespoke system test scripts and a hardware test rig.

The Targeted Time and Materials contract allowed the client to have full visibility of progress and costs throughout the project.

## Key Project Facts

Team Size: 15 engineers

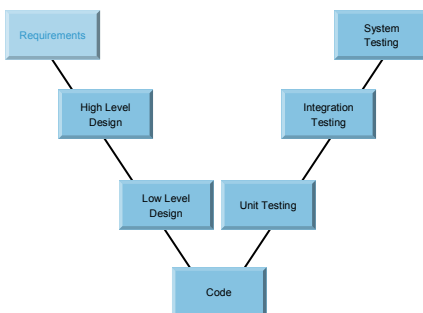
Duration: 18 months

Contract Type: Targeted Time & Materials

Tools/Languages: DOORS, ARTISAN UML, Ada, AdaTEST, SPARK, Polyspace

Standards: EN 50128 SIL 4 (CENELEC)

Lifecycle Involvement:



## Project Overview

Resource Engineering Projects were awarded a contract to produce a suite of operating system software services from which the customer could then build various applications for the rail industry.

The software executed on bespoke hardware cards developed by the customer, which would be mounted in industrial enclosures for deployment on trains and trackside sites. The products control functions such as automated train operation and traffic movement.

The overall system was assessed by the client's safety assessor as requiring the highest level of safety critical consideration due to the danger of loss of life should the system fail. Therefore, the most rigorous level of the rail industry standard, EN 50128 Safety Integrity Level (SIL) 4, was applied.

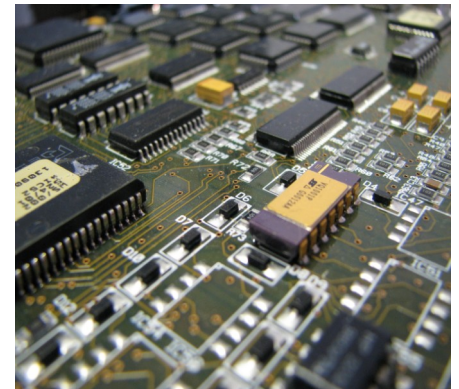
The customer provided DOORS requirements and prototype code to use as a starting point. A software architecture, high-level design, and then low-level detailed design were all developed in UML using ARTISAN.

Ada code was then written and statically analysed using SPARK (syntax checks) and Polyspace (data flow analysis) to reduce the chance of errors.

This Ada code could then be dynamically tested against its design using the unit test tool AdaTEST. This dynamic testing proved not only that the code was functionally correct,

but also that there were no scenarios where the algorithms could fail.

Finally, the code was tested as an integrated system on a hardware test rig to prove compliance with the high level design and the customer's requirements



Peer reviews were conducted at the end of every software lifecycle stage by an independent engineer to prove that the output was suitable to be passed to the next stage.

All activities were conducted using processes and standards from the internal Quality System, which was proven to comply with the requirements of EN 50128 through the use of a compliance matrix.

The project successfully concluded and led to further work on the successor to the system.

## The Resource Engineering Projects Advantage

### Experience:

Over 15 years experience of software design for real-time, safety critical, embedded applications using expert project management and engineers. Proactive approach to challenges adds value to projects and keeps the client's best interests in the forefront.

### Safe Hands:

Quality product and service guaranteed. Internal, client, and independent audits passed as a matter of course. Continual improvement ensures optimal performance and quality is always maintained.

### Flexibility:

Many types of service packages are available, from support for a discrete project phase within the client's team, to full "fire and forget" solutions where total ownership, responsibility and accountability for the software lifecycle can be entrusted.

### Price:

Fixed Price, Time and Materials and Targeted Time and Materials contracts are all available, and the advantages of each can be discussed up front to ensure the client has the flexible or fixed arrangement that suits their needs.

## Accreditation

