CANTATA

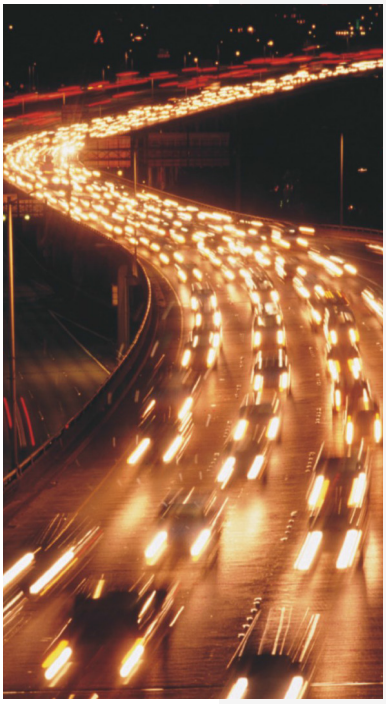
QA SYSTEMS
The Software Quality Company

SECTOR Automotive

Case Study

HIGHWAYS AGENCY

Highways Agency



ABOUT THE COMPANY

The Highways Agency is an Executive Agency of the Department for Transport (DfT), and is responsible for operating, maintaining and improving the strategic road network in England on behalf of the Secretary of State for Transport.

"Cantata was chosen to do this because it gave all the functionality needed to test to the IEC 61508 SIL 1 standard!"

Highways Agency and the NASS Project

The Highways Agency (HA) is responsible for managing, maintaining and improving the motorway and trunk road network in England. Several computer systens are implemented to help with the task of avoiding congestion. The National Motorway Communication System 2 (NMCS2) is a major system, used to control roadside equipment and monitor road conditions.

HA decided to run an Active Traffic Management (ATM) pilot project on one section (in the West Midlands) of the UK motorway network. The aim of the ATM was to make better use of existing road space, to increase capacity and ease congestion, by controlling traffic according to actual and predicted road conditions.

The HA went out to tender for the development of a new subsystem called the Network ATM Supervisory Subsystem (NASS), to form an additional element within the existing NMCS2 and future ATM systems. NASS takes real-time actual traffic flow data, combines this with historical traffic flow data, and then predicts future flows. If congestion is predicted, NASS will evaluate a number of predefined traffic control plans to avoid or minimise the predicted congestion, selecting the optimal plan. NASS will then issue requests for the settings of roadside signals and message signs to implement predefined traffic control plans.

The project's first milestone was a "proof of concept" (PoC) system, which came in at about 20 KLoC and completed Factory Acceptance Tests (FAT). The second phase was for the production of a demonstrator system to be supplied to Traffic Engineering consultants working for the HA. The purpose of this system was to allow the consultants to refine the rules and algorithms, internal to NASS, for its safe and efficient functioning. This was approximately three times the code size (60KLoC) of the initial PoC system.

The third phase involved NASS being delivered to the HA's West Midlands Regional Control Centre (RCC), located in Quinton. This was gradually integrated with all the other systems running at the RCC. At this point, NASS could be used to directly request sign and signal settings, thereby influencing drivers using the West Midlands motorway network with a view to reducing/mitigating congestion.

System Safety and IEC 61508

The HA decided on the use of IEC 61508, as a result of considering the hazards involved. At the start of the NASS project, it was assessed that the safety level appropriate for the project was SIL 1. This relatively low grading reflected the fact that NASS did not directly control any hazardous equipment, but was involved in issuing requests for traffic signs and signal settings – which could have safety consequences when acted upon.

QA Systems GmbH | Schwieberdinger Strasse 56, 70435, Stuttgart, Germany
Tel: +49(0)711/138183-0 | www.qa-systems.de

QA Systems Ltd | 2 Palace Yard Mews, BA1 2NH, Bath, United Kingdom
Tel: +44(0)1225581150 | www.qa-systems.com

NASS Software Design

Having agreed the system requirements in detail for the PoC phase, software design followed a method based on use of UML. The design hierarchy led to the identification of sub-systems, comprising of software components, which were either executables or libraries (DLLs). Further OO design decomposition led to the identification of classes, for which module specifications were created ready for coding and testing by programmers. The module specs detailed class public and private methods with code flow shown in pseudo-code, and class test plans.

Testing Strategy

The IEC 61508 standard calls for validation planning and, furthermore, that testing be the main validation method for software. Accordingly, the NASS project team, together with the HA, drew up a test strategy which included a formalised approach to testing each and every entity at each identifiable stage of the project. Each entity had its own test plan, which detailed as appropriate the configurations, inputs and expected outputs which, when run successfully, would give the required confidence in the correct working of the entity under test. At the higher levels, the test plans were contained in a separate (version-managed) document; at the lower levels, test plans were included in the design specification.

Throughout IEC 61508, there are demands to the effect that test results should be generated to show that tests have been run and 'satisfactorily completed'. This put quite a necessity on the team to ensure that, not only were they using tools that would make the various testing activities as easy and repeatable as possible, but also that the tests should, as far as possible, be self-documenting.

Code and Module Testing

Following the classic 'V-model' lifecycle principles and IEC 61508, the software engineers's first task, after programming the classes, was to test them. Cantata was chosen to do this because it gave all the functionality needed to test to the IEC 61508 SIL 1 standard. The basic requirement is to test every class in isolation and to demonstrate code coverage to the levels of 100% entry-point (every function/method called at least once) and statements. In fact, the reasonable decision was made to additionally test to 100% condition coverage. This was more work than the basic project SIL demanded, but it was felt by the developers to give a useful additional level of confidence. Since every class had a number of external interfaces, not all of which could be stubbed, the Cantata 'wrapping' facility was vital in allowing such isolation testing to be completed as planned. Stubbing involves the replacement of an external function with a programmable simulation having the same interface. Wrapping allows for the 'real' external code to be included in the test build, but with the option to intervene at the interface in order to, for example, check values being passed out or alter values being returned to the code under test.

Integration Testing

Cantata was also used for component testing. This formed the first level of integration testing, and was aimed at verifying the correct working of each NASS executable or DLL against specifications defined in the appropriate level of design. The testing involved calling public interfaces of the component under test, and stubbing or wrapping calls to external functions. Since NASS had its own database, the component tests included 'real' database code so that testing included the option to initialise the database and check that updates to the database were as expected.

The project created and maintained a fairly elaborate regression test facility which allowed for nightly builds and re-runs of each class and component test in the entire system. This served very well to enhance confidence in the change impact analysis system, by ensuring that changes in one module were completely and properly compensated for in other affected modules and tests.

CANTATA

QA SYSTEMS
The Software Quality Company

IEC 61508:2010 ISO 26262:2011 Certified

After testing the components, the project test strategy called for sub-system testing. Since 100% coverage had already been achieved during unit testing, integration testing could be allowed to live up to its name – namely testing the integration of the software units. The team, with the agreement of the HA, determined that 100% entry-point coverage was suitable to demonstrate the completeness of the integration tests. This was exactly in-line with the 61508 requirement [7.4.8.3] to demonstrate that, "all software modules… interact correctly to perform their intended function".

System Level Testing

Following sub-system testing, the team carried out a further series of System Integration tests. These tests mainly served as a dry-run to gain confidence before going into the customer-witnessed Factory Acceptance Tests. It was noteworthy that the system integration tests ran smoothly and only revealed a few design anomalies. The last layer of testing before the NASS was allowed to be installed at the RCC was called Interaction testing. This was carried out at the offices of another HA contractor, Peek Traffic, and involved running NASS on a rig which included NMCS2 equipment in exactly the same configuration as the live NMCS2 system. The intention here was to ensure that NASS could interact correctly with other live systems at the RCC. Finally, Site Acceptance tests were held at the RCC to demonstrate that the live NASS was operating correctly and safely with the rest of the NMCS2 system.

Conclusion

A properly run 61508 project, even at a relatively low SIL, can be demanding on test time. We wish to reinforce the point that testing is, on one level, about providing reassurance to developers that they can move with reasonable confidence from one stage of the project to another. At a different level, it can provide confidence to other stakeholders (e.g. the customer) that the system will work safely and reliably when installed on site. A good project generally works from a test strategy (i.e. determine in advance at what stages and levels in the lifecycle testing should be carried out), and will demand that test plans exist for each entity to be tested; testing should not be ad hoc! Testing needs to generate results as evidence of test completion (i.e. be self-documenting). Furthermore, testing needs to be conducted in a repeatable fashion because the one thing you can be sure of is the need to run and re-run tests at all levels many times.

CERTIFICATION IEC 61508

Cantata has been classified a **Class T2 Tool**, as usable in development of safety related software up to **SIL 4** as defined by the **IEC 61508** standard.


CERTIFICATE NO FS/71/220/13/0017

For information on tool certification, please visit:
www.qa-systems.com/cantata

CERTIFICATION ISO 26262

Cantata has been classified as usable in development of safety related software up to **ASIL 4** as defined by the **ISO 26262** standard.

TCL1 can be reached.

"All software modules interact correctly to perform their intended function"

All case study text has been approved by the relevant customer.
QA Systems acquired the Cantata business taking over all development, support and sales from IPL in March 2012.
Cantata is the extension of the Cantata++ tool.