Breaking News: From safety-critical systems to award-winning smart trailer applications

Haldex is a Swedish public company operating globally in the commercial vehicle industry (heavy trucks, trailers and buses), with an annual turnover of around €450 million and approximately 2,200 employees across 23 locations.

Haldex’s primary activities are vehicle dynamics and safety. They are particularly well known for their braking and suspension systems.

Haldex Commercial Vehicle Systems has been using PRQA’s Static Analysis solutions for more than a decade. QA-C and MISRA C have been essential elements in the company’s software development process since 2002, and have been used when developing embedded software for safety-critical braking systems for commercial trailers. More recently Haldex has also started to use QA-C++ to develop its award winning Fleet+ solution. Fleet+ extracts the raw data from Haldex’s embedded devices, providing additional information to operators to enable them to manage their fleets more effectively.

In Brief

Industry: Automotive

Safety-critical braking system
- **Business driver:** Development of high quality code for safety-critical embedded software
- **Why PRQA/benefits:** “QA-C is an indispensible part of our development process, it is inconceivable that we would ship any safety-critical software without having used this tool to check our code.”

Fleet+, fleet management application
- **Business driver:** Development of value added application (non safety-critical)
- **Why PRQA/benefits:** 25% of the defects found earlier in the development cycle. ROI based decision, payback on QA-C++ less than 18 months
Developing embedded software for safety-critical braking systems

Clearly Haldex’s embedded software is being deployed in safety-critical applications. The Quality Management System as adopted by the Commercial Vehicle Systems division is certified as compliant to ISO/TS 16949. This standard is based on ISO 9001 and applies to the design/development, production, installation and servicing of automotive-related products. It emphasizes continual improvement, defect prevention and the reduction of variation and waste in the supply chain. Note that the ISO 26262 functional safety standard only applies to passenger cars below 3500kg and is therefore not directly applicable to Haldex’s products. In relation to software development TS16949 provides Haldex with high level guidelines - such as “verifying conformance to all specified requirements” - but is not prescriptive as to how this should be achieved.

Haldex is keen to pursue “best practices” and has therefore chosen to adopt the MISRA C coding guidelines. This has not been mandated by their customers, but rather Haldex see this as a key requirement, and indeed a prerequisite to the development of high quality code for safety-critical applications. Equally important is having a tool that can automatically analyze their software (which is typically up to 90,000 lines of code) and identify non-compliances to the MISRA C rule-set. And one of the key criteria in tool selection was accuracy, most importantly the ability to identifying genuine non-compliances (no false negatives) and also minimizing false positives (“noise”). Consequently Haldex’s embedded software engineering team, based in Redditch, UK has been using QA·C with MISRA compliance module consistently since 2002.

Dudley Harrison, Chief Engineer, Trailer Systems stated, “QA·C is an indispensible part of our development process, it is inconceivable that we would ship any safety-critical software without having used this tool to check our code.”

Looking to the future

Haldex is in the process of migrating their embedded products to a new platform. The aim will be to reuse as much of the proven legacy code as possible, however Haldex is very aware that just because this software is robust on one platform, there is no guarantee that this will also be the case on the new platform. As they start to prepare for this migration Haldex will be looking very carefully at all the QA·C messages relating to “portability”. These messages identify specific areas of source code where the behavior of the executable is likely to be impacted by the choice of compiler / platform.

Robin Sayce-Jones, Senior Software Engineer, identified a second area where Haldex would like to work more closely with PRQA, “Over the years we have become increasingly aware of the need for an effective deviation management process - whereby justifiable non-compliances can be authorised and recorded. Legitimate deviations are absolutely permitted under MISRA and PRQA’s coding standards experts can provide us with independent guidance on how best to implement these deviations. We will also look to PRQA for advice as we consider the transition to the most recent version of the standard, MISRA C:2012.”

“QA·C is an indispensible part of our development process, it is inconceivable that we would ship any safety-critical software without having used this tool to check our code.”

– Dudley Harrison, Chief Engineer,
  Trailer Systems

www.qa-systems.com 2
Haldex was very conscious that the sensors in their core braking components were generating a huge quantity of data and that this data would be very useful to fleet operators. This data includes key parameters such as:

- Brake performance
- Vehicle speed
- Axle load
- Stability events
- Trailer mileage
- Reservoir pressure
- Road conditions

Haldex has therefore created Fleet+, an application which collects and presents this data, bringing improved transparency to trailer operators by analyzing the conditions to which the chassis, axles and tires have been subjected. This data can be used to identify trends and statistical anomalies, differentiating the performance of the vehicle from that of the driver, maximizing overall safety and optimizing the total cost of ownership.

Obviously the requirements demanded of the embedded software used in the braking components are much more stringent than those needed for the Fleet+ reporting tool. The performance of the former is clearly safety-critical, and the potential consequences of any unanticipated behavior of features such as ABS or traction control would be extremely serious. The Fleet+ application did not need to be developed to the same exacting standards as the embedded software as any issues in this reporting tool would not have an immediate direct impact on safety. However, it was also evident that any defects in the Fleet+ user interface (GUI) were much more likely to be visible to the end-user.

The Fleet+ application is written in C++ using a Visual Studio 2010 IDE. Already familiar with the benefits of QA·C, Haldex turned again to PRQA, this time in relation to QA·C++, the C++ version of the tool.

Robin Sayce-Jones, Senior Software Engineer stated, “Prior to purchasing QA·C++ we analysed all the C++ code that we had generated over the previous 12 months. We looked specifically at “customer impacting defects”, those which were material and would have been evident to end users. We found that 25% of the defects which had escaped from the coding phase and were subsequently discovered during unit and system test would have been identified earlier by QA·C++ (during the coding phase). Our analysis concluded that it took us on average 2 man days longer to fix any defect discovered later in the process. The payback on QA·C++ was less than 18 months.”

Fleet+ is the winner of the Trailer Innovation Award 2013

This pan-European awards scheme involving leading road transport magazines from ten European countries is held every two years, to tie in with IAA (Internationale Automobil-Austellung) commercial vehicles show in Hannover, Germany. Haldex Fleet+ won the “Smart Trailer” category.
In conclusion

For more than 10 years Haldex has considered static analysis with QA·C (and MISRA coding guidelines) to be an indispensible part of their safety-critical embedded software development process.

When assessing the use of PRQA tools for other projects - specifically projects such as Fleet+, where the safety related requirements are less stringent - it was already self-evident that QA·C++ would improve software quality, but now it was also important to consider the financial impact. With an ROI analysis showing a payback of less than 18 months, Haldex came to the conclusion that using QA·C and QA·C++ not only helped them to deliver higher quality code, but also saved them money!

QA Systems and Programming Research Ltd

QA Systems is an authorised reseller of the QA·C / QA·C++, QA·Verify static testing tools and their compliance module add-ons, which are owned by Programming Research Ltd. QA·C ®, QA·C++ ® and QA·Verify ® are registered trademarks of Programming Research Ltd. These tools and this document are the copyright © 2013 of Programming Research Ltd. Third party trademarks, logos and trade names appearing in this document are the trademarks and property of their respective owners.

QA·C, QA·C++ and QA·Verify, offer the closest possible examination of C and C++ code. All contain powerful, proprietary parsing engines combined with deep accurate dataflow which deliver high fidelity language analysis and comprehension. They identify problems caused by language usage that is dangerous, overly complex, non-portable or difficult to maintain. Plus, they provide a mechanism for coding standard enforcement.

Contact Us

For further information regarding QA·C, QA·C++ and QA·Verify and compliance module add-ons, please contact QA Systems at info@qa-systems.com where appropriate QA Systems will re-direct you to Programming Research Ltd.