LDRA

Software Technology

Aerospace Software Development

What have they learnt that would benefit the automotive sector?

Article by Bill StClair originally published in Automotive Electronics Magazine April/May 2005

automotive electronics

Aerospace Software Development

Bill StClair of LDRA

By 2010 it is predicted that electronics will account for 40% of overall car costs. Coupled with this the software complexity in basic vehicle components means it is not possible to prove correctness using existing software development techniques alone and as a consequence the automotive industry risks bringing unverified software products to market. In a competitive market place no car manufacturer wants to have a vehicle recalled due to technical problems. The costs and public relations embarrassment would have the potential to destroy a brand.

The aerospace industry has been at the forefront of software development for the past 30 years and the lessons learnt and approaches that aerospace companies have utilised bring proven methodologies and techniques that ensure good quality and high reliability. The automotive industry has also taken great strides in this direction with the introduction of MISRA C and more recently MISRA-C:2004. The MISRA standard provides considerable assistance for ensuring software adheres to a strict quality model with the obvious benefits of the quality improvements that this brings.

As a largely rules-based standard, however, it is acknowledged that MISRA is not the complete package. (Indeed what standard is!) Important areas of the software development lifecycle such as requirements analysis, quantitative coverage analysis and unit testing are largely overlooked. These are techniques that have been employed to great effect in the aerospace industry as they form the backbone of the RTCA (Radio Technical Commission for Aeronautics) standard DO-178B, Software Considerations in Airborne Systems and Equipment Certification.

Given the many similarities between software based control systems that are now being applied to automotive vehicles and those that have been developed and applied to modern aircraft for many years it would seem an obvious approach to seek to define best practice based upon experience and feedback from both industries.

Indeed this is exactly the approach that is now being applied in some of the largest aerospace projects. Take for example the multi-billion dollar JSF (Joint Strike Fighter) project. When the decision was made to standardise on the C/C++ programming languages for much of the key avionics control systems the project quickly adopted the MISRA guidelines. The MISRA guidelines are applied in conjunction with the full DO-178B requirements to provide a development model that addresses both quality and reliability.

The MISRA guidelines are applied in conjunction with the full DO-178B requirements to provide a development model that addresses both quality and reliability.

What additional features does the Do-178B standard bring to the software development lifecycle?

The Do-178B standard has a number of key sections, however the following software related sections are most relevant to this discussion:.

Section 5.0 (Software Development Process) specifies that software must meet certain software coding process requirements (Section 5.3). These include adherence to a set of programming standards and traceability from low-level design requirements to the source code.

Section 6.0 (Software Verification Process) details the software coverage analysis to be used to identify which requirements were not tested and which structures had not been exercised.

Section 6.4.4.2 (Structural Coverage Analysis Requirements) has a key objective of analysis to determine which code structure was not exercised by the requirements-based test procedures. The requirements based test cases may not have completely exercised the code structure, so structural coverage analysis is performed and additional verification produced to structural coverage.

DO-178B imposes comprehensive structural coverage requirements on software because, if code coverage is not monitored, there is the possibility that errors will still be present at the completion of testing. This is especially true when testing complex code containing multiple conditions, that have not been executed by any of the test cases. Consequently, the DO-178B test verification process greatly reduces the risks associated with safety-critical software development and contributes to highly reliable products.

How could Do-178B assist the automotive sector?

As described above the DO-178B standard with its greater emphasis on quantitative coverage analysis and requirements plugs several key gaps in the MISRA standard and hence, when used in conjunction with MISRA, has the potential to provide an extended model that addresses issues of both quality and reliability. Current feedback from projects that have adopted this approach is that real cost and reliability gains can be made from such an approach and this can only benefit the automotive industry in what is an increasingly competitive marketplace.

> "If code coverage is not monitored, there is the possibility that errors will still be present at the completion of testing."

What does the future hold?

The development of software in the automotive sector is becoming increasingly important. As concerns about software quality and reliability increase it would seem logical to look to the lessons learnt in other industries when seeking to define and implement appropriate testing practices. Current development focus within the automotive industry would suggest that an increasing reliance upon software based automotive control systems is inevitable and hence, for the good of the industry and its customers, now is the time to put in place appropriate practices to ensure the necessary safety and reliability of such systems.

LDRA Headquarters
Portside, Monks Ferry,
Wirral, CH41 5LH
Tel: +44 (0)151 649 9300
e-mail: info@ldra.com

LDRA Technology Inc. (US)
Lake Amir Office Park
1250 Bayhill Drive Suite # 360
San Bruno CA 94066
Tel: (650) 583 8880

www.ldra.com