Realities and practicalities of developing software under ISO 26262 for safety-related systems

ISO 26262 – ASIL partitioning / decomposition

The primary market for Protean’s product is series production passenger vehicles. A consequence of supplying into this market is the need to comply with the requirements of the international standard ISO 26262 (Road vehicles – Functional safety).

One of the core early stage activities under ISO 26262 is the identification and risk classification of hazards based on the following criteria:

- **Severity** - an estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation, ranging from S0 (no injuries) to S3 (fatal)
- **Probability of exposure** - the probability of being in an operational situation that can be hazardous, if coincident with a failure, ranging from E0 (incredibly low) to E4 (highly probable)
- **Controllability** - an estimate of the ability of the driver to gain sufficient control of the hazardous event to avoid the specified harm or damage, ranging from C0 (controllable in general) to C3 (uncontrollable).

About Protean Electric

Protean Electric is an award-winning technology company that has developed an in-wheel electric drive system for hybrid, plug-in hybrid and battery electric light-duty vehicles.

Headquartered in Detroit (Troy), with engineering and manufacturing operations in UK and China, Protean Electric has Venture Capital funding from US and China, including an injection of $84 million in 2012.

Protean Drive™ is a fully-integrated, direct-drive solution that combines in-wheel motors with an integrated inverter, control electronics and software – no separate large, heavy and costly inverter is required. Each motor packages easily in the unused space behind a conventional 18- to 24-inch wheel and can use the original equipment wheel bearing. The direct-drive configuration reduces part count, complexity and cost, so there is no need to integrate traditional drivetrain components such as external gearing, transmissions, driveshafts, axles and differentials.

Demonstration vehicles with Protean Drive™ technology include Volvo, Ford, Guangzhou Automobile Group, Vauxhall and BRABUS / Mercedes.
Based on the risk associated with a given hazard, the hazard is assigned an Automotive Safety Integrity Level (ASIL) from A to D, with D being the most stringent. Once hazards have been assessed and categorized, safety goals are formulated. Functional safety requirements are in turn derived from these safety goals and are assigned to the preliminary architecture with each requirement also being assigned an ASIL based upon the safety goal and related hazard that it is addressing. As well as providing an indication of risk, the ASIL may also be considered an indicator of how much development work is required to ensure that systematic errors don’t creep in when implementing a specific requirement.

Protean, as would be expected of any experienced team developing under ISO 26262, has considered methods for reducing the development burden on individual subsystems, including not only their motors, but also other related ECUs within the vehicle. ISO 26262 describes a technique known as ASIL decomposition where safety requirements may be implemented redundantly on architectural elements allowing a lower ASIL to be assigned to each of these decomposed safety requirements. Protean has considered the partitioning of their subsystems extremely carefully - reflecting the fact that the cost and complexity of compliance typically increases by an order of magnitude with each step from ASIL A to D.

Clearly Protean’s assessment needed to focus on the hazards and risks associated with their unique solution, and specifically having separate electric motors driving each wheel. After extensive simulation, testing and analysis, they identified several hazards, one of which was rated as ASIL D; if the imbalance in power delivered by each motor across an axle exceeds a specific limit that depends upon the weight of the vehicle, a typical driver would find it difficult to maintain control of the vehicle. However, through ASIL decomposition, Protean has been able to reduce the maximum ASIL level of safety requirements allocated to the motor from ASIL D to ASIL B(D) by ensuring that a) the motors and b) the vehicle controller independently check the difference in power across the axle. The saving in development and test effort makes the trade-off of having two independent ASIL B(D) requirements compared to a single ASIL D requirement well worthwhile.

ISO 26262 – MISRA

The link between ISO 26262 and the MISRA C guidelines is very clear, with ISO 26262 stipulating that design and coding guidelines shall be used to address topics such as the “use of language subsets” [Section 6, Table 1], with the following explicit objectives:

- exclusion of ambiguously defined language constructs which may be interpreted differently by different modellers, programmers, code generators or compilers.
- exclusion of language constructs which, from experience easily lead to mistakes, for example assignments in conditions or identical naming of local and global variables.
- exclusion of language constructs which could result in unhandled run-time errors.

“ISO 26262 essentially mandates MISRA coding guidelines when developing certifiable software. This is a good call.”

Richard Burke, Software and Systems Manager

Furthermore, ISO 26262 then specifically identifies MISRA C (and MISRA AC AGC) as examples of coding guidelines for C.

As Protean’s Software and Systems Manager, Richard Burke observed, “ISO 26262 essentially mandates MISRA coding guidelines when developing certifiable software. This is a good call – MISRA is a very sound coding guideline that is widely adopted by developers implementing safety critical designs across a wide variety of industries and applications.”
“MISRA compliant” code

“In general, the question as to when code is considered to be “MISRA compliant” is a very interesting one and not quite as straightforward as it initially appears,” ventured Richard.

The first consideration is in relation to deviations. MISRA legitimately provides the flexibility to deviate from non-mandatory rules – but on the proviso that these are documented and supported by the appropriate peer-reviewed justifications. Protean’s approach is to start with the full set of MISRA rules and developers strive to write fully compliant code from day one. Deviations are indeed made, but only by exception and, where the logic is very strong, for example to exploit some very specific functionality in the compiler/hardware. The senior members of Protean’s software team clearly have the experience to make sound judgements, but they are also anticipating the fact that this area is subject to careful scrutiny by auditors.

“We are impressed by the performance of QA·C, it is very accurate and we see that it is finding issues that other tools have missed.”

Huw Jones,
Senior Software Test Engineer

Protean has also consciously transitioned from MISRA C:2004 to MISRA C:2012, in recognition of the fact that the latter is tighter and provides more detailed examples, thus helping to make the justifications for any deviations more objective and consistent.

The second key consideration is in relation to the effectiveness of the automated static analysis tools used to parse the code. Protean has had direct experience of a number of tools and MISRA checkers. Currently they use two. An initial MISRA check is performed by the compiler to provide high level feedback on a subset of key non-compliances. The main priority of compilers is to make the process of compiling as effective and consistent as possible, functionality such as MISRA checking is secondary. Protean, therefore, performs additional much more robust analysis with QA·C using its dedicated MISRA C:2012 compliance module. Huw Jones, Senior Software Test Engineer stated, “We are impressed by the performance of QA·C, it is very accurate and we see that it is finding issues that other tools have missed. We are particularly conscious of the dangers of false negatives and the false sense of confidence that can be created when tools fail to detect genuine issues”.

The third key consideration relates to the certification of the tools. Gareth Price, Protean’s Principal Software Engineer, shared his experience from a previous safety–critical project (an aerospace project which needed to comply with DO-178B), “Our auditor required us to provide evidence that one of our verification tools was fit for purpose. Ultimately we needed to generate this evidence ourselves, a costly and time consuming exercise. Investing in tools which are already pre-certified by the vendor is a “no-brainer” even when further usage characterisation is required”.

Auto-generated code

Protean also raised the topic of automatic code generation as an adjunct to the verification dialogue. They do use SysML - but primarily for design, visualization and modelling - and have resisted the logical next step, to auto-generate code from SysML models. They have come to the conclusion that in general it is more efficient to simply hand generate the relevant code. This is partially because the code base is small (~100k lines of code), but also because this increases Protean’s control over their code and simplifies verification. Having said that, the sections of code which perform closed loop torque control are generated from simulation models and one of the challenges that Protean faces is to avoid the generation of warnings on auto-generated code during static code analysis.

Fortunately QA·C is able to identify auto-generated code and can be configured to stop displaying these warning messages, helping developers to focus on their “own” hand generated code. (Interestingly, a similar comment was made in relation to compiler libraries.Headers, where it is Protean’s intention ultimately to substitute these with in-house code.)
Easing the transition from proof of concept to production

One final lesson-learned and a consistent thread throughout all our discussions, was the fact that right from the early development stages (design and the proof of concept), Protean’s very clear focus had been on the requirements of the subsequent production phase. They have therefore been very proactive in adopting “fit for purpose” SDLC (Software Development Life Cycle) processes, standards and toolsets in anticipation of production. As Gareth summarized, “When we looked at our customer base and the broader automotive supply chain, it is evident that QA·C is recognised by the industry as a highly effective tool when it comes to MISRA compliance and is also certified to ASIL D. This tallied with our own prior hands-on experience of the tool, and adopting QA·C was, therefore, an easy decision for Protean.”

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 © 2014 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.

About Protean Electric

Protean Electric is a leading clean technology company that designs, develops and manufactures the Protean Drive™, a fully integrated, in-wheel motor, direct-drive solution. Protean Electric is strategically positioned to play a major role in the hybrid and electric vehicle market by offering a combination of packaging advantages, new vehicle design opportunities, performance benefits and cost savings.

Protean is funded by Oak Investment Partners, GSR Ventures and Jiangsu New Times Holding Group. Protean Electric has operations in the United States, United Kingdom, China and Hong Kong. For more information, visit www.proteanelectric.com

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.