The growing importance of safety-related functionality

When behind the wheel driving, the last thing a driver wants to experience is loss of steering, braking, or any other safety-related function. It is a foregone conclusion that consumers rely on the safe and proper operation of their cars today. But with continued electrification and innovation of features, more functions are relying on electronics and software support.

To support the development of safety-related functionality on electronics and software, actors across the industry have joined forces and standardized the rules for evaluation and development of safety features in automotive vehicles. This work has been captured in the ISO 26262 specification, learning from the experiences of the earlier IEC 61508, and adapting them for automotive use. At the same time, the automotive industry has worked together to define a set of interfaces and behaviors to serve as a foundation for the creation of automotive systems, and to enable specialists to focus their efforts in foundational software, while the automotive companies and their Tier 1 suppliers focus on creating safe and cost-effective systems. This has resulted in the creation of the AUTOSAR specification, which is now the de-facto standard for electronic system development.

Mentor’s AUTOSAR solution is aligned with both of these the standards and can be rolled out with the needs of modern ECU implementation. VSTAR is providing high quality AUTOSAR embedded software that can be used either as a COTS component according to the SEooC concept, or according to a mutually agreed upon DIA. Both options are available regardless of the level of hazard being mitigated by the device, up to ASIL D.

Safety Element out of Context (SEooC)

Mentor® Automotive VSTAR™ modules are available as Safety Element out of Context (SEooC) where all specified AUTOSAR requirements are treated as safety requirements ensuring that the software delivered is of the highest quality following top industry standard development methods, including:

- AUTOSAR versions 4.2 and 4.0.3 according to ISO 26262
- Supports any ASIL A-D
- Components available as SEooC based on AUTOSAR requirements
- All deliveries customizable with DIA
- Pre-certified SW
- Specific releases certified on request

RELATED MENTOR PRODUCTS:

- Mentor® Automotive Volcano™ VSx Tool Suite – Completely integrated for top-down vehicle system and ECU design. VSTAR is part of the comprehensive Mentor Automotive Volcano AUTOSAR toolchain which includes:
  - Volcano Vehicle System Architect™ (VSA) – Architecture design tool
  - Volcano VSA COM Designer™ – Network design tool
  - Volcano Vehicle System Builder™ (VSB) – ECU configuration tool
  - Volcano Vehicle Systems Integrator™ (VSI) – Simulation tool
  - Volcano Vehicle Systems Utilities™ (VSU) – Utilities tool
- Mentor® Embedded Sourcery™ CodeBench and Analyzer – Embedded systems development and analysis tools offering deep insight and trace data visualization.
- Mentor® Embedded Nucleus® SafetyCert™ – Mentor’s safety-certified real-time operating system (RTOS) that can be certified for use in ISO 26262 compliant systems.
- Mentor® Automotive ReqTracer™ – Provides documentation at any stage of development and manages the impact of requirement changes, resulting in better control, predictability, and improved product quality.
full requirements traceability, MISRA conformance, dedicated coding guidelines, and complete verification. Included in the safety package is all necessary documentation which allows the developer to deploy Mentor’s AUTOSAR solution in a safety-critical system with confidence. Included in this safety package is the crucial safety manual, which describes how the software component may be integrated with the rest of the operation of the device.

The same methodology is applied to all Mentor add-ons to AUTOSAR; these are developed according to the same model where all additional requirements are treated as safety requirements.

Development Interface Agreement (DIA)

If the target project, for any reason, cannot be satisfied with AUTOSAR requirements and deliverables with the predefined Mentor extensions, additions to the VSTAR SEooCs can be developed under a Development Interface Agreement (DIA) which defines the additions to the VSTAR development. The DIA is defined together and agreed with the VSTAR Safety Manager. The DIA can specify additions such as additional requirements, non-AUTOSAR components, customer specific delivery artifacts and development schedules, etc. Essentially, any safety relevant extension to the standard SEooC product offering will be specified and mutually agreed upon in the DIA.

Tool qualification

As embedded code is developed according to the required ASIL, it is imperative that the related tools are of equal quality. VSTAR tooling comes with safety manuals and artefacts to ensure conformance to the tool qualification requirements of ISO 26262. These documents form an aligned product fit with the rest of the VSTAR package.

Certification

Mentor Automotive will, upon request, certify any functional safety module, or any of the VSTAR tools with an ISO 26262 certificate, issued by an internationally respected certification authority. Currently provided pre-certified to ASIL B are the operating system (OS), Watchdog stack, E2E, and CRC modules. Further pre-certification is planned; please consult your Mentor Graphics or Mentor Automotive VSTAR representative for further details.

More about Mentor Automotive

Mentor Automotive provides advanced systems engineering solutions with a leading portfolio of automation design tools and software, built on deep expertise in systems engineering, to help customers solve the most complex design challenges facing the industry. Solutions reside in three key areas for automotive electrical and electronic design: connectivity and networking; in-car experience; and subsystems and technology.

For the latest product information, call us or visit: www.mentorautomotive.com

©2016 Mentor Graphics Corporation, all rights reserved. This document contains information that is proprietary to Mentor Graphics Corporation and may be duplicated in whole or in part by the original recipient for internal business purposes only, provided that this entire notice appears in all copies. In accepting this document, the recipient agrees to make every reasonable effort to prevent unauthorized use of this information. All trademarks mentioned in this document are the trademarks of their respective owners.

Autosar is a registered trademark. The registered trademark Linux® is used pursuant to a sublicense from LMI, the exclusive license of Linus Torvalds, owner of the mark on a worldwide basis.