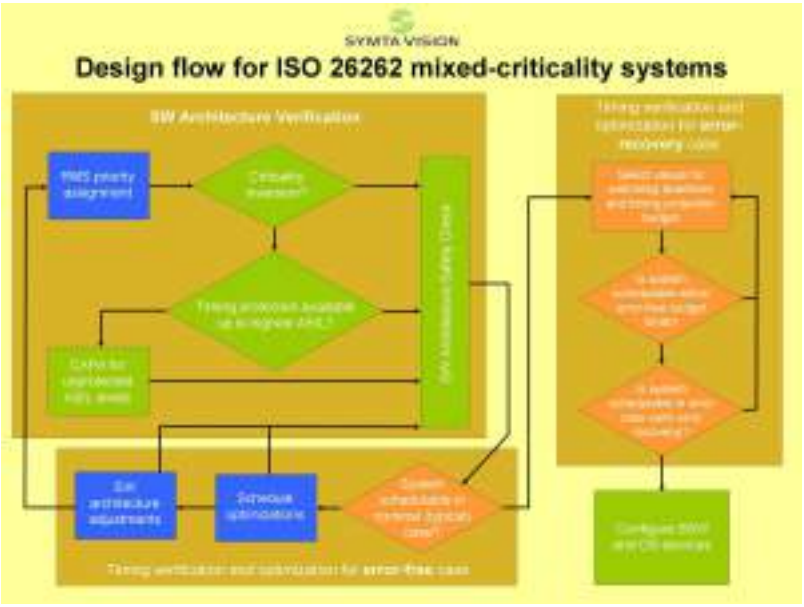
Methodology supports ISO 26262-compliant design of mixed-criticality automotive electronics

ECN Europe

Symtavision [1]'s SymTA/S methodology now supports the design of ISO 26262 compliant mixed-criticality automotive electronics systems. SymTA/S overcomes inherent safety versus efficiency conflicts, especially when 'freedom from interference' must be realised between software partitions with different criticality levels.



[2]The SymTA/S methodology meets the primary ISO 26262 requirement to provide reliable coverage for failure and error-free scenarios by undertaking timing analyses to optimise and verify the ECU software schedule. Crucial to this is the ability to use SymTA/S timing analyses to select configurations for OS services such as watchdog timeouts and timing protection budgets rather than simply react to timing failures while the target system is running.

"Designing for ISO 26262 is an extremely hot topic," said Dr. Marek Jersak, CEO of Symtavision. "With the advent of mixed-criticality ECUs in automotive electronic systems, the established design patterns for building ECU schedules are unsuitable as they trade off efficiency for safety. Using SymTA/S for the design of ISO 26262 compliant mixed-criticality automotive electronic systems allows ECU schedules to be created, analysed, optimised and verified that are not only safe and certifiable but also efficient."

To build ISO 26262 compliant ECU schedules that are both safe and efficient, the SymTA/S methodology draws on a combination of the established RMS (Rate Monotonic Scheduling) and the recently proposed CAPA (Criticality As Priority Assignment) timing schedule strategies coupled with procedural guidelines, based

on extensive SymTA/S timing analysis, on how safety can be verified and efficiency determined. RMS, which is currently used extensively in the industry, yields compact, resource-efficient pre-emptive timing schedules for AUTOSAR and OSEK, but it cannot cope with mixed-criticality requirements as priority is given to tasks with the shortest cycle time without reference to safety requirements and criticality levels. On the other hand, a CAPA strategy can ensure the necessary 'freedom from interference' between tasks that ISO 26262 demands but this comes at the cost of a significant reduction in resource efficiency.

Using timing analysis data from SymTA/S, the ISO 26262 compliant design methodology enriches key aspects of both the RMS and CAPA schedule design patterns with guidelines on how to select priorities, when and how to use Watchdogs or Timing Protection, and when the software architecture needs to be adapted in terms of cycle times and runnables-to-task mapping. Furthermore, SymTA/S reliably covers error-free and failure scenarios of various kinds, and hence provides evidence that the software and safety architectures are suitable.

"Already proven on real-world ISO 26262 compliant mixed-criticality automotive electronics systems, the SymTA/S is an invaluable aid for software architects in the planning phase of ECU software integration," concluded Dr. Marek Jersak, CEO of Symtavision. "The ability to select appropriate measures to ensure efficiency and certifiability as well as deliver safety at the lowest possible hardware cost is crucial to ISO 26262 ECU schedule design."

Links:
[1] http://www.symtavision.com
[2] http://ecneurope.files.wordpress.com/2012/04/250412-symtavision.jpg