ENHANCING AUTOSAR SAFETY MECHANISMS FOR ISO 26262 FUNCTIONAL SAFETY REQUIREMENTS

[1]Noh, Soonhyun *, [1]Kim, Myungsun, [1]Hong, Seongsoo
[1]Dept. of Electrical and Computer Engineering, Seoul National University, Rep. of Korea

KEYWORDS – ISO 26262, functional safety, ASIL, AUTOSAR, software fault detection

Research objectives
In the modern automotive industry, the importance of functional safety in electric/electronic (E/E) systems is increasing. To extensively address automotive functional safety issues, a global functional safety standard named ISO 26262 was proposed. The essence of ISO 26262 is a hazard analysis and risk assessment scheme named ASIL (Automotive Safety Integrity Level). Each E/E system is assigned an ASIL level that has clearly specified safety requirements. The AUTOSAR (AUTomotive Open System Architecture) has been actively adopting safety mechanisms to satisfy such requirements but it still falls short of expectation. In this paper, we propose enhanced safety mechanisms for AUTOSAR to fill such a gap.

Methodology
ISO 26262 classifies software faults into three categories: (1) faults on timing and execution, (2) faults on memory and (3) faults on exchange of information. However, the current safety mechanisms of AUTOSAR are incapable of detecting all these types of faults. First, it fails to detect the blocking of a task while it is running. This prevents the detection of a fault in the first category. Second, it cannot detect delayed data transmission between two ECUs. This may conceal a fault in third category. We add two safety mechanisms to AUTOSAR so that it can detect all three types of software faults listed in ISO 26262. We first propose an enhanced deadline supervision mechanism to detect the blocking of a task. We also introduce an end-to-end protection mechanism that can detect the delayed transmission of data. We implement our solution on TriCore™ Starter Kit to evaluate the effectiveness of the proposed approach.

Results
In order to help detect software faults listed in ISO 26262, we introduce two fault detection mechanisms for AUTOSAR. We first propose to enhance the deadline supervision mechanism so that it can monitor program execution flows and check a deadline miss between two checkpoints on the program: start checkpoint and end checkpoint. Compared to the original deadline supervision mechanism of AUTOSAR, the proposed mechanism can detect deadline misses caused by task blocking, before the task's end checkpoint. To do so, it periodically checks how much time has passed since the start checkpoint and immediately returns an error when the deadline is violated. We also propose an end-to-end protection mechanism that checks delayed transmission. The time difference between sent time and received time is computed for every message reception. We conducted experiment on TriCore™ Starter Kit and demonstrated that the proposed solution successfully detected faults as desired.

Limitations of this study
The current study covers the functional safety requirements of ISO 26262 only partially. In order to fully support ISO 26262, additional safety mechanisms should be incorporated.

What does the paper offer that is new in the field including in comparison to other work by the authors?
Since R4.0.3, AUTOSAR has been adopting mechanisms to address the safety requirements of ISO 26262 but it is still yet to be completed. To make AUTOSAR guarantee these safety requirements better, this paper proposes two new safety mechanisms.

Conclusions
In this paper, we proposed two safety mechanisms to detect software faults in order for AUTOSAR to better address the safety requirements of ISO 26262. They are the enhanced deadline supervision mechanism and the end-to-end protection mechanism. We validated the effectiveness of the proposed mechanisms with TriCore™ Starter Kit.