HARDWARE PROGRESS

A DVCon Europe 2019 conference paper, jointly authored by Renesas and OneSpin Solutions, considered innovative chip safety analysis. **Jörg Grosse** and **Sergio Marchese** discuss its findings

In today's vehicles, according to AUDI, microelectronics enable over 80% of vehicle innovation and high-end cars may contain more than 100 electronic control units (ECUs) controlling both safety-critical and entertainment functions, as well as implementing advanced driver-assistance systems (ADAS).

As a consequence, electro-migration, cosmic radiation, and other physical phenomena may corrupt the behaviour of integrated circuits (ICs) and cause both transient and permanent faults that could lead to dangerous system failures.

The Toyota unintended acceleration case is a well-known, and unfortunate, example of the potential consequences of hardware failures.

When considering a large fleet of cars, transient and permanent fault events could occur on a daily basis, so it is of the utmost importance to include safety mechanisms (SMs) that prevent and control hardware failures.

ISO 26262, the functional safety standard for road vehicles, requires a quantitative failure mode, effects, and diagnostic analysis (FMEDA) of automotive chips, and engineers must demonstrate that a particular IC, or a safety element out of context (SEooC), includes a sufficient level of fault protection, according to the automotive safety integrity level (ASIL) of the target application.

An IC controlling the steering system, for example, will likely satisfy the most stringent integrity level, ASIL-D.

Quantitative FMEDA

FMEDA is an established, systematic process to carry out a quantitative analysis of failure modes and diagnostic capabilities of an IC (see oposite).

FMEDA has three key steps: (1) validation of the IC safety architecture and partitioning of hardware functions and faults according to failure modes; (2) determination of the diagnostic coverage, which measures the ability of safety mechanisms to prevent safety goal violations; and (3) computation of the ISO 26262 hardware safety metrics.

ISO 26262 defines three crucial metrics: (1) the single-point fault metric (SPFM); (2) the latent fault metric (LFM); and (3) the probabilistic metric for random hardware failures (PMHF).

Single-point or residual faults cause a violation of safety goals. Latent faults, on the other hand, do not cause failures on their own but can do so if a second fault occurs. Latent faults are also called multi-point faults of order two.

SMs aim at reducing the number of residual faults so that the target SPFM is achieved. They can detect and indicate the presence of a fault and, in some cases, they may also be able to correct the effects of a fault and allow the system to continue operation without disruption. Unfortunately, SMs can also be affected by faults.

Residual faults in SMs could lead to system failures, rather than preventing them. Moreover, a fault affecting an SM could remain latent and compromise its diagnostic capabilities.

A second fault, which potentially can occur much later and that should be detected by the compromised SM, could be missed and lead to a dangerous IC malfunction. This is one important reason why latent faults also need careful consideration.

FMEDA is a time consuming and costly task, even for ASIL-B targets. Extensive fault simulation is a brute-force, effort-intensive approach to determine safety metrics. Its results are not rigorous as they depend on the simulation stimuli. Fault classification using formal methods is more efficient but may incur complexity issues.

Efficient safety analysis

Last year, Renesas Electronics and OneSpin Solution presented a paper

adobe.stock.com

titled, "ISO 26262 Fault Analysis in Safety Mechanisms" at the 2019 DVCon Europe conference. It introduced an automated, efficient, and scalable FMEDA process.

The process is demonstrated on two hardware modules with error-correcting code (ECC) memory protection as safety mechanism (see right). Single error correction and double error detection (SECDED), or even double-error correction and triple-error detection (DECTED), are commonly used in field-programmable gate array (FPGA) and application-specific integrated circuit (ASIC) systems on chips (SoCs).

The safety analysis step uses a safety aware hardware partitioning process, automated through the Fault Contribution Analysis (FCA) App. Failure modes are associated with design subparts delimited by key design signals, including protected outputs of the intended function, and diagnostic outputs of SMs.

Each SM subpart can be classified into two categories: (1) active, if its faults can propagate to the outputs of the intended function (observation points); and (2) passive, if its faults can only propagate to the diagnostic outputs of the SM (diagnostic points).

Subparts are processed to produce fault lists and attributes (e.g., estimated silicon area). It is worth noting that the safety analysis step is scalable to large, complex devices, thus being free from the shortcomings of fault simulation and standard formal technology.

Figure 1: The quantitative FMEDA process delivers ISO 26262 work product and safety metrics

The results of the hardware partitioning step immediately provide conservative, estimated safety metrics. Fault simulation or formal based fault analysis can be used only for specific subparts, should the estimated results not achieve the target ASIL.

The Fault Propagation Analysis (FPA) App and Fault Detection Analysis (FDA) App automate this additional fault analysis step, which in effect reduces the pessimism of the estimated metrics to improve results. The FPA App identifies safe faults, which are faults that cannot cause violation of the safety goals because they do not propagate to safety-critical outputs. The FDA App identifies faults that will always be detected and indicated by an SM.

Finally, the fault analysis results of each subpart can be combined to derive safety metrics for the entire SoC. This step is also automated through the Hardware Metrics Computation (HMC) App.

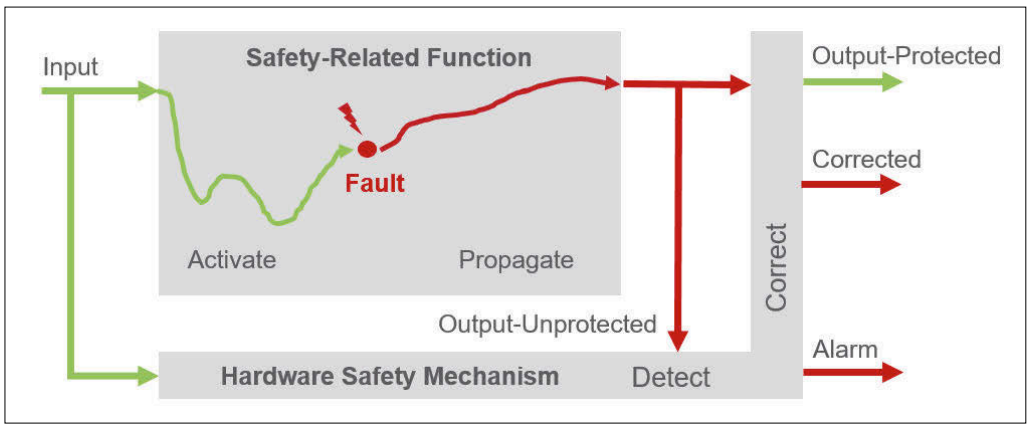

Figure 2: Architecture of a hardware safety mechanism with error detection and correction

In summary

ISO 26262 requires evidence that the SPFM and LFM achieve sufficiently high values, depending on the target ASIL. This may require accurate identification of the residual and latent faults, also in the SMs.

The computation of hardware safety metrics for a large SoC with multiple SMs often relies on manual analysis from experts and fault simulation. Manual analysis is effort-intensive and error-prone. Fault simulation requires substantial computational resources, and significant engineering effort to develop a testbench and justify appropriate workloads.

The paper, discussed here, from Renesas and OneSpin introduces an alternative, scalable approach for the computation of hardware safety metrics.

Large SoCs can be decomposed into parts and subparts using tools for safety-aware partitioning that require minimal user input. Fault classification results of subparts can be quickly estimated. If conservative estimates fall short of the target, accurate fault classification can be selectively deployed. This may include the identification of safe, residual, and latent faults in SMs with and without error-correcting capabilities. Automated, rigorous fault classification can be executed without a testbench or fault simulation by using formal-based technology.

At present, large organisations providing automotive SoCs and semiconductor IPs often rely on internal tools to improve their IC development flow.

Start-up companies struggle with safety compliance, as they need to focus their investment on their unique capabilities and may find it hard to hire safety experts.

The automotive industry needs mature and easy-to-use electronic design automation (EDA) solutions that leverage best practices across multiple companies and IC projects, reducing the cost of safety compliance and the need for experts. The solution outlined in this article aims to address these challenges.