ISO 26262: Better be safe with modelling and simulation on system-level

Joachim Hößler (hoessler@ikv.de)[1], Sven Johr (sven.johr@twt-gmbh.de)[2], Thang Nguyen (thang.nguyen@infineon.com)[3], Stephan Schulz (stephan.schulz@eas.iis.fraunhofer.de)[4], and Gert-Jan Tromp (g.j.tromp@dizain-sync.com)[5]

[1]ikv++ technologies, [2]TWT Science & Innovation, [3]Infineon Technologies, [4]Fraunhofer Gesellschaft IIS/EAS, [5]Dizain-Sync

INTRODUCTION (or REQUIREMENTS)

Since the introduction of the ISO 26262 standard, today's development behaviour of automotive industry is strongly affected to a safety oriented working culture. Furthermore, the number of functionalities and complexity with high integration is rapidly increasing in modern automotive electronics making mixed-signal SoC design become trend in automotive nowadays. On top of that, high pressures to produce reduced time-to-market, first-time-right design are additional key elements. These facts pose great challenges for designers at different design level from system to hardware components, embedded software. An effective utilization of modelling and simulation facilitates the design process so that these challenges can be met. As such, this work focuses on developing an *ISO 26262 compliant* modelling and simulation workflow supporting system level development of safety-related items, including mixed-signal hardware component and custom embedded software at micro-controller side.

OBJECTIVES

The major objective is a modelling and simulation workflow that is ISO 26262 compliant and bridges the gaps between different modelling techniques and development steps by the following activities:

1. *functional safety analysis* including Hazard and Risk analysis (HARA) in order to derive the safety requirements;
2. *functional modelling and allocation* of functions to system components;
3. *identification of malfunctions.*

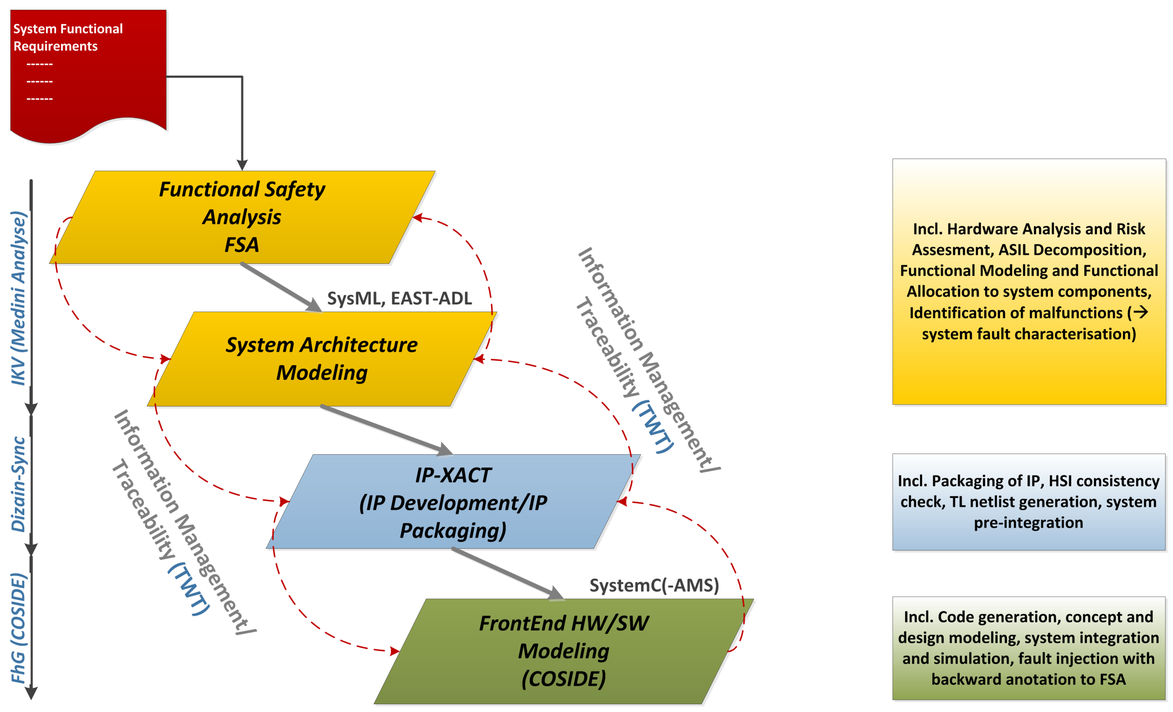
For instance, the *identified malfunctions* are used to derive input for fault injection activities (required by the ISO 26262 standard) and, thus, to simulate the system under faulty conditions caused by defects or electromagnetic interference. Based on the simulation results appropriate safety mechanisms are defined and developed. Subsequently, the previously defined fault injection runs are used in order to validate the developed safety mechanisms.

Moreover, the proposed modelling workflow should enable traceability of requirement changes and management from system level down to hardware/software component level and back. This is not only one of the most important requirements of the ISO 26262 standard but also helps to strengthen the consistency of the information flow from multidisciplinary design teams.

RESULTS

Depicted in the Figure is the overview of the proposed modelling and simulation workflow. One of the challenges for a (generic) workflow is the heterogeneity in terms of languages and tools used across the various design and development stages. For example, the functional design is often done informally in functional dependency diagrams (e.g. SADT in Visio, PowerPoint, or Excel), while the system architecture uses a (semi-)formal modelling language (e.g. SysML, EAST-ADL). Our workflow utilises SysML, SystemC, and SystemC AMS as modelling languages. Each language is supported by a specific tool to develop the system. mediniAnalyze from IKV is used to conduct the functional safety analysis, from the hazard analysis to the functional safety concept and to the safety architecture, including functional allocation and ASIL decomposing at the later step. The system architecture is then modelled using SysML. The tool includes as well the capability of mapping requirements into subsystem/system architect models. SystemC and SystemC-AMS will be supported by COSIDE® for subsystem components development to system integration, its simulation, and verification activity. The workflow is highly automated using packaging of IP with the IEEE standard IP-XACT allowing automatic generation of Hardware Software Interface (HSI) interconnects, test bench and verification environment and verification software.

RESULTS



CONCLUSIONS

We have introduced our ISO 26262 compliant modelling and simulation workflow. The workflow follows the methodology prescribed by the ISO standard and uses tools and languages as, for instance, mediniAnalyze, IP-XACT, COSIDE®, ReqIF and Reqtify.

In summary, HARA is considered on a SysML model present in the tool mediniAnalyze and the results of the analysis are used with IP-XACT in order to handle over those results to the simulation tool COSIDE®.

For simulation within COSIDE®, prefilled SystemC modules based on the SysML model are generated. Moreover, modules and netlists are generated from the IP-XACT description such that a seamless transition from definition to implementation is given.

In our workflow, the *safety information* ranging from HARA down to the system design in SysML, is exported in the ReqIF format and will be used within IP-XACT as reference point within the “vendorExtension.”

For the airbag SoC the undeveloped event E15 from the FTA, the related safety information, i.e. TSR that are allocated to the system's safety architecture, is exported in ReqIF and then used in the IP-XACT description as a reference point within the XML description. We use the “vendorExtension” with its *get* and *set* commands as given in the IP-XACT standard for that.

REFERENCES

[1] D. Cuddeback, A. Dekhtyar, and J. H. Hayes. Automated Requirements Traceability: The Study of Human Analysts. In Requirements Engineering Conference (RE), 2010 18th IEEE International, pages 231-240, September 2010.

[2] O. C Z Gotel and A. C W Finkelstein. An analysis of the requirements traceability problem. In Requirements Engineering, 1994., Proceedings of the First International Conference on, pages 94-101, April 1994.

[3] IBM. IBM - Rational RequisitePro. http://www-03.ibm.com/software/products/de/reqpro, 2014.

[4] W. Kruijtzer et al. Industrial IP Integration Flows based on IP-XACT standards. In Design, Automation and Test in Europe, 2008. DATE '08, pages 32-37, March 2008.

[5] Dassault Systèmes. CATIA Systems Engineering - Reqtify. http://www.3ds.com/de/produkte-und-services/catia/funktionsumfang/catia-systementwicklung/requirements-engineering/reqtify/, 2014.

[6] TVS. Requirements - TVS. http://testandverication.com/solutions/requirements/, 2014.

Add acknowledgments, organization involved, logo’s contact information here