Model-based Method to achieve EMC for Distributed Safety-Relevant Automotive Systems

Andreas Baumgart*, Klaus Hörmaier†, Gerhard Deuter‡
*Carl von Ossietzky Universität Oldenburg
Email: andreas.baumgart@uni-oldenburg.de
†Infineon Technologies Austria AG
Email: klaus.hoermaier@infineon.com
‡TWT GmbH - Science & Innovation
Email: gerhard.deuter@twt-gmbh.de

***Abstract*—Automobiles contain an increasing number of distributed Electrical and Electronic systems. Among such systems, Electromagnetic Compatibility (EMC) is a major issue that impacts functional safety and requires a high verification effort. The automotive standard for functional safety ISO 26262 already provides requirements for EMC and refers to agreed standards. It addresses the topic during the development process in order to obtain a tolerable level of risks arising from possible causes for system malfunctions. Yet, a coherent process for EMC and functional safety on a concept level is missing. With this publication a model-based method is provided that connects specification, design, and analysis of functional as well as physical characteristics for distributed safety-relevant systems with EMC simulations. By applying our method, potential coupling paths and EMC issues can be systematically identified, analyzed and addressed by introducing counter measures at a concept level of the development process. The resulting technical design is compliant to a technical safety concept and traceable with respect to electromagnetic characteristics of affected hardware components and wires.**

Keywords–Electromagnetic compatibility (EMC); Model-based design; Automotive; ISO 26262; Safety-relevant systems

I. INTRODUCTION

Today's cars contain an increasing amount and variety of Electrical and Electronic (E/E) systems. Thereby, many of them implement safety-relevant functions. The ISO 26262 is the agreed automotive standard for functional safety, which provides requirements and recommendations for the development of such systems.

One issue addressed by that standard is EMC for a safety-relevant system and its environment. Electromagnetic interference (EMI) between hardware components is a typical cause for failure dependencies (e.g., common cause failures) and for systematic failures in hardware components that realize functions of safety-relevant systems. Physical characteristics of hardware components and interconnecting wires can provide coupling conditions leading to critical malfunctions. Therefore, EMC must be addressed when defining a safety concept for a safety-relevant E/E system and when designing its hardware such that it is sufficiently robust against EMI. However, the parameter space for a specific EMC problem is typically very large. Thus, the evaluation of its electromagnetic (EM) properties is very complex. Trying to simulate all hardware components on a detailed level requires enormous effort. Abstraction of the EMC problem with conservative over-approximation of EMC can help. In order to reduce the complexity and to ensure functional safety w.r.t EMC this work presents a guideline on how to tackle the problem on the system level of the safety process.

The proposed method is a combination of analysis and simulation-based test methods. It allows a systematic identification and evaluation of safety-relevant malfunctions and faults related to EMC. We propose a model-based approach together with contracts. It allows specifying dependencies between functional and physical characteristics of distributed and interconnected components. With it the EMC problem can be addressed for distributed system development. Typically, contracts are used to model and analyze functional characteristics of E/E systems. The electromagnetic influence of hardware components and connector systems (wiring harness) and their relationship to functional system properties is neglected. Thus, we propose a meta-model together with a corresponding workflow to address this problem. In order to cope with the complexity of the EMC problem the scope of this paper is limited to electrical near field coupling. Since the paper refers mainly to the ISO 26262, we use the wording and terms from this standard.

This paper is structured as follows. We first describe the state of the art with regard to this publication. In the following section we introduce the basics of contracts, functional safety according to the ISO 26262, and multi-perspective modeling. Finally, we define the meta-model and the workflow of the proposed methodology in IV and discuss its benefits.

II. STATE OF THE ART

In this section, the state of the art is described and discussed regarding methods for safety-relevant automotive systems, EMC, model-based methods including existing standards and tools as well as related work.

A. Safety-relevant automotive systems

Today's automotive system engineering processes and quality management guidelines take into account the topic functional safety respecting the standard ISO 26262 [1] that has been effective since 2011. The standard addresses EMC in the context of robustness as well as systematic and dependent failures on different levels of abstraction, i.e., system and hardware level. Standardized testing methods are referenced for usage to ensure EMI robustness of hardware components as well as parts and to address EMC in system integration tests. Depending on the ASIL safety goals and derived safety requirements may only be violated with a maximum failure rate which is analyzed using quantitative methods like Fault Tree Analysis (FTA) or by applying fault metrics. FTA is

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-371-1

defined in [2]. A typical topic regarding the analysis of fault-trees is the analysis of cut-sets and the determination of minimal cut-sets as shown in [3]. In order to analyze the quantitative influence of common cause failures like those related to EMI the parent standard IEC 61508 [4] suggests the usage of a β-factor analysis. The analysis is systematic using a table with questions to determine the β- factor. Implementation assumptions including EMC-related wire alignment such as cable alignment and further environmental characteristics are considered in this catalog of questions. The analysis is for instance supported by the tool FaultTree+ [5] or by Medini Analyze from IKV[6].

B. EMC

EMC is a major topic for automotive industry and subject to many publications, standards and physical simulation tools. A detailed description of cross talk in the automotive environment is given in [7]. The number of tool, suitable for modelling and simulation of EMI of car components seems quite limited. Yet their number increases. EMC Studio [8], for example, provides a useful framework to simulation EMI between cables and devices. The same is possible with FEKO [9]. Both tools allow defining a cable tree, attaching circuits and simulating the interference in terms of parasitic voltages, currents, and critical frequency ranges. Powerful hybrid tools such as COMSOL Multiphysics [10], also allow correct simulation of EMI providing a profound knowledge of electromagnetism. All those tools are equally suitable for the evaluation of EMI at a fixed geometry. The data obtained from such simulation is available for formulating or refining contracts, which can be used in the authors evaluation process.

The authors focus on the development of such a simulation tool which is also able to optimize cable and cable tree geometry with regard to EMC for given external boundary conditions, such as a case or housing. With regard to the topic of functional safety discussed above, an overview about the impact of functional safety on EMC is provided by Kado et al. [11]. The authors of that publication discuss environmental factors like temperature and ageing effects and note their importance for EMC. According to them, a safety manager must have an overview on all EMC activities. Failure modes caused by EMI have to be taken into account during the hazard analysis and risk assessment. Inductive and deductive safety analyses as well as fault injection tests need to be performed. Common cause failures with regard to environmental conditions need to be identified for all safety-critical functions to determine appropriate measures. A respective test plan should be created with regard to EMC relevant characteristics and traceability of EMC related documents needs to be ensured.

C. Model-based approaches

Capturing the complexity is one challenge for safety-relevant systems and also for EMC. This challenge is often addressed by model-based methods and tools supporting them. One related formalism is the use of contracts. Contracts have been subject to various research projects in the context of safety-relevant systems like SPEEDS [12], CESAR [13] or SPES2020 [14]. The contracts enable formal requirements engineering and systems engineering by explicitly distinguishing between assumptions and promises of system components. An overview about contracts is provided by Benveniste et al. [15]. Formal representations of assumptions and promise are often discussed, e.g., regarding the use of Linear Temporal Logic (LTL) formulas for functional conditions or other pattern-based expressions with defined syntax and semantics for various aspects. Among other things virtual integration testing is defined for contracts with functional and safety characteristics allowing formal analysis of consistency and compatibility between system components as well as checking the correct implementation of a contract by components with derived contracts. To analyze integration of components regarding physical conditions typically tools like Simulink [16] or Modelica [17] are referenced. Modelling languages can be used to describe design artefacts and their relationships such as system components and requirements to be satisfied on different abstraction levels and architectural perspectives as described by Damm et al. [18]. An architectural modelling language for automotive system design is EAST-ADL [19]. It addresses topics like hardware modelling, error modelling and traceability between design and requirements on different abstraction levels and architectures. Hardware connectors between hardware components are considered as wires. It is possible to allocate requirements (including requirements on EMC) to both, connectors and components. The alignment of wires can be described by using descriptive concepts from the Harness Description List (HDL) [20]. Functional design traceable with the topological layout of wires can be defined in the tool PREEvision from Vector. It provides different architectural views including a logical architecture view, a hardware architecture view, a wiring harness view, and a geometric view. Therefore, reasoning about the alignment of wires is possible with PREEvision.

D. Related work

A methodology similar to the approach of this document is proposed in previous work [21]. The methodology suggests the usage of contracts to cope with environmental factors related to physical conditions in a dependent failure analysis with regard to the topology of a safety-related automotive system. Simulation methods were recommended to determine potential dependent failures. This approach instruments the heterogeneous rich components (HRC) meta-model developed in the SPEEDS project [22] in order to model contracts. The method is evaluated for temperature. It will be shown how the approach can be extended to investigate wire installations and EMC together with physical simulations.

E. Discussion

From our point of view the presented state of the art lacks in the missing interaction between EMC and functional safety aspects. On the one hand, EMC is typically addressed on detailed levels (II-B), which incorporates several risks. Adhering to the recommendations of standards leads to over-engineered (too robust) systems, or is not necessarily complete regarding all safety-relevant EMI faults of a system under design. Furthermore, the consistency of a system's EMC properties with its electromagnetic environment is not ensured at design time. Unintended additional development loops can therefore be required. On the other hand, an ISO 26262 compliant safety process is systematic and starts at an early stage of system design. But, the standard does not define exact methods or formalisms to integrate and analyze relevant EMC

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-371-1

properties with derived safety concepts. In order to perform a β-factor analysis for EMI-related dependent failures EMC characteristics of the system implementation must be known. A systematic design process and derivation of requirements is not considered. The discussed model-based methods, formalisms, and tools only partially address the needs to address EMC in an automotive safety process. For instance, existing contract based methods do not address EMC. Formalisms like EAST-ADL or KBL and tools like PREEvision do not allow to define and analyze all relevant EMC characteristics with functional and hardware architectures or wiring harnesses.

Thus, we propose a method to combine functional and safety views of a system under design with a physical view. By using concepts from the previously published approach [21], extending it with concepts from HDL and PREEvision we are able to link and analyze an automotive wiring topology and related EMI) with a functional safety concept compliant to the ISO 26262.

The main difference to the state of the art is the systematic approach for EMC in the context of safety relevant automotive systems. Starting with the requirements on the level of a functional safety concept, technical EMC requirements are consistently derived for concepts of a safety concept and its environment. EMC requirements are made explicit in terms of physical assumptions and promises for all relevant components.

III. BASICS

Our methodology builds upon contracts, functional safety, EMC principles and multi–perspective modelling.

A. Contracts

Our approach includes the usage of contracts. They provide a component specification framework for distributed system development. The usage of contracts allows a formalized argumentation about the combination of the single component's specifications in a defined environment. Contract-based reasoning can be used for early validation in distributed development with different suppliers or company divisions and for the reuse of existing designs. Within the contract specifications, different viewpoints such as functional, safety or physical concerns can be addressed.

The basic idea of contracts is a structured specification of component characteristics in terms of assumption - promise pairs. Crucial for contracts is the explicit definition of assumptions made on the integration environment of a single component. The component itself is considered as a black box. Characteristics promised in the component's specification are only guaranteed if the corresponding assumption holds.

In particular, compatibility between contracts of distributed components and their combined integration in a context with a contract on a higher level of abstraction can be analyzed by applying contract based methods like a Virtual Integration Test (VIT) as shown in [18].

In order to illustrate the structure of contracts, the following contract specifies a function with a promised execution time for processing an output signal b, assuming that an input signal a is available at a certain frequency: Assumption: "a occurs at most every 100 ms." Promise: "whenever a occurs b occurs at most after 80 ms.

B. EMC, Functional Safety and ISO 26262

The automotive functional safety standard ISO 26262 [1] provides a framework of requirements, activities, and recommendations to achieve functional safety for automotive E/E systems. According to this standard, functional safety is a property of E/E systems that guaranties the "*absence of unreasonable risk due to hazards caused by malfunctioning behavior*".

In an early stage of the safety process the E/E system is defined in its boundary on vehicle level as item. For this item hazardous malfunctions are identified in a hazard analysis and risk assessment. These hazards are considered in different operational scenarios as risks. An Automotive Safety Integrity Level (ASIL) is determined and assigned to the risks, rating a risk as safety relevant (ASIL A to D) or as a matter of an established quality management (QM). Safety goals are derived from the safety relevant risks. They go along with further requirements for the system design depending on the ASIL. For each safety goal functional safety requirements are derived, defining together the functional safety concept. They consist of technology independent definitions on how safe states are maintained by a system's elements in order to achieve a safety goal. Dependent failures caused by, e.g., EMI have to be taken into account. Reasoning about them on the level of the functional safety concept typically requires knowledge about the technical realization, which is not complete at that stage of the process. Yet, preliminary architectural assumptions and environmental constraints are typically available and can be refined. Therefore, dependent failures have to be taken into account when defining the technical safety concept and when arguing about its compliance to the functional safety concept. When deriving technical safety requirements from the functional safety requirements, analysis methods like a FTA are recommended to "*identify causes of systematic failures and the effects of systematic faults*". EMC violations are systematic causes related to the integration environment of a hardware element (victim) implementing parts of a safety relevant system. Therefore, EMC is related to integration testing. Also, when reusing an existing technical design, environmental conditions such as EMC shall be checked before implementing a system. Additionally, on hardware level the "*level of robustness shall be demonstrated using feasible test methods*" for which the ISO 26262 refers to typical standards such as ISO 7637 "*Road vehicles - Electrical disturbances from conduction and coupling*". To test whether an EMC-related environmental conditions is relevant for functions safety, the safety-relevant situations must first be identified in the safety process.

C. Electromagnetic Compatibility (EMC)

A component is EM compatible when the emitted interference is low enough to not affect other components or systems and is robust enough not to be influenced by other sources of disturbance. As shown in Figure 1, each atomic EMC problem consists of an aggressor, the victim and at least one coupling path. EMC can generally be improved from three different angles in a system: Reduction of the interference generated by the aggressor, improving EM decoupling or improving the victim's robustness. Simulation of the system can be used to determine the most effective counter measure or verified the compatibility.

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-371-1

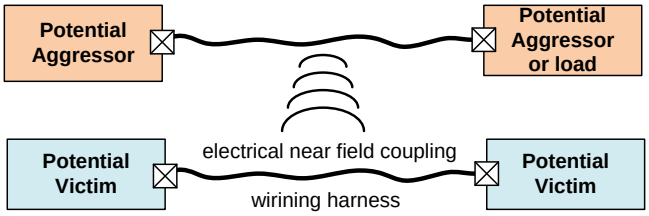

Figure 1. Overview of the aggressor, the coupling path and the victim

In electrical engineering, EM coupling is typically modeled as a feedback from the victim to the aggressor. To describe the aggressor, the victim and the coupling path as impedance networks, design models, and measured data can be used. The component's impedances are either determined by measuring S-parameters or extracted from the design model. Regarding the aggressor, a guideline for modelling an Integrated Circuits (IC) black box emission model is given in [23]. For the characterization of external aggressors the standard IEC 61000-2 [24] can be used. The coupling path can be modeled, as shown in [7], by using a lumped transmission line model.

Currently, simulations use a configurable aggressor model, able to emit standardized output. The victim can be specified either by its impedance or an equivalent circuit. Modelling and simulation of the coupling path is a more complex task. Coupling between wires depends on different variables including their geometry, their materials, and additional surrounding conductors such as a housing. Given all specific parameters for the coupling path, one can calculate the frequency and temperature-dependent coupling parameters, resistance, conductance, capacitance, and inductance per unit length (including their parasitic components) for the specific transmission line(s). An equivalent circuit can be defined, the aggressor and victim model added and the crosstalk simulated using SPICE or any other circuit solver (for a simple schematic model see Figure 2). Those solvers usually instrument different numerical methods (various matrix solvers, finite elements, finite differences) to obtain results for the system of coupled differential equations describing the time and frequency behavior of the circuit. Using suitable numerical methods, qualitative and quantitative results can be obtained in time and frequency domain. Using such EMI simulation in the context of functional safety analysis will be discussed in Section IV-B. The complexity of the simulated system is usually only limited by the simulation hardware.

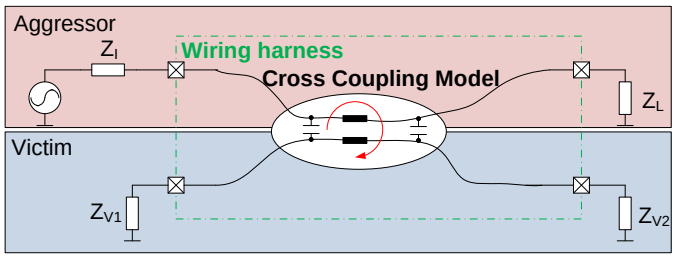

Figure 2. Schematic circuit for aggressor, wiring harness (coupling path) and victim with impedances.

Currently, any possible dependence of EMC to the victim or aggressor operation modes must be considered in the general analysis and cannot be handled by such a simulation. The operation modes of the victim and the aggressor have influence on their EMC properties.

D. Multi-Perspective Modelling

Since EMC is a physical property respective characteristics need to be related to functional design for a model-based argumentation in the context of functional safety. A recent approach described in research projects like SPES 2020 [18] is the description of models at different structural viewpoints called perspectives. Their elements are related to another by means of allocation. This allows for the separation of concerns while preserving a system's properties. For the perspectives the viewpoints operational, functional, logical, and geometrical are considered where this work's focuses on the last three. Functions are mapped to an architectural description in the logical perspective with decomposed and interconnected logical components as a "*description of the logical solution independent from technological constraints*" [25]. A model in a technical perspective is a description of a system's hardware and software, their interactions, as well as their technical and physical properties and constraints. In a geometrical perspective, a model describes the topological layout of a system i.e., a definition of physical positions claimed by elements of a hardware architecture within a reference coordinate system. The idea and the concepts of multi-perspective modelling provide an important base for the proposed EMC method, which will be discussed in IV.

IV. Design Methodology

In this section, the proposed methodology for contract based automotive EMC is presented. At first, the application of the meta-model is discussed. Then the EMC-workflow is presented. We conclude with a comparison of the disadvantages and advantages of our method.

A. Meta–Model

The model that we propose for EMC-related safety analysis extends hardware modelling concepts from EAST–ADL by contracts, wires, and topological information as depicted in Figure 3. The model can be used as an extension of EAST-ADL in order to support the workflow discussed in section IV-B. EAST–ADL is implemented in different ways such as profiles for several UML tools (e.g. Eclipse / Papyrus UML) or with the EATOP platform, all listed by the EAST-ADL association [26]. The concepts and relationships of the model can also be used in a meta-model of a Reference Technology Platform, discussed in research projects like CESAR, MBAT or CRYSTAL, to support the workflow with integrated and interoperating tools, as shown, for instance, in [27]. EAST–ADL allows modelling of a hardware architecture with hardware components, parts and logical as well as electrical connections. The proposed extension allows the definition of contracts with regard to the concepts of the HRC meta-model [21]. The contracts contain specifications of assertions that define the assumptions and promises of the contracts. EAST–ADL allows to allocate requirements to architectural elements like hardware components by using the concept of a satisfy-link. We extend the satisfy-link concept such that contracts can be allocated to the architectural elements. By introducing concepts for wires

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-371-1

in our extension, contracts can be allocated to wires of a wiring harness, too. Prototypes (instances) of such wires are related to hardware connectors via a wire mapping allowing assignment of physical properties to the hardware connectors. A crucial part of our proposed model is the introduction of a geometric view with topological information as discussed in previous work [21]. Topological elements can be defined like a component hierarchy with topological nodes as parts and routed interconnection segments in between them. Looking at PREEvision and HDL one would distinguish between hierarchies of installation spaces and locations as topological nodes and installation routes described by topological segments with defined curves between such nodes. Geometrical information is assigned to the hardware elements like prototypes of hardware components and wires by installing them to the topological elements. By such an installation, physical space claimed by the elements of the hardware architecture is defined. Reasoning about physical properties like distance, length of wires, or alignment of wires is enabled this way. These properties are needed for analyses like a dependent failure analysis w.r.t. environmental factors such as EMC.

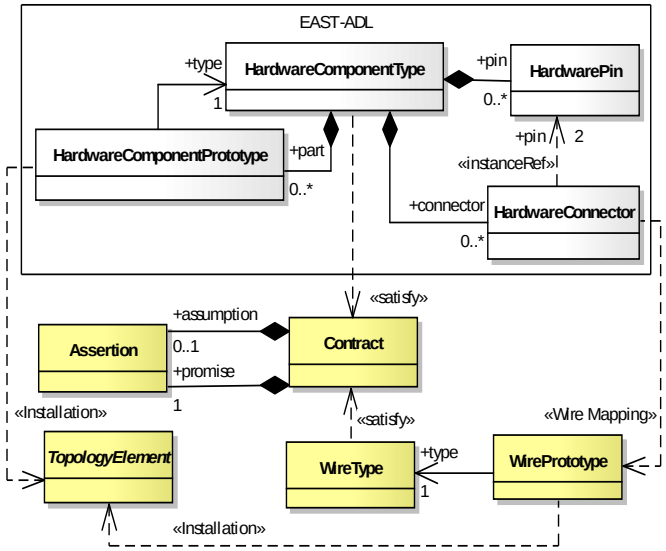

Figure 3. Overview on the meta-model concepts and relationships

A generic instance of the proposed meta–model is as follows. With existing EAST–ADL concepts an automotive hardware architecture with the hardware components of a vehicle (typically ECUs, actuators, sensors) is modelled as described in [19]. By using the concepts and relationships of the proposed EAST-ADL extension, depicted in Figure 3 and described above, a model can be defined in a way that it can be used for the proposed workflow. Safety requirements are formulated as contracts by using the `Contract` concept. Like in [22], assumption and promise of a contract are modelled using the `Assertion` concept with an attribute to carry the descriptions of the respective conditions. As considered by EAST–ADL for safety requirements the contracts are allocated to the `HardwareComponentTypes` of the hardware components by using the `≪satisfy≫` link concept indicating that a hardware component shall satisfy the contract. The wiring harness of a vehicle is modelled by using the concept `WirePrototype` for every wire of the wiring harness. Each wire is typed by a `WireType` defining the type of the wire with its properties. As intended by the proposed methodology the properties are defined in contracts using the `Contract` concept, as described above, and the `satisfy` link concept. A `HardwareConnector` becomes a wire by using the `≪Wire Mapping≫` link concept between a `HardwareConnector` and a `WirePrototype`. The geometric perspective for the hardware architecture and the wiring harness is defined by using the *`TopologyElement`* concept. With it the geometric topology of the vehicle is defined and its installation spaces. Furthermore, with this concept installation locations for the hardware components and routes for the wires are defined. Details on how to define a geometric architecture with concrete topology elements are given in [21]. The hardware components are assigned installation locations by using the `≪Installation≫` link concept between a `HardwareComponentPrototype` and the related *`TopologyElement`*. The hardware components of the hardware architecture are assigned installation locations by using the `≪Installation≫` link concept between a `HardwareComponentPrototype` and the related *`TopologyElement`*. The wires of the wiring harness are assigned routes by using the `≪Installation≫` link concept between a `WirePrototype` and the related *`TopologyElement`*.

For a model-based realization of our workflow, different architectural, mapping, and requirement views are required. These include technical hardware architecture, wiring harness, geometric topology, contract-based requirements, and mapping relationships between the respective views. The proposed meta-model provides concepts and relationships needed for the required views. The development of a technical safety concept (TSC) for an item w.r.t. ISO 26262 is usually done by the Original Equipment Manufacturer (OEM) before the actual implementation is done by the suppliers on hard- and software level. Our goal is to specify and validate EMC on system level in an environment of preliminary architectural assumptions with technical safety as well as functional and EMC requirements.

B. Proposed workflow

The prerequisites for our workflow, as illustrated in Figure 4, consist of a Functional Safety Concept (FSC) with functional safety requirements. The functional safety requirements are allocated on system elements that belong to preliminary architectural assumptions. Typically, dependent failure situations cannot be addressed in the functional safety concept because a refined architecture description must be known. Dependencies between functions mainly arise with lower abstraction levels (implementation details), like e.g., shared resources or physical implementation. For EMC, dependent failures regarding EMI and systematic failures in the TSC affecting the elements of the item are investigated. To address EMI faults, the requirements specifications of other electrical systems are also taken into account. The technical specifications and requirements for the wiring harness must be checked as well, because they describe the possible coupling paths. To rate the EM coupling paths, an existing geometrical model that defines the topology of the technical elements and the wiring harness is used. The entire

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-371-1

topology model is created by mapping the technical elements and the elements of the wiring harness to the geometrical topology elements as described by the meta-model.

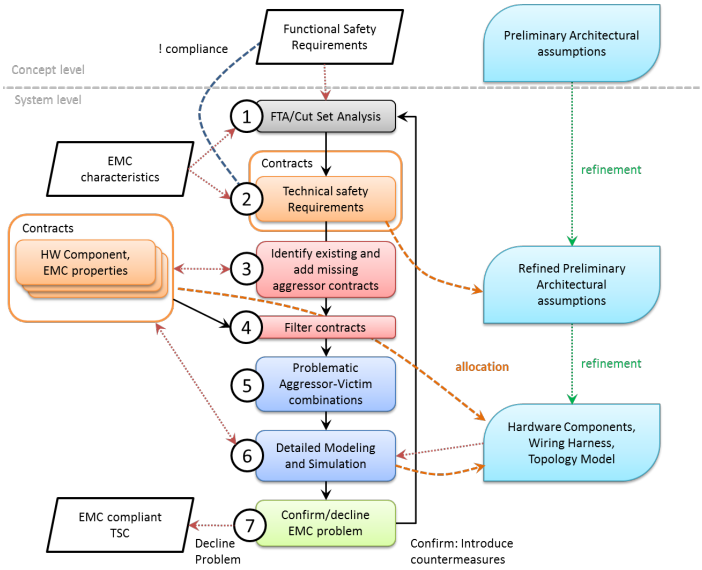

Figure 4. Proposed workflow

The first step (1) of the proposed method is a FTA and a cut-set analysis. In the FTA combinations of possible cause (faults) are analyzed which lead to violations of the safety goals assigned to the item. How to perform a cut-set analysis can be found in [2] or [28]. Additionally, the preliminary architectural assumptions are refined towards an architectural description with technical elements of the item that become hardware components (e.g., sensors, ECUs, actuators). In the FTA also faults related to EMI are visible as base events. The refined preliminary architectural assumptions allow to address failures with regard to the hardware components of the item and to derive a TSC that respects EMC for the hardware components as possible victims. Therefore EMC-related faults are included.

An example for an EMI related fault is the radio frequency (RF) signal, which is inadvertently identified as valid signal. We define EMC faults as violations of electrical-constraints caused by coupled RF signals. These characteristics have to be considered in the FTA leading to base events in the fault tree, which can be potentially caused by disturbances or coupling with other systems. With the cut-set analysis the combinations of the faults including EMC faults, which lead to violations of the safety goals for the item are extracted from the fault-tree.

In the second step (2), the technical safety requirements are formulated. They are derived from the functional safety concept as well as from the FTA and cut-set analysis results including the EMC faults. For each functional specification that can be violated by an EMC fault according to the fault-tree an EMC assumption is formulated. The EMC assumption specifies an EMC constraint whose violation leads to the EMC fault. For instance for the fault "RF-voltage at sensor port" an assumption is formulated "RF-voltage at sensor port in [-5 V, 5 V]. Note: Other EMC assumptions can address electromagnetic characteristics including frequency, time, power or current. The contract defining the technical safety requirement consists of the EMC assumption and the related functional specification as promise. The technical safety requirements are allocated to the technical elements of in the preliminary architectural assumptions. By neglecting the EMC characteristics of the assumptions in the technical safety requirements existing contract-based integration analysis tests, as shown in [29], can be used in order verify compliance between the TSC and the FSC. The compliance between the TSC and the physical environment w.r.t. EMC is analyzed in later steps.

The next step (3) aims to elicit the potential aggressor contracts and the EMC properties. Typically, all technical elements can act as EM aggressors w.r.t. the technical elements of the item including its own. At this point it is assumed that the OEM has already decided which components will be installed. We assume that the requirements specifying EM properties take the form of contracts. In a new environment all contracts are not necessarily available. Thus, data has to be requested by the suppliers or the components have to be characterized. The assumption is typically a functional condition e.g., given by a LTL formula or similar concept like the Requirements Specification Language (RSL) described in [18]. The promise is a physical condition that depends on e.g., input voltage range and operating mode. An example for contracts with physical conditions regarding EMC in the promise is given with the following contracts. They are written down using natural language pattern.

Contract 1:
Assumption: *(mode = off implies SwitchingTime $>$ 20 ms)*;
Promise: *mode = off implies RF voltage(power_out) in [-0.1 V, 0.1 V] with a inner resistance higher 120* Ω,
Contract 2:
Assumption: *(mode = on implies SwitchingTime $\geq$ 10 us)*;
Promise: *mode = on implies RF voltage(power_out) in [-20 V, 20 V] with a inner resistance higher 120* Ω,
Contract 3:
Assumption: *(mode = error implies 10 ns $<$ SwitchingTime $<$ 10 us)*;
Promise: *mode = error implies RF voltage(power_out) in [-120 V, 120 V] with a inner resistance higher 18* Ω.

The result of step 3 will typically be a large amount of EM aggressor contracts. Step 4 therefore targets a reduction of the amount of involved EM aggressor contracts by filtering. For the filtering an ideal coupling path is assumed, which is the worst case. An assumption on a voltage between -5 V and 5 V is not violated by hardware components with a guaranteed RF voltage between -5 V and 5 V. So the contract
Contract 1:
Assumption: *(mode = off implies SwitchingTime $>$ 20 ms)*;
Promise: *mode = off implies RF voltage(power_out) in [-0.1 V, 0.1 V] with a inner resistance higher 120* Ω,
from step 3 is not taken. The result is a set of critical victim - aggressor combinations (including modes of operation), for which the TSC is violated. Due to the overestimation not necessarily all of the combinations will violate the TSC in the implementation. Therefore, refinement of the models and analysis as described in Step 5 is necessary.

In Step 5, the correct physical model is created reducing the overestimation. For each critical victim - aggressor combinations from step 4, the coupling model is generated using the physical and geometrical information from

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-371-1

the specifications. An example for a contract specifying characteristics of a wire is

Contract 1:

Assumption: *(shielding type = braided & manufacturer_tolerance > -5% frequency range = [10 Hz to 200 kHz])*;

Promise: *shielding_thickness* $\geq$ *1 mm; attenuation* $>$ *10 dB*

These models can be simulated using the method described in Section III-C or commercial tools (e.g., FEKO, EMC Studio).

Each outcome of an executed simulation has two possible states regarding the EMC assumptions of the victim:

- The EMC assumptions are not violated within the simulated EM environment with the respective aggressors and coupling paths.
- They are violated by the simulated environment.

For the victim - aggressor combinations that remain after filtering and violate the EMC assumptions, adequate counter measures are specified. Possible measures w.r.t to EMC faults and their impact are described as follows:

- For a violation of an EMC assumption the robustness of the victim has to be increased by changing the EMC assumption (e.g., immunity against RF voltages up to 20 V instead of 5 V).
  Impact: Introduction of hardware measures to achieve a better EM immunity. This will eventually be covered by the supplier.
- If there are no degrees of freedom for the victim's specification, modification of the wiring harness can be required. This can lead to stronger requirements for the affected parts of the wiring harness (e.g., a cable within the harness must be shielded) or to a modification of the geometry of the wiring harness (e.g., change the install of a wire from an identified coupling path to another location).
  Impact: Coordination with the person responsible for the wiring harness.
- If there are no degrees of freedom for the specification of the victim and the wiring harness, it seems reasonable to strengthen the aggressors EMC promises (e.g., voltage output in case of error below 20 V instead of 50 V).
  Impact: Coordination with the person responsible for the aggressor.
- If there are violations of EMC assumptions in case of failures related to the aggressors (e.g., error states) and there are no degrees of freedom for changes on aggressor, victim or wiring harness, the respective EMC assumption can be removed and instead a safety mechanism is specified. The definition of the safety mechanism takes the form of a contract and is specified in the promise. The safety mechanism typically defines how a safe state is maintained (e.g., Promise: *Whenever the voltage at sensor port is larger than 20 V the sensor interface shall deliver the code "No valid data"*.
  Impact: New verification of compliance between functional and technical safety concept.

The order of the different measures is exchangeable and depends on the effort to be spent as well as the influence of the OEM on the affected suppliers. After a "safety measure" has been chosen, the fault tree is adjusted and the cut-set Analysis performed again. The modification(s) have to be applied to the requirement specifications and the TSC, also, the architecture models have to be adjusted. Depending on the modification, some simulation models might not change and therefore don't need to be investigated again. The determination of such models will not be discussed during this work.

C. Summary

The benefits of the presented method are the following: Coarse filtering of dependencies and identification of possibly safety-relevant problems have been simplified by using a systematic model-based approach with contracts. Early validation of the TSC for typical EMC problems is possible, reducing unnecessary iteration loops during testing and development. Changes and/or removal of hardware components do not necessarily force a reevaluation of the TSC. A less pessimistic EMC design is possible, the OEM can reduce overprotection of individual technical system elements. Including topological information to the safety analysis allows characterization of the EM coupling paths. The approach and the proposed meta-model allows traceability of functional and physical specifications in the safety process.

The drawbacks, on the other hand, are: Assumptions about the completeness of the system definitions must be made. If a technical system element is added, a major change is committed, which results in reevaluation of the TSC. The restriction to near field coupling is an approximation, as simulation of all possible EM disturbances is not possible. Also, the initial effort to specify the architecture is large.

To summarize, a structured approach for identification of EMI problems of safety-relevant automotive systems has been shown. It is important to point out, that conditions of a component's physical environment are now accessible for investigation of safety concerns on system level. The use of contracts allows to consider EMC victims and aggressors as black boxes. Their EMC characteristics are identified as part of the safety lifecycle w.r.t. the ISO 26262. An argumentation about their integration is done at an early stage of the development process and takes the geometric topology into account.

V. Conclusion

In this paper, we proposed a methodology to address EMC for safety-relevant automotive systems. For the methodology we consider contract-based specifications and a meta-model that allows to characterize functions and their relationship to distributed E/E components in a hardware topology with EMC properties. The proposed model is a possible extension of EAST-ADL and allows modelling of topological information for a hardware architecture and to determine the alignment of wires forming coupling paths. The model ensures traceability of related engineering as well as analysis and test information as required by the ISO 26262. By applying the proposed method an early validation of EMC characteristics is enabled on system level before E/E components are actually built and integrated. The dependency between OEM and supplier can therefore become less pessimistic. Safety-relevant EMC problems are identified and addressed on concept level. In contrast to existing methods that make assumptions on a system's implementation regarding EMI robustness in safety-analyses and consider robustness tests on lower design levels

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-371-1

with the proposed method safety-relevant EMC characteristics are identified and validated at an early stage of the development process. They are systematically written down in requirements using contracts for involved components of a safety-relevant system and its physical environment. With the proposed method the effort needed to achieve EMC in a development process for a safety-relevant automotive system is focussed on safety-relevant EMI characteristics.

VI. ACKNOWLEDGMENT

The research leading to these results has received funding from the ARTEMIS Joint Undertaking under grant agreement Nr. 295311, and Nr 269335, as well as from the German Federal Ministry of Education and Research (BMBF) under the grant number 01IS11003L and the Austrian Research Promotion Agency FFG under the program "Forschung, Innovation und Technologie für Informationstechnologien (FIT-IT)".

REFERENCES

[1] ISO, *Road Vehicles - Functional Safety*. International Standard Organization, November 2011, ISO 26262.

[2] W. Vesley, F. Goldberg, N. Roberts, and D. Haasl, *Fault Tree Handbook*. U.S. Nuclear Regulatory Commision, 1981.

[3] T. Peikenkamp, A. Cavallo, L. Valacca, B. Eckard, M. Pretzer, and E. M. Hahn, "Towards a Unified Model-Based Safety Assessment," *Assessment*, pp. 275–288, 2006.

[4] IEC, *Functional safety of electrical/electronic/ programmable electronic safety-related systems*, iEC 61508, all parts.

[5] [Online]. Available: www.isograph.com

[6] ikv++ technologies ag, *Medini^{TM} analyze functional safety analysis for ISO 26262* , February 2013, Version 2.1.

[7] S. Alexandersson, "Automotive electromagnetic compatibility - Prediction and Analysis of Parasitic Components in Conductor Layouts," Ph.D. dissertation, Lund University, 2008.

[8] [Online]. Available: www.emcos.com/

[9] [Online]. Available: www.feko.info

[10] [Online]. Available: www.comsol.com

[11] R. Kado, J. J. Nelson, and W. Taylor, "Impact of Functional Safety on EMC: ISO 26262," in *Proceedings of SAE 2013 World Congress & Exhibition, Detroit, MI, USA*, April 2013, SAE Technical Paper 2013-01-0178, 2013, doi:10.4271/2013-01-0178.

[12] [Online]. Available: www.speeds.eu.com

[13] [Online]. Available: www.cesarproject.eu/

[14] [Online]. Available: http://spes2020.informatik.tu-muenchen.de/

[15] A. Benveniste, B. Caillaud, D. Nickovic, R. Passerone, J.-B. Raclet, P. Reinkemeier, A. Sangiovanni-Vincentelli, W. Damm, T. Henzinger, and K. Larsen, "Contracts for Systems Design," INRIA, Research Report N°8147, November 2012, project-Teams S4.

[16] [Online]. Available: www.mathworks.com

[17] [Online]. Available: www.modelica.org

[18] W. Damm, A. Baumgart, E. Böde, M. Büker, G. Ehmen, T. Gezgin, S. Henkler, H. Hungar, B. Josko, M. Oertel, T. Peikenkamp, P. Reinkemeier, I. Stierand, and R. Weber, "Architecture Modeling," OFFIS, SPES2020 Project Result, March 2011.

[19] EAST-ADL Association, *EAST-ADL Domain Model Specification*, May 2013, version V2.1.11.

[20] M. Ungerer and O. Rabe, *Harness Description List (KBL)*, 2005, Version 2.3 SR-1.

[21] A. Baumgart, "A Contract-Based Installation Methodology for Safety-Related Automotive Systems," in *Proceedings of SAE 2013 World Congress & Exhibition, Detroit, MI, USA*, April 2013, SAE Technical Paper 2013-01-0192, 2013, doi:10.4271/2013-01-0192.

[22] SPEEDS Project, *SPEEDS L-1 Meta-Model*, May 2009, SPEEDS WP.2.1 Deliverable D.2.1.5, Revision 1.0.1.

[23] IEC, *IEC62433-2-1, Ed.1 - EMC IC modelling Part 2-1: Theory of black box modelling for conducted emission*. International Electrotechnical Commission, 2009.

[24] ——, *IEC61000-2 Environment: description, classification; compatibility levels*. International Electrotechnical Commission, 2008.

[25] K. Pohl, H. Hönninger, R. Achatz, and M. Broy, *Model-Based Engineering of Embedded Systems: The SPES 2020 Methodology*. Springer, 2012, ISBN 978-3642346132.

[26] EAST-ADL Association, "EAST-ADL Association," Website, http://www.east-adl.info/, 2013.

[27] A. Baumgart and C. Ellen, "A Recipe for Tool Interoperability," in *Proceedings of MODELSWARD 2014*. SCITEPRESS, 1 2014, pp. 300–308.

[28] Goble, *Control Systems Safety Evaluation and Reliability, 3rd Edition*. International Society of Automation (ISA), 2010.

[29] W. Damm, B. Josko, and T. Peikenkamp, "Contract based ISO CD 26262 safety analysis," in *Proceedings of SAE 2009 World Congress & Exhibition, Detroit, MI, USA*, April 2009, SAE Technical Paper 2009-01-0754, 2009, doi:10.4271/2009-01-0754.

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-371-1