Rethinking transport
27–30 April 2020

TRA 2020 HELSINKI

Proceedings of 8th Transport Research Arena TRA 2020, April 27-30, 2020, Helsinki, Finland

DEIS – Dependability Engineering Innovation for smart transportation

Eric Armengaud[a]*, Cem Kaypmaz[b], Erhan Ozkaya[b], M. Zeller[c], S. Longo[d], M. Melis[d], R. Groppo[e], E. O'Carroll[f], D. Schneider[g], J. Reich[g], Y. Papadopoulos[h], I. Sorokos[h], T. Kelly[i], I. Habli[i], R. Wei[i], F. Villa[j], G. Regan[k]

[a]*AVL List GmbH, Hans List Platz 1, Graz 8020, Austria*
[b]*AVL Research and Engineering Turkey, Akpınar Mahallesi Tuna Caddesi Ballıca Sokak No: 1 34885. Sancaktepe Istanbul, Turkey*
[c]*Siemens AG, Wittelsbacherplatz 2, Munich 80333, Germany*
[d]*GM Global Propulsion Systems – Torino Srl, Corso Castelfidardo 36, Torino 10129, Italy*
[e]*Ideas&Motion S.r.l., via Santa Margherita 8, Alba 12051, Italy*
[f]*Portable Medical Technology Ltd, 66 Pairc Chuiminn Kilcumin, Killarney Kerry V93V6K4, Ireland*
[g]*Fraunhofer IESE, Fraunhofer-Platz 1, 67663 Kaiserslautern, Germany*
[h] *University of Hull, Cotthingham road, Hull HU6 7RX, United Kingdom*
[i] *University of York, Heslington, York North Yorkshire YO10 5DD, United Kingdom*
[j] *Politecnico of Milano, Piazza Leornado da Vinci 32, Milano 20133, Italy*
[k]*Dundalk Institure of Technology, Dublin road, Dundalk, Ireland*

Abstract

Ensuring appropriate dependability of modern industrial systems is becoming more and more challenging due to the raising complexity of modern embedded systems and the introduction of connectivity, possibly leading to ad-hoc creation of systems' configuration. State-of-the-art dependability analysis techniques, applied during design phase, provide limitation in terms of scalability with respect to the system size and in terms of runtime flexibility and ad-hoc reorganization. The DEIS project[†] addresses these important and unsolved challenges by developing technologies that form a science of dependable system integration. Main contributions of this paper are (a) the introduction of the DDI concept and DEIS outcomes available for the community, (b) the illustration of DDI usage to increase functional safety development efficiency for railways systems, (c) the usage of DDI for data privacy management in context from Intelligent physiological parameter monitoring for road transportation, and (d) the introduction of DDI for trusted runtime collaborative platooning for road transportation.

Keywords: dependability; functional safety; SOTIF; data privacy; railway; automotive

* Corresponding author.
E-mail address: eric.armengaud@avl.com

1. Introduction

Cyber-Physical Systems (CPS) harbour the potential for vast economic and societal impact in domains such as mobility, home automation and delivery of health. At the same time, if such systems fail they may harm people and lead to temporary collapse of important infrastructures with catastrophic results for industry and society. CPS is the key to unlocking their full potential and enabling industries to develop confidently business models that will nurture their societal uptake. Using currently available approaches, however, it is generally infeasible to assure the dependability of Cyber-Physical Systems. CPS are typically loosely connected and come together as temporary configurations of smaller systems which dissolve and give place to other configurations. The key problem in assessing the dependability of CPS is that the configurations a CPS may assume over its lifetime are unknown and potentially infinite. State-of-the-art dependability analysis techniques are currently applied during design phase and require a priori knowledge of the configurations that provide the basis of the analysis of systems. Such techniques are not directly applicable, can limit runtime flexibility, and cannot scale up to CPS.

The DEIS project [1] addresses these important and unsolved challenges by developing technologies that form a science of dependable system integration, see Fig 1. In the core of these technologies lies the concept of a Digital Dependability Identity (DDI) of a component or system. The DDI targets (1) improving the efficiency of generating consistent dependability argumentation over the supply chain during design time, and (2) laying the foundation for runtime certification of ad-hoc networks of embedded-systems.

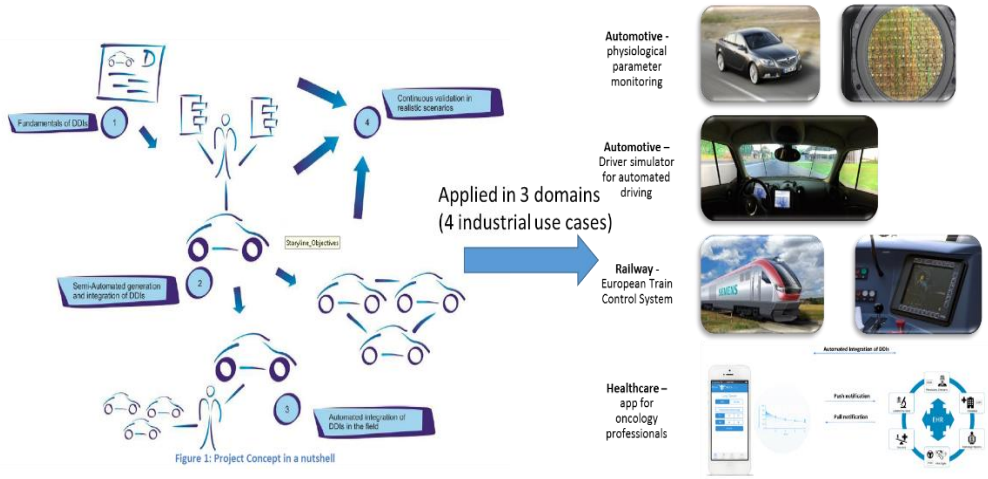

Figure 1 - DEIS project at a glance

Main contributions of this paper are (a) the introduction of the DDI concept and DEIS outcomes available for the community, (b) the illustration of DDI usage to increase functional safety development efficiency for railways systems, (c) the usage of DDI for data privacy management in context from Intelligent physiological parameter monitoring for road transportation, and (d) the introduction of DDI for trusted runtime collaborative platooning for road transportation.

2. The DDI concept

The general idea of a Digital Dependability Identity (DDI) is to create and maintain modular dependability models on the level of units of composition to support integration and reconfiguration scenarios at development time and at runtime. On the one hand, a unit of composition can thus be a component, which is manufactured by a supplier and integrated by an OEM. In this case, the OEM would integrate the DDIs of all supplier components with and into the DDI of the final product. The DDI would ideally provide all of the dependability-relevant information required for the integration in a modularized and formal way, thus enabling tool-supported semi-automated integration of the different supplier DDI to synthesize the OEM product DDI.

On the other hand, at runtime, DDI are a means to tackle the issue of dependability-related uncertainties and unknowns when dynamically integrating different systems in a cooperative CPSoS context. Based on the DDI, systems are enabled to negotiate their mutual dependability-related guarantees and demands and to verify relevant

context assumptions in a fully automated way. Moreover, a continuous dependability-related monitoring and management of CPSoS is enabled during operation, thus guaranteeing that important dependability requirements are never violated. It shall be noted, that runtime DDI operate on a higher level of abstraction as compared to a development time DDI, what is necessary to enable the fully automated evaluation.

In the DEIS project, a DDI metamodel has been developed called Open Dependability Exchange (ODE)[‡], see [2]. The ODE utilizes the SACM 2.0 [3], the Structured Assurance Case Meta-Model of the Object Management Group, as a core ingredient and a backbone. In addition, the ODE contains a range of auxiliary metamodels, which are interlinked with both, the SACM and between each other, see Fig. 2. Based on the ODE, DEIS developed tool support for synthesizing DDI and for integrating them across different parties and tools along the value chain. More precisely, four different model-based safety engineering tools (ComposeR of Siemens [4], ACME of UoY [5], HipHops of UoH [6] and safeTbox of Fraunhofer [7]) have been augmented to support (at least parts of) the ODE and to be able to export, import and semi-automatically integrate DDI.

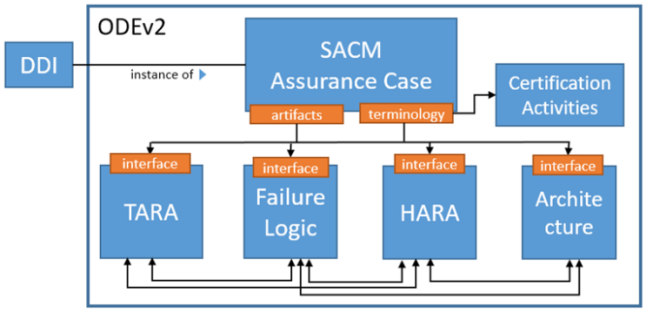

Figure 2 - DEIS Open Dependability Exchange

By establishing this kind of formal traceability between different aspects in the ODE, DDIs represent an integrated set of dependability data models (=What is the evidence data?) that are generated by engineers and are reasoned upon in dependability arguments (=How is the evidence data supporting the claim?). A DDI is, therefore, an evolution of classical modular dependability assurance models, in that several separately defined dependability aspect models are now formally integrated allowing for comprehensive dependability reasoning. DDIs are produced during design, certified when the component or system is released, and then continuously maintained over the lifetime of a component or system. DDIs are used for dependable integration of components into systems during development.

A DDI contains information that uniquely describes the dependability characteristics of a system or component. DDIs are formed as modular assurance cases, are composable and can be synthesized to create more complex DDIs from the DDIs of constituent systems and system components. The DDI of a system contains a) claims about the dependability guarantees given by a system to other systems b) supporting evidence for the claims in the form of various models and analyses and c) demands from other connected systems being necessary to support the claims.

Figure 3 shows the principal building blocks of CPS dependability assurance visualizing how the DDI Dependability Engineering Framework bridges the gap between a CPS use case description and its dependable operation at runtime. The starting point for all dependability assurance activities is the description and planning of the functionality that the CPS shall render for its stakeholders, which may be either direct system users, companies or even the society. An essential property of a CPS function is that it is executed on multiple independent systems leading to a required distribution of dependability assurance over multiple system manufacturers. For example, a platooning CPS function is executed on multiple trucks of potentially different manufacturers. Enabling cooperative function execution while still allowing decoupled development is only possible by making development and runtime execution interfaces explicit for both functional and quality aspects. Concretely, structural and behavioral aspects of the intended CPS function need to be made explicit along with assured constraints regarding their quality bounds.

DDIs are concerned with the comprehensive and transparent assurance of dependability claims. Thus, each assurance activity and each artifact contained in a DDI is motivated by a root dependability claim that defines the sufficient risk reduction regarding a dependability property such as safety, security, availability or reliability. The

[‡] https://github.com/DEIS-Project-EU/

definition of acceptable risk reduction is typically derived from domain-specific risk management standards targeting different risk causes such as functional safety causes (e.g. ISO 26262), causes related to functional insufficiencies and foreseeable misuse (e.g. SOTIF PAS 21448) or causes due to cyber-security threats (e.g. ISO/SAE 21434). These standards contain requirements for assessing risk criticality and reducing risks to an acceptable level. Note that existing standards do not specifically consider CPS challenges as of now. However, the DDI framework has been defined generally enough to be open for the structured extension with contents from future risk management standards specific for CPS assurance challenges.

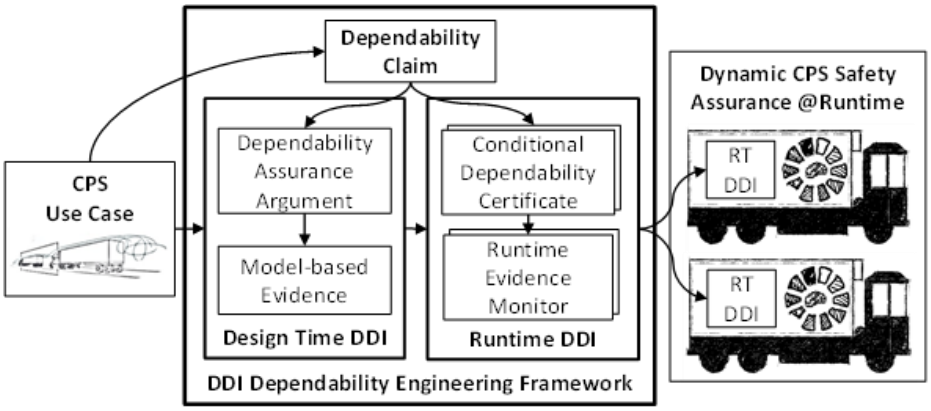

Figure 3 - DDI Dependability Engineering Framework Overview

Having a dependability claim to be assured for the CPS function, the next step is the systematic planning of risk management activities. These activities create necessary evidence for supporting the system engineers' reasoning that the dependability claim holds for the developed system or CPS. For both risk management planning and dependability assessment purposes, an explicit argument is indispensable inductively relating the created evidence to the top-level claim through several step-wise layers of argumentation. Note that, while the performed activities and produced artifacts vary depending on the kind of risk that is being managed, the general need for argumentation supported by evidence is mandatory for all risks. DDIs deal with dependability risks, thus the currently supported design time DDI assurance activities and evidence focus on well-established dependability methods such as hazard and risk analysis, safety and security analyses, safety design concepts, validation, and verification. These activities proved sufficient over the last decades in demonstrating the dependability of closed embedded systems not being affected by the CPS challenges. In addition, reliance on model-based approaches already compensates for the increasing complexity of closed systems. Thus, we believe model-based development is also necessary for assuring CPS.

The open and adaptive nature of CPS, combined with their increased need for environmental operational awareness to render optimal functionality, increases their complexity tremendously. To assure with sufficient confidence that CPS behavior is dependable in all situations, dependability assessment of those situations is mandatory. A common way to simplify this process is to build the system using worst-case assumptions about the environment, specific for the managed risk. Thus, we only look at the most critical situations and constrain system behavior to be dependable in those situations. The problem with this strategy is that worst-case assumptions lead to performance loss ("A non-driving car is safe, but has no utility!"). An alternative to unacceptable performance due to design time worst-case assumptions is to enable the CPS to reason about dependability at runtime. This alternative involves determining the worst case of the current operational situation instead of acting according to the worst case of all possible situations. This approach avoids the commonly known state space explosion problem but demands engineering dependability intelligence into the CPS. Such dependability intelligence builds upon the design time assurance case by equipping a system with pre-certified knowledge about dependability guarantees it can offer and dependability demands it needs from other systems or the environment to render those guarantees (Conditional Dependability Certificates). Additionally, the dependability intelligence needs to monitor both CPS and environment for changes (Runtime Evidences) that affect dependability. Based on such changes, it can reason about possible CPS configurations leading to dependable CPS behavior in different situations. Summarizing, runtime DDIs are a reduced form of pre-certified design time dependability assurance cases, containing only those dependability artifacts and reasoning intelligence required for monitoring dependability-relevant context changes and reacting to them in a dependable way. Regarding the engineering of concrete runtime DDIs, the DEIS consortium focused on the usage of Conditional Safety Certificates (ConSerts) [10] for expressing modular,

variable and fully formalized safety concepts including required runtime evidences enabling safety guarantee-demand matching and thus a basic form of dependability reasoning at runtime. For monitoring CPS state and environment, the consortium is exploring state-based probabilistic methods such as Bayesian Networks (BNs) and Hidden Markov Models. Consortium partners published a conceptual framework using BNs to supervise and manage safety of a truck platooning system during operation in [11].

3. DDI usage to increase functional safety development efficiency for railways systems

The European Train Control System (ETCS) provides standardized train control in Europe and eases travelling with trains crossing the borders of all countries in Europe. Thus, enabling "plug & play" of railway systems scenarios as a long-term objective. However, in such "plug & play" scenarios guaranteeing the systems' dependability requirements pose new challenges. Consequently, certification activities require accurate planning and must react quickly to changes within the system development process. Systems in the railway domain are also produced by various stakeholders in the value chain (such as national or even regional public transport authorities, national safety authorities, railway undertaking, OEMs, suppliers, etc.) and, therefore, safety information about components and subsystems (rolling stock, track-side and railway systems) need to be interoperable and exchangeable.

ETCS (Level 2) consists of an on-board and a trackside system (e.g. Balises, Radio Block Center, etc.). Both sub-systems must fulfil the safety requirement as defined in Subset-091 (Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2) of the ERTMS/ETCS specification. Moreover, trackside and on-board system are often provided by different vendors. ETCS on-board and trackside systems must meet the specified safety requirements specified in Subset-091 in order to be safely integrated in any interoperable railway system.

In this use case, we use DDIs to interchange safety-relevant information (including e.g. safety requirements, models, and assessments) during the development life-cycle of the trackside and the on-board ETCS units. The safety requirements specified in Subeset-091, which must be taken into account by the suppliers of ETCS systems, are provided in form of DDIs. The suppliers of on-board or trackside systems can build the systems with the help of the safety information formalized by the DDIs. Later during the system integration phase of the development life-cycle, the suppliers also provide safety information of the trackside or on-board ETCS system in form of DDIs. Hence, an on-board or trackside system can be integrated into an existing railway system and interact in a safe manner with the pre-existing systems within the railway systems. Moreover, the safety case of an ETCS system (either trackside or on-board) shall be generated based on the information provided by the sub-system / component DDIs.

In this ETCS use case, we utilize DDIs to represent the information provided in the safety assurance process of the ETCS system. A high-level overview of a DDI and its contents for the ETCS example is depicted in Figure 4 The ETCS DDI's backbone is the system-level safety argument expressed in SACM. As described in Sec. 2, the concrete safety argument contains a process-related part motivated by safety requirements from CENELEC EN 50129 and a product-related part mostly driven by the ETCS specification. In hierarchical system (of system) structures, the refinement of the system-level safety argument results in safety requirements to be satisfied by the subsystems, in the ETCS case by the trackside and onboard subsystems. Note that the principal structure of the trackside system DDI (lower part of Figure 4) is almost equal to the ETCS DDI, with the exception that the root (=the safety guarantees to be given) of the trackside safety case are the interface safety requirements posed by the ETCS integrator. From that point on, a safety argument needs to be provided by the trackside system manufacturer within the context of the trackside system. This safety argument is supported by evidence artifacts synthesized from various kinds of models such as failure logic, architecture or process models. The most notable innovation introduced by DDIs is that the source models for evidence are formally linked to the argument bits supported by them and organized within an all-embracing container. This characteristic together with the possibility to automatically match demanded and satisfied requirements in different DDIs (see the "Trackside System Safety Requirements" demanded by the ETCS system and satisfied by the trackside system) enable efficient safety-related collaboration across multi-tier supply chains and semi-automated change management through explicitly defined exchange interfaces. The full instantiation of the DDI approach for the ETCS system has been described in [12].

Today, dependability engineering is purely document based. Different design and safety analysis artefacts such as graphics, tables, or safety analysis models are included in documents to compile a safety case. Individual documents are interlinked by referencing the respective documents. Reuse is only possible by referencing existing documents or by using copy-and-paste which is only possible in very few and restricted cases.

The DDI concept is based on models which can be interlinked on a fine-granular level by referencing the respective model elements. Thereby, specific models or model elements can be referenced in different scenarios and in different DDIs. Hence, models (or parts of models, such as Component Fault Tree elements) can be easily reused and integrated into a new DDI. Since the currently used methods allow reuse only in a very limited way, the effort for building a safety case today is nearly the same as for a completely new product despite the fact that the new product may show only modifications of a previous product.

The DDI approach enables fine-granular reuse of specific parts of models created during the system design and the safety assessment. Furthermore, model composition can be applied thus leveraging a considerable potential for effort reduction. Moreover, the model-based DDI approach enables consistency by allowing the definition and automation of consistency checks for the different parts of the ODE model. Hence, constancy between system models, safety analyses and safety argumentation can be improved significantly. Hence, with the DDI approach, time and effort in the certification of systems (or sub-systems) in the railway domain can be reduced significantly by interchanging and reusing dependability information across the value chain of the railway domain. Thus, safe travel not only within the system of national railway operators but also across the borders or European countries can be ensured in a cost-efficient way.

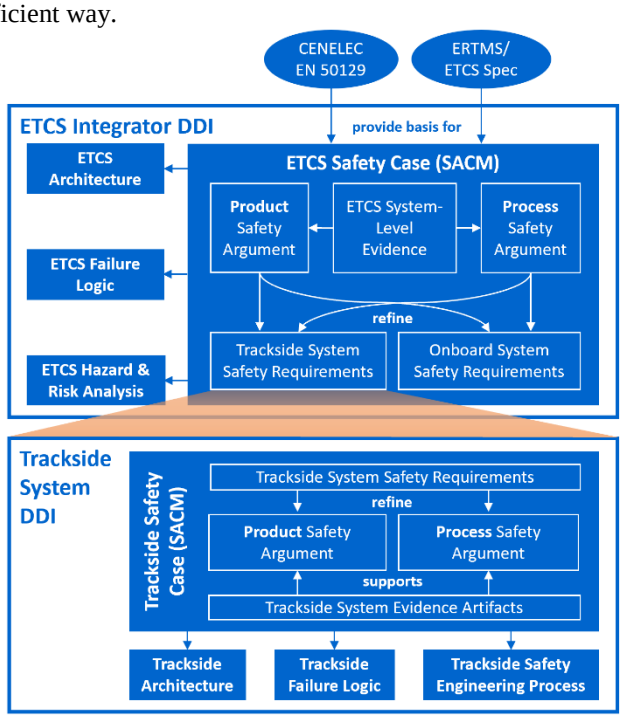

Figure 4 - High-level contents of ETCS and trackside DDIs

4. DDI usage for data privacy management in context from intelligent physiological parameter monitoring for road transportation

This use case is a stand-alone Dependable Physiological Monitoring System (DPMS) for automotive application, developed in a driving simulator to reproduce real-life conditions, see Figure 5. Smart and reliable connectivity and a non-invasive adaptive learning-based solution will go beyond traditional available systems in driving scenarios. Here, the proposed Single-Photon Avalanche Diode (SPAD) array imaging system will identify physiological parameters such as Heart Rate (HR), Respiration Rate (RR), Heart Rate Variability (HRV), Inter-Beat Interval (IBI) and Oxygen-Saturation (SpO2) in real time. In order to identify physiological parameters with higher accuracy and robustness, the system is developed with adaptive methods and approaches. This brand-new feature contains a comprehensive package of technologies, tools and services that support the drive session in evaluating the occupant's health status. In the case of a health emergency this new feature, which has been introduced in new generation connect vehicles with (even limited) autonomous capabilities, shall process hard decision making at run-time and trigger different "actions" to mitigate the risk of vehicle accidents and people injuries.

Based on the emergency condition detected, the system may select three different remedial action according to severity level, staring from a simple feedback request from the driver (severity 3), to the emergency manager medical call (severity 2), and finally the activation of autonomous drive features (severity 1). From a safety perspective, all the possible paths shall evaluate the risk to health. Part of the safety argumentation requirements enable different features on the vehicle, for example, moving the vehicle to the emergency lane / the nearest safe area, or in case of high danger, drive the vehicle to the Hospital / First Aid Services (depending on autonomous level capabilities).

The physiological data (including the streaming video) is sensitive with regards to General Data Protection Regulation (GDPR), therefore the requirements from the recent GDPR regulation need to be implemented. The proper management of data privacy aspects plays a key role to enable the industrialisation of this application. On the security side, DMPS requires the identification of criticalities by employing the Threat Assessment and Remediation Analysis (TARA) methodology and related Attack Trees models. This approach identified and assessed cyber vulnerabilities and selected countermeasures which were effective at mitigating those vulnerabilities.

The TARA methodology enables detailed modelling of the potential security threats to the system's critical elements and identifies appropriate requirements and counter-measures to mitigate the cumulative risk. Further refinement of the causes that can lead to an attack being successful, and highlight vulnerabilities, is performed using an appropriate qualitative analysis technique, such as security attack trees. In safety risk management, harm is considered as physical injury or damage to the health of people, or damage to property or the environment. However, because harm (in a security sense) can also include reduction in effectiveness, or breach of data and systems security, it is appropriate to create a security risk management process (as companion to safety risk management process) to allow the organization to assess the additional risks associated with effectiveness and system/data security. If the processes are integrated, there could be an inclination to drop the evaluation of those risks that do not lead to harm (in the safety sense), which can lead to incomplete or inconsistent security controls.

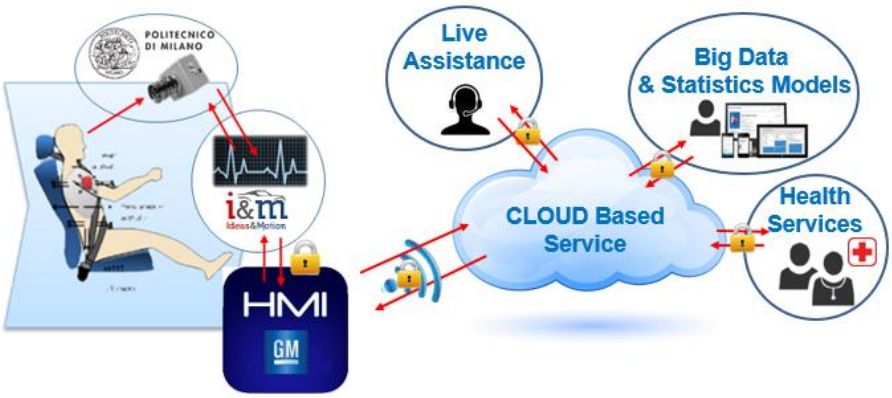

Figure 5- Dependable Physiological Monitoring System

Additionally, security risk assessment models typically use assessment factors that are different from safety risk assessment. Furthermore, integrating safety and security risk assessment into a single general risk management process may result in major modifications to a well-functioning safety risk management process. Security risks that impact safety, should also be captured in the organization's safety risk management process. A specific risk assessed as "must mitigate" in one model might be assessed as "does not need further mitigation" in the other. Risk control measure(s) should be applied to bring the risk into the acceptable range in both assessment models. There will be risks managed in the security risk assessment that are not propagated to the safety risk management process. An example would be a risk of compromise of the confidentiality of protected health information that is not considered harm (in the safety sense), but clearly requires mitigation by the security risk management process. There are also business and reputation risks associated with a security compromise that are not considered harm in the safety sense. A security compromise that leads to harm (in the safety sense) should be managed within the security risk management process and propagated for assessment using the organisation's safety risk management process. An example of a security risk that is also a safety risk is a malicious attacker gaining access to a sensing solution device's code, altering that code, and causing the device to malfunction. This malfunction may have the potential to cause harm to the driver and/or passengers.

With DDI adoption the GDPR requirements are handled by the DDI's security package (TARA) to ensure the privacy and protection of personal data and provide data subjects with certain rights. Any compromise of GDPR requirements that could lead to harm in the safety sense is propagated for assessment in the DDI's HARA. GDPR requires a risk-based approach to data security. Article 35 requires companies to perform data protection impact assessments (the controller shall, prior to processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data) to assess and identify risks to individuals' data. In this case the potential for theft of personal data is considered a security risk and will be dealt with using the **TARA** which assesses the likelihood of a successful attack, in addition to its *impact*.

The application of DDI during design time contributes also to the consolidation of the so called "Privacy by Design" that means select the best solution to fulfill Confidentiality and Integrity requirements on the data treated, but also to be compliant with all steps needed to reach the GDPR compliancy, as showed below. DDI solution adopted by the DPMS features, guarantee the fulfillment of the requirements like Perimeters, Data portability and Data Breach notification requested by the European regulation.

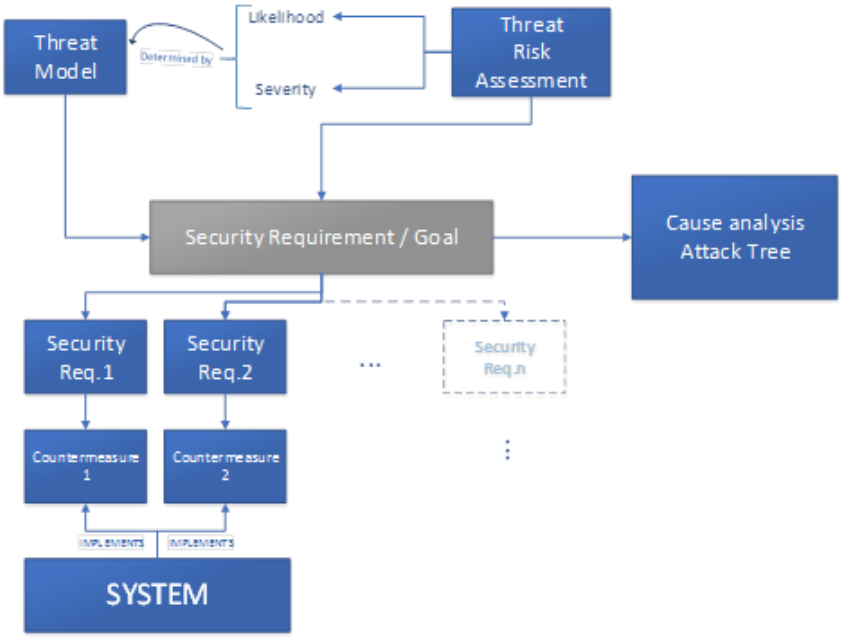

Figure 6- DPMS general security model

5. Introduction of DDI for trusted runtime collaborative platooning in road transportation

The aim of platooning is to automate lateral and longitudinal control of the vehicles which follow the lead vehicle, in order to save significant amounts of energy, by reducing aerodynamic drag force due to decreasing the distance between vehicles. This will have the effect of reducing fuel consumption, CO2 emissions and increasing highway capacity. Also, as the following vehicles can brake immediately, with zero reaction time, it has the potential to improve safety. Platooning technology reduces the stress of stop-and-go driving. It is an advanced form of Cooperative Adaptive Cruise Control.

The use-case is to develop cooperative control algorithms for the platooning of trucks using AVL VSM [8] for the comprehensive evaluation of complex platooning algorithms. The use-case environment contains an extensive package of tools and services that support 'in the vehicle modeling' and enables improvement of various vehicle attributes from the initial concept to the testing phase with highly realistic vehicle simulations. AVL VSM is generally used to predict vehicle behaviour in the field of complicated concept development as platooning algorithms. The use-case environment allows for further simulation such as long platoons, various scenarios like intervening vehicle, vehicles with different load and load type capabilities, handover the control from platooning to ACC and ACC to platooning in the case of a communication loss or in an emergency situation. The environment paves the way for analyzing the differences of precisely predicted results such as fuel consumption between the described scenarios and enables the convenient parametrization within the user-defined constraints. While simulating the highly nonlinear systems like a truck; all the specifications related to aerodynamics, tyres,

drivetrain, road, environment and scenario etc. are required for AVL VSM in order to achieve realistic simulation of the truck. The environment completes the simulation and reports the results using all of the specifications in linearized equations of the truck.

The fundamental work has focused on controlling an “ego truck” which is virtually equipped with V2V communication abilities, as well as environmental sensors. Environmental sensors are used to make the platooning safer while driving, or in the case of a loss of platoon communication, and it is also used for lane level positioning. The loss of communication and switching to ACC mode are simulated during platooning which can cause dangerous situations in real life scenarios.

The problem of platooning introduces new challenges that traditional approaches to the development of dependability-critical systems cannot address effectively. Specifically, the capacity of the platoon to dynamically change its vehicle composition necessitates the negotiation of relevant services between CPS during operation. Such services include creation and dissolution of the platoon, merging into the platoon etc. We refer to this service negotiation as a form of Dynamic Safety Management (DSM) [9]. Systems responsible for service negotiation require runtime information of the observable operational context. This information can be incorporated into the decision-making directly, or can be filtered through sets of dependability analyses. The aim of this process is to arrive at timely decisions regarding the performance or denial of a CPSoS service at a given level of quality.DDIs support the DSM concept by providing structural support for designing solutions and facilitating efficient implementation. Towards this end, we envision that DDIs which are produced during development are used to synthesize DDIs employed at runtime. In Figure 7, suppliers and OEMs exchange CPS models to develop, integrate and assure their systems. DDIs are produced and involved in the ongoing exchange, communicating dependability service and system requirements and analysis results. When the CPS are released into operation, the DDIs produced during development are also embedded within them. The embedded DDIs are used by the constituent CPS to perform DSM and integrate into CPSoS. The lower part of Figure 7 describes how, as the DDIs used during development transition to those embedded and used during runtime, model detail is reduced while model formalism is increased. This trade-off is necessary to maintain performant operational behavior.

To understand the implications of the runtime DDI and the model detail vs formalism trade-off, more detail on one of the DSM-oriented mechanisms supported by DDIs is now provided. Conditional Safety Certificates (ConSerts) [10] are an initial step towards DSM. ConSerts modularize safety interfaces for configurations including variants of safety guarantees with different levels of required confidence. These ConSert models are evaluated at runtime to check whether a set of configurations of multiple systems exists that allows a dependable operation. Runtime DDIs combine ConSerts alongside mechanisms for supervising the collective and observable operational context of the constituent CPS.

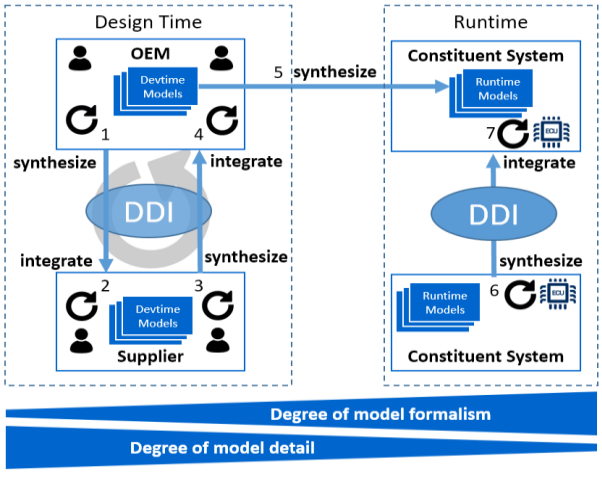

Figure 7 – From design-time to runtime DDI execution

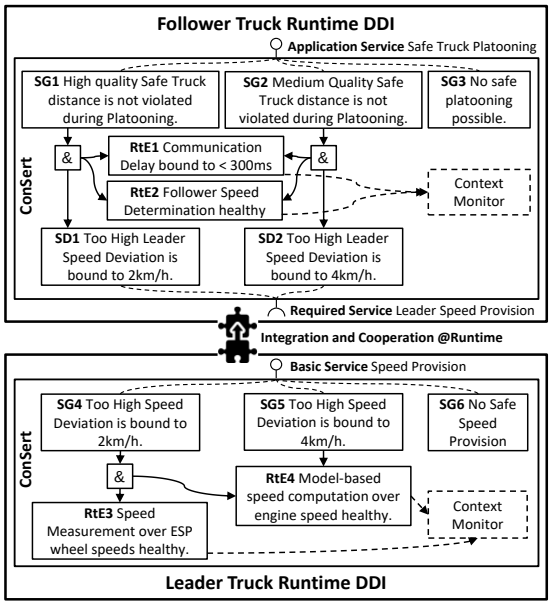

Figure 8 – Platooning runtime DDI

To illuminate further how these runtime DDIs operate, Figure 8 presents exemplary ConSerts for a follower and leader truck in a platoon. In the follower’s ConSert, the service being provided is ‘Safe Truck Platooning’. This

assurance is provided at three levels of safety quality (SG1-SG3), with the last being a lack of assurance in the service. The higher quality SG1 imposes specific requirements on the communication quality (RtE1) and the ability of the follower to correctly ascertain the speed of the leader truck (RtE2). These requirements are expressed as Runtime Evidences (RtE) and linked to a context monitor. The monitor is tasked with collecting observations from sensors and other sources (even other monitors) over a time period. As the context monitors update their observations, they provide relevant updates to their linked ConSerts to maintain an accurate view of the observed context. The final feature of ConSerts depicted in Figure 8 is the composition between the leader and follower ConSert. In order to determine that a safe distance is maintained between vehicles, the following vehicle must ascertain the leader's speed. Given the lower potential deviation from the estimated speed (SD1) can be assured by the leader ConSert, the higher quality safety goal (SG1) for the overall service can be provided (assuming RtE1 and RtE2 are also satisfied).

6. Conclusion

Trusted collaboration is a key issue for all kinds of CPS-supported automated systems. With the H2020 DEIS project and the DDI approach, significant methodology advances have been introduced both to increase efficiency during development time and to enable trusted collaboration during runtime. The DDI core concepts have been presented in this paper, as well as their scalability to address three industrial use cases with different focus. This proposed dependability engineering approach, while applicated here in the transportation related application, is not limited to a specific domain.

Acknowledgement

Dependability Engineering Innovation for automotive CPS. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732242, see www.deis-project.eu

References

[1] Armengaud E. et al. (2018) DEIS: Dependability Engineering Innovation for Industrial CPS. In: Zachäus C., Müller B., Meyer G. (eds) Advanced Microsystems for Automotive Applications 2017. Lecture Notes in Mobility. Springer, Cham, ISBN: 978-3-319-66972-4

[2] DEIS consortium, Specification of the Open Dependability Exchange metamodel and documentation of the fundamental concept of Digital Dependability Identities, Deliverable D3.1, 2018, available at http://www.deis-project.eu/dissemination/

[3] OMG, Structured Assurance Case Metamodel specification V2.1, March 2019, available at https://www.omg.org/spec/SACM/

[4] Höfig, K., Zeller, M., & Heilmann, R. (2015). ALFRED: a methodology to enable component fault trees for layered architectures. 41st Euromicro Conference on Software Engineering and Advanced Applications (pp. 167-176). IEEE.

[5] Hawkins, R., Habli, I., Kolovos, D., Paige, R., & Kelly, T. (2015). Weaving an assurance case from design: a model-based approach. 16th International Symposium on High Assurance Systems Engineering (pp. 110-117). IEEE.

[6] Papadopoulos, Y., & McDermid, J. (1999). Hierarchically Performed Hazard Origin and Propagation Studies. Proceedings of the 18th International Conference on Computer Safety, Reliability and Security (pp. 139-152). LNCS 1608.

[7] Schneider, D. (2018, 03 24). Integrated Safety Engineering with safeTbox. Retrieved from: https://www.iese.fraunhofer.de/en/competencies/safety_engineering/tools_safety/safetbox.html

[8] https://www.avl.com/-/avl-vsm-4-

[9] Trapp, M., Weiss, G. & Schneider, D., 2018. Towards safety-awareness and dynamic safety management. s.l., s.n.

[10] Schneider, D. & Trapp, M., 2013. Conditional Safety Certification of Open Adaptive Systems. ACM Trans. Auton. Adapt. Syst. (ACM Transactions on Autonomous and Adaptive Systems), 8(2), pp. 1-20.

[11] Kabir, S., Sorokos, I., Aslansefat, K., Papadopoulos, Y., Gheraibia, Y., Reich, J., Saimler, M., Wei, R. (2019) A Runtime Safety Analysis Concept for Open Adaptive Systems. In: Papadopoulos Y., Aslansefat K., Katsaros P., Bozzano M. (eds) Model-Based Safety and Assessment. IMBSA 2019. Lecture Notes in Computer Science, vol 11842. Springer, Cham. Available online at: https://doi.org/10.1007/978-3-030-32872-6_22

[12] Reich J., Zeller M., Schneider D. (2019) Automated Evidence Analysis of Safety Arguments Using Digital Dependability Identities. In: Romanovsky A., Troubitsyna E., Bitsch F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2019. Lecture Notes in Computer Science, vol 11698. Springer, Cham. Available online at: https://doi.org/10.1007/978-3-030-26601-1_18