DEIS: Dependability Engineering Innovation for Cyber-Physical Systems

Ran Wei[1], Tim P. Kelly[1], Richard Hawkins[1], and Eric Armengaud[2]

[1] University of York, United Kingdom
ran.wei,tim.kelly,richard.hawkins@york.ac.uk
[2] AVL List GmbH, Austria
eric.armengaud@avl.com

Abstract. The open and cooperative nature of Cyber-Physical Systems (CPS) poses a significant new challenge in assuring dependability. The DEIS project addresses this important and unsolved challenge by developing technologies that enable a science of dependable system integration. Such technologies facilitate the efficient synthesis of components and systems based on their dependability information, covering application domains such as automotive, railways, home automation and healthcare.
The DEIS project will bring significant impact to the CPS market by providing new engineering methods and tools reducing development time and cost of ownership, as well as supporting integration and interoperability of dependability information over the product life-cycle and over the supply chain.

1 Project Information

- **Project acronym**: DEIS
- **Project title**: Dependability Engineering Innovation for Cyber Physical Systems (CPS)
- **Project funding**: Total cost €4,889,290 (funded by H2020-EU.2.1.1)
- **Project partners**: AVL List GmbH (project coordinator), Siemens AG, General Motors Powertrain-Europe SRL, Ideas & Motion SRL, Portable Medical Technology Ltd, Fraunhofer Gesellschaft zur Förderung der angewandten forschung E.V, University of Hull, University of York, Politecnico of Milano, RSRC at Dundalk Institute of Technology.
- **Project start date/duration**: 01 January, 2017 / 36 months.

2 Background

It is expected that in the future, the physical and digital worlds will merge into a largely connected globe. This is backed by the emergence of notions such as Cyber-Physical Systems (CPS). CPS harbour the potential for vast economic and societal impact in domains such as automotive, health care, home automation,

etc. At the same time, if these systems fail, they may cause harm and lead to temporary collapse of important infrastructures, with catastrophic consequences for industry and society. Therefore, in order to realise the full potential for innovation of CPS, it is important to ensure the dependability of CPS.

CPS are typically loosely connected and come together as temporary configurations of smaller systems which dissolve and give place to other configurations. Therefore, the configurations CPS may assume over its lifetime are unknown and potentially infinite. Thus, currently available approaches are not possible to assure the dependability of CPS and it is a grand technology challenge to address the dependability of CPS.

The DEIS project identifies this challenge and takes a first step towards dependability assurance of CPS by focusing on system safety and security, because assuring safety of CPS is an indispensable prerequisite in order to realise their economic and social potential.

The key innovation in the approach of the DEIS project is the concept of Digital Dependability Identity (DDI), which was outlined by key partners of DEIS in [1]. A Digital Dependability Identity (DDI) contains all the information that uniquely describes the dependability characteristics of a CPS or a CPS component. This includes two key aspects: (a) attributes that describe the systems or components dependability behaviour, such as faults and possible fault propagations through the CPS architecture, which can be described using concepts from the theory of safety contracts; and (b) requirements on how the component interacts with other entities in a dependable way, described in terms of the level of trust and assurance. DDI is therefore an evolution of current modular dependability assurance models for systems. It is produced during design, issued when the component is released, and then continuously maintained over the complete lifetime of a component or system. DDIs are used for the integration of components into systems during development as well as for the dynamic integration of systems into *systems of systems* in the field.

Based on the concept of DDI, the DEIS project seeks to provide a modelling and integration framework that lays the foundation for assuring the dependability of CPS.

3 Identified Challenges and Project Concept

A DDI is potentially a very useful digital artefact - It is a versatile dependability assurance case, the utility of which spans from component design to in-the-field operation of a CPS. However, the production and use of DDIs for heterogeneous systems poses a number of significant technological and engineering challenges that are pertinent and important in industry and motivate the objectives of the DEIS project.

DEIS identifies the following challenges for DDI:

1. **Universal exchange of dependability information**
   - Currently there is a lack of common model representations for the exchange of dependability information. Thus, a precondition for DDI is the existence of an open dependability metamodel.
   - DDIs should be sufficiently expressive to enable the component integrator to compile DDIs from the sub-components DDIs, for system synthesis.
   - DDIs should optionally shield sensitive details through abstraction to protect the component provider's intellectual property.
2. **Efficient dependability assurance across industries and value chains**
   - Component providers should be able to generate DDIs based on the dependability information of their components/systems that is already available in their existing tools.
   - It must be possible to include the information contained in DDIs into the dependability assurance lifecycle and tool chain of the component integrator, to cater with the change in component/system requirements and integration context.
   - Dependability should be considered from the early stages of design, so that a model-based approach can be adopted to enable automation, and eventually the automatic synthesis of systems/DDIs.
3. **Dependable integration of systems in the field**
   - In CPS, dependability cannot be fully assured prior to deployment. This requires certain degree of automation in evaluation of DDIs. Thus, DDIs must become executable specifications.
   - DDIs must be stored in a centralised repository so that they can be accessed in a uniform way, and changes in them are synchronised.
   - Fully automated evaluation of DDIs required for highly dynamic environments.

To address these major technology and research challenges, the DEIS project sets out a four-stage innovation cycle, as illustrated in Figure 1. The first stage aims at the fundamentals of DDIs, such as the definition of a universal format of DDIs based on an open information model for the exchange of dependability information. The second stage is to provide semi-automated and increasingly automated support for generating DDIs out of existing design and safety models, as well as for integrating the DDIs of sub-components into DDIs of larger systems by integrators. The third stage facilitates dependable integration of systems in the field though automated evaluation of DDIs that includes the concept of executable DDIs on-board. Finally, the fourth stage is to have continuous validation of the project results in realistic scenarios and case studies.

4 Project Objectives

Based on the identified challenges and the project concept, the objectives of the DEIS project are set out as the following.

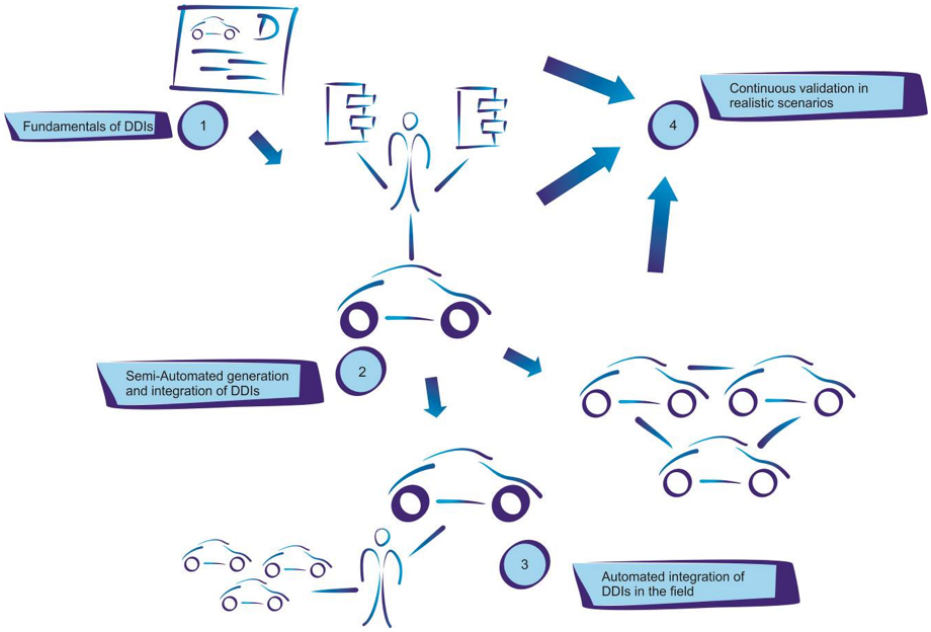

Fig. 1: DEIS project concept

Objective 1. An open dependability exchange (ODE) metamodel and a universal format for specifying DDIs

Based on existing work, DEIS will produce an Open Dependability Exchange (ODE) metamodel. ODE provides the means to express, connect and communicate dependability information. With ODE, it would be possible to specify the level of trust of assured dependability properties with respect to the trust of the issuer and to the trust level of the promised services during field operation. DDIs should also be generated based on the information defined in ODE. DDIs will also be formalised in order to support their semi-automated evaluation.

Measurable sub-objectives of objective 1 are:

1. Definition of the Open Dependability Exchange (ODE) metamodel
2. Definition of general form of Digital Dependability Identity (DDI)
3. Tooling support for the manual modelling of DDIs
4. Tooling support to check the validity of DDIs

Objective 2. A framework for the creation and modular synthesis of DDIs

Once an appropriate format for the ODE and DDIs is defined, DEIS will provide support for the creation and modular synthesis of DDIs from existing dependability information. Such support is a prerequisite for the practical applicability of the approach. Thus a framework that serves such purpose will be developed, covering the following sub-objectives:

1. Tooling support for expressing existing dependability models in ODE-compliant format
2. Algorithms and tooling support for synthesis of DDIs
3. Algorithms and tooling support for integration of DDIs into the dependability assurance cases
4. Algorithms and tooling support for change-impact analysis on DDIs

Objective 3. A framework for the in-the-field dependability assurance in CPS

A framework which enables the dependable integration of open CPS is required. Such framework consists a centralised DDI registry which is publicly available on-the-cloud. By using the centralised DDI registry, system manufacturers can check if their systems can be dependably integrated with already existing systems. Beside the centralised DDI registry, the framework should also enable on-board evaluation. With on-board evaluation, systems carry DDIs with them and evaluate if they can collaborate with each other in the field.

The framework covers the following sub-objectives:

1. Development of infrastructures for evaluation of integration of new systems in the field
2. Development of algorithms for the on-board evaluation of DDIs

Objective 4. Development of autonomous and connected CPS use cases for different application domains, and validation of applicability and scalability of the DDIs

The scope of the project and the technology it develops is wide reaching and fundamental for CPS and the industries involved in the project (road transport, railway, healthcare). As such, the project results are expected to create significant impact. For this reason, it is a further objective of the project to validate the results in four realistic scenarios based on representative projects.

The studies of the four scenarios covers the following sub-objectives:

1. Evaluation of effectiveness of approach
2. Evaluation of applicability across industries
3. Evaluation of runtime mechanisms
4. Evaluation of systems produced in four case studies

5 Related Work

In order to ensure successful project results, the project will not aim at developing an entirely new solution. In fact, the project will use, wherever appropriate, the results from other previous and current projects. In particular, projects that are related to DEIS are:

– VETESS: Verification and Testing to Support Functional Safety Standards

- SPES XT: Software Platform Embedded Systems
- SAFECER: Safety Certification of Software-Intensive Systems with Reusable Components
- CESAR/CRYSTAL: Cost Effective Small AiRcraft/CRitical sYStem engineering AcceLeration
- SAFE: Safe Automotive soFtware architEcture
- EMC^2: Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments
- SafeAdapt: Safe Adaptive Software for Fully Electric Vehicles
- OPENCOSS: Open Platform for EvolutioNary Certification Of Safety-critical Systems
- D-MILS: Distributed MILS for dependable information and communication infrastructures
- MAENAD: Model-based Analysis & Engineering of Novel Architectures for Dependable electric vehicles
- ATESST2: Advancing Traffic Efficiency and Safety through Software Technology phase 2
- COMPASS: Comprehensive Modelling for Advanced Systems of Systems

The research in DEIS can also be based upon different existing approaches, like Component Fault Trees [3] and HiP- HOPS [4] for dependability analysis, GSN [5] for specifying safety cases, SACM [6] for specifying structured assurance cases, or ConSerts [7] as a starting point for runtime certification. All of these approaches were defined by partners involved in DEIS and have proven their value in many practical applications. The fundamental competence and previous work results provided by the partners involved in DEIS therefore build a sound basis, which gives confidence that the project objectives are achievable within the proposed time and budget of the project.

6 Expected Outcomes

CPS market accounted for almost €472 billion in the automotive, industrial, medical, aerospace and defence industries in 2012[3]. By improving the development of dependable CPS and supporting the ad-hoc connection of dependable systems during field operation, DEIS holds the opportunity to bring a significant impact on the existing market and be an enabler for future solutions based on dependable CPS.

For the automotive market, providing means for ensuring dependability of collaboration at runtime will be the enabler to gain market shares in novel market segments. For the railway market, in particular, European rail transport, the harmonisation and supervision of safety certification are essential in a Single European Railway Area and for railway suppliers to deliver cost-efficient

[3] https://ec.europa.eu/digital-single-market/en/news/european-industrial-strategic-roadmap-micro-and-nano-electronic-components-and-systems

and quality products. For the healthcare market, the need for improved science system integration for dependable, autonomous and connected CPS is also imperative.

The expected outcomes based on the objectives mentioned in Section 4 are:

1. Definition of the ODE metamodel and the specification of DDI.
2. A semi-automated framework for the generation and evaluation of DDIs.
3. A framework for the in-the-field dependability assurance in CPS.
4. Autonomous and connected CPS use cases, which is shown in Figure 2.

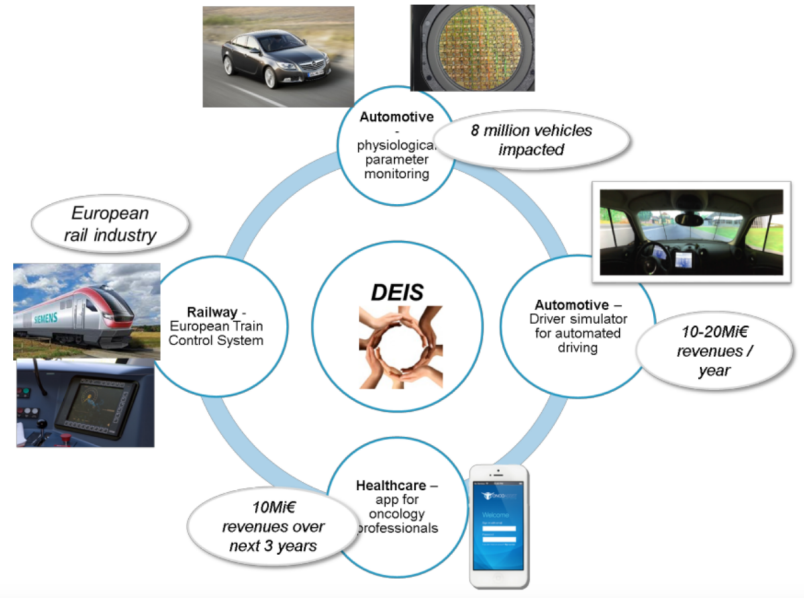

Fig. 2: Expected impact of the use cases on their respective markets.

7 Current Status

DEIS has been running for 3 months. Currently, requirements are being elicited among the partners of DEIS, which include:

- Requirements for the exchange of dependability-related information (ODE), and the specification of modular DDIs;
- Requirements for the tooling support needed to check the validity of the available dependability information and to model DDIs;
- Requirements for applying the DEIS approach within the automotive, healthcare and the railway domain and evaluating the project results compared to the state-of-the-art and the state-of-practice.

Acknowledgements This project has received funding from the European Unions Horizon 2020 research and innovation programme under grant agreement No 732242.

This paper summarises the project description, concepts, and plan from the original DEIS proposal. We acknowledge the original authors of the original DEIS proposal:

- Eric Armengaud, Nadine Knopper, Stephen Jones, Mario Oswald and Gerhard Griessnig (**AVL List GmbH, Austria**)
- Martin Rothfelder, Kai Höfig and Marc Zeller (**Siemens AG, Germany**)
- Alberto Pisoni, Federico Galliano and Massimiliano Melis (**General Motors Powertrain-Europe S.r.l, Italy**)
- Riccardo Groppo, Alberto Manzone, Paolo Santero and Marco Novaro (**Ideas & Motions S.r.l, Italy**)
- Eoin O'Carroll, Kevin Bambury and Richard Bambury (**Portable Medical Technology Ltd, Ireland**)
- Mario Trapp and Daniel Schneider (**Fraunhofer-Institute for Experimental Software Engineering, Germany**)
- Yiannis Papadopoulos (**University of Hull, United Kingdom**)
- Federica Villa, Franco Zappa, Alberto Tosi and Marco Marcon (**Politecnico di Milano, Italy**)
- Fergal McCaffery and Anita Finnegan (**RSRC ad Dundalk Institute of Technology, Ireland**)

References

1. D. Schneider, M. Trapp, Y. Papadopoulos, E. Armengaud, M. Zeller, and K. Hfig. Wap: Digital dependability identities. In *2015 IEEE 26th International Symposium on Software Reliability Engineering (ISSRE)*, pages 324–329, Nov 2015.
2. Phillip J Windley. *Digital Identity: Unmasking identity management architecture (IMA)*. " O'Reilly Media, Inc.", 2005.
3. Bernhard Kaiser, Peter Liggesmeyer, and Oliver Mäckel. A new component concept for fault trees. In *Proceedings of the 8th Australian Workshop on Safety Critical Systems and Software - Volume 33*, SCS '03, pages 37–46, Darlinghurst, Australia, Australia, 2003. Australian Computer Society, Inc.
4. Yiannis Papadopoulos and John A McDermid. Hierarchically performed hazard origin and propagation studies. In *Proceedings of the Computer Safety, Reliability and Security: 18th International Conference, SAFECOMP'99 Toulouse, France, September 27–29, 1999*, pages 139–152. Springer Berlin Heidelberg, 1999.
5. Tim Kelly and Rob Weaver. The goal structuring notation–a safety argument notation. In *Proceedings of the dependable systems and networks 2004 workshop on assurance cases*. Citeseer, 2004.
6. Object Management Group. Structured Assurance Case Metamodel. http://www.omg.org/spec/SACM/. Accessed 27-04-2017.
7. Daniel Schneider and Mario Trapp. Conditional safety certification of open adaptive systems. *ACM Trans. Auton. Adapt. Syst.*, 8(2):8:1–8:20, July 2013.