DDI: A novel technology and innovation model for dependable, collaborative and autonomous systems

Eric Armengaud
Armengaud Innovate GmbH, Austria
eric@armengaud.at

D. Schneider, J. Reich, I. Sorokos
Fraunhofer IESE, Germany
{daniel.schneider, jan.reich, ioannis.sorokos}@iese.fraunhofer.de

Yiannis Papadopoulos
University of Hull, United Kingdom
y.i.papadopoulos@hull.ac.uk

Marc Zeller
Siemens, Germany
marc.zeller@siemens.com

Gilbert Regan
Lero @DKIT, Ireland
gilbert.regan@dkit.ie

Georg Macher
Graz University of Technology, Austria
georg.macher@tugraz.at

Omar Veledar
AVL List GmbH, Austria
omar.veledar@avl.com

Stefan Thalmann
University of Graz, Austria
stefan.thalmann@uni-graz.at

Sohag Kabir
University of Bradford, UK,
s.kabir2@bradford.ac.uk

***Abstract*— Digital transformation fundamentally changes established practices in public and private sector. Hence, it represents an opportunity to improve the value creation processes (e.g., "industry 4.0") and to rethink how to address customers' needs such as "data-driven business models" and "Mobility-as-a-Service". Dependable, collaborative and autonomous systems are playing a central role in this transformation process. Furthermore, the emergence of data-driven approaches combined with autonomous systems will lead to new business models and market dynamics. Innovative approaches to re-organise the value creation ecosystem, to enable distributed engineering of dependable systems and to answer urgent questions such as liability will be required. Consequently, digital transformation requires a comprehensive multi-stakeholder approach which properly balances technology, ecosystem and business innovation. Targets of this paper are (a) to introduce digital transformation and the role of / opportunities provided by autonomous systems, (b) to introduce Digital Depednability Identities (DDI) - a technology for dependability engineering of collaborative, autonomous CPS, and (c) to propose an appropriate agile approach for innovation management based on business model innovation and co-entrepreneurship.**

Keywords—collaborative autonomous systems, business innovation, dependability, co-entrepreneurship

I. INTRODUCTION

The fast-paced global transformation is riding on the wave of digitalization, driven by disruptive innovation and affecting both industry and society. Key technologies and paradigms of this transformation are, amongst others, artificial intelligence (AI), big data, low-power computing, Internet of Things (IoT) and Cyber-Physical systems (CPS). These technologies and paradigms are, in turn, enabled and facilitated by the technological advances we have seen in the relevant base technologies such as advanced semiconductors including mixed-signal, sensor, and power electronics technologies. The transformation affects all industry sectors and will eventually disrupt our society. We are now only touching the surface; there is still a huge potential to be unlocked – and a variety of challenges to be mastered. This opens up major opportunities in different industries, starting from the semiconductor industry and the systems sectors. For example, the embedded systems industry is a significant job-creator, which is contributing to Europe's 34% share of world production of embedded systems with particular strengths in the automotive sector, aerospace and health [1]. AI, digital security and connectivity are particular areas that have also been identified as strategic technologies by China in its Made in China 2025 strategy [2], by South Korea under a USD 1.5 billion initiative [3], and by the US as part of a strategic programme run by the US National Science Foundation [4].

Digitalization and autonomous systems are expected to change our everyday lives and open up new business opportunities for nearly all application domains. For smart transportation (automotive, aeronautics, rail, maritime and logistics sectors), digitalization is expected to support efficient, environmentally friendly, autonomous and safe mobility. Regarding smart production and energy management, digitalization will provide greater efficiency and flexibility in management and operations for process automation, manufacturing, conventional/renewable power plants, energy conversion, smart grids and smart metering. For smart cities and urban areas, digitalization will provide greater benefits to citizens via smart, safe and secure cities, energy efficient buildings and green infrastructure (traffic management, lighting, water and waste management). Regarding smart homes, digitalization will enable the uptake of services and solutions such as home monitoring, health services and assisted living.

In order to actually unlock this potential, a variety of challenges needs to be mastered. Digital transformation requires a comprehensive multi-stakeholder approach properly balancing technology, ecosystem and business innovation, and appropriately addressing dependability aspects. This paper aims to (a) introduce challenges related to digital transformation (Section II), (b) introduce methods for dependability engineering of collaborative, autonomous Cyber-Physical Systems (CPS) (Section III), and (c) propose innovation management approaches based on business model innovation and co-entrepreneurship (Section IV).

II. CHALLENGES FOR DEPENDABLE, COLLABORATIVE, AUTONOMOUS SYSTEMS

A. *The technology and ecosystem challenge*

Digitalization disrupts many industry sectors by bridging the gap between heterogeneous skills and markets. It increases productivity through optimisation over the entire supply chain, and lays the foundations for entirely new services and

applications. Already now, new services emerge through the convergence of applications domains [5]. In general, digitalization and collaborative autonomous systems are relying on a complex technology stack consisting of (a) connected edge devices (i.e. CPS) in charge of interacting with the physical world to locally digitalize relevant information and respond to their environment; (b) the data platforms and analytics, targeting data gathering, organization, processing and communication management; (c) tailored, market-specific applications for value creation for the customer while relying on the lower layers. The associated data management is complemented by dependability (e.g., safety, security, reliability) and trustworthiness, as well as interfaces toward external data markets and digital ecosystems [6].

Consequently, a comprehensive approach is required for digital transformation to properly balance technology, ecosystem and business innovation, and to appropriately address dependability aspects [7], [8]. First, the proper management of a complete digital technology stack and tailoring according to a given application domain will be necessary. Second, the identification of appropriate partners and cooperation models for efficient development and deployment of the proposed technical solution will be required. Finally, business innovation relates to the identification and deployment of new businesses and revenue models to better address real customer needs.

B. *The dependability challenges of collaborative, autonomous systems*

A first challenge is caused by the distribution and the often heterarchical organisation of systems. A heterarchy is a system or organisation where the elements are unranked and non-hierarchical or can be ranked in different ways. Cyber-Physical Systems-of-Systems (CPSoS) are inherently distributed, loosely connected and non-hierarchical. Individual systems within a CPSoS are produced by different stakeholders and there is no overarching specification or authority to guarantee their dependability when they meet in various configurations. None of the systems typically has total control and authority over others. This means that the dependability of the overall system cannot be interpreted as a set of goals that are related to the behaviour of one system and to which other systems contribute. The latter is possible in more conventional systems organised as hierarchies of subsystems. It is possible, for example, to express the safety requirements of a car as a set of integrity requirements that must be achieved by its components as dictated by the safety standard ISO26262. However, it is not possible to use a single reference starting point from which one could express the requirements for safety in the totality of a transport system, which is composed of connected autonomous cars and smart infrastructure. A car comprises of a hierarchy of components, while the connected transport system is a heterarchy of systems where no system has priority or absolute control in terms of safety. This heterarchical organisation poses a major challenge for the state-of-the-art on dependability. The challenge applies both to new standards as well as cutting edge research, e.g. model-based safety analysis, model-checking or other formal methods (e.g. contract-based design). Both, standards and current research mostly assume a hierarchical organisation of the system, decomposition of systems into subsystems, and clear hierarchical authority of control.

A second challenge is caused by the inevitable incompleteness of dependability models anyone would attempt to do a priori at design time for a CPSoS. A traffic system of connected and autonomous cars and smart infrastructures does not have a finite set of configurations. Given the unpredictable nature of CPSoS and the infinity of configurations, any a priori dependability models and most analyses, including critical safety analyses, that try to encompass a CPSoS are likely to be incomplete. Indeed, all state-of-the-art dependability analysis and assurance techniques assume a bounded system; which means that full a priori certification before operation is impossible when the CPSoS is unbounded and its configurations cannot be enumerated. These systems collaborate with other systems in highly dynamic and unpredictable environments, hence, adapting their behaviour in response to changes in the context of operation, workload, physical infrastructure, and network topology.

III. TECHNOLOGY INNOVATION: DEPENDABLE, COLLABORATIVE, AUTONOMOUS SYSTEMS

A. *State of the art*

A fundamental problem of current dependability engineering processes hampering effective assurance lies in the fact that safety argument models are not formally related to the evidence models supporting the claim. Such evidence models include for example hazard and safety analysis models and dependability process execution documentation. The Digital Dependability Identity (DDI) [9], introduced in the DEIS project [10], targets an improvement by explicitly linking evidence (e.g., dependability data models), and claims (dependability arguments). A DDI is, therefore, an evolution of classical modular dependability assurance models, allowing for comprehensive dependability reasoning by formally integrating several separately defined dependability aspect models. DDIs are produced during design, certified on system/component release, and then maintained over the system/component lifetime.

DDIs incorporate sophisticated safety arguments expressed in the Structured Assurance Case Metamodel (SACM) and safety-related evidence models in form of an integrated, tool- and company-independent meta-model, the *Open Dependability Exchange* (ODE) meta-model, which is an extension of the Open Safety Metamodel (OSM) developed in the SPES project [11]. DDIs are flexible and define guarantees supported by a variety of logically connected evidence which may include goal hierarchies, fault trees and Bayesian nets. The DDI guarantees may only be deliverable by a system if certain properties hold in the environment. The AMASS project focusses on organizing safety cases, formalized in the Common Assurance and Certification Metamodel (CACM) [12] to model risk management standard terminology. Integrating CACM in the DDI is ongoing work to extend the latter with further formalization capabilities regarding concepts and terminology from dependability standards as well as evidence management processes. In contrast, there are pure runtime safety monitor approaches such as [13], which dynamically assess risk at runtime and react appropriately. The DDI improves upon these works by seamlessly integrating design-time safety assurance and runtime monitoring.

B. *Dependability engineering with DDI*

Dependability Claim. DDIs are concerned with the comprehensive and transparent assurance of dependability claims. Each assurance activity and each artefact contained in

a DDI is motivated by a root dependability claim defining risk reduction for a dependability property such as safety, security, availability or reliability. The definition of acceptable risk reduction is typically derived from domain-specific 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 ISO/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.

Design-time Dependability Assurance. Having a dependability claim to be assured for the CPS function, risk management activities must then be systematically planned. These activities create necessary evidence for supporting the system engineers' reasoning that the dependability claim holds for the developed system/CPS. For both risk management planning and dependability assessment purposes, an explicit argument inductively relates created evidence to the top-level claim through layers of argumentation. While the performed activities and produced artefacts vary depending on the kind of risk that is being managed, 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, and verification & validation.

Runtime Dependability Assurance. 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. 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 [14]. 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. Clearly, equipping systems with such dependability intelligence is a challenge in its own. We believe, however, that there is no real alternative and the returns by far outweigh the investments. Runtime assurance can be an enabler for new functions, can improve performance by continuous system optimization, can support the reorganization of the ecosystems and can be a key ingredient for realizing dependability DevOps and continuous engineering [8].

There is an important question regarding the location of the intelligent functionality and analytics required by component DDIs within the CPSoS. In general, this will depend on the nature of application and the computational capability of its components. In many applications, fairly simple IoT components which lie on the "Edge" of a network will not have capabilities for storing and executing DDIs which means that data and functionality might have to reside in "Cloud" servers and communication will be needed to complete analytics and intelligent functions. However, this is not ideal in many applications where response time must be strictly observed and where latencies are crucial for correct operation. "Fog" computing is an emerging technology which promises to address some of these challenges by providing intermediaries between cloud and edge components with performance speed and security in mind. The integration of DDIs with "Fog" computing [27] thus needs to be investigated.

Securing the DDI while it is 'in transit' and while it is 'at rest' is critical**.** The DDI can be in transit between components within a system, or between system to cloud server, or between systems. A DDI is ‚at rest' when it is stored statically within a CPS, for instance, in local memory or on a cloud storage. In both cases, assuring confidentiality and integrity is essential. An authentication process, fine grained access control, key management processes, and industry standard cryptographic algorithms are required to assure confidentiality and integrity of the DDI. For security 'in-transit' between two components, the DDI is encrypted using a Advanced Encryption Standard (AES-256) key which can be presigned or generated and shared between two components on the fly using the Elliptic-Curve Diffie–Hellman (ECDH) protocol. Furthermore, to secure the communication between two components, security communication standards and guidelines need to be taken into account, for example NIST 800-121 which is the Guide to Bluetooth Security. Use Message Authentication Code (MAC) to assure that the content of the DDI is not altered or changed while it is 'in transit'. Additionally, policies for firmware upgrade and installation, and policy for port management auditing are required. These policies assist with ensuring the confidentiality and integrity of DDI in transit between system components. For transit between system and cloud server, it is recommended to use the HTTPS (Hyper Text Transfer Protocol Secure) protocol. Additionally, the DDI will be encrypted using the AES-256 cryptographic algorithm. For DDIs in transit between systems, the following considerations need to be taken into account: Are the systems involved in the exchange pre-certified or do they need to be certified on the fly; Choice of the encryption key, which depends on device resources (i.e. computational power, memory etc.) and the KMS cost; Is the communication to be one-to-one between systems, and/or broadcast to all systems in the network.

For 'data at rest' which involves intellectual property concerns, or is significant for the system's functionality, or is personal data, then it may be prudent or even mandatory to encrypt the data. Encryption safeguards the data's confidentiality to malicious attackers, as its contents are inaccessible even when the attacker gains access to it through the system's alternative defenses. Encryption also protects the integrity of the data, as attempts to change the data are both

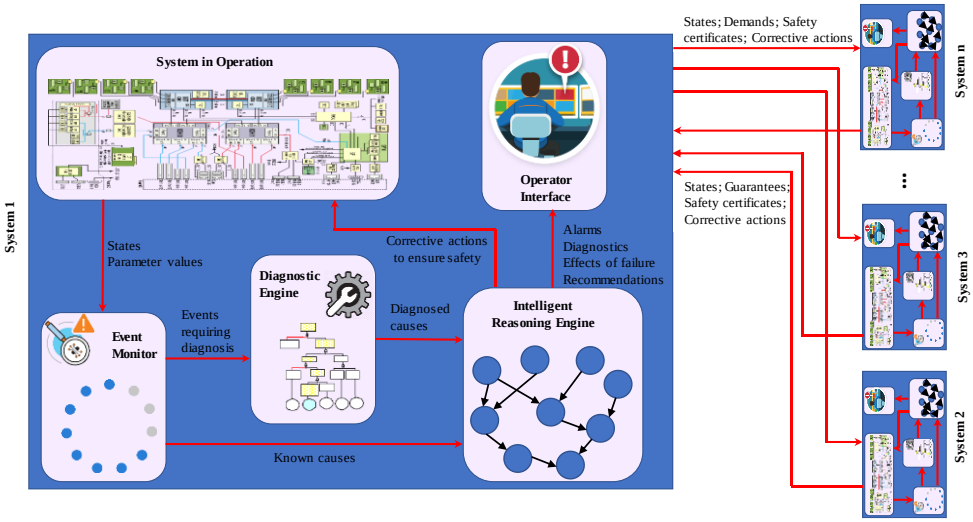

Figure 1: Intelligent Solution Framework for Safety Assurance of Autonomous Systems of Systems

harder to accomplish and easier to detect. A Proper Access control and Role Management needs to be in place so that only authorised application has access to the DDI. Use the AES-256 key to encrypt the DDI before storing into copoment local memory to assure security "in-rest". For cloud storage, the 'Encryption at rest' feature should be enabled. For files stored in Cloud 'Storage Service', the storage should be encrypted at the file level. Additionally, files should not be publicly accessible. Further details on how the DDI is secured can be found in [15].

C. Toward runtime dependability engineering for collaborative and autonomous systems

Figure 1 shows the proposed intelligent solution framework for providing safety assurance for CPSoS. The framework is formed as a distributed multi-agent system to provide safety assurance of autonomous CPSoSs, where each agent will be responsible to observe and enforce the dependability of the individual physical system and the agents will cooperate to assure the safety of the whole system.

An intelligent agent, presented as Intelligent Reasoning Engine (IRE) in Figure 1, interfaces to its respective system, operators and the CPSoS. As seen in the figure, the IRE of a particular system receives inputs from the system itself and also from the other systems that are part of the CPSoS. The inputs received from its own system are based on real-time monitoring of the system. For monitoring, an Event Monitor is utilised, which determines the occurrence of events using real-time sensory data. This data is generated by the component or system, e.g. sensor readings, or maintenance events and can be stored for offline analysis. The modelling of an event monitor may vary depending on the application area. Complex Event Processing (CEP) [16] could, for instance, be used to capture complex data streams, process a large number of events, and automatically correlate the events in the context of predefined constraints. This will help to identify events and their potential causes. If the causes of an event cannot be known with certainty, thus requiring diagnosis, the information will be passed to the Diagnostic Engine. For instance, while monitoring low-level events, a detected condition may reflect the symptom of failures, not underlying causes. Therefore, such symptoms are expected to be diagnosed before making a conclusion about the health of system components. Interested readers can find more information on fault diagnosis in [17].

From the above discussion, we can see that with the help of an Event Monitor and Diagnostic Engine, an IRE can receive information about the state of the system, its parameters and the operational environment. An intelligent agent of one system can receive different information from the agents of other systems. This information may include, but not necessarily be limited to, states, parameter values, dependability guarantees, safety certificates, any recommended actions etc. After processing the information received from both within the system and outside the system, an IRE can make decisions and communicate them as output to both its own system and other collaborating systems. For its own system, such outputs contain corrective measures to force the system to operate safely. Moreover, alarms are raised, and recommendations are provided to the operator interface. The outputs provided to the outside systems may contain its own state information, dependability demands, safety certificates, corrective actions to assure safety, etc.

Following the primary detection and diagnosis of events, dependability-relevant events are handled by a set of model-based high-level IREs. The IREs can exist independently of each other together with their corresponding systems and assist them in dependability related tasks. However, as different systems meet or come together in a configuration, we expect that their respective IREs collectively form a parallel, distributed dependability certification system for the CPSoS as a whole. This distributed certification system is a multi-agent system incorporating several agents which operate locally on their models but also communicate and collaborate between them. Exchange of information about the state of other systems, their perception of the environment, and the reasoning from IREs of other systems help to reduce ambiguity and improve reasoning about dependability at the system level, e.g. to certify operations that involve many systems, assess collective risk or decide on corrective actions.

To provide safety certificates and further dependability management functions (e.g. recommended actions to avoid hazardous situations), the IREs operate on a knowledge graph, which is an ontology that integrates metadata in a machine-interpretable representation. We incorporate appropriate IRE models into the knowledge graph to enable the executing of dependability algorithms at runtime. For this purpose, the DDI is used [18]. The information can be captured in textual format and/or by using one or more safety artefacts such as in the

form of fault trees, Conditional Safety Certificate (ConSerts [14]), Bayesian Networks [19], Markov chains [20], Petri nets, etc. Using these models, the key attributes that define the systems' or components' dependability behaviour are captured, for instance, in the form of faults and potential fault propagation models. Additionally, requirements on how the component/subsystem interacts with other components/subsystems of the CPSoS in a dependable way is captured in terms of the level of trust and assurance. By basing the runtime knowledge graph on DDIs, the knowledge is assured to be correct by design-time dependability processes.

IV. BUSINESS MODEL INNOVATION THROUGH CO-ENTREPRENEURSHIP

A. *Alternative business models for co-innovation*

Aside from creating opportunities to improve and optimize existing businesses, digitalization also supports new forms of business models. In that respect, data-driven technologies are the central diver, paving the path for data-driven business models [21]. The key modification from traditional business models is that data-driven business models exploit data as the key value proposition [22]. As dependable, collaborative and autonomous systems rely on advanced sensor technologies and create huge amounts of data, data-driven business models are strongly appealing. Therefore, one may assume a strong correlation between the scope of the system model (technical) and the resulting scope of the reachable business model, e.g., powertrain, vehicle, mobility user, or energy systems. On one hand, data-driven business models evolve from existing business models by complementing existing products and services with data and analytical insights [23]. On the other hand, data-driven business models can be established from scratch by selling data or information-based offerings as a stand-alone product or service [24]. Aside from providing new opportunities, data-driven business models also pose new risks. In case of data or information as the value proposition, organizations need to carefully reflect the associated risks to avoid the unwanted disclosure of competitive knowledge for example [25].

Famous business disruptors exist in different markets: Amazon becoming one of the largest bookshops without any physical stores, AirBnB becoming the largest provider of accommodations without owning any real estate; Tesla disrupting the automotive market with e-mobility. These examples illustrate the importance of business model innovation – combined with technology innovation – to disrupt the market. The market and ecosystem of current traditional industry domains (e.g., manufacturing, automotive, aerospace to name a few) are organized in a strong hierarchical manner. The original equipment manufacturers (OEM, e.g., car or aeroplane manufacturer) are responsible for their product and the management of their suppliers. This strong hierarchical market organization is a limiting factor for innovation (a) in terms of agility of technology innovation to provide new services not (yet) integrated into the full product, and (b) in terms of market innovation since the alternative business channels are difficult to set-up. The capability to efficiently address innovative business model patterns [26] with dependable, collaborative, autonomous systems represent a huge opportunity. For example, the business model pattern "experience selling" can be addressed with cognitive systems to better reason and react to their environment. Similarly, "guaranteed availability" can be addressed thanks to the higher resilience of autonomous systems and their capability to adapt to new situations.

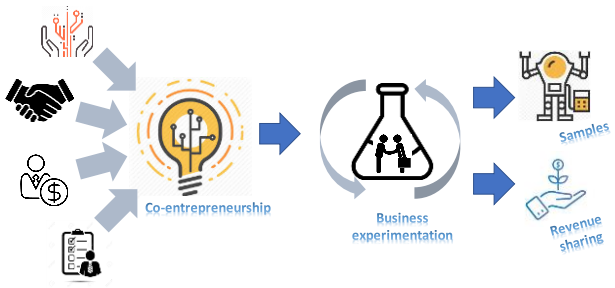

Figure 2: Introducing business experimentation (open

B. *Increasing the agility of innovation management through co-entrepreneurship*

From the previous section, it is evident that technology expertise is necessary, yet not sufficient for innovation (comprising technology, business and ecosystem). Figure 2 introduces the concept of business model experimentation relying on co-entrepreneurship. Core principles rely on (a) make digitalization accessible for all, and especially smaller entities; (b) entrepreneurship empowerment for partner engagement; (c) digital playground as an incubator for technology and business experimentation; and (d) risk and revenue sharing (crowdsourcing) as a relevant alternative for the uptake of customized digital transformation. In this innovation process, the first step is to form a group of innovators. Typically, four roles are required: (a) the technical expert developing and deploying a dedicated technology, (b) the business expert able to interface to the customer and design a business model and value proposition, (c) the investor to manage the start capital required for this innovation, and (d) the manager to manage the initiative from an organizational perspective. The resulting business experimentation can be explored in different ways.

The private person(s) challenge: *"[Dig]iMAGINE a digital solution customized for your private needs"*: a (group of) private person(s) is challenging the innovation community with a specific need. The capability to formalize this need and find other early customers, respectively co-investors and co-entrepreneurs, will be a key factor to trigger such digital transformation with a very limited budget.

The SME challenge: *"[Dig]iMAGINE a group of entrepreneurs supporting on demand your business"*: The SME has a clear view of the business and is requiring support for technology development and deployment. The key aspect will be crowdsourcing to address efficiently this challenge.

The technology provider challenge *"[Dig]iMAGINE a community of entrepreneurs and business experts able to create a business out of your technology brick"*: in this case, a key technology is available and business development is required for market uptake. The key aspect will be the efficient mapping to different markets and application domains.

The large company challenge: *"[Dig]iMAGINE a playground for digital business innovation where a prototype can be matured with customers without impacting your brand or your business logic"*: in this situation, a large enterprise introduces a new business model. The business experimentation (e.g., new customer segments, new ways to address the customers, new revenue models) may not

endanger existing business and brand. The key aspect is the platform to perform business experimentation and the process to re-integrate the matured business in the core entity.

Following the entrepreneurship philosophy (technology provider challenge), the outcomes of the DEIS project have been made publicly available through a dedicated GitHub repository[1]. Through the introduced DDI technology, it is expected that a large number of products can be enhanced following the *cross-selling* (new services through collaborative systems), *experience selling* (cognitive systems better reacting to their environment), *guaranteed availability* (health monitoring and identification of alternative service provision) or *leverage customer data* business model patterns.

V. Conclusion

The successful development, deployment and uptake of dependable, collaborative and autonomous systems will require a disruption in the way to design, cooperate and conduct business. From a technology point of view, a shift from full system toward component-based approach will be required to develop resilient systems able to discover their environment and develop collaborative strategies to optimize their mission. From a dependability point of view, an understanding of components promises and capabilities, as well as the capability to reason on integration will be required. From a business and ecosystem point of view, new approaches to collaborate and to share revenues will be required. Undoubtedly, the range of capabilities unveiled by the technology solutions are likely to act as business enablers for radically new business models. Therefore, agile innovation processes enabling the onboarding of multiple ranges of complementary experts will be required for the full uptake of dependable, collaborative autonomous systems.

Acknowledgement

This paper is supported, in part, by Science Foundation Ireland grant 13/RC/2094, by the Horizon 2020 programme within the OpenInnoTrain project (grant agreement 823971) and will be further enhanced in the H2020 SESAME project (grant agreement 101017258).

References

[1] Thompson, Haydn; Paulen, Radoslav; Reniers, Michel; Sonntag, Christian; Engell, Sebastion; D2.4 Analysis of the State-of-the-Art and Future Challenges in Cyber-physical Systems of Systems; CPSoS - Cyber-physical Systems of Systems; 2016; https://www.cpsos.eu/wp-content/uploads/2015/02/D2-4-State-of-the-art-and-future-challenges-in-cyber-physical-systems-of-2.pdf

[2] ISDP; Made in China 2025; Institute for Security & Development Policy; 2018; https://isdp.eu/content/uploads/2018/06/Made-in-China-Backgrounder.pdf

[3] Dutton, Tim; Barron, Brent; Boskovic, Gaga; Building an AI World – Report on National and Regional AI Strategies; CIFAR; 2018; https://www.cifar.ca/docs/default-source/ai-society/buildinganaiworld_eng.pdf

[4] NSTC; The national artificial intelligence research and development strategic plan: 2019 update; National Science & Technology Council; 2019;https://www.whitehouse.gov/wp-content/uploads/2019/06/National-AI-Research-and-Development-Strategic-Plan-2019-Update-June-2019.pdf

[5] Thalmann, S., Fessl, A., & Pammer-Schindler, V. (2020, January). How Large Manufacturing Firms Understand the Impact of Digitization: A Learning Perspective. In Proceedings of the 53rd Hawaii International Conference on System Sciences.

[6] Eric Armengaud, Bernhard Peischl, Peter Priller, Omar Veledar, Automotive meets ICT – enabling the shift of value creation supported by European R&D, SIA CESA 2018, Versailles, France

[7] Ilvonen, Ilona, et al. "Reconciling digital transformation and knowledge protection: a research agenda." Knowledge Management Research & Practice 16.2 (2018): 235-244.

[8] Schneider, D., & Trapp, M. (2018). B-space: dynamic management and assurance of open systems of systems. Journal of Internet Services and Applications, 9(1), 1-16.

[9] Schneider, D., et al.: WAP: Digital Dependability Identities. In: Proc. Of IEEE Int. Symposium on Software Reliability Engineering (ISSRE). pp. 324–329 (2015)

[10] DEIS Consortium: Dependability Engineering Innovation for Cyber-Physical Systems Project Dissemination: http://www.deis-project.eu/dissemination/ Accessed: 21/05/2019

[11] Pohl, K., Hönninger, H., Achatz, R., Broy, M. (eds.): Model-Based Engineering of Embedded Systems – The SPES 2020 Methodology (2012)

[12] de la Vara, J.L., et al.: Model-based specification of safety compliance needs for critical systems: A holistic generic metamodel. Information and Software Technology 72 (2016)

[13] Trapp, M.; Schneider, D.; Weiss, G.: Towards Safety-Awareness and Dynamic Safety Management.In:14th Europ. Dependable Computing Conf. (EDCC). Iasi, Romania. (2018)

[14] Schneider, D.: Conditional Safety Certification for Open Adaptive Systems. Dissertation. Technical University of Kaiserslautern, Germany. ISBN: 978-3-8396-0690-2. (2014)

[15] Regan, G., McCaffery F., Chandra Paul,P., Sorokos, I.; Reich,J., Armengaud,E.,and Zeller,M. (2020). "Securing a Dependability Improvement Mechanism for Cyber Physical Systems". Software Engineering Research and Practice(in press).

[16] E. Wu, Y. Diao, and S. Rizvi, "High-performance complex event processing over streams," in Proceedings of the ACM SIGMOD International Conference on Management of data. New York, New York, USA: ACM Press, 2006, pp. 407–418.

[17] J. Chen and R. J. Patton, Robust model-based fault diagnosis for dynamic systems, 3rd ed. Springer Science & Business Media, 2012.

[18] Jan Reich, Daniel Schneider, Ioannis Sorokos, Yiannis Papadopoulos, Tim Kelly, Ran Wei, Eric Armengaud, Cem Kaypmaz: Engineering of Runtime Safety Monitors for Cyber-Physical Systems with Digital Dependability Identities. SAFECOMP 2020: 3-17

[19] Lerner, U., Parr, R., Koller, D., Biswas, G., et al.: Bayesian fault detection and diagnosis in dynamic systems. In: Proceedings of the Seventeenth National Conference on Artificial In-telligence (AAAI-00), pages 531-537, Austin, Texas. (2000)

[20] Lee, J. M., Kim, S.J., et. al: Diagnosis of mechanical fault signals using continuous hidden Markov model. Journal of Sound and Vibration, Volume 276, No. 3-5. Elsevier. (2004).

[21] Loebbecke, Claudia, and Arnold Picot. "Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda." The Journal of Strategic Information Systems 24.3 (2015): 149-157.

[22] G. Seiberth, Data-driven business models in connected cars, mobility services and beyond, BVDW research N0 01/18, April 2018, see https://www.bvdw.org/fileadmin/user_upload/20180509_bvdw_accenture_studie_datadrivenbusinessmodels.pdf

[23] Wixom, Barbara H.; Ross, Jeanne W. (2017): How to Monetize Your Data. In: MIT Sloan Management Review, S. 1–4.

[24] Dremel, C., Herterich, M. M., Wulf, J., & Vom Brocke, J. (2018). "Actualizing Big Data Analytics Affordances: A Revelatory Case Study." Information & Management (in press).

[25] Fruhwirth, Michael, Viktoria Pammer-Schindler, and Stefan Thalmann. "To Sell or Not to Sell: Knowledge Risks in Data-Driven Business Models." (2019), Pre-ICIS SIGDSA Symposium, 2019.

[26] Oliver Gassmann, Karolin Frankenberger, Michaela Csik, The Business Model Navigator: 55 Models That Will Revolutionise Your Business, 2014, ISBN: 978-1292065816

[27] Mahmud R., Kotagiri R., Buyya R. (2018) Fog Computing: A Taxonomy, Survey and Future Directions Internet of Everything, Di Martino *et al.* (eds) pp 103-130, Springer

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