DLR Institute of Systems Engineering for Future Mobility – Technical Trustworthiness as a Basis for Highly Automated and Autonomous Systems

André Bolles, andre.bolles@dlr.de; **Willem Hagemann,** willem.hagemann@dlr.de; **Axel Hahn,** axel.hahn@dlr.de; and **Martin Fränzle,** martin.fraenzle@uol.de

■ **ABSTRACT**
The newly established Institute of Systems Engineering for Future Mobility within the German Aerospace Center opened its doors at the beginning of 2022. Emerging from the former OFFIS Division Transportation after a two-year transition phase, the new institute can draw on more than thirty years of experience in the research field of safety-critical systems. With the transition to the DLR, the institute's new research roadmap focuses on technical trustworthiness for highly automated and autonomous systems. Within this field, the institute will develop new concepts, methods, and tools to support the integration and assurance of technical trustworthiness for automated and autonomous systems during their whole lifecycle – from the early development through verification, validation, and operation to updates of the systems in the field.
■ **KEYWORDS:** autonomous systems; technical trustworthiness; verification; validation; artificial intelligence; safety; dependability; autonomics

THE ADVENT OF AUTONOMOUS SYSTEMS

The transition to a sustainable transport system constitutes an important pillar among the measures addressing climate change. Besides the greenhouse gas emissions of the transport sector, we can see additional challenges, like congestion, lots of space reserved for transportation (streets and parking spaces), noise, and safety issues. While the electrification of vehicle drive trains directly addresses greenhouse gas emission reduction, automation of vehicles can contribute to overcome also many of the other challenges.

During the last decade, we have already seen an increasing number of applications using more or less intelligent and self-acting systems. Smartphones, software agents, and artificial intelligence, sometimes in the consumer market having names like Alexa and Siri, assist us in decision-making. They provide us with well-defined advertisements, help recruiters to identify suitable job candidates, and even help qualify loan applications for bank employees. With the progressive use of artificial intelligence and automation technology in safety-critical cyber-physical systems such as autonomous vehicles, new classes of systems are emerging (cf. SafeTRANS 2021). (This also holds for other safety critical areas like health, energy, industry, farming, etc. Due to the fact that the new DLR institute is focusing on transportation, this paper is focused on autonomous driving.) These systems will be deployed into highly dynamic environments, first to understand their impact, then to implement their decisions autonomously using their actuators in the physical world. The advent of autonomously acting cyber-physical systems capable of cooperation in frequently changing contexts and no longer subject to direct human control places novel and high demands on developing methodologies that ensure their trustworthiness.

Since today computing power allows sophisticated artificial intelligence models to recognize complex patterns in the real world and derive suitable actions from such percepts, from a functional perspective, the goal of autonomous driving appears imminently achievable. However, this technology then directly links to the real world. Decisions made by vehicles may directly harm humans and may cause catastrophic failures. Thus, it is imperative to ensure these systems' safety and additional properties, as described in the following sections.

The SafeTRANS roadmap on "safety,

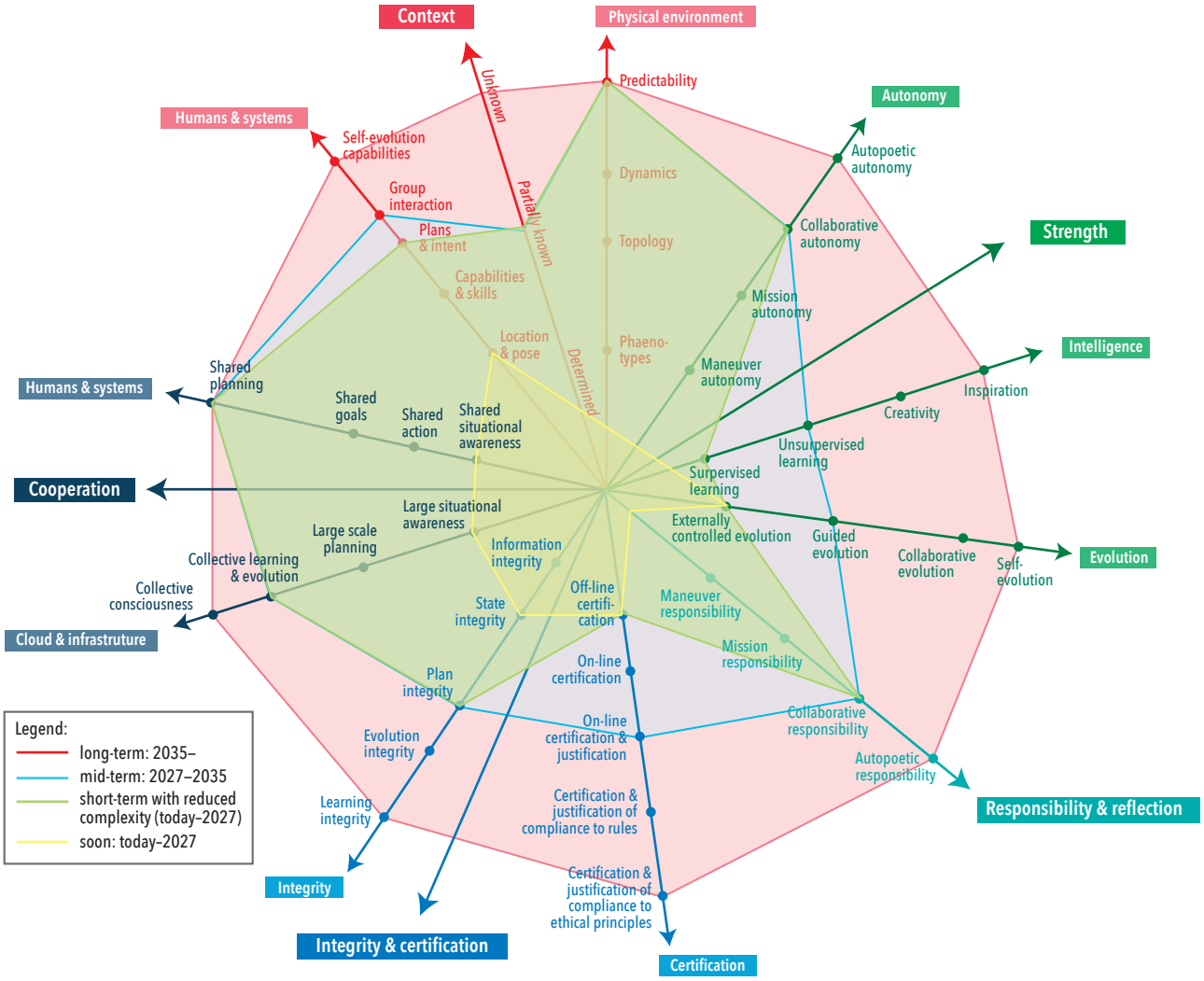

Figure 1. Roadmap for future man-machine systems (SafeTRANS 2021); The authors have translated the legend within that diagram

security, and certifiability of future man-machine systems" (SafeTRANS 2021) dares a look into the future of autonomous systems. It sketches several dimensions of the complexity of these systems, as shown in the following figure taken from the roadmap, and forecasts how autonomous systems will cover these dimensions within the years to come.

Based on this SafeTRANS roadmap, the DLR Institute of Systems Engineering for Future Mobility defined its research roadmap in an internal unpublished concept paper (DLR 2020) explored in further detail below.

From the diagram above, we can see five main axes "cooperation," "context," "strength," "responsibility & reflection," and "integrity & certification." Besides these main axes, additional secondary axes refining the related concepts can be found. As a newly founded DLR institute, we identified for our research roadmap that we can distinguish two types of complexity dimensions from this figure: functional dimensions and extra-functional dimensions. The axes "cooperation," "context," and "strength" reflect functional dimensions, sketching functional capabilities of autonomous systems. On the other hand, "responsibility & reflection" and "integrity & certification" reflect extra-functional dimensions, sketching necessary mechanisms and properties to be fulfilled by autonomous systems to consider them trustworthy. We are conscious that different viewpoints are possible here. However, this distinction helps us to define our roadmap as sketched in the following paragraphs (A slightly modified view on the axes was developed in the internal paper (DLR 2020) but will be omitted here for space reasons.)

SafeTRANS considers the dimension "Cooperation" to describe the future cooperation capabilities of systems, systems-of-systems, a comprehensive group of systems of a specific domain, or even cross-domain groups of systems (SafeTRANS 2021, p 61). Cooperation in this context means cooperation between the systems but also between systems and humans (cf. SafeTRANS 2021, p. 61).

The dimension "context" describes the complexity of the environment, which the systems considered need to be able to handle (see SafeTRANS 2021, p. 43). From the diagram and the description in the roadmap, one can see that the degree of uncertainty increases along the axes shown and that the degree of controllability decreases correspondingly (cf. SafeTRANS 2021, p. 43-ff). Future human-machine systems, assuming a development along the defined axes, will be able to act in more complex environments with much more uncertainty and less controllability of environmental parameters. By this, they will be able to handle many more situations and realize increasingly complex tasks.

The dimension "strength" represents the capability of systems to successfully accomplish application-specific objectives in a self-determined manner (see SafeTRANS p. 27) (As this dimension refers to certain inherent capabilities of a system, we also call it the "System Capabilities" dimension in our institute.). This requires systems to understand and analyze even unfamiliar contexts

DECEMBER 2022
VOLUME 25/ ISSUE 4

(subdimension "intelligence"), adapt to those contexts in order to increase the scope of possible actions (subdimension "evolution"), and finally achieve the desired goal autonomously through a complex sequence of individual or cooperative actions (subdimension "autonomy")(cf. SafeTRANS 2021, p. 27-ff.).

In our understanding, these dimensions sketch a roadmap on how, in which context, and with which complexity, uncertainty, and uncontrollability human-machine systems will be able to achieve goals in the future. However, assuming that all these capabilities will become true, the following and similar questions still need to be raised:

Will these systems then automatically be trustworthy enough, for example, to put our children into an autonomous vehicle and have them be driven by it to their grandparents in the neighboring city without the possibility of intervening? How can we prove such trustworthiness?

The central term to be discussed here is **trust** (The definition of this term and its implications for the research questions of the new DLR institute is ongoing work.) We are convinced that the question above is covered by the other two dimensions of the roadmap, "Integrity & certification" and "Responsibility."

(SafeTRANS 2021) describes "integrity & certification" as a dimension covering mechanisms to ensure consistency and trustworthiness in decision-making and to enable recovery of system integrity after integrity violations (cf. SafeTRANS 2021, p. 85). This is the primary dimension that the DLR institute has focused its research on. All methods, concepts, processes, and tools, including formal verification, model-based systems engineering, contract-based design, virtual certification, monitoring, and diagnosis, can be partially captured under this dimension. However, whatever is needed in the future to ensure system integrity strongly depends on what system capabilities will look like along the dimensions of "cooperation", "context" and "ctrength" (cf. SafeTRANS 2021, p. 85-ff.). Therefore, the DLR Institute of Systems Engineering for Future Mobility is embedded into a network of other institutes (internal and external to DLR) discussing future capabilities of autonomous systems to ensure trustworthiness from the very beginning.

In addition to the dimensions above, the final dimension, "responsibility & reflection," widens the perspective on the extra-functional properties of autonomous systems. The more autonomy and capabilities future human-machine systems acquire, the stronger the need to answer additional questions only marginally explored today. Some of these questions are already sketched in (SafeTRANS 2021, p. 77, translation made with deepl.com and partially edited by the authors):

- "What can machines be responsible for?"
- "What may or can machines decide?"
- "Will machines in a future 'human machine society' be partners of humans or will they even decide over them?"
- "How much autonomy do we want to grant machines?"

These are predominantly ethical and societal questions rather than technical ones. However, answers to these questions strongly depend on the degree of trust we place in machines. Thus, to increase autonomy in an accepted way, we need to increase their trustworthiness. Aside from integrity, there are additional questions that need to be answered to increase trustworthiness with respect to machine autonomy. The concept of responsibility described by SafeTRANS sketches additional challenges to address, which we summarize into the following exemplary questions (SafeTRANS 2021, p. 77-ff. (Additional and similar questions have been defined in the internal institute's concept paper (DLR 2021))

- How can ethical and societal values be implemented into autonomous systems?
- How can compliance with ethical and societal values be ensured during operation and how can this be made transparent?
- How can we enable machines to evaluate consequences of their action in advance?
- How can we enable machines to build trust in other machines and humans?

This list is incomplete, but it demonstrates the future need for broad research initiatives. It seems clear that a deep understanding of ethical and societal values that influence today's social coexistence between humans will have to be implemented into machines in the future to generate technical trustworthiness. Unlike between humans however, trustworthiness of machines will probably not be generated by long-lasting cooperation between humans and machines or by simple test mechanisms like a short driver's license exam. In the case of machines, we expect that each brick for generating trustworthiness needs to be verified and validated. Thus, we assume that in the future, besides classical verification and validation approaches, we also need more and more advanced approaches covering not only technical characteristics but also technical implementations of non-technical concepts.

In (Liggesmeyer 2017), Peter Liggesmeyer, as the director of the "Fraunhofer Institute for Experimental Software Engineering IESE" (https://www.iese.fraunhofer.de/, last visit: July 14, 2022), underlined that technical as well as ethical and legal questions are demanding answers with respect to autonomous systems. Though the term "autonomik" actually is considerably older (for example, compare the research programme on "Autonomics – Autonomous and simulation-based systems for medium-sized companies" that ran from 2008 – 2014 (BMWK 2022)). Also others propose interdisciplinary research in this field (Koopmann and Wagner 2017), it was Liggesmeyer who in (Liggesmeyer 2017) publicly proposed a discipline of "autonomik." The authors agree with (BMWK 2022) to translate this term as "Autonomics" for building reliable and trustworthy autonomous systems in an overarching interdisciplinary way. We picked up this idea during the founding phase of the new DLR Institute of Systems Engineering for Future Mobility. We agree with Liggesmeyer's proposals and think that besides computer science aspects, also perspectives from other technical and non-technical disciplines need to be considered in an integrated way, such as for example mechanics/robotics, social sciences, natural sciences, philosophy, ethics, law, neurosciences, psychology, and biology. Our vision is that for the development and operation of autonomous systems, we will need entirely new systems engineering methods, development approaches, tools, and concepts. We strongly believe that the disciplines referenced above can learn from each other by transferring methods and tools from non-technical sciences to technical sciences and vice versa. This will generate completely new approaches for systems engineering and for the other disciplines. In line with this, the detailed consideration of the complexity facets for future cyber-physical systems development in (Törngren and Sellgren 2018) shows that there is an additional need for education and awareness raising on complexity as well as research into efficient overarching organizational structures and processes. As an illustration, one example could be to integrate social science models for generating trust between humans with formal methods from computer science to support the generation of trust between humans and autonomous systems. We expect that these kinds of synergies will be lifted by strongly integrating the disciplines along the whole life-cycle of an autonomous system, including the development and operational phases. Based on this scope, we place the focus of our new institute on the development of technical methods, tools, processes,

and concepts, that enable and ensure the generation of trust in autonomous systems. By doing this, we are expanding our area of expertise, which in the past mainly focused on safety or dependability, and include the non-technical aspects that will require extended technical support in the future within autonomous systems.

TECHNICAL TRUSTWORTHINESS AS AN ESSENTIAL BASIS FOR AUTONOMOUS SYSTEMS

The division Transportation of OFFIS, as the predecessor of the recently founded DLR institute, had a strong focus on methods and tools guaranteeing safety respectively dependability for human-cyber-physical systems (HCPS – An overview about this term can be found in (Zhiming and Wang 2020)). With respect to this, the term dependability has been understood as defined in Avizienis et al. 2004. With the founding of the new DLR Institute and the definition of its roadmap (DLR 2020), the focus on dependability was broadened as explained in the following.

Since we believe that artificial intelligence will play a significant role in the trustworthiness of autonomous systems, we had a look into research on ethical principles for artificial intelligence. Jobin and her colleagues identified that "there is an emerging convergence around the following principles: transparency, justice and fairness, non-maleficence, responsibility and privacy (Jobin et al. 2019 p. 391)." Although Jobin and her colleagues identify the diversity in interpretations of these terms, within the several works analyzed in their study (Jobin et al. 2019, pp. 391-ff.), we agree that these five principles will become essential considerations for autonomous systems. Within the unpublished internal DLR roadmap paper (DLR 2020), the combination of these five principles, together with dependability, is defined as the comprehensive concept of technical trustworthiness (Assuming that privacy and confidentiality are meaning the same, dependability and privacy are also covering all attributes security is covering in (Avizienis et al. 2004) and by this our definition of technical trustworthiness also covers security.) We believe that this definition and the combination of technical and non-technical issues are compatible with the requirements on trustworthy AI given in the Ethics Guidelines for Trustworthy AI by the Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission (AI HLEG 2019). Notwithstanding this, we will probably refine the definition of technical trustworthiness and related research questions in the future.

In our opinion, it will be essential that at least the aforementioned ethical principles will be considered from the very beginning of the development of autonomous systems to avoid generating mistrust against such systems. We need to start doing so now, and therefore we need to involve technical and non-technical sciences as detailed above.

The first step in this direction will be further to refine the definition and implications of technical trustworthiness (We are especially open for including even more principles to be considered here.). These implications, in addition to their technical nature, may lead to research questions within other disciplines. The new DLR institute, in this context, aims to establish collaborations between researchers from several technical and non-technical disciplines and to intensify existing ones in order to address these questions from the very beginning. This is done, for example, through the Research Center on Human-Cyber-Physical Systems at the University of Oldenburg (https://uol.de/fzhcps, last visit: June 17, 2022).

METHODOLOGICAL CONTRIBUTION FROM THE NEW DLR INSTITUTE

The DLR Institute of Systems Engineering for Future Mobility is aligning its research and development activities along the DevOps approach (Overviews can be found for example in (Ebert et al. 2016 and (Mayank and Singh 2021)). It focuses on the development of methods, tools, processes, and concepts for the assurance of technical trustworthiness for autonomous systems through the whole life-cycle – meaning from the beginning design, development and build phases, through the verification and validation phases and incorporating the operational phases covering deployment, operation, monitoring and updates of the systems in the field. (Decommissioning of autonomous systems will also need to be addressed, although it is not always covered when talking about DevOps.). This is, on the one hand, reflected in the organizational structure as follows:

- "The department Systems Theory and Design (THD) considers all phases of design, development, verification and validation of highly automated and autonomous traffic systems. Methods and tools are developed that enable mechanisms for technical trustworthiness and responsibility, ensure integrity and demonstrate appropriate properties already at the design stage of a system (DLR 2022)."
- "The department System Evolution and Monitoring (EVO) considers all phases during the operation of highly automated and autonomous traffic systems. The focus of this department is on the development of methods and tools that enable a trustworthy evolution of systems and that monitor and ensure compliance with integrity, responsibility and trust measures at system runtime (DLR 2022)."
- "The department Application and Evaluation (ANE) identifies application-specific requirements for integrating and ensuring technical trustworthiness, responsibility, and integrity. At the same time, this department provides platforms to evaluate the methods and tools developed in the THD and EVO departments and integrates them into industry-relevant processes. The ANE department contributes these results to standardization and regulatory activities (DLR 2022)."

On the other hand, this is also reflected in the thematic organization. Within the DLR Institute of Systems Engineering for Future Mobility, thematic clusters — so-called assets — summarize and integrate all activities that are related to specific topics. These thematic assets either have a methodological approach, application-, or technology-driven focus. The methodology-driven assets (Application driven and technology driven assets focus on maritime traffic simulation, testbeds and digital twins.) focus on the topics of:

- scenario-based verification and validation,
- continuous timing assurance,
- human modeling,
- automation risks, and
- online updates and upgrades.

All these assets, sketched below, integrate research done in several projects. This allows building on earlier project results, developing synergies between projects, and professionalizing research prototype development and demonstrations in industrially relevant use cases. Furthermore, complete toolchains can be set up in order to evaluate the research results within seamless processes and to identify gaps that demand further research to become closed. The following paragraphs give a short overview about the thematic orientation of the assets mentioned above.

"*The first asset* [scenario-based verification and validation] *is concerned with developing and prototyping methods and tools that can be used in scenario-based verification and validation approaches for automated transportation systems. Our main focus is formally*

specifying relevant abstract scenarios that are readable by humans while also being machine readable. This allows us to automatize the verification and validation which increases confidence in e.g., safety of the systems due to a dramatically increased number of executed tests while reducing the manual effort from humans (Birte Neurohr, project lead of the asset on scenario-based verification and validation, DLR)."

"*Ensuring timing properties is a crucial aspect in safety-critical systems at both design time and run-time. For example, safe operation of a highly automated vehicle includes the ability to react on appearing obstacles in a specified maximal time span. Asset 2 'continuous timing assurance' provides methods and tools enabling specifying, verifying and monitoring of timing properties along the system lifecycle (from specification, to implementation and test in the development phase, over monitoring, to diagnosis and feedback to the developers in the operations phase). The asset also establishes expertise on the underlying DevOps processes in which these methods and tools are applied, as they (1) are integral parts of many safety standards that must be followed in industry, and (2) should match the requirements and state-of-the-art of industrial practice. The capability of a continuous timing assurance is of crucial importance for all manufacturers and suppliers of future highly automated learning systems, because they are especially challenged by regular software updates and the repetitive real-time proof* (Kim Grüttner, Head of Department System Evolution and Operation, DLR)."

"*Our asset 'human modelling' provides human models that can be used as so-called virtual test drivers or as virtual co-drivers. We research techniques and formalisms to model how humans interact with machines in complex traffic situations. These models are able to recognize and predict human behaviour. As virtual test drivers they are used to test design variants of human-machine interaction for safety critical systems. Such virtual tests can be done very early in the system development process before testing with real humans. As virtual co-drivers they are used to recognize the state of the driver and to predict her/his actions in order to initiate interventions in hazardous situations. We research not only driver models but also models of seafarers and aircraft pilots* (Andreas Lüdtke, Group Leader Human-Centered Engineering, DLR)."

"*The asset 'automation risks' deals with the question how to identify and analyze hazards and triggering scenario properties that arise from the introduction of automated and automatic systems. Therefore, it focuses on the development of methods and tools to find relevant factors influencing the criticality for system classes as well as identify and quantitatively assess newly occurring sources of harm within a specific system* (Lina Putze, project lead of the asset on automation risks, DLR)."

"*The fifth asset [online updates and upgrades] deals with software updates for individual modules of safety-critical systems. Tools are being developed to evaluate the correctness of a new software version in the overall system during development (virtual integration testing). For the safety-critical system, methods are developed to replace individual software modules separately with new versions without endangering the safety of the overall system. For this purpose, methods and tools are developed to secure the update process itself as well as to monitor the system properties after the update. This is of particular importance for suppliers to the automotive industry because it ensures that the increasingly complex automotive software can be continuously tested and further developed* (Domenik Helms, Group Leader Deployment and Updates, DLR)."

Covering the lifecycle of autonomous systems is important for the DLR Institute of Systems Engineering for Future Mobility since we believe that trust between humans and autonomous systems is something that will — similar to that between humans — evolve. Additionally, we think it will not be possible to design, develop and certify a system once without iterations between development and operation — at least due to changing environments.

THE FUTURE DEVELOPMENT OF TRUSTWORTHINESS

Finally, let us look at the future development of technical trustworthiness as foreseen in the institute's research roadmap (DLR 2020). The institute's roadmap is based on the estimated developments in the SafeTRANS roadmap (SafeTRANS 2021), depicted in Figure 1. It mainly addresses scientific goals along the complexity dimensions of "integrity & certification" and "responsibility & reflection". For the time to 2027, this covers mainly the yellow area and with respect to specific aspects like "maneuver responsibility" also the green area depicted Figure 1. The research and development for the time after 2027 will be analogous to (SafeTRANS 2021) covering the green, blue, and light red areas. ■

ACKNOWLEDGMENTS

Acknowledgments go to the whole team involved in defining the research roadmap for the new DLR institute presented in this paper. This team consisted of the management team – namely Kim Grüttner, Eckard Böde, Andreas Lüdtke, Eike Möhlmann, Domenik Helms, Bernd Westphal, Sebastian Feuerstack, Arne Lamm, Günter Ehmen, Michael Siegel, and authors Axel Hahn and André Bolles. Furthermore, we also thank the senior researchers involved of the division Transportation from OFFIS — namely Ingo Stierand, Jan-Patrick Osterloh, and Gregor Nitsche. Additional thanks go to Werner Damm for his strategic and scientific support during the founding phase of the new DLR institute. We are also thankful to the program management transportation of the DLR and the partner institutes for helping us to align the roadmap with existing DLR strategies. Furthermore, special thanks also go to SafeTRANS, namely Jürgen Niehaus, who supported us with his expertise on their roadmap.

REFERENCES

- Avizienis A., J.-C. Laprie, B. Randell, and C. Landwehr. 2004. "Basic Concepts and Taxonomy of Dependable and Secure Computing." In *IEEE Transactions on dependable and secure computing* 1 (1): 11 – 33. doi: 10.1109/TDSC.2004.2.
- Deutsches Zentrum für Luft- und Raumfahrt e. V. 2021 (DLR). "Institute of Systems Engineering for Future Mobility – Description of the new DLR research institute in Oldenburg." unpublished internal paper.
- Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR). 2022. "Institute of Systems Engineering for Future Mobility – Brief description of the three departments." https://www.dlr.de/se/en/desktopdefault.aspx/tabid-15540/, last visit: June 14, 2022.
- Ebert, C., G. Gallardo, J. Hernantes, and N. Serrano. 2016, "DevOps." In *IEEE Software* 33 (3): 94-100. doi: 10.1109/MS.2016.68.

- Federal Ministry for Economic Affairs and Climate Action (BMWK). 2022. "Autonomics - Pioneer for Industry 4.0." https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AbgeschlosseneProgrammeProjekte/Autonomik/autonomik.html, last visit: July 14th, 2022.
- Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission. 2019. "Ethics Guidelines for Trustworthy AI." https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, last visit: October 27th, 2022.
- Jobin, A., M. Ienca, and E. Vayena. 2019. "The global landscape of AI ethics guidelines." In *Nature Machine Intelligence* 1: 389 – 399. doi: 10.1038/s42256-019-0088-2.
- Koopmann, P., M. Wagner. 2017. "Autonomous Vehicle Safety: An Interdisciplinary Challenge." In *IEEE Intelligent Transportation Systems Magazine* 9 (1): 90 – 96. doi: 10.1109/MITS.2016.2583491.
- Liggesmeyer, P. 2017. "Autonome Systeme – Editorial." In *Informatik Spektrum* 40 (5): 399. doi: 10.1007/s00287-017-1046-1.
- Mayank G., R. Singh. 2021. "DevOps: A Historical Review and Future Works." In *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*: 366 – 371. doi: 10.1109/ICCCIS51004.2021.9397235
- SafeTRANS e. V. 2021. "Safety, Security, and Certifiability of Future Man-Machine Systems." https://www.safetrans-de.org/de/Uploads/AK_2018_RLE_CPS/SafeTRANS_RM_SSC_FMMS_Roadmap_V2.pdf?m=1611136486, last visit: May 27, 2022.
- Törngren, M., U. Sellgren. 2018. "Complexity challenges in development of cyber-physical systems." In Marten Lohstroh, Patricia Derler, Marjan Sirjani (ed.), *Principles of modeling: Essays dedicated to Edward A. Lee on the occasion of his 60th birthday*: 478 - 503. doi: 10.1007/978-3-319-95246-8_27.
- Zhiming, L., and J. Wang. 2020. "Human-Cyber-Physical Systems: Concepts, Challenges, and Research Opportunities." In *Frontiers of Information Technology & Electronic Engineering* 21 (11):1535–1553. doi: 10.1631/FITEE.2000537.

ABOUT THE AUTHORS

André Bolles is head of the department "Application and Evaluation" and temporary head of the department "System Theory and Design" within the DLR Institute of Systems Engineering for Future Mobility. His background is in computer science. From 2011 to 2021, he was group manager (2011–2018) and director (2018–2021) within the division "Transportation" of OFFIS, where focused on autonomous shipping and highly automated driving. He was involved in the founding of the new DLR Institute and within this process participated in the definition of the new research roadmap of the institute. Today his research focuses on the technical trustworthiness of autonomous systems.

Willem Hagemann is a researcher at the DLR Institute of Systems Engineering for Future Mobility. His background is in mathematics and computer science. He joined the new institute in early 2022, working in the group Evidence for Trustworthiness. Before that, he was a research associate at the University of Oldenburg. His research interests are explainability for autonomous systems and formal verification of cyber-physical systems.

Axel Hahn is the director of the DLR Institute of Systems Engineering for Future Mobility. Before that, he was a professor at the University of Oldenburg for System Analysis and Optimization and a board member of OFFIS. He coordinated the founding phase of the new DLR institute and was strongly involved in defining its research roadmap.

Martin Fränzle is a professor for Foundations and Applications of Systems of Cyber-Physical Systems at the University of Oldenburg. He was the scientific director within the division Transportation of OFFIS and is continuing this activity within the newly founded DLR institute. In this position, he was involved in developing the research roadmap for this institute.