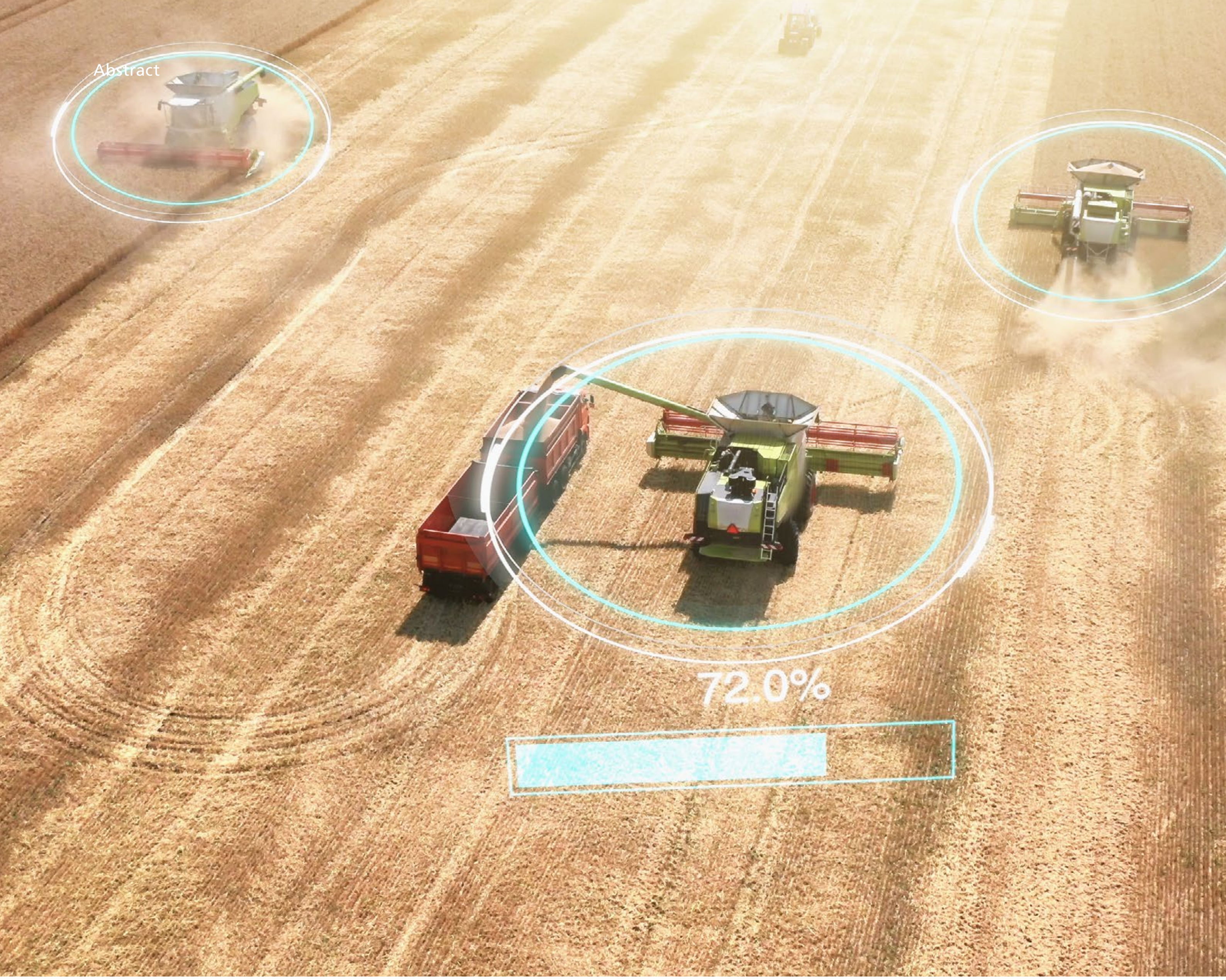
Fraunhofer
IESE

Whitepaper

Pioneering Situation-aware Autonomy and Safety for Off-Highway Machinery in Unpredictable Terrain



Abstract

A limiting factor for the large-scale deployment of autonomous off-road machinery is the lack of reliability and proof of safety. Assuring these aspects is not just complex but hard, and remains an open research topic: Off-road domains are frequently changing, and the overall variability prevents the consideration of every important aspect of the environment or situation during the development phase. In contrast, humans are extremely capable of adapting to unforeseen events and acting safely under such uncertainty. A common strate-gy is therefore to adopt biology-inspired methods, like implementing human-like cognition and reasoning, to maintain safety.

This whitepaper highlights research approaches aimed at addressing the abovementioned challenges, including handling perceptive uncertainty by imitating human cognition.
Also, it depicts how safety and availability can be simultane-ously increased by considering the situa-tional context. Finally, it provides an outlook on future research concerning the limitations of robotic systems, such as acquiring new skills in unforeseen situations and reasoning about the given context.

Introduction

In the past, many technology demonstrators highlighted the capabilities of autonomous off-road machinery [1, 2]. A limiting factor for the large-scale deployment of such systems is the lack of reliability and proof of safety. Off-road environments are more complex and unstructured than on-road scenarios. Thus, unforeseen situations arise frequently and must be handled autonomously and safely. A primary difference between autonomous and traditional systems is that the surroundings and specific situations have become a part of the autonomous system itself, in addition to the system. Accordingly, creating sophisticated automated machinery mainly addresses two fields of research: robotics and safety engineering.

Various challenges must be addressed to achieve reliable and safe machine autonomy.

Challenge 1: Autonomy and reliability

The first is to empower the machinery to solve the overall task, such as navigating to a target destination or working autonomously in a hazardous environment. This includes deploying specialized hardware, sensor systems, software frameworks, and advanced control and perception concepts to realize the system's autonomy.

Challenge 2: Safety

Complementary to robotic research, safety engineering systematically assesses hazards and risks to reduce the impact of failures or mitigate harm to an acceptable level. The goal is to ensure safety during design and runtime. Accordingly, many safety standards, such as ISO 13849: 2021 (Safety of machinery – Safety-related parts of control systems) or IEC 62061: 2023 (Safety of machinery – Functional safety of safety-related control systems), describe precise safety measures.

Challenge 3: Complexity of the domain

A unique property of the off-road domain is its environmental versatility and variability. Specifying an operational design domain (ODD) aims to subdivide the general problem space and define safety boundaries for the system, such as provided by ISO 34503: 2023 (Road Vehicles – Test scenarios for automated driving systems – Specification for operational design domain). For example, an ODD will define precise conditions for an algorithm to work safely [3], such as daytime and illumination thresholds. Unfortunately, off-road complexity makes it hard to specify and describe necessary properties completely [4]. The high number of permutations leads to a vast set of rules even for simple off-road environments, preventing the scaling of such a solution [5]. Therefore, state-of-the-art ODD approaches are not yet considered significantly advanced for off-road scenes.

Challenge 4: Being performant and safe

Traditional safety engineering and safety assurance limit the performance of autonomous systems because they are often over-restrictive [6, 7]. Hazardous situations arise from specific and unforeseen circumstances. Therefore, worst-case assumptions are frequently applied to address such events. However, they rarely occur and restrict overall performance.

This whitepaper provides insight into research addressing these challenges. Initially, a review of sources of uncertainty highlights the shortcomings and challenges of state-of-the-art perception and control systems. Furthermore, adopting human cognition strategies enables machinery to reason about its surroundings and adapt to the unforeseen. Finally, incorporating situational conditions into a vehicle's safety allows tailoring safety to the actual circumstances.

Sources of uncertainty

In general, robot perception must address different kinds of uncertainty that negatively affect performance and, subsequently, decision-making and safety. Autonomous machinery relies strongly on sensors to perceive its surroundings, which is part of a robot's bottom-up processing. Therefore, handling **sensory disturbances** is essential. Different sources of sensory uncertainty exist that have to be addressed. First, the **sensing principle** affects measurement quality. For example, a laser beam scatters over distance, and camera-intrinsic parameters define the appearance of an image [8]. Also, the vehicle itself acts on sensors due to the driving or working task, vibrations, and motions. Moreover, **environmental disturbances** affect measurements, such as illumination, weather, or dust [9]. In addition, **object-based disturbances** exist, including obstructed, dirty, or altered objects.

Context-based uncertainty affects top-down processing. Off-road scenes change properties, such as the ground friction of a rocky surface over the course of a day, which is not easily perceivable but requires domain knowledge and experience.

Additionally, model- or rather **modeling-based uncertainties** exist. This source of uncertainty is related to linking sensory information to context information. For example, tree detection can be realized by detecting cylindric structures in the environment [10]. However, such detectors work only for specific environments and under certain conditions [11]. Especially for Machine Learning systems, this topic covers additional aspects such as training data selection, model setup, and assurance of scope compliance [12, 13].

Fig. 1: Deep furrows change the appearance of a track

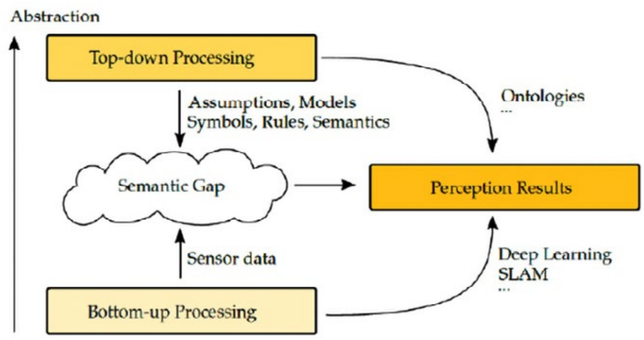


Fig. 2: Sources of uncertainty and the semantic gap of linking knowledge information with sensory data [11]

Thinking like a human

Unlike autonomous robots, human operators are extremely capable of understanding particular situations and adapting to their surroundings. Consequently, adopting biology-inspired methods has great potential to improve autonomous machinery.

Human perception deals with different types of uncertainties throughout different perceptive processing steps.

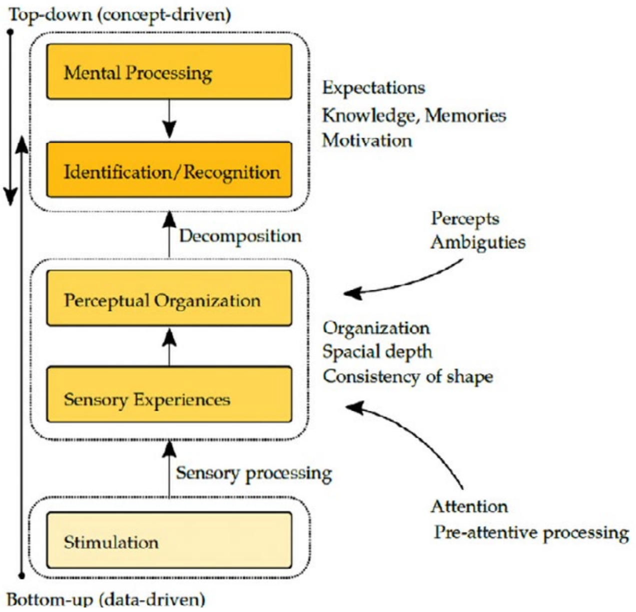


Fig. 3: Stages of human cognition [11, 14]

Applying extra processing steps to perception systems significantly increases perceptive performance and reliability [11].

Pre-attentive processing can be realized through systematic **quality assessment**. This allows bottom-up evaluation and filtering of low-quality data before the actual processing happens. Therefore, it can reduce false detection during later processing since algorithms operate only on data with known and tolerable absolute data quality measures, such as a particular maximum standard deviation of data points. This processing step and the resulting data quality evaluation support fulfilling the widely adopted standard ISO 21448: 2022 (Road vehicles – Safety of the intended functionality (SOTIF)).

Fig. 4: Quality assessment for image exposure evaluation

Attentive processing allows selecting relevant data according to the current task and attractiveness of the surroundings. This is a guided process that is simultaneously bottom-up and top-down. State-of-the-art off-road machinery has many sensor systems that cannot be processed simultaneously, especially with many different classifiers running in parallel. Therefore, a meaningful choice has to be made at an early stage to ensure performance. Furthermore, controlled data reduction can decrease the impact of disturbances and wrong classifications since unrelated information is not considered for processing. **Task-based** attentive data selection uses top-level domain knowledge to guide perception and remove irrelevant information. Examples are focusing on a specific spatial driving or working area, object types, colors, surface roughness, or other properties. **Attraction-based** attentive processing completes the data selection since a purely top-down choice might miss relevant features. It allows focusing on salient environmental features. Examples are sudden movements or rapid color changes. This completes the attentive assessment of an off-road scene beyond the given task.

Fig. 5: Attentive processing highlights a suddenly moving object, which allows prioritization

Another key element of human-like cognition is **context assessment**. In contrast to quality and attentive assessment, context assessment represents pure top-down processing and is the link to world knowledge, memories, and past experiences. Such information is usually available through on- and offline databases or mapping information [15]. The dynamic incorporation of knowledge and subsequent mental processing is crucial for detecting inconsistencies in prediction and classification.

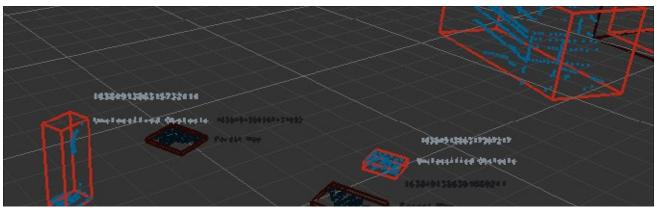


Fig. 6: Semantic reasoning based on map and knowledge data allows for the rejection of implau-sible classification results

Context assessment includes selecting classification algorithms according to the given context, predicting the corresponding classification results, and cross-checking the actual results using object properties, such as consistency of shape, plausibility of detection time, detection location, motion, and detection frequency.

The principle of **expectation and surprise** allows for evaluating overall performance and reliability. A consistent prediction indicates high performance, while a wrong prediction creates surprise. A surprise indicates a low perceptive performance. Thus, previous assumptions about the off-road context no longer apply. For example, the environment may have suddenly changed, or situations such as a particular object type were not considered. Alternatively, there could be missing parts, such as a person who has disappeared.

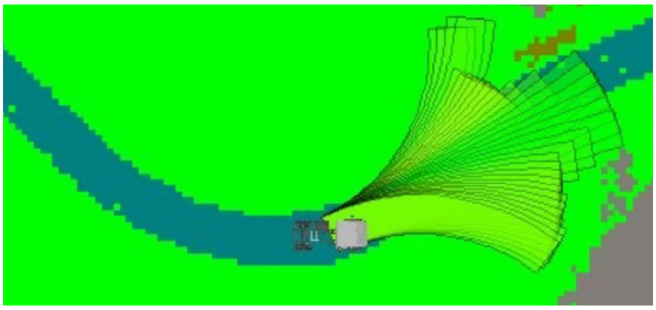


Fig. 7: Off-road track prediction (blue) using histori-cal data [16].

Therefore, perception must be able to adapt and minimize surprises, e.g., by changing the perception strategy. If a surprise is significant and lasting, this indicates that the system is no longer reliable and safe. Accordingly, a minimum-risk maneuver should be applied to switch to a safe state.

Behavior networks

The behavior-based paradigm is well-established for creating safe and adaptive autonomy for off-road robots. Behavior-based systems are highly robust and fault-tolerant due to the fundamental properties of **modularization** and behavior **interaction**. This modeling approach enables software decomposition into highly reusable behavior modules that run in parallel, allow multi-goal-following, and provide redundancy [11].

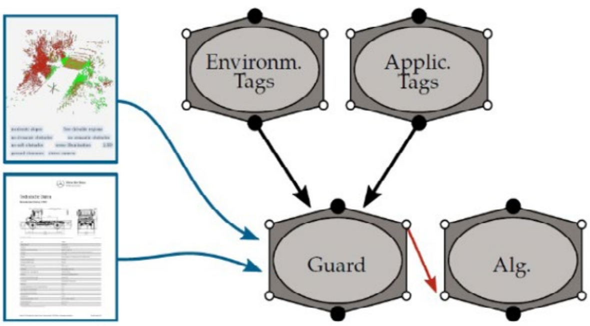


Fig. 8: Example of runtime selection of algorithms based on environmental properties and the application using behavior networks [11].

Unlike traditional sense-plan-act architectures, decision-making occurs in a decentralized manner on a component base. Behaviors interact through standardized interfaces to increase or decrease the relevance of other behaviors within the overall network. Behavior networks separate data flow from arbitration flow. This allows realizing **non-discrete states** and **processing ambiguous, sometimes conflicting goals**, a key benefit for handling off-road domains. At some point, data fusion decides which behavior is most relevant and resolves the ambiguities.

Examples are adaptive data fusion based on the perceived data quality [8] or the selection of algorithms during runtime based on the environmental context [11]. Consequently, behavior networks are exceptional at trading off contradicting goals and properties.

The approach is well suited for realizing complex control and perception systems for off-road machinery. The performance benefits of behavior networks compared to traditional methods have been successfully demonstrated in various use cases, such as forestry, agriculture, search and rescue, construction, and urban off-road areas.

a) Tandem roller performing autonomous asphalt compaction

b) Autonomously driving Unimog in a landfill

Fig. 9: Examples of off-road robots using behavior networks [11]

Situational risk assessment

Safety for autonomous off-road machinery depends strongly on situational circumstances. Sometimes, the scenario requires high availability under uncertainty. For example, robots working in disaster response or dynamic situations like hill climbing cannot be stopped easily but must continue their task to avoid severe consequences.

Consequently, hazards and corresponding safety differ according to the situation at hand. Thus, safety must be decomposed based on situational risks, and **situational safety parameters** must be applied. Therefore, safety parameters must change during runtime. Also, the situational context must be linked to risk assessment and risk management to ensure high performance and safety at the same time.

A **decomposable domain description** is an initial step for off-road safety assessment and **hazard and risk analysis**. The Pegasus layered model [17] provides a promising approach for segmenting domains into different levels. The method was originally developed for on-road vehicles but can be transferred to the off-highway domain. First, L1 handles **spatial features** such as surface geometry and surface conditions. Next, L2 considers **infrastructure**, such as warning panels or gates. L3 addresses **temporal changes** to the surroundings, such as a temporary trench or pathway blocked by a fallen tree. The next level, L4, regards **dynamic objects** in the environment, such as pedestrians, machinery, or animals. L5 features **environmental conditions** like weather, temperature, humidity, and illumination. Finally, L6 handles **digital information** and **communication**, such as map services.

Subdividing the domain in a structured and systematic way minimizes the risk of missing relevant safety features. It allows for comparing the performance and helps understand the autonomous systems by successively adding more difficulty and complexity.

Situational assessment, including risk assessment, is followed by dynamic risk management (DRM). DRM represents **assurable parameter management** for the nominal safety function of autonomous machinery. Therefore, safety-related parameter changes are **proven safe**, and DRM increases **performance while maintaining safety**, which is also called **safetility**.

A convenient DRM method is the SINADRA [18] approach, which uses Bayesian networks to predict the likelihood of risk-relevant situations and adjust the parameters of the nominal function accordingly.

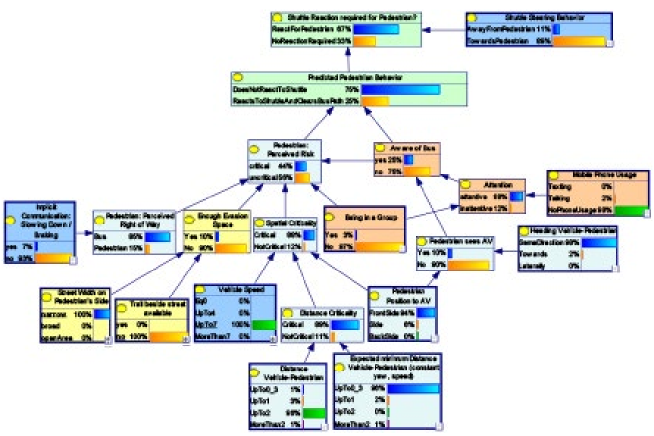


Fig. 10: Example of Bayesian-based risk assess-ment of nearby pedestrians for an autonomous machine.

Role of safety standards

Standardization provides commonly accepted guidelines for developing safe machinery. Usually, standards are not legally binding but allow for referring to state-of-the-art technology and represent a **consensus of the industry** concerning best practices. Therefore, conformity to safety standards supports the argument that products are safe and reliable.

Safety standards also provide crucial support for industry as well as knowledge transfer. Companies often lack **R&D capacity** and R&D development time. Existing budgets are only available to bring products and new features to market without the capabilities to develop research transfer solutions. Therefore, research transfer must be addressed by standardization. Below is an overview of the most relevant safety standards for off-highway machinery.

Various standards concern the **safety of machinery**, such as the general safety standards **IEC 61508**: 2010 (Functional safety of electrical/electronic/programmable electronic safety-related systems), **ISO 12100**: 2018 (Safety of machinery – General principles for design – Risk assessment and risk reduction), ISO/TR 22100: 2021 (Safety of machinery – Relationship with ISO 12100), and the above- mentioned standards **ISO 13849** and **IEC 62061**.

Safety sensors and safety stops are addressed by **IEC 62998**: 2021 (Safety of machinery – Safety-related sensors used for the protection of persons) and **ISO 13850**: 2015 (Safety of machinery – Emergency stop function – Principles for design).

The safety evaluation and testing procedures of **autonomous vehicles** are covered by **UL 4600**: 2023 (Standard for Safety for Evaluation of Autonomous Products) and **ISO 34502**: 2022 (Road vehicles – Test scenarios for automated driving systems – Scenario-based safety evaluation framework), including the standard for ODD design **ISO 34503**.

There is a variety of standards specifying **data quality and uncertainty**, such as **ISO/IEC 23894**: 2023 (Information technology – Artificial intelligence – Guidance on risk management), **ISO TR 5469**: 2024 (Artificial intelligence – Functional safety and AI systems), and the successor standard **ISO 22440**: 2024 (Artificial intelligence – Functional safety and AI systems). Uncertainty quantification is addressed by **DIN SPEC 92005**: 2024 (Artificial Intelligence – Uncertainty quantification in machine learning), **ISO/IEC DIS 5259**: 2023 (Artificial intelligence – Data quality for analytics and machine learning (ML)), and **ISO 25223**: 2021 (Information Technology – Artificial Intelligence – Guidance and requirements for uncertainty quantification in AI systems).

The incorporation of **pre-existing software**, an important performance factor for development, is addressed by **ISO/PAS 8926**:2024 – Functional safety of Road vehicles – Use of pre-existing software architectural elements).

Current research efforts are concerned with **transferring the proposed solutions to standardization**. Initial successes include direct impact on standards such as ISO TR 5469 and DIN SPEC 92005.

Conclusion and takeaways

This whitepaper addressed the challenges and opportunities of autonomous off-road machinery. It highlighted the difficulties and uncertainties of perception, the corresponding safety issues, and the need for standardization. The paper proposed a biology-inspired concept for designing self-adaptive systems that adapt to their surroundings and current context. Situational risk assessment allows for decomposing safety functionality and tailoring safety margins appropriate for such context.

Different takeaways indicate future developments of autonomous systems and provide impulses to rethink off-road autonomy.

Takeaway 1: Think like a human

Human perception is powerful and serves as a blueprint for designing perception and safety systems that can adapt to their surroundings. Today, autonomous systems are often static. Requirements and architectures have been derived during development time and cannot be adapted during runtime. Some techniques, such as Machine Learning, have the general ability to adapt but are opaque, and safety and reliability are not assured. Behavior networks represent a missing link to make systems adaptive and certifiable.

Takeaway 2: It is all about interaction

Simultaneous bottom-up and top-down processing is key to highly performant, reliable, and safe machinery. Sensory information is often ambiguous, and the context defines how the interpretation should be done. Therefore, perception and control systems must change during runtime and adapt to environmental circumstances. This can be achieved through decomposition and interaction.

A critical remark is that algorithms or Machine Learning models are not standalone perception solutions but part of a bigger perception system that requires systematic pre- and post-assessment. The bare-metal deployment of such models is a frequent misconception in state-of-the-art autonomy.

Takeaway 3: Situational context matters

Context defines how to interpret sensory measurements and how to assess risk. Therefore, systematic context incorporation is crucial for autonomous machinery. Connecting symbolic knowledge, such as heavy rain, to sensory measurements is challenging. This challenge has been solved by deploying non-discrete modeling techniques, such as Bayesian and behavior networks, which can handle and resolve conflict information.

Takeaway 4: Don't get surprised

Surprise is an important indicator of system health and context compliance. Therefore, robotic systems should provide expectations that can sometimes result in surprises. An unsurprised autonomous system is working within the predefined specification. However, sometimes it is necessary to go beyond what is known and previously expected.

Future perspective: Managing the unforeseeable

Creating safe off-road machinery for known environments and domains is already extremely challenging. However, sometimes the demands on off-road machinery go far beyond that goal, and autonomy must manage the unforeseeable. The concepts presented above provide the foundation for navigating this field of future research.

One key to discovering the boundaries of the design domain for autonomous systems lies in correctly predicting properties and recognizing whether an expectation is unmet. A robot's cognition system aims to minimize such surprises. However, sometimes a surprise cannot be resolved through parameter adaptation or behavioral network reorganization; instead, it represents an actual unconsidered situation. This threshold can be detected based on situational assessment and can be managed with situational risk management.

Future research aims to enable autonomous operation even under conditions beyond this point and in unknown circumstances. Therefore, the machinery must reason about environmental properties to learn new capabilities ad hoc. Since data interpretation depends on context information, this capability has to be realized through symbolic analysis and semantic processing.

The concepts presented in this whitepaper may have the potential to achieve such capabilities. Accordingly, they are being systematically enhanced to enable such skills and prove whether this hypothesis can hold. For instance, a robot could reason using the motions and actions of other vehicles in its surroundings to learn new strategies. One example could be learning about new pathways not yet considered for traveling. For example, the system could learn to drive over a bush that is theoretically traversable but would be regarded as an obstacle otherwise.

The capabilities of autonomous systems will increase enormously in the future based on experience and the transfer of pre-existing knowledge to new domains. As a result, the safety engineering of these approaches in the off-road domain will experience a shift in mindset since, from a certain point, things will go wrong. One future challenge will be to safeguard against the highest impact risks and tolerate minor, less relevant failures.

References

1. K. Berns, P. Wolf, (2022), Aktuelle Forschung im Bereich des autonomen Fahr- und Arbeitsbetriebs von Nutzfahrzeugen, Jahresmagazin AUTOMATION + ROBOTIK, pp. 2-7
2. K. Berns, P. Wolf, P. Deoli, (2022), Universelle Nutzfahrzeugkonzepte zum autonomen Arbeiten in herausfordernden Umgebungen, CVC News 2, pp. 20-24
3. G. Weiss, M. Zeller, H. Schoenhaar, C. Drabek, A. Kreutz, (2024), Approach for Argumenting Safety on Basis of an Operational Design Domain, Proceedings of the IEEE/ACM 3rd International Conference on AI Engineering - Software Engineering for AI (CAIN ‚24). Association for Computing Machinery, New York, NY, USA, 184–193
4. K. Berns, K.-D. Kuhnert, C. Armbrust, (2011), Off-road Robotics – An Overview, KI - Künstliche Intelligenz: Vol. 25, No. 2. Springer. PISSN: 1610-1987. pp. 109-116
5. P. Wolf; T. Ropertz; P. Feldmann, K. Berns, (2019), Combining Onthologies and Behavior-based Control for Aware Navigation in Challenging Off-road Environments, Proceedings of the 16th International Conference on Informatics in Control, Automation and Robotics - Volume 2: ICINCO
6. Q.H. Jan, P. Wolf, K. Berns, J. Reich, M. Wellstein, (2022). Integration of human skeleton posture models into REACTiON for realizing dynamic risk management. Berns, K., Dressler, K., Kalmar, R., Stephan, N., Teutsch, R., Thul, M. (eds) Commercial Vehicle Technology 2022. ICVTS 2022. Proceedings. Springer Vieweg, Wiesbaden
7. P. Wolf, (2024), Ensuring Safe Autonomy: Navigating the Future of Autonomous Vehicles, S. Bernardi, T. Zoppi (Editors), Fast Abstracts and Student Forum Proceedings - EDCC 2024 - 19th European Dependable Computing Conference, Leuven, Belgium, 8-11 April
8. P. Wolf, K. Berns, (2021), Data-fusion for robust off-road perception considering data quality of uncertain sensors, IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Prague, Czech Republic, 2021, pp. 6876-6883
9. J. Egelhof, P. Wolf and K. Berns, (2022), »Disturbance and Particle Detection in LiDAR Data,« IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society, Brussels, Belgium, pp. 1-6
10. C. Heupel, P. Wolf, K. Berns, (2024), Tree-SLAM: Localization and Mapping in Dense Forest Environments for Autonomous Vehicles, Berns, K., Dressler, K., Kalmar, R., Stephan, N., Teutsch, R., Thul, M. (eds) Commercial Vehicle Technology 2022. ICVTS 2024. Proceedings. Springer Vieweg, Wiesbaden
11. P. Wolf, (2022), Cognitive Processing in Behavior-Based Perception of Autonomous Off-Road Vehicles, Verlag Dr. Hut GmbH, München
12. M. Kläs, L. Sembach, (2019). Uncertainty Wrappers for Data-Driven Models, in Romanovsky, A., Troubitsyna, E., Gashi, I., Schoitsch, E., Bitsch, F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2019. Lecture Notes in Computer Science
13. M. Kläes, R. Adler, I. Sorokos, L. Joeckel, J. Reich, (2021), Handling Uncertainties of Data-Driven Models in Compliance with Safety Constraints for Autonomous Behaviour, 17th European Dependable Computing Conference (EDCC), Munich, Germany, 2021, pp. 95-102
14. P. G. Zimbardo, R. J. Gerrig, (2004), Psychologie, 16th ed., München, Germany: Pearson Studium
15. P. Wolf, A. Vierling, T. Ropertz, K. Berns, (2020), Advanced scene aware navigation for the heavy duty off-road vehicle Unimog, IOP Conference Series: Materials Science and Engineering, Volume 997, The 9th International Conference on Advanced Concepts in Mechanical Engineering - ACME 2020 4-5 June 2020, Iași, Romania. pp. 012093
16. M. Kremer, P. Wolf, D. Meckel, K. Berns, K., (2024), Global Map Generation Using Local Feature Grid Maps for Autonomous Vehicles in Frequently Changing Off-road Environments. In: Lee, SG., An, J., Chong, N.Y., Strand, M., Kim, J.H. (eds) Intelligent Autonomous Systems 18. IAS 2023. Lecture Notes in Networks and Systems, vol 795. Springer, Cham
17. M. Scholtes, L. Westhofen, L. R. Turner, K. Lotto, M. Schuldes, H. Weber, N. Wagener, C. Neurohr, M. H. Bollmann, F. Körtke, J. Hiller, M. Hoss, J. Bock, L. Eckstein (2021), 6-Layer Model for a Structured Description and Categorization of Urban Traffic and Environment, in IEEE Access, vol. 9, pp. 59131-59147
18. J. Reich and M. Trapp, (2020), SINADRA: Towards a Framework for Assurable Situation-Aware Dynamic Risk Assessment of Autonomous Vehicles, 16th European Dependable Computing Conference (EDCC), Munich, Germany, 2020, pp. 47-50

Imprint

Author
Dr. Patrick Wolf | Fraunhofer IESE

Layout
Bettina Wassermann

Image sources
Cover, Back: iStock.com/Scharfsinn86
p. 2: iStock.com/DedMityay
p. 4: iStock.com/Trebor Eckscher

DOI: 10.24406/publica-3516

Publisher
Fraunhofer Institute for
Experimental Software Engineering IESE
Fraunhofer-Platz 1 | 67663 Kaiserslautern
Germany

Contact

Dr. Patrick Wolf
Senior Safety Engineer
Dept. Safety Engineering
Phone: +49 631 6800-2289
patrick.wolf@iese.fraunhofer.de

Fraunhofer IESE
Fraunhofer-Platz 1 | 67663 Kaiserslautern
Germany

www.iese.fraunhofer.de