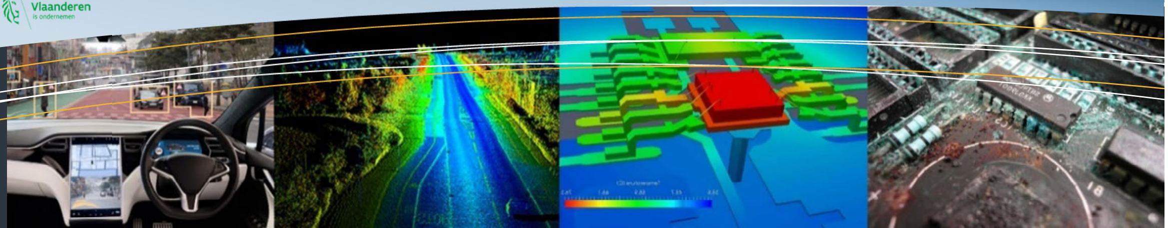
this research was performed with the support of the Eureka PENTA and EURIPIDES programmes

Trustable electronics for safe, reliable automotive aviation and industrial applications



Trustable (sensor-driven) electronics for Automotive, Aviation and Industrial Applications

With the emergence of autonomous vehicles and smart mobility, transport and road travel are undergoing a transformation. New technologies are paving the way towards easier, more efficient journeys and the goal of zero traffic fatalities. As critical tasks are increasingly transferred to vehicles and machines, it is vital to have trust that they will operate safely and reliably at all times. This, in turn, implies that the electronic components and systems in these vehicles and machines must be completely 'trustable' (trustworthy). Safety and reliability are non-negotiable requirements. The TRUST-E project is addressing these needs through the development of methodologies and processes for trustable electronic components, modules, and systems that can be used in automotive and aviation applications, and in industrial settings. It will prove their effectiveness by means of three 'Digital Eye' demonstrators, covering each of the three application areas.

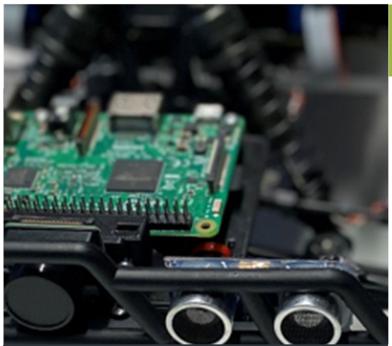
Design of Condition Monitoring for Trustable Electronics in Intelligent Cyber-Physical Systems

Within the project **TRUST-E** (EUREKA PENTA EURIPIDES, 2020006), a novel technology for trustable electronics in advanced products of cyber-physical systems has been developed. This technology, referred to as "Digital Eye", aims to enable a significant enhancement of real-time monitoring and data processing for feedback and self-learning capabilities directly within sensory systems based on low power, high-performance processing chips.

Electronic systems for future vehicles and industrial machines must not only function flawlessly in harsh conditions but also have a long lifetime, which might be up to 30 years in some cases. Yet today, many of the necessary technologies still have critical limitations. Smart sensors, which 'see' their environment, provide signals that still are too fragmented and incompletely fused into information to be directly usable for decision-making and acting in real-time. In addition, usual methods for assessing which existing consumer components could be used in automotive and industrial applications cover only hardware not software. Moreover, there are no certification schemes for electronic systems that simultaneously assess both hardware and software. Consequently, smart approaches to functional safety for safe operation – such as predictive 'health management' for fault detection and AI algorithms tailored to local computing capabilities within vehicles or machines are required.

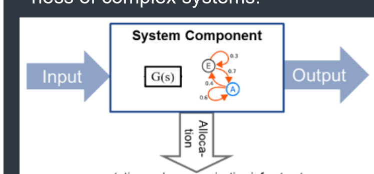
Given these needs, TRUST-E is targeting a significantly increased trustworthiness of complex systems, focusing on advanced sensor systems across the whole chain from single components, via modules, to system integration. It will deliver innovations in hardware reliability, safety, health / lifetime monitoring, and the use of embedded AI techniques for highly demanding applications in sensing and Edge computing for mobility. These applications are, for example, autonomous vehicles and semi-automated wheelchairs, as well as aviation guidance systems, and collaborative industrial machines. The envisaged demonstrators will provide a holistic view of novel capabilities, with a focus on trustworthiness and AI that ensures the dependability of real-time responsiveness, fault tolerance, risk management and Automotive Safety Integrity Level (ASIL) conformity in resource- and energy-constrained embedded distributed systems and applications as mentioned above.

The overall approach is characterized by an integration of PoF (Physics of Failure) and DD (Dependent Failure). While PoF is concerned with the analysis of physical properties that can lead to faults, DD involves the analysis of system-wide consequence of component failures. PoF and DD approaches commonly used in industries for safety analysis, such as FTA(Fault Tree Analysis) and FMEA(Failure Mode and Effects Analysis). The key technological innovation, referred to as "Digital Eye", aims to enable a significant enhancement of real-time CM (Condition Monitoring) with data processing for feedback and self-learning capabilities directly within sensory systems based on low power, high-performance processing chips. The concept is characterized by an integration of the operational feedback and self-learning capabilities across the system hierarchy.



Condition Monitoring for FDIR and PHM

Electronic systems for automotive and industrial machines must not only function flawlessly in harsh conditions but also have a long lifetime, which might be up to 30 years in some cases. The faults of components can arise from design errors, manufacturing defects, component wear and tear, or caused by incompatible inputs, external events, or environmental conditions. These faults can then manifest in different ways depending on the type of system or component and can range from minor issues to catastrophic failures. Detecting and mitigating faults is an important aspect of ensuring the reliability and safety of complex systems, such as aircraft, spacecraft, and industrial equipment. CM constitutes one of the most important measures for FDIR (Fault Detection, Isolation and Recovery) and PHM (Prognostics and Health Management) that are of critical importance for ensuring the trustworthiness of complex systems.



For a component, CM can be applied for monitoring its context inputs and outputs, its internal functional behaviours and performance, the underlying computation and communication infrastructures.

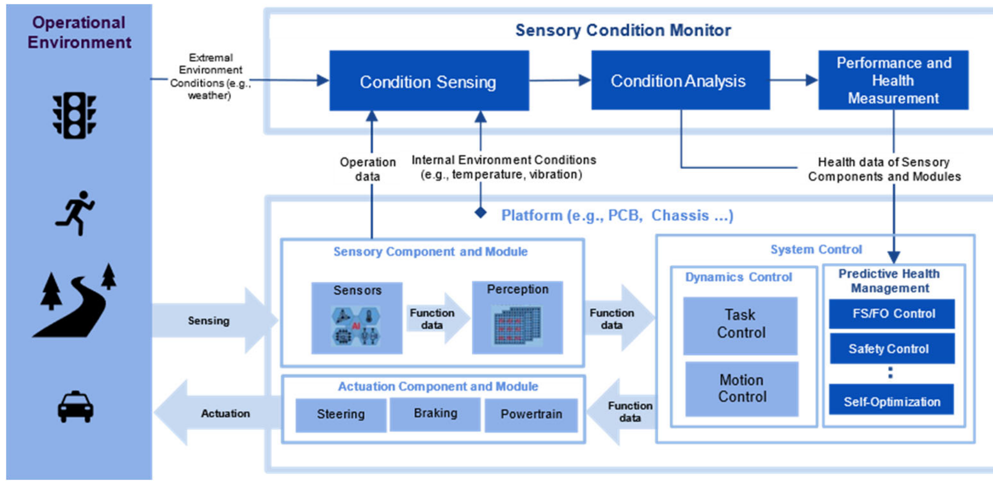


Figure 1. One functional example of deploying condition monitoring for sensory module in an automotive vehicle.

The TRUST-E support for condition monitoring consists of some fundamental services for the situation sensing, condition assessment, RUL (remaining useful lifetime) estimation and health management. These functions can be implemented either as software services or as hardware dies. In the most demanding cases, AI capable dies (ICs or microcontrollers) with built-in AI accelerator would be preferrable. One example of implementing condition monitoring for sensory module in automotive vehicles is shown in **Figure 1**. The system consists of 1). the platform (such as a vehicle chassis), the sensory components and modules (i.e. sensors and perception units), the actuation components and modules, and the dynamics control system; 2). the services for condition monitoring and health management, including sensory condition monitor(s) and a predictive health management unit. The vehicle sensors include lidar, radar and camera that process the gathered signals from the operational environment tother other sensory components for the signal amplification, filtering, noise reduction, etc.

The vehicle perception unit typically fuses the sensory data and conducts feature extraction and world-modelling for the dynamics control. The condition monitoring and health management support is addressed to mitigate the influences of the faults and degradation performance of the sensing and actuation subsystems caused by specific environmental conditions (e.g., weather and road conditions) as well as specific platform conditions (e.g., thermal stress, strain, vibration). The overall objective is also to assess the component lifespan and thereby to enhance the overall system's efficiency. The functional content includes the analyses of operational conditions, performance and health status, and the control decisions regarding dynamic health management including FS/FO control, safety control, etc. In particular, the condition sensing collects the operational data, from the target components and the platform (regarding e.g., temperature and vibration). The condition analysis and performance and health measurement components evaluate the condition sensing output to generate health data, which is then sent to the health controller. The health controller is designed to interact with the vehicle dynamics control system that control the driving behaviors of vehicle. For example, the state and input matrices of the system, along with the operation objectives, are formulated as a function of the degradation performance index. This index is determined using statistical and machine learning algorithms.

The work of TRUST-E addresses the challenges of CM for sensory components or systems posed by complex workload and fault conditions. The main reason for such challenges is due to the existence of a wide range of functional and technical parameters, stochastic operational behaviors and trajectories. For example, when AI-enabled functions are used (e.g., for object detection and tracking), the sensory component could contain many millions of parameters (weights and biases) that are trained for approximating certain function of problem solving. As a result, the number of possible combinations of states is

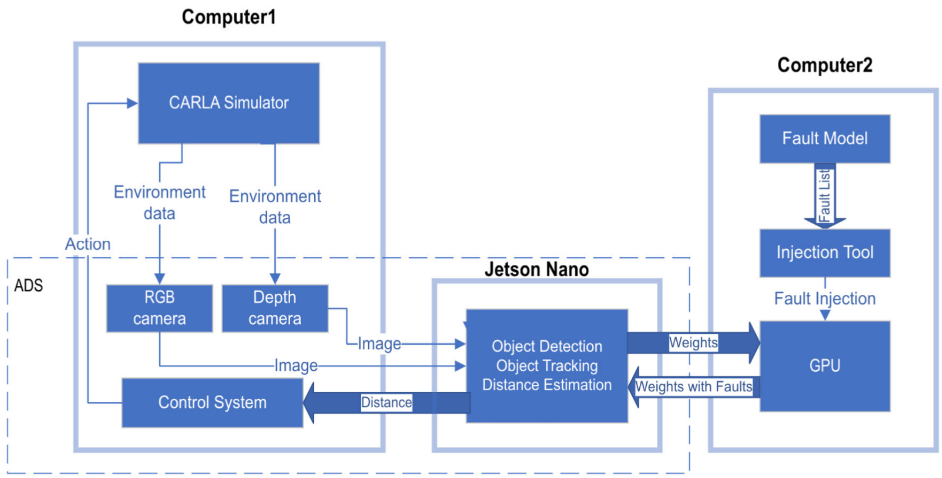


Figure 2. One virtual environment developed to investigate the training of condition monitoring algorithms for ML/AI enabled perception components. The first part(Computer1 and Jetson Nano) is responsible for running the ADS in a hardware-in-the-loop simulated environment. The external operational environment is simulated by CARLA (http://carla.org/). The second part (Computer2) is responsible for fault injection into the perception components.

enormous and functional correctness can only be given probabilistically. Besides, small perturbations in input values may result in huge differences in the output due to the AI models' non-linearity.

The TRUST-E methodology combines model-based system specification and data-driven learning for the design of CM services. The work considers the usages of both symbolic transition-system models (e.g., Markov Process for the calculation for the likelihood of specific events), and statistical analysis (e.g., Hypothesis testing, Bayesian Analysis for determining if a system satisfies certain properties). ML/AI based methods are used to support both model-based and data-driven verification techniques. Different Recurrent Neural Network (RNN) models, such as Long Short-Term Memory Networks (LSTM), are used to approximate complex nonlinear stochastic behaviors. Unsupervised-learning methods are employed for supporting anomaly analysis by means of statistical models (e.g. GMM) according to the underlying structure of data through the use of algorithms like Expectation- Maximization (EM). CM based on ML/AI methods can be particularly useful for system components that are inherently based on ML/AI models where the operational features of labels are expensive to obtain. The design of CM service in a specific system involves the specifications of operational signals and data to be observed and collected, operational conditions to be measured and inferred, and the assessment of conformity regarding the expected conditions.

Exploring Opportunities by Combining Physical Testing, Analysis and Virtual Simulations

Physical testing of the system components, such thermal cycling, provides valuable insights into component fault models and supports the design of advanced test cases by fault-injection testing. It helps identify potential component failure modes, validates the fault models, specifies component Remaining useful life (RUL), and improves the robustness and resilience. By combining physical testing with other virtual analysis and testing techniques, the approach by TRUST-E aims to enhance the understanding of faults and degradations in sensory components and to support the generation of synthetic operational data by virtual simulation for the training of CM services. See **Figure 2** for one example. Within this approach, simulations for specific components, modules, and entire systems constitute the basis for the generation of operational data as physical testing with real hardware and in the real environment is often dangerous, time-consuming, or costly. The combination with physical testing and analysis facilitates the design of test cases targeting the fault scenarios that are of particular concern for the CM design.

Related publications for further reading:

1. Peng Su and Dejiu Chen, "**Using Fault Injection for the Training of Functions to Detect Soft Errors of DNNs in Automotive Vehicles**", New Advances in Dependability of Networks and Systems. DepCoS-RELCOMEX 2022. Lecture Notes in Networks and Systems, vol 484. Springer, Cham. 2022.
2. Kaveh Nazem Tahmasebi and Dejiu Chen, "**A Fault Injection Tool for Identifying Faulty Operations of Control Functions in Automated Driving Systems**", New Advances in Dependability of Networks and Systems. DepCoS-RELCOMEX 2022. Lecture Notes in Networks and Systems, vol 484. Springer, Cham. 2022.
3. Yan Feng Yu, Kaveh Nazem Tahmasebi, Peng Su, and Dejiu Chen, "**Robust Safety Control for Automated Driving Systems with Perception Uncertainties**", ACD 2022 (16th European Workshop on Advanced Control and Diagnosis). Recent Developments in Model-Based and Data-Driven Methods for Advanced Control and Diagnosis, Springer Cham.2023
4. Yizhi Chen, Yarib Nevarez, Zhonghai Lu, and Alberto Garcia-Ortiz, "**Accelerating Non-Negative Matrix Factorization on Embedded FPGA with Hybrid Logarithmic Dot-Product Approximation**", IEEE 15th International Symposium on Embedded Multicore/Many-core Systems-on-Chip, 2022.
5. Omar Mohammed, Parthib Khound, Bart Vandevelde and Frank Gronwald, "**Health Index Modelling for Trustable Electronic Sensor Systems in an Autonomous Application**", Proceeding of Smart Systems Integration Conference, 2023.
6. Peng Su, Tiyanyu Fan and Dejiu Chen, "**Scheduling Resource to Deploy Monitors in Automated Driving Systems**", Proceeding of 18th International Conference on Dependability of Computer Systems, DepCoS-RELCOMEX 2023. 2023.

ROYAL INSTITUTE OF TECHNOLOGY

Contact: Dejiu Chen, Ph.D.
Docent, Associate Professor
Unit of Mechatronics and Embedded Control
KTH Royal Institute of Technology
SE-10044 Stockholm
Sweden
Mail: chendj@kth.se
Tel: +46 8 790 64 28