With funding from the:

Federal Ministry of Research, Technology and Space

ConnRAD – Connectivity and Resilience for Automated Driving

Final Presentation **23.10.2025**

ConnRAD
Connectivity & Resilience for automated Driving Functions in Germany

Fault Injection Framework – Evaluation Method for Resilience

Nijinshan Karunainayagam, Nils Gehrke, Xiyan Su
Institute of Automotive Technology, Technical University of Munich

Fault Injection – An evaluation method for Resilience

To evaluate the trust KPIs on a low level, the systematic injection of faults into the system is used. For this purpose, a fault injection framework is developed on specified requirements, namely real-time capability, independence from the target system, and compatibility with the target system.

To meet the defined requirements, a modular architecture was chosen for the fault injection framework, enabling flexible extension and adaptation. For this, the target system (TUM Teleoperation Software Stack) is conducted to identify information about the particular interfaces and data streams. Resulting, a method is developed, parsing the system's messages and topics and providing an opportunity to manipulate the original data by intersecting the original data stream and replacing it with a new data stream containing the adapted data. This method is evaluated and validated with defined test cases within the target system.

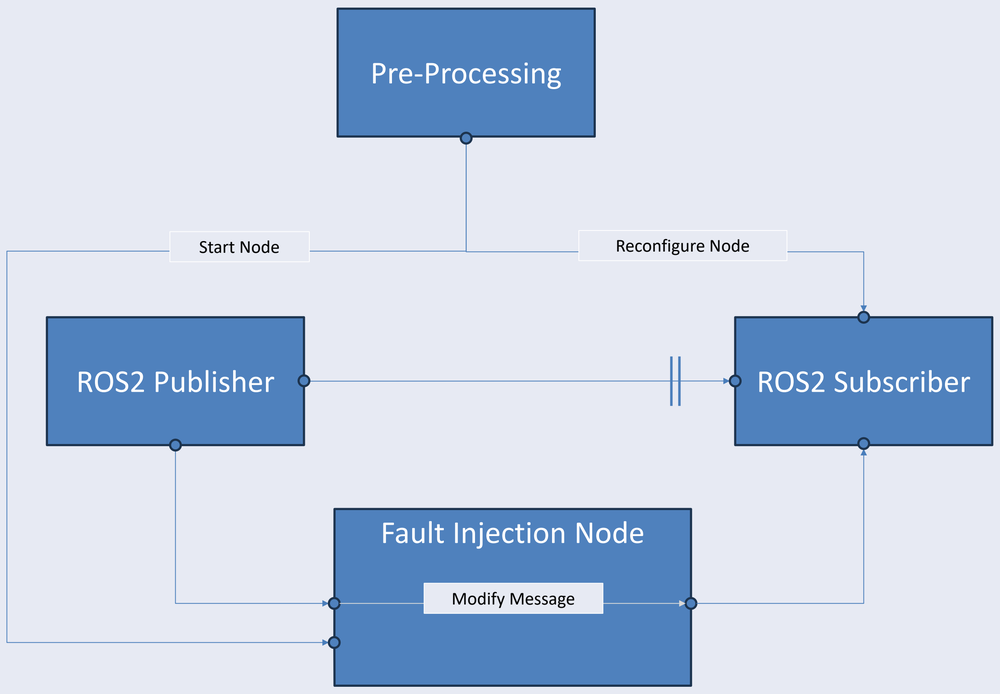
Requirements

Real-Time Capability – The fault injection framework should operate in real-time and ensure data adaptation at runtime. This brings more realism of fault scenarios into the system

Independence to Target System – The fault injection framework should be separated from the target system, e. g. no fault injection class within the target system. This comes with an independent start without adapting the need to adapt the target system beforehand. Further, the target system returns to its original state after stopping the fault injection operation.

Compatibility with Target System – The fault injection framework can handle all data streams of the target system, including custom data types and streams.

Fault Injection Framework - Architecture



The system analysis of the teleoperation software system conducted one main data stream, namely a topic based communication since ROS2 is used as a middleware. Thus, a topic-based fault injection method is developed intercepting and modifying ROS2 messages.

First of all, the fault injection operation temporarily disconnects the subscriber node from its original topic. This subscriber node is then terminated and relaunched with a remapped topic. Another „Fault-Injection Node" listens to the original topic to apply modifications to specific variables of the ROS2-message. With these modification, the message is republished on the new topic, which completes the fault injection operation. A termination of the fault injection system, the original system state is restored by relaunching the subscriber node with the original topic mapping.

Evaluation Fault Injection Framework

To evaluate the developed fault injection approach, different scenarios within the teleoperation software system are defined and examined.

The effectiveness of the fault injection operation is measured based on the following criteria:

- The injected faults appear correctly within the data stream and are observable in the video output of the simulation environment of the teleoperation software system
- The faults persist for the intended duration without premature termination
- The system return to its original state once the fault injection is terminated, with no residual effects remaining

Application on Trust KPIs

Trust KPIs are derived from system fail cases, which represent critical scenarios where system behavior deviates from expected norms. These fail cases are linked to underlying faults that can occur during operation. By systematically injecting faults into the syste, fault models can be simulated to reproduce these fail cases. This enables the evaluation of how sensitive the defined quality metrics are to specific fault conditions. Through this process, the robustness and relevance of trust KPIs can be assessed and fine-tuned, ensuring they accurately reflect the system's ability to maintain reliable and trustworthy performance under adverse conditions