Service ID S00215

Location Poland

Testing of error handling, failure monitoring, and safety related to cyber t

Provider service

Łukasiewicz - Pozna ski Instytut Technologiczny

Link to content

https://agrifoodtef.eu/services/testing-error-handling-failure-monitoring-and-safety-related-cyber-threats

Type of Sector

Arable farming, Food processing, Greenhouse, Horticulture, Livestock farming, Tree Crops, Viticulture

Accepted type of products

Design / Documentation, Physical system, Software or AI model

Type of service

Cybersecurity, Performance evaluation

Description

As part of the service, its provider offers to grant access to the possibility to perform and carry out specialised tests for artificial intelligence systems and robots, aimed at detecting system faults, monitoring failures, and providing reliable assessments of cybersecurity risks present in the operation of IT systems, computer systems, data transmission, etc. These are now necessary measures to ensure the safe, reliable, and secure operation of artificial intelligence systems, autonomous vehicles, and robots. They require continuous testing by their user, the owner, which goes beyond basic functionality. In addition, continuous monitoring of failures through sensor data, system logs, and performance indicators is crucial to identify potential problems before they escalate. These activities are also part of a continuous cybersecurity threat assessment of owned ICT systems, databases, etc.

How can the service help you

The service provides support to the client in the form of granting access to the possibility to perform and carry out specialised tests for artificial intelligence and robotic systems, aimed at detecting system faults, monitoring failures, and providing reliable assessments of cybersecurity threats used in the work of IT systems, computer systems, data transmission, etc. The service is also aimed at customers who do not have access to such data, allowing them to carry out their intentions in the form of, e.g., tests of their computer systems and control systems, allowing them to regain full efficiency after a failure. The service is mainly aimed at customers who do not have the possibility to access this type of data, allowing them to realise their intentions in terms of, e.g., testing their computer systems and control, allowing for full recovery after a breakdown or malfunction. The service provider offers access to continuous monitoring of systems for early detection of symptoms leading to failure.

Data from sensors, system logs, or system performance indicators will be used for this purpose. The collection and factual and ongoing analysis of such data is key to identifying potential problems, providing a real safeguard against escalation. As part of the service, the service provider offers to conduct robust cybersecurity threat assessments, including, among other things, simulated intrusion attempts. These activities, in turn, help to reveal weaknesses in controlled systems, enabling the implementation of strong security measures.

How the service will be delivered

As part of the service, we employ a methodology in line with the guidelines of commonly applicable documents (standards, directives, etc.). Based on this, we will plan and carry out actions necessary to comprehensively test the robustness of a given system.

We require a specification of the customer needs as well as the system under consideration to be delivered. All information is treated confidentially, with the option to sign a Non-Disclosure Agreement (NDA). If the tests need to comply with specific industry standards or regulations, kindly inform us in advance. The timeframe and costs are determined individually based on the scope and complexity of the tests. We ensure flexibility and professional support at every stage of the testing process, including both physical and virtual analyses. Please feel free to contact us to discuss the details and tailor the service to your unique needs.

Service customisation

Our service is based on a structured process allowing us to carry out specialised tests for artificial intelligence and robotic systems, aimed at detecting system faults, monitoring failures, and at reliable assessment of cyber security risks present in the operation of IT systems, computer systems, data transfer, etc.

The time, duration, and other details of the process can be adjusted according to the characteristics of a problem at hand and specific customer needs. The customer needs to provide the system to be tested. The process is flexible and tailored to specific needs, ensuring professionalism and commitment at every stage of our collaboration. As a result, the customer will obtain the detailed report from the analyses as well as relevant guidelines.