Stability under every possible circumstance is a goal for a lot of applications. This problem applies to the network stack ANIS of the real-time operating system PikeOS developed by SYSGO. PikeOS requires security and stability because it is used in areas, e.g., airborne systems, where unstable software could cause severe damage. A proven way to ensure the stability and security of software is testing. Fuzzing is an automated testing technique that generates randomized inputs for the application to find bugs, vulnerabilities, or crashes within the application. Another testing technique is long-run testing, which exposes an application to some input for longer periods.
Because ANIS is a product usually shipped with PikeOS, it must follow the same security standards. We have developed a testing tool for the ANIS network stack, using the two mentioned techniques and emphasizing the option to configure such a test. This testing tool exposes the ANIS to various scenarios that could stress the stack and uses fuzzing to create a combination of these scenarios automatically, which could crash the network stack. The developed test is implemented with a small set of scenarios that expose ANIS to various network traffic. The test can be extended to work with more scenarios. All scenarios have a predefined set of parameters determined by the fuzzer. Changing the parameters of the scenarios diversifies generated network traffic. The scenarios and their parameters are automatically generated every round by the fuzzer. The fuzzer has another set of parameters that give users a way to influence how the data for the test is generated.