Fraunhofer IOSB

ISuTest®

Automated vulnerability detection in accordance with the Cyber Resilience Act and IEC 62443

Fig. 1: Test setup of ISuTest® in the Fraunhofer IOSB laboratory in Karlsruhe. Source: Fraunhofer IOSB

Motivation

Industrial components are often used behind the scenes: modern traffic light control systems at junctions, trains, power stations and hospitals cannot function without them. They also control and monitor entire factory halls, read sensor data and process it, sometimes with real-time requirements.

But what do all industrial components have in common? A network connection, a "digital element" according to the Cyber Resilience Act (CRA) of the European Union (EU). Through this connection, they are accessible via the network – and therefore in principle also vulnerable to attack. What happens in the event of an attack? Sometimes railway display boards fail, sometimes hospitals shut down, or a workpiece in production does not meet the required quality.

Against this background, the EU has issued the CRA, which obliges manufacturers of components with digital elements to develop and test them safely. Otherwise, they may no longer be placed on the market within the EU from December 2027. The IEC 62443 standard for the protection of industrial communication networks describes such a secure development life cycle for manufacturers of industrial components. Automated vulnerability scanning via the network interface is an essential part of this. This means that all protocols that could impair the robustness of the components must be extensively tested for vulnerabilities.

ISuTest®
Industrial Security Testing

» ISuTest® as building block for certification.

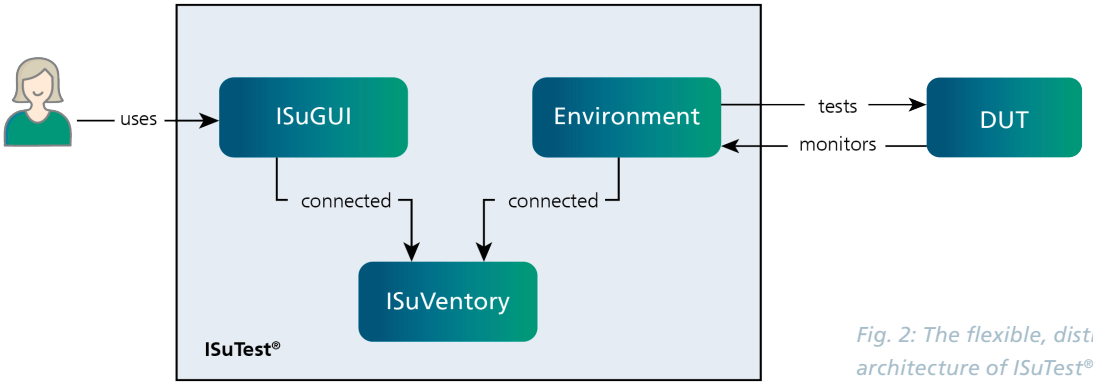

Fig. 2: The flexible, distributed architecture of ISuTest®.

Testing like an attacker

The Industrial Security Testing Framework ISuTest® is a tool for finding vulnerabilities in the implementations of automation components. It has been developed at Fraunhofer IOSB in Karlsruhe in the Industrial Cybersecurity group since 2016. ISuTest® is designed as an open, extensible framework. It supports manufacturers in setting up and performing a test as well as in isolating vulnerabilities in order to reproduce the error with the developer. An exemplary test setup of ISuTest® as used in the Fraunhofer IOSB laboratory is shown in Figure 1.

The vulnerability test by ISuTest® is carried out using fuzzing techniques. Network packets are slightly modified and sent to the component in the same way as an attacker would. ISuTest® does not require any insight into the internal workings of the device; the specification of the communication protocols is sufficient. This means that any device with a network interface can be tested; it is a so-called black box test. In addition, further protocols can easily be added to ISuTest® to fulfil the IEC 62443 requirement for testing all offered protocols.

The architecture of ISuTest® is shown in Fig. 2. It is a distributed client-server infrastructure. The actual test is carried out by the Environment. Using the ISuGUI graphical user interface, the user configures components to be tested, starts tests and conveniently evaluates completed tests. The ISuVentory is the central database, file repository and communicator. At the smallest configuration level, all components are installed on a local PC. At the largest expansion stage, many users work with ISuGUIs via VPN with an ISuVentory in a Kubernetes cluster and several Environments.

Monitoring like in the functional tests

ISuTest® uses monitoring to recognize whether a component is still working as intended during and after a test. Classic IT monitoring is used, for example, to test whether the device can still be pinged or whether the web server is still delivering data. ISuTest® can also monitor any process parameters. In the simplest case, these are the digital output values of an actuator. The process of a switch, however, is its switching functionality, which is evaluated. Basically, the same procedures can be used here that are already used in the functional tests.

Just as ISuTest® can control other test tools and enrich them with process monitoring, for example, it can also be controlled remotely itself. The REST API specified in OpenAPI allowstests to be started at selected times and the test results to be returned in machine-readable form. This means that security tests can be triggered by existing CI/CD systems and tickets can be created in return if ISuTest® has discovered a potential vulnerability.

Successful in daily use

ISuTest® is aimed at manufacturers and integrators of industrial components. ISuTest® can be used both in test centres and during development. ISuTest® has been in commercial use for several years now and has already identified hundreds of vulnerabilities. These successes show that with ISuTest® the vision of "Security by Design" does not have to remain a vision.

More Informationen

www.isutest.com

Contact

Steffen Pfrang
Information Management and Production Control
phone +49 721 6091 357
steffen.pfrang@iosb.fraunhofer.de

Dr. Christian Haas
Information Management and Production Control
phone +49 721 6091 605
christian.haas@iosb.fraunhofer.de

Fraunhofer IOSB
Fraunhoferstr. 1
76131 Karlsruhe
www.iosb.fraunhofer.de/en