Fraunhofer
IOSB

FRAUNHOFER INSTITUTE OF OPTRONICS, SYSTEM TECHNOLOGIES AND IMAGE EXPLOITATION IOSB

ISuTest
Industrial Security Testing

INDUSTRIAL-SECURITY-TESTING-FRAMEWORK ISuTest

AUTOMATED. MODULAR. REPRODUCIBLE.

Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB

Fraunhoferstraße 1
76131 Karlsruhe

Contact
Information Management and Production Control

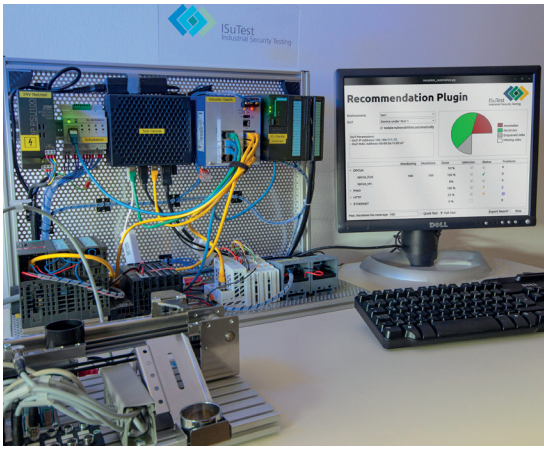
Dr.-Ing. Christian Haas
Phone +49 721 6091-605
christian.haas@iosb.fraunhofer.de

www.isutest.com
www.iosb.fraunhofer.de

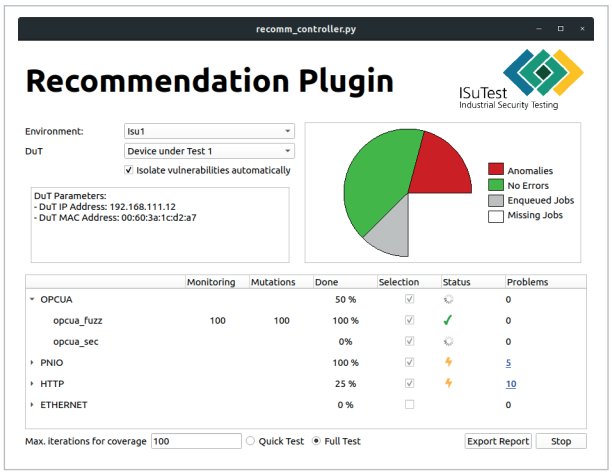
Industrial IT Security

In addition to classic quality features, robustness in terms of IT security is becoming increasingly important for automation components. Reports of successful attacks on industrial plants as well as standards such as IEC 62443 mean that more and more plant operators and integrators are paying attention to IT security when selecting components.

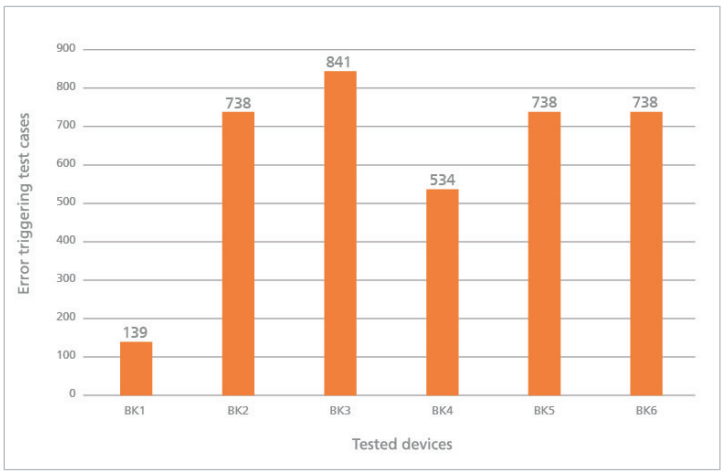
In order to increase the IT security of automation components, potential points of attack and vulnerabilities must be identified and eliminated. Black-box security testing can be used for this purpose. Here, the component to be tested is viewed from the perspective of an attacker via the network interface. This has the advantage that even purchased components can be tested for their quality.



Exemplary test setup of ISuTest



Screenshot of the GUI of ISuTest



Number of test cases that led to an error during our bus coupler study [1]

ISuTest – Vision

Our vision is the comprehensive spreading of the concept *Security by Design* in the automation industry. An essential component of this is an automated vulnerability search, which is carried out by automation experts during the development process. This makes it possible to find vulnerabilities already in the development phase and to eliminate them before delivery.

But also components already in gain benefit from the vulnerability search. Because only errors that are detected can be corrected by the manufacturer.

ISuTest – Functionality

ISuTest, our framework for industrial security testing, performs automated vulnerability tests. Thereby the device under test is considered as a black-box, which also allows to test purchased components. The tests take place via the network interface.

Due to its modular structure, ISuTest can examine the implementation of various Ethernet-based protocols. This includes industrial protocols like PROFINET or OPC UA, but also standard Internet protocols like TCP, UDP and HTTP. It is also easy to integrate definitions of proprietary protocols into ISuTest and include them in the tests.

ISuTest puts a special emphasis on the reproducibility of security tests. ISuTest is operated via a graphical user interface, which makes the technical complexity usable even for automation experts without deep security knowledge.

ISuTest – Application

ISuTest is already successfully used in various scenarios: Market-ready or already in use components are analyzed in the Fraunhofer IOSB security laboratory with ISuTest with regard to their IT security. In addition, we ourselves have carried out serial examinations of industrial components to evaluate ISuTest and discovered dozens of vulnerabilities. This includes a study which examined different bus couplers [1]. Some of the results are shown in the Figure above, which presents the number of test cases that led to an error in the respective device.

Interested manufacturers and integrators use independent instances of ISuTest to examine prototypes. By means of test installations, first experiences with the use of ISuTest can be gained before it is fully integrated into the daily development process.

For a complete integration of security testing, ISuTest is integrated into existing test infrastructures. Each of these deployment scenarios of ISuTest contributes to getting closer to the vision of a comprehensive dissemination of the concept *Security by Design*.

[1] Pfrang, S., & Borcherding, A. (2019). Security Testing für industrielle Automatisierungskomponenten: Ein Framework, sein Einsatz und Ergebnisse am Beispiel von Profinet-Buskopplern, IT-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung : Tagungsband zum 16. Deutschen IT-Sicherheitskongress. - Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn. - Gau-Algesheim: SecuMedia Verl.. - 978-3-922746-82-9 (ISBN). - (2019).