Fraunhofer
IOSB

FRAUNHOFER-INSTITUT FÜR OPTRONIK, SYSTEMTECHNIK UND BILDAUSWERTUNG IOSB

ISuTest
Industrial Security Testing

INDUSTRIAL-SECURITY-TESTING-FRAMEWORK ISuTest

AUTOMATISIERT. MODULAR. REPRODUZIERBAR.

Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung

Fraunhoferstraße 1
76131 Karlsruhe

Ansprechpartner
Informationsmanagement und Leittechnik

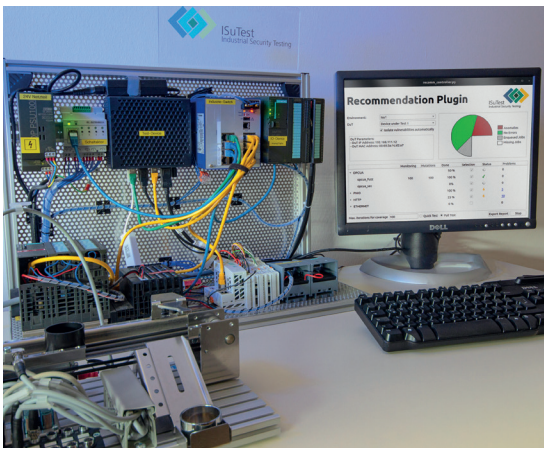
Dr.-Ing. Christian Haas
Telefon +49 721 6091-605
christian.haas@iosb.fraunhofer.de

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

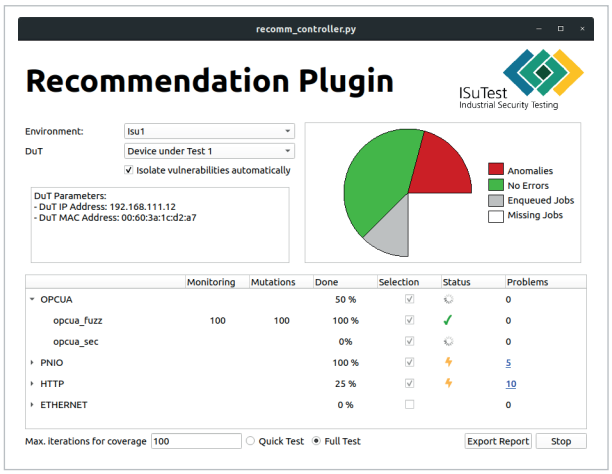
Industrielle IT-Sicherheit

Neben klassischen Qualitätsmerkmalen gewinnt die Robustheit im Hinblick auf IT-Sicherheit bei Automatisierungskomponenten immer mehr an Bedeutung. Sowohl Berichte über erfolgreiche Angriffe auf Industrieanlagen als auch Normen wie die IEC 62443 haben zur Folge, dass immer mehr Anlagenbetreiber und Integratoren bei der Auswahl der Komponenten auf IT-Sicherheit achten.

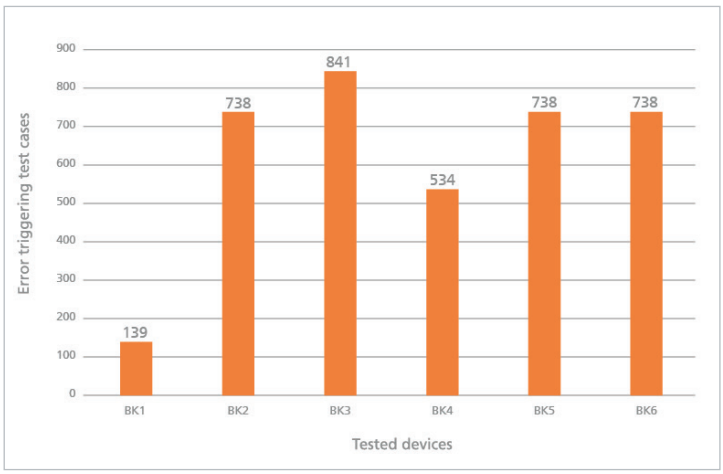
Um die IT-Sicherheit von Automatisierungskomponenten zu erhöhen, müssen potentielle Angriffspunkte und Schwachstellen ermittelt und behoben werden. Dafür kann Black-Box Security-Testing eingesetzt werden. Hierbei wird die zu testende Komponente aus Sicht eines Angreifers über die Netzwerkschnittstelle betrachtet. Das hat den Vorteil, dass so auch zugekaufte Komponenten auf ihre Qualität überprüft werden können.



Beispielhafter Testaufbau von ISuTest



Screenshot der GUI von ISuTest



Fehler-auslösende Testfälle der Buskopplerstudie [1]

ISuTest – Vision

Unsere Vision ist die umfassende Verbreitung des Konzepts *Security by Design* in der Automatisierungsbranche. Dabei ist ein wesentlicher Baustein eine automatisierte Schwachstellensuche, die von Automatisierungsexperten entwicklungsbegleitend durchgeführt wird. Diese ermöglicht es, bereits in der Entwicklungsphase Schwachstellen zu finden und vor der Auslieferung zu beheben.

Aber auch bereits produktiv eingesetzte Komponenten profitieren von der Schwachstellensuche. Denn nur Fehler, die entdeckt werden, können durch den Hersteller behoben werden.

ISuTest – Funktionsweise

ISuTest, unser Framework für industrielles Security-Testing, führt automatisierte Schwachstellentests durch. Dabei wird das zu testende Gerät als Black-Box betrachtet, wodurch auch zugekaufte Komponenten untersucht werden können. Die Untersuchungen finden über die Netzwerkschnittstelle statt.

Durch seinen modularen Aufbau kann ISuTest die Implementierungen diverser Ethernet-basierter Protokolle untersuchen. Dies umfasst industrielle Protokolle wie PROFINET oder OPC UA, aber auch Standard-Internetprotokolle wie TCP, UDP und HTTP. Ebenso ist es leicht möglich, Definitionen von proprietären Protokollen in ISuTest zu integrieren und in die Tests einzubeziehen.

Einen besonderen Schwerpunkt legt ISuTest auf die Reproduzierbarkeit der Security-Tests. Die Bedienung von ISuTest erfolgt über eine grafische Benutzeroberfläche, die die technische Komplexität auch für Automatisierungsexperten ohne tiefe Security-Kenntnisse nutzbar macht.

ISuTest – Einsatz

ISuTest kommt bereits in verschiedenen Szenarien erfolgreich zum Einsatz: Marktreife oder bereits im Einsatz befindliche Komponenten werden im Sicherheitslabor des Fraunhofer IOSB mit ISuTest im Hinblick auf ihre IT-Sicherheit analysiert.

Daneben haben wir selbst zur Evaluation von ISuTest Reihenuntersuchungen von industriellen Geräten durchgeführt und Dutzende von Schwachstellen entdeckt. Insbesondere haben wir eine Studie zur Untersuchung verschiedener Buskoppler durchgeführt [1]. Ausgewählte Ergebnisse dieser Studie werden in der Abbildung oben dargestellt.

Interessierte Hersteller und Integratoren nutzen eigenständige Instanzen von ISuTest, um Prototypen zu untersuchen. Mittels Testinstallationen können erste Erfahrungen mit dem Einsatz von ISuTest gesammelt werden, bevor es vollständig in den täglichen Entwicklungsablauf integriert wird.

Für eine vollständige Integration der IT-Sicherheits-Untersuchungen wird ISuTest in bestehende Test-Infrastrukturen integriert. Jedes dieser Einsatzszenarien von ISuTest trägt dazu bei, der Vision der umfassenden Verbreitung des Konzepts *Security by Design* näher zu kommen.

[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).