Fraunhofer IOSB

ISuTest®

Automatisierte Schwachstellensuche gemäß dem Cyber Resilience Act und IEC 62443

Abb. 1: Testaufbau von ISuTest® im Fraunhofer-IOSB-Labor in Karlsruhe. Quelle: Fraunhofer IOSB

Motivation

Industrielle Komponenten sind häufig im Verborgenen im Einsatz: Moderne Ampelsteuerungen an Kreuzungen, Züge, Kraftwerke und Krankenhäuser funktionieren nicht ohne sie. Daneben steuern und kontrollieren sie ganze Fabrikhallen, lesen Sensordaten aus und verarbeiten sie teils mit Echtzeit-Anforderungen.

Doch was haben alle industriellen Komponenten gemein? Einen Netzwerkanschluss, also ein »digitales Element«, wie es im Cyber Resilience Act (CRA) der Europäischen Union (EU) heißt. Über diesen Anschluss sind sie per Netz erreichbar – und damit auch angreifbar. Was passiert im Fall eines Angriffs? Mal fallen Anzeigetafeln der Bahn aus, mal stellen Krankenhäuser den Betrieb ein oder ein Werkstück in der Fertigung erhält nicht die geforderte Qualität.
Vor diesem Hintergrund hat die EU den CRA erlassen. Die Verordnung verpflichtet Hersteller von Komponenten mit digitalen Elementen, diese sicher zu entwickeln und zu testen. Andernfalls dürfen sie ab Dezember 2027 nicht mehr innerhalb der EU auf den Markt gebracht werden. Der IEC-Standard 62443 zum Schutz industrieller Kommunikationsnetze beschreibt solch einen sicheren Entwicklungslebenszyklus für Hersteller industrieller Komponenten. Die automatisierte Schwachstellensuche über die Netzwerkschnittstelle ist dabei ein wesentlicher Bestandteil. Das heißt, alle Protokolle, die die Robustheit der Komponenten beeinträchtigen können, müssen ausführlich auf Schwachstellen getestet werden.

ISuTest®
Industrial Security Testing

» ISuTest® als Baustein zur Zertifizierung.

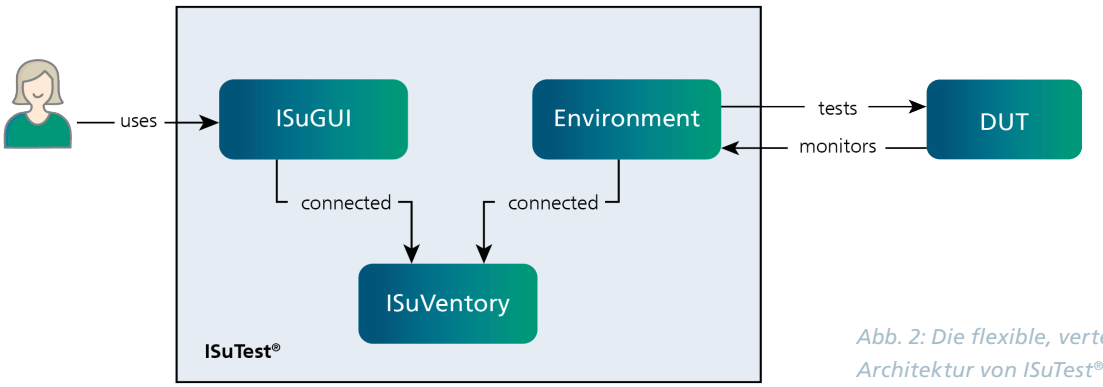

Abb. 2: Die flexible, verteilte Architektur von ISuTest®.

Testen wie ein Angreifer

Das Industrial Security Testing Framework ISuTest® ist ein Werkzeug, um Schwachstellen in den Implementierungen der Automatisierungskomponenten zu finden. Es wird seit 2016 am Fraunhofer IOSB in Karlsruhe in der Gruppe Industrielle Cybersicherheit entwickelt. ISuTest® ist als offenes, erweiterbares Framework entworfen. Es unterstützt seine Nutzer von der Einrichtung eines Tests über die Durchführung bis hin zur Isolation von Schwachstellen zum Nachstellen des Fehlers beim Entwickler. Ein beispielhafter Testaufbau von ISuTest®, wie er im Fraunhofer-IOSB-Labor zum Einsatz kommt, ist in Abbildung 1 dargestellt.

Der Schwachstellentest durch ISuTest® erfolgt mittels Fuzzing-Techniken. Dabei werden Netzwerkpakete leicht verändert und an die Komponente gesendet, wie dies auch ein Angreifer tun würde. ISuTest® braucht dabei keinerlei Einblick in die Interna der Komponente, es reicht die Spezifikation der Kommunikationsprotokolle. Damit kann jedes Gerät mit Netzwerkschnittstelle getestet werden. Es handelt sich um einen sogenannten Black-Box-Test. Darüber hinaus können für ISuTest® weitere Protokolle leicht hinzugefügt werden, um die IEC-62443-Anforderung nach dem Test aller angebotenen Protokolle zu erfüllen.

Die Architektur von ISuTest® ist in Abbildung 2 dargestellt. Es handelt sich um eine verteilte Client-Server-Infrastruktur. Den eigentlichen Test führt das Environment durch. Mittels der grafischen Benutzeroberfläche ISuGUI konfiguriert der Benutzer zu testende Komponenten, startet Tests und wertet abgeschlossene Tests komfortabel aus. Zentrale Datenbank, Dateiablage und Kommunikator ist das ISuVentory. In der kleinsten Ausbaustufe werden alle Bestandteile auf einem lokalen PC installiert. In der größten Ausbaustufe arbeiten viele Benutzer mit ISuGUIs über VPN mit einem ISuVentory in einem Kubernetes-Cluster und mehreren Environments.

Überwachen wie beim Funktionstest

Damit ISuTest® erkennen kann, ob eine Komponente während und nach einem Test noch funktioniert wie vorgesehen, setzt es Monitoring ein. Klassisches IT-Monitoring testet beispielsweise, ob sich das Gerät noch anpingen lässt oder der Webserver noch Daten liefert. Darüber hinaus kann ISuTest® beliebige Prozessparameter überwachen. Im einfachsten Fall sind das digitale Ausgangswerte eines Aktors. Der Prozess eines Switches ist hingegen seine Switching-Funktionalität, die evaluiert wird. Grundlegend können hier dieselben Verfahren zum Einsatz kommen, die schon in den Funktionstests genutzt werden.
ISuTest® kann nicht nur andere Testtools ansteuern und sie zum Beispiel mit dem Prozess-Monitoring anreichern, sondern kann auch selbst ferngesteuert werden. Die in OpenAPI spezifizierte REST-API erlaubt es, Tests zu gewählten Zeitpunkten zu starten und die Testergebnisse maschinenlesbar zurückzuliefern. Damit können Security-Tests durch bestehende CI/CD-Systeme getriggert und im Gegenzug Tickets erstellt werden, wenn ISuTest® eine potenzielle Schwachstelle entdeckt hat.

Erfolgreich im täglichen Einsatz

Zielgruppe von ISuTest® sind Hersteller und Integratoren von industriellen Komponenten. Dabei kann ISuTest® sowohl in Testcentern als auch entwicklungsbegleitend eingesetzt werden. Bereits seit mehreren Jahren im kommerziellen Einsatz, konnte ISuTest® bereits hunderte Schwachstellen identifizieren. Diese Erfolge zeigen, dass mit ISuTest® die Vision von »Security by Design« keine Vision bleiben muss.

Weitere Informationen

www.isutest.de

Kontakt

Steffen Pfrang
Informationsmanagement und Leittechnik
Tel. +49 721 6091 357
steffen.pfrang@iosb.fraunhofer.de

Dr. Christian Haas
Informationsmanagement und Leittechnik
Tel. +49 721 6091 605
christian.haas@iosb.fraunhofer.de

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