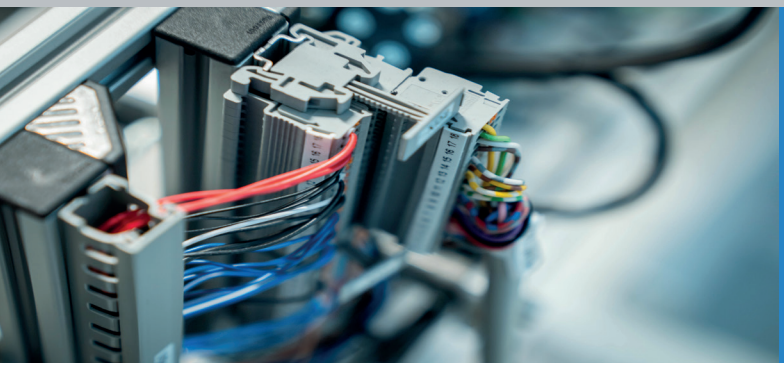
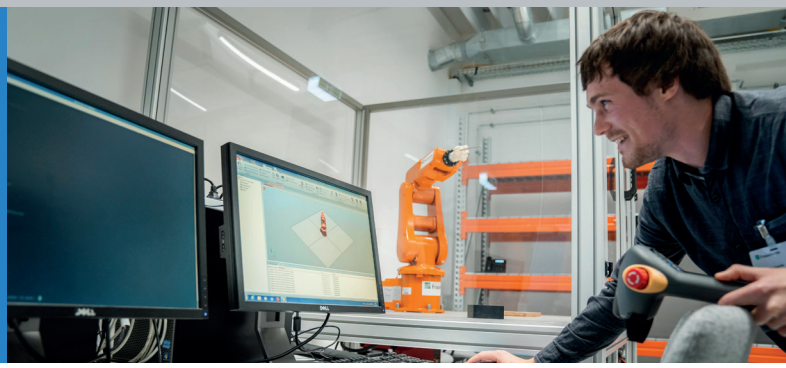
Fraunhofer
AISEC

FRAUNHOFER-INSTITUT FÜR ANGEWANDTE UND INTEGRIERTE SICHERHEIT AISEC





INDUSTRIAL SECURITY LABS

1 *Feldbus einer Industrieanlage*
2 *Simulierter Angriff auf Roboterarm*

Das Fraunhofer AISEC verfügt über mehrere Industrial-Security-Labore, die praktische Security-Arbeiten in den unterschiedlichsten Bereichen ermöglichen. Das Angebotsspektrum reicht hier von Analysen in den Bereichen vernetzte Produktion, Industrie 4.0, Internet der Dinge bis hin zur Untersuchung der Sicherheit im Bereich Gebäudeautomation. Damit steht unseren Forscherinnen und Forschern eine gesicherte und vertrauenswürdige Umgebung für qualifizierte und kompetente Sicherheitsuntersuchungen der unterschiedlichsten Arten zur Verfügung. Durch entsprechende Simulationsumgebungen ist es außerdem möglich, reale Komponenten zu ergänzen und so realitätsnahe Umgebungen für Sicherheitsanalysen zu schaffen. Die Serverlandschaft des Fraunhofer AISEC ermöglicht außerdem eine erhöhte Rechenkapazität für mehr Simulationen (Augmented und Virtual Reality).

MODELLFABRIK FÜR SECURITY-ANALYSEN

In einem der Laborräume für Industrial Security wurde das Modell einer Produktionsstraße mit mehreren Teilstationen aufgebaut. Dieser Nachbau ermöglicht die Verwendung echter, praxiserprobter Industriekomponenten. Durch den modularen Aufbau kann die Produktionsstraße eine Vielzahl von möglichen Anwendungsfällen und aktuellen Bedrohungsszenarien unter realistischen Bedingungen abbilden. So ist es unseren Wissenschaftlerinnen und Wissenschaftlern möglich, die Sicherheit in der Produktion und Fertigung auf vielfältige Weise zu überprüfen.

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Lichtenbergstraße 11
85748 Garching bei München

Kontakt
Bartol Filipovic
Abteilungsleiter »Product Protection and Industrial Security«
Telefon +49 89 322 99 86-128
bartol.filipovic@aisec.fraunhofer.de

www.aisec.fraunhofer.de

1 *Modell einer Produktionsstraße*
2 *Vernetzte Produktion*

SECURITY FÜR GEBÄUDEAUTOMATION

Ein weiterer Demonstrator ermöglicht die Untersuchung gängiger intelligenter und vernetzter Installationstechnik, beispielsweise in der Gebäudeautomation und -sicherheit. Durch Computer-gestützte Trainings- und Experimentiersysteme ist es möglich, Angriffe auf Gefahrenfrühwarnsysteme wie Feuer- oder Rauchmelder sowie gegen Einbruchssysteme und Sensoren zu simulieren. Auch hier ist es möglich, die realen Umgebungen und Komponenten durch geeignete Simulationen zu ergänzen. So können Schutzmaßnahmen entwickelt und getestet werden, um die Sicherheit für Geräte und Kommunikationsprotokolle gemäß Stand der Technik sicherzustellen.

MECHATRONIK-DEMONSTRAOTOR

Als praxisnahes Untersuchungs- und Experimentierobjekt betreibt das Fraunhofer AISEC in seinen Industrial-Security-Laboren einen Mechatronik-Demonstrator, der charakteristische mechanische und elektronische Komponenten aus der Automatisierungstechnik in einer kompakten Anlage zusammenfasst. Dabei werden Aktuatoren wie Greifer, Förderbänder, Vereinzelungsmagazine und Montageautomaten gemeinsam mit passenden Sensoren durch industrieübliche Steuergeräte und Anzeigemodule betrieben. Die Anlage erlaubt den Forscherinnen und Forscher des Fraunhofer AISEC einerseits, konkrete Angriffe zu erproben, die Folgen solcher Angriffe zu demonstrieren und gleichzeitig Security-maßnahmen umzusetzen und zu testen.

ANGEBOT

Security für Gebäudeautomation

- Risikoanalysen und Penetrationstests für vernetzte Geräte und Dienste
- Security für Geräte und Kommunikationsprotokolle gemäß Stand der Technik
- Entwicklung und Test von Schutzmaßnahmen
- Knowhow- und Manipulationsschutz
- Angriffserkennung und Integritätsüberwachung
- Netzwerk- und Feldbus-Security
- Datensouveränität und sichere Datenspeicherung

Security in der Fertigung

- Risikoanalysen und Penetrationstests für vernetzte Produktionssysteme
- Untersuchung aktueller Bedrohungsszenarien unter realistischen Bedingungen
- Darstellung einer Vielzahl praxisnaher Anwendungsfälle
- Projektspezifische Untersuchungen durch individuelle Anpassungen
- Knowhow- und Manipulationsschutz
- Angriffserkennung und Integritätsüberwachung
- Anonymisierung und Datenschutz für Maschinendaten
- Ergänzung realer Komponenten durch Simulation für Security-Analysen
- Beratung bei der Umsetzung von Security-Normen und -Standards