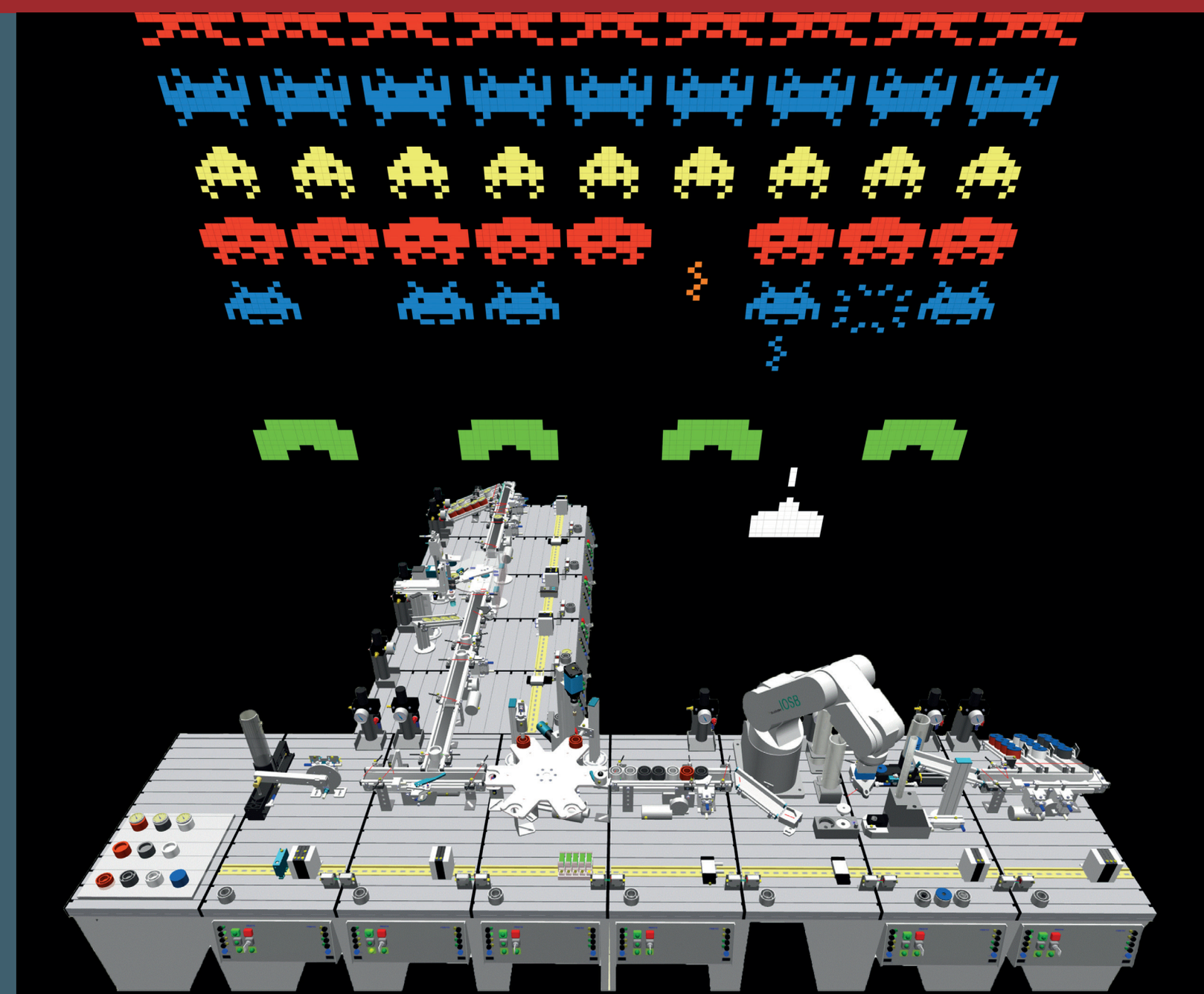
Fraunhofer
IOSB

FRAUNHOFER-INSTITUT FÜR OPTRONIK, SYSTEMTECHNIK UND BILDAUSWERTUNG IOSB

IT-SICHERHEITSLABOR FÜR DIE PRODUKTION
IT-SECURITY FOR INDUSTRIAL PRODUCTION



CLOUD-DIENSTE
IM UMFELD INDUSTRIE 4.0

In der Industrie 4.0 besitzen alle Komponenten in Produktionsanlagen und Fabrikumgebungen erweiterte Intelligenz und kommunizieren untereinander. Clouddienste ermöglichen dabei, die notwendige Verarbeitungsleistung nicht in den Komponenten sondern mit gemeinsam genutzten IT-Ressourcen flexibel und bedarfsgerecht bereitzustellen. Die Komponenten selbst können dabei kleiner und kostengünstiger ausfallen, sie integrieren nur noch lokale Schnittstellen, Kommunikationsdienste und Notfallfunktionen. Durch Anpassung und Erweiterung *in der Cloud* können neue und verbesserte Funktionen schnell und einfach eingeführt werden.

Kontakt:
Birger Krägelin
IT-Sicherheitsbeauftragter
birger.kraegelin@iosb.fraunhofer.de
+49 721 6091-454

Bei einer Kommunikation über das Internet besteht zusätzlich die Möglichkeit, Informationen und Visualisierungen zur Überwachung oder Steuerung bei Bedarf überall abzurufen und z. B. Tablets oder Smartphones in die betrieblichen Abläufe zu integrieren.

Voraussetzung hierfür sind zuverlässige Kommunikationsverbindungen (Verfügbarkeit) und angepasste Sicherheitsmaßnahmen, um die eindeutige Identifikation der beteiligten Kommunikationspartner sicherzustellen (Authentizität) und den Zugriff Fremder auf Daten und Verarbeitungsfunktionen zu verhindern (Vertraulichkeit).

Besondere Risiken entstehen dabei einerseits durch Implementierungsfehler der Sicherheitsfunktionen in den einzelnen Komponenten oder deren fehlerhafte Konfiguration beim Einsatz, andererseits entsteht durch die Zentralisierung von IT-Ressourcen ein *Single Point of Attack*, der Angreifern neue Möglichkeiten eröffnet.

Das IT-Sicherheitslabor verfügt daher über eine eigene Private Cloud, in der neue Anwendungen getestet und Sicherheitsprobleme untersucht werden können. Die Flexibilität dieser IT-Ressourcen wird dabei auch genutzt, um schnell komplexe Netzwerkstrukturen für unterschiedliche Fabrikszenarien zu konfigurieren, um Angriffe gegen Komponenten und Funktionen durchzuführen und die Auswirkungen verschiedener Sicherheitsfunktionen zu untersuchen.

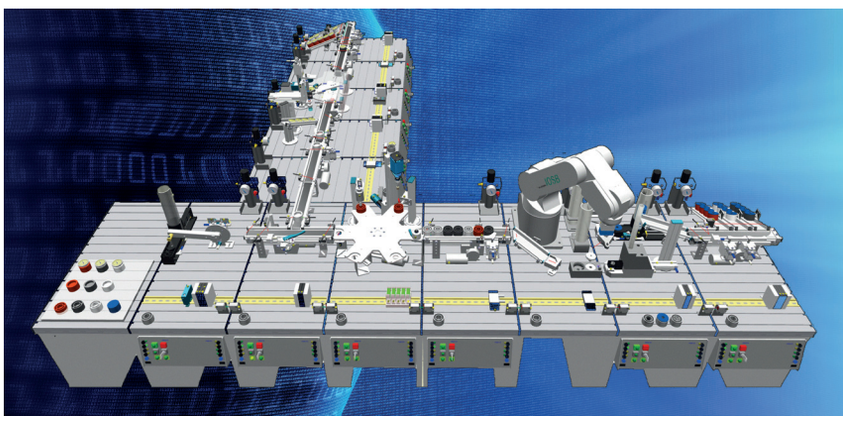
CLOUD-SERVICES IN THE INDUSTRIE 4.0 ENVIRONMENT

In Industrie 4.0, all components in production facilities and factory environments feature extended intelligence and communicate with each other. Cloud services allow the required processing capacity to be provided not in the components themselves, but – flexibly and in line with demand – through shared IT resources. This, in turn, allows the use of smaller, cheaper components that incorporate only local interfaces, communication services and emergency functions. Through adaptation and expansion in the cloud, new and improved functions can be introduced quickly and easily.

Communication via the Internet furthermore allows information and visualizations to be retrieved from anywhere on demand to monitor or control operational processes and integrate, for example, tablets or smartphones.

Reliable communication links (availability) and customized security measures are required to ensure the unique identification of legitimate communication partners (authenticity) and prevent unauthorized access to data and processing functions (confidentiality).

The particular risks associated with this approach result, on one hand, from implementation errors in the security functions of individual components or an incorrect configuration in use, and, on the other hand, the single point of attack presented by centralized IT resources, which opens up new possibilities for intruders.



The IT security lab therefore has its own private cloud, in which new applications can be tested and security issues investigated. The flexibility of these IT resources is also used to quickly configure complex network structures for various factory scenarios to carry out attacks against components and functions and to investigate the effects of various security functions.

Contact:
Birger Krägelin
IT-Security Officer
birger.kraegelin@iosb.fraunhofer.de
+49 721 6091-454

FUNKTIONEN

Funktionalität des IT-Sicherheitslabors

Die Durchführung von IT-Sicherheitsuntersuchungen erfordert einerseits eine von produktiven Netzen abgeschottete IT-Infrastruktur und andererseits soll diese Infrastruktur die Zielumgebung möglichst gut annähern. Das hier vorgestellte IT-Sicherheitslabor ist in diesem Sinne eine Test- und Demonstrationsumgebung, in der sich Sicherheitsuntersuchungen an industriellen IT-Komponenten durchführen lassen.

Das Sicherheitslabor bildet die gesamte hierarchische IT-Infrastruktur eines Fabrikstandortes mit Büronetz sowie Netzen für Produktionsplanung, Produktionsüberwachung und Produktionssteuerung nach. Diese wirklichkeitsnahe IT-Netzwerkumgebung ist teilweise aus typischen industriellen Netzelementen aufgebaut und teilweise in einer Cloud als virtuelle Netzwerkstruktur abgebildet.

In diese Umgebung sind einzelnen industrielle Steuerungskomponenten (Speicherprogrammierbare Steuerungen) sowie weitere Unterstützungssysteme integriert, die einen kleinen Fertigungsprozess steuern und überwachen. Dieser Fertigungsprozess existiert in Form eines Simulationsprogramms, welches das entsprechende Verhalten von Fertigungskomponenten realisiert und visualisiert.

Neben der so beschriebenen Fabrikumgebung wurde die Infrastruktur mit einer Reihe von Applikationen instrumentiert, die die Netze des abgebildeten Fabrikstandortes und die darin befindlichen Komponenten in sicherheitstechnischer Hinsicht überwachen und mögliche Angriffe signalisieren können. Darüber hinaus sind Werkzeuge zur Durchführung von Angriffen verfügbar.

Im Rahmen des vorgestellten IT Sicherheitslabor arbeiten wir an der Weiterentwicklung von Werkzeugen – speziell für industrielle Produktionsumgebungen - zur Sicherheitsüberwachung, zur Signalisierung von Sicherheitsalarmen und zur Angriffserkennung, unter anderem auch durch den Einsatz von Lernverfahren zur Erkennung von Anomalien. Des Weiteren dient diese Umgebung der sicherheitstechnischen Evaluierung im Rahmen von Produktentwicklungen.

Kontakt:
Jörg Kippe
Sichere Kommunikations-
architekturen
joerg.kippe@iosb.fraunhofer.de
+49 721 6091-337

FEATURES

Functionality of the IT security laboratory

IT security investigations require an IT infrastructure that is both isolated from productive networks and replicates the target environment as accurately as possible. The IT security lab presented here is such a test and demonstration environment, in which security investigations on industrial IT components can be carried out.

The security lab replicates the entire hierarchical IT infrastructure of a factory site, complete with office, production planning, and production control and monitoring networks. This realistic IT network environment consists partly of typical industrial network elements and partly of a cloud-based virtual network structure.

The environment integrates individual industrial control components (programmable logic controllers) and other support systems, which monitor and control a small manufacturing process. This production process exists in the form of a simulation program, which implements and visualizes the behavior of production components.

In addition to the described factory environment, the infrastructure has been equipped with a variety of applications that provide security monitoring of the simulated factory networks and their components and signal possible attacks. Tools to carry out attacks are also available.

In the context of the presented IT security lab we are working on the further development of tools – specially for industrial production environments – for security monitoring, signaling security breaches and intrusion detection, including the use of learning methods for the detection of anomalies. This environment also serves for safety evaluation in product development.

Contact:
Jörg Kippe
Secure Communication Architectures
joerg.kippe@iosb.fraunhofer.de
+49 721 6091-337

OPC UA

Logging, Security Mechanismen, Authentifikation

OPC Unified Architecture (OPC UA) und Informations-Sicherheit – Sicherheit um jeden Preis?

Neben der funktionalen Sicherheit und der Zuverlässigkeit spielt gerade die Informationssicherheit eine bedeutende Rolle in der industriellen Automatisierung. Durch die Öffnung der Produktionsnetzwerke müssen Standard-Kommunikations- und Managementplattformen, die Informationen aus der Produktion über Netzwerkinfrastrukturen zugänglich machen, ein großes Augenmerk auf einen angemessenen, aber variablen Schutz der kommunizierten Informationen legen. OPC UA, als ein solcher Vertreter, spezifiziert daher mögliche Mechanismen, die es im Bedarfsfall zu nutzen gilt. Diese sind nicht OPC UA-spezifisch, sondern folgen in der Praxis vorherrschenden Mechanismen. Das Fraunhofer IOSB setzt OPC UA in laufenden Forschungsprojekten, aber auch in vielen Industrieprojekten ein.

Neben der Benennung möglicher Angriffsszenarien, wie z. B. das unerlaubte Eindringen in das System, die Verfälschung von Werten, Nachrichten und Anmeldedaten, das Abhören der Kommunikation oder auch das Kompromittieren von OPC UA Servern durch eine Nachrichtenflut, werden in den Spezifikationen auch umsetzbare Gegenmaßnahmen genannt. Für Nutzer oder Gruppen kann beispielsweise der Zugriff auf einen UA Server oder seine Knoten geregelt werden. Diese Authorisierungsmechanismen ermöglichen es, allgemein oder basierend auf der Identität eines Anwenders den lesenden, schreibenden oder ausführenden Zugriff zu beschränken. So kann für bestimmte Personen in bestimmten Rollen, bspw. den Servicetechniker, der Zugriff auf entsprechende Informationen geregelt sein. Dies wird am Fraunhofer IOSB beispielsweise im Projekt SecurePLUGandWORK genutzt.

Neben der vorbeugenden Sicherung werden aber auch erfolgreiche und erfolglose Verbindungsversuche ebenso aufgezeichnet wie Konfigurationsänderungen, Zurückweisungen von Sessions und können entsprechende Ereignisse auslösen. An Hand der erfassten Daten kann beispielsweise das versuchte Eindringen frühzeitig erkannt werden und die Erkennung entsprechender Angriffe basierend auf Klassifikationssystemen erfolgen.

Kontakt:
Dr.-Ing. Miriam Schleipen
Informationsmanagement und Leittechnik
miriam.schleipen@iosb.fraunhofer.de
+49 721 6091-382

OPC UA

Logging, Security Mechanism, Authentification

OPC Unified Architecture (OPC UA) and information security – security at any price?

In addition to functional safety and reliability, information security plays a specially important role in industrial automation. The increasing connectivity of production networks with the outside world demands a strong focus on an adequate but sufficiently flexible protection of production data made available through network infrastructures by standard communication and management platforms.

The OPC UA communication protocol specifies possible mechanisms for this purpose, which can be used as needed. These are based on the mechanisms most commonly used in practice and are not specific to OPC UA. The Fraunhofer IOSB uses OPC UA in ongoing research projects and in many industrial projects.

In addition to naming potential attack scenarios, such as intrusions into the system, corruption of values, messages and login data, interception of communication or compromising OPC UA servers with message floods, the specifications also list possible countermeasures.

For users or groups, access to a UA server or its nodes can, for instance, be regulated. With these authorization methods, read, write, or execute access can be defined either globally or based on the user's identity. This allows access to required information to be granted only to specific users in certain roles, such as service technicians. At the Fraunhofer IOSB, this function is used, for example, in the SecurePLUGandWORK project.

In addition to preventive security, successful and failed connection attempts, configuration changes and denied sessions are also recorded and can trigger appropriate events. From the collected data, intrusion attempts and attacks can, for example, be detected early based on classification systems.

Contact:
Dr.-Ing. Miriam Schleipen
Information Management and Production Control
miriam.schleipen@iosb.fraunhofer.de
+49 721 6091-382

LEISTUNGSANGEBOT
SERVICE OFFERING

Mit dem IT-Sicherheitslabor (IT-SiLab) bietet das Fraunhofer IOSB eine flexible und leistungsfähige Test- und Simulationsumgebung, um Sicherheitsrisiken in Ihrer Produktionsumgebung zu identifizieren und Gegenmaßnahmen zu testen.

Wir bieten Ihnen:

- eine praxisnahe IT-Sicherheitsberatung, zugeschnitten auf Ihr Produktionsnetz
- eine Analyse der Sicherheitsrisiken in Ihrem Produktionsnetz
- Konzeption und „Härtetest" von Gegenmaßnahmen durch simulierte Angriffe
- Beratung bei der Konzeption sicherer IT-Architekturen für Ihre Produktionsumgebung
- Integrierte Sicherheitswarn- und Überwachungs-systeme
- sichere OPC UA Server mit Logging und Authentifizierung

With the IT Security Lab (IT-SiLab) Fraunhofer IOSB offers a flexible and powerful test and simulation environment In order to identify security risks in your production environment and to test counter measures.

We offer:

- IT security consulting with a practical orientation, tailored to your production network
- security risk analysis in your production network
- design and acid test of counter measures by means of simulated attacks
- consultancy for the design of secure IT architectures for your production environment
- integrated security warning and monitoring systems
- secure OPC UA server with logging and authentication

WWW.IOSB.FRAUNHOFER.DE

Kontakt:
Birger Krägelin
IT-Sicherheitsbeauftragter
Fraunhofer IOSB
birger.kraegelin@iosb.fraunhofer.de
+49 721 6091-454