

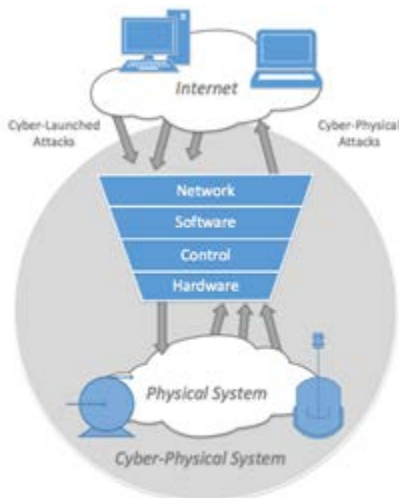
# Verbesserung der Sicherheit von Informationsprozessen in Produktionssystemen



Die Verbesserung von Sicherheit von Informationsprozessen im Lebenszyklus im Lebenszyklus von industriellen Produktionssystemen gewinnt zunehmend an Bedeutung. Zunehmende Verwendung von Softwarekomponenten und entsprechende Entwicklungsprozesse im globalen und verteilten Umfeld erfordern neue Ansätze für Entwicklung, Qualitätssicherung und Sicherheit.

Industrielle Produktionssysteme, wie Roboter, Fertigungszellen oder Stahlwerke, steuern leistungsstarke und risikoreiche physikalische Prozesse und müssen Domänen spezifische Standards für **Sicherheit, Umwelt** und **Qualität** erfüllen. Die Erfüllung dieser Standards ist herausfordernd für traditionelle Produktionssysteme, speziell für **cyber-physical production systems** im Kontext der Industrie 4.0 Initiative.

Im Lebenszyklus eines Produktionssystems werden **Informationsprozesse** für Erstellung, Änderung, Austausch und Verwendung von Engineering-Daten verwendet, um das geplante Produktionssystem und dessen Teile zu entwerfen, konfigurieren und zu verifizieren.



**Informationssicherheit** und **Cyber-Security** bilden das Fundament in modernen vernetzten Umgebungen, um die Lieferung von Engineering-Artefakten in der benötigten Qualität sicher zu stellen, um Risiken für Wissensspionage, Diebstahl und Sicherheitslücken abzuschwächen und um die Sicherheit während Betrieb und Wartung zu gewährleisten.

Traditionell laufen Produktionssysteme und entsprechende Entwicklungsprozesse in isolierten Umgebungen ab und umfassen wenige Anforderungen an IT Sicherheit. Derzeitige Entwicklungen setzen aber auf globale Production Systems Engineering (PSE) Prozesse mit zentraler Datenhaltung; Verbindungen werden meist über das Internet hergestellt und kommunizieren mit Partnern über teilweise nicht vertrauenswürdige Kanäle. Auch herkömmliche Produktionssysteme mit modernen Ersatzteilen (z.B. WLAN Komponenten) können unbeabsichtigt mit dem Internet verbunden sein und so Sicherheitsrisiken beinhalten.

## Änderungen im PSE Engineering

Die Einführung moderner Informationstechnologien beinhaltet zahlreiche Änderungen im PSE Prozess.

**Zentral erreichbare Daten-Repositories.** Vereinfacht gesprochen, bearbeiten Ingenieure in unterschiedlichen Engineering Disziplinen Kernfunktionen, Mechanik, Elektrik, Medien und Steuerungssoftware. Meist werden in einzelnen Disziplinen spezialisierte Werkzeuge ohne direkten Datenaustausch zur Verfügung gestellt. Heutzutage werden Daten vermehrt bi-direktional zwischen einzelnen Werkzeugen durch Experten ausgetauscht; beispielsweise können Änderungen in der Elektrik auch mechanische Änderungen erfordern, etwa durch die Auswahl eines unterschiedlichen Schalters. Um die Handhabung dieser Änderungen zu erleichtern, werden alle Daten in einem zentralen Datenspeicher abgelegt und spezialisierten Werkzeugen über definierte Schnittstellen und einem gemeinsamen Datenformat, wie etwa AutomationML, zugänglich gemacht.

**Globale Kollaboration mit (teilweise) nicht vertrauenswürdigen Quellen.** Die steigende Anzahl, Größe und Komplexität von Entwicklungs- und Erneuerungsprojekten erfordert eine höhere Anzahl von verteilten Teams. Vielfach müssen auch lokale Anbieter in Projekte mit eingebunden werden. Während die lokale Expertise in vielen Fällen hilfreich ist, kann sie im Einzelfall das Spionage-Risiko in sich bergen. Daher wird IPR in großen und

verteilten Projekten zunehmend wichtig.

Bei der Anwendung **moderner Informationstechnologien in einem PSE Umfeld** müssen zwei wesentliche Faktoren berücksichtigt werden: (i) moderne und etablierte Praktiken aus der Wirtschaftsinformatik können nicht unmittelbar im industriellen Umfeld eingesetzt werden; (ii) Angriffsszenarien unterscheiden sich wesentlich von typischen Systemen in der Business IT.

## Wichtige Forschungsrichtungen

Änderungen im PSE Lebenszyklus eröffnen neue Forschungsrichtungen:

- *Secure Modelling* von Angriffsszenarien im PSE Lebenszyklus.
- *Automated and secure testing* von industriellen Produktionssystemen bereits vor der Inbetriebnahme.
- *Verbesserung von Engineering Prozessen* für PSE im Hinblick auf sichere, flexible und agile Praktiken.
- Entwicklung von flexiblen, transparenten und semi-automatisierten *Werkzeugketten* zur Unterstützung des PSE Lebenszyklus.
- *AutomationML* kann effizienten Datenaustausch in Werkzeugketten ermöglichen, um Qualitätssicherung, Testautomatisierung und Prozessverbesserung zu unterstützen.

## Key Messages

- Effiziente, flexible und sichere **Qualitätssicherung** und **Testautomatisierung** in PSE.
- Effizienter und sicherer **Datenaustausch** in Werkzeugketten in verteilten Entwicklungsprozessen.
- **Verbesserung von Engineeringprozessen** für die flexible Konfiguration in PSE Projekten.



## Contact:

Prof. Dr. Stefan Biffli  
TU Wien  
stefan.biffli@tuwien.ac.at  
qse.ifs.tuwien.ac.at

Prof. Dr. Arndt Lüder  
Otto von Guericke University Magdeburg  
Arndt.lueder@ovgu.de  
www.iaf-bg.ovgu.de

Dr. Edgar Weippl  
Secure Business Austria gGmbH  
edgar.weippl@sba-research.org  
www.sba-research.org