

## SDL-CPPS

Secure Development Lifecycle for Cyber-Physical Production Systems

<b>Programm / Ausschreibung</b>	FoKo, Qualifizierungsseminare, Qualifizierungsseminare 5. AS	<b>Status</b>	abgeschlossen
<b>Projektstart</b>	01.12.2018	<b>Projektende</b>	31.05.2019
<b>Zeitraum</b>	2018 - 2019	<b>Projektlaufzeit</b>	6 Monate
<b>Keywords</b>	Cyber-physische Systeme; Cyber Security; Industrie 4.0; sicherer Entwicklungszyklus; sichere industrielle Steuerungssysteme		

### Projektbeschreibung

Die umfassende Vernetzung von einzelnen Bauteilen und Komponenten mit cyber-physischen Produktionssystemen (engl. Cyber-Physical Production Systems – CPPS) bildet das Fundament der digitalen Fabrik, die auf revolutionäre Weise eine ressourceneffiziente Fertigung individueller Produkte ermöglichen soll. Ungeachtet dessen steigt gleichermaßen der Vernetzungsgrad des Engineering-Prozesses dieser Produktionssysteme. Die in der Designphase von CPPS modellierten Daten werden mittels vernetzter Repositories den Projektbeteiligten unterschiedlicher Organisationen zugänglich gemacht – adäquate Sicherheitsmechanismen zum Schutz der Artefakte finden jedoch oftmals keine Berücksichtigung. Dies hat zur Folge, dass neben dem wertvollen geistigen Eigentum auch die Produktionsanlagen dem Risiko eines zielgerichteten Angriffs ausgesetzt sind. Cyberkriminelle könnten bereits in den frühen Entwicklungsphasen des CPPS Schwachstellen einschleusen, die dann erst im laufendem Betrieb ausgenutzt werden. Auf diese Weise könnten manipulierte CPPS unbemerkt weitere Industriekomponenten infizieren und sogar Prozessabläufe in der Fabrik subtil sabotieren. Um dieser Bedrohungslage entgegenzuwirken, muss Informationssicherheit fest im Entwicklungsprozess von CPPS verankert sein. Dies stellt jedoch selbst große Unternehmen vor eine Herausforderung, zumal einschlägige Schulungen gänzlich fehlen.

Das Ziel dieses Qualifizierungsseminars ist daher die Vermittlung von praxisrelevantem Wissen zur Einführung des sicheren Entwicklungszyklus für cyber-physische Produktionssysteme (SDL-CPPS). Die Qualifizierungsmaßnahme behandelt demzufolge die einzelnen Phasen des SDL-CPPS, angefangen von der Bedrohungsmodellierung und dem sicheren Design von CPPS über bewährte Sicherheitskonzepte für die Implementierung bis hin zu der Verifikationsphase und dem sicheren Wartungsprozess im laufendem Betrieb. Erfahrungswerte von Unternehmen, die bereits einen sicheren Softwareentwicklungszyklus (SDLC) integriert haben, zeigen, dass mit diesem ganzheitlichen Sicherheitskonzept eine wesentliche Verbesserung erzielt werden kann. Um einen ähnlichen Fortschritt zu erreichen und die drohende Gefahr durch Hackerangriffe abzuwenden, ist das geplante Qualifizierungsseminar speziell auf die Sicherheitsanforderungen von CPPS im Industrieumfeld abgestimmt. Das Qualifizierungsseminar bietet den teilnehmenden Personen einen tiefen Einblick in die elementaren Inhalte des SDL-CPPS, die mittels Impulsvorträgen, Workshops und Präsentationen vermittelt werden. Der starke Praxisbezug sowie ein maßgeschneidertes Seminarkonzept steht bei der Gestaltung des Weiterbildungsprogramms im Vordergrund. Die Teilnehmerinnen und Teilnehmer sollen auf diese Weise optimal auf die Einführung des SDL-CPPS in ihrem Unternehmen vorbereitet werden und gegen die Cyber-Bedrohungen, veranlasst durch die umfassende Vernetzung im Zuge

von Industrie 4.0, gerüstet sein.

### **Projektkoordinator**

- Hochschule für Angewandte Wissenschaften St. Pölten GmbH

### **Projektpartner**

- Xylem - Science and Technology Management GmbH
- Commend International GmbH
- Neuron Engineering Tools GmbH
- Limes Security GmbH
- Ing. Punzenberger Copa-Data GmbH
- Software Quality Lab GmbH
- Trustworks GmbH in Liqu.