SHIFT

Sichere Simulationstechnologien für cyber-physische Systeme

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2020	**Status**	abgeschlossen
Projektstart	01.04.2022	**Projektende**	30.09.2024
Zeitraum	2022 - 2024	**Projektlaufzeit**	30 Monate
Keywords	Sicherheit, cyber-physische Systeme, Simulation, Training		

Projektbeschreibung

Cyber-physische Systeme (CPS) bezeichnen den Zusammenschluss und die Verbindung von softwaretechnischen mit mechanischen oder elektronischen Komponenten, die über eine Dateninfrastruktur kommunizieren. Aufgrund der Digitalisierung und Vernetzung sind Cybersicherheitsvorfälle leider keine Seltenheit mehr in CPS, wie beispielsweise Stuxnet oder WannaCry gezeigt haben. Beispiele für CPS sind unter anderem industrielle Steuerungsanlagen (ICS), aber auch in der Satellitennavigation, Airtraffic-Management, sowie in der Medizintechnik zu finden.
Technische Simulationsumgebungen können einen geschützten Raum bieten, um Cyberangriffe in CPS besser verstehen und vorbereiten zu können. In einer Simulationsumgebung können Konsequenzen von Cyberangriffen analysiert werden, neue Algorithmen zur Erkennung von Angriffen entwickelt und neue resilientere Architekturen für CPS entworfen werden. Zudem können diese Simulationsumgebungen auch für Schulungen und Vorfallsübungen herangezogen werden und zum langfristigen Aufbau von Wissen und Fähigkeiten von Personal beitragen. Die Herausforderung ist in der Umsetzung jedoch, dass viele Technologien für CPS kommerziell lizenziert werden und nur wenige quelloffene Lösungen zur Verfügung stehen. Dies und weitere Faktoren erschweren die Entwicklung von technischen Simulationsumgebungen und verhindern dadurch, dass ein gemeinsames Wissen im Aufbau und der Umsetzung von technischen Simulationsumgebungen für CPS erzeugt werden kann.
Das Projekt SHIFT zielt darauf ab sichere technische Simulationsumgebungen für CPS zu entwerfen und zu entwickeln. Es zielt dabei auf vier Hauptaspekte ab: (1) Die Konzeptionierung und Entwicklung von technischen Simulationsumgebungen für CPS wird in zwei Anwendungsgebieten, industrielle Steuerungsanlagen (ICS) und globale Navigationssatellitensysteme (GNSS) in CPSLabs, einer Laborumgebung für CPS, umgesetzt. (2) Die technische Simulation von Cyberangriffen in ICS und GNSS, die ermöglicht Konsequenzen von Angriffen zu untersuchen und Algorithmen zur Erkennung zu entwickeln. (3) Förderung und Entwicklung von digitalen Kompetenzen im Bereich CPS für verschiedene Zielgruppen (z.B. Behörden, Betreiber wesentlicher Dienste (BwD)) durch z.B. Schulungen oder die Integration in Ausbildungsschienen. (4) Die Einbindung der Benutzer in die Gestaltung und Evaluierung der CPSLabs anhand von Vorfallsübungen oder Schulungen, um eine möglichst hohe Akzeptanz zu erzielen.
SHIFT unterstützt durch die CPSLabs die Technologieentwicklung und -simulation in CPS, die unter anderem Kerntechnologien für BwDs sind. Die CPSLabs unterstützen die Verbesserung von Wissen und Fähigkeiten im Bereich ICS und

GNSS einzelner Mitarbeiter und tragen dadurch zur Robustheit von BwDs und anderen Organisationen in Österreich bei. Die Umsetzung von SHIFT ermöglicht eine verbesserte Vorbereitung gegen Cybervorfälle und ebnet den Weg zur Stärkung der Resilienz der BwDs und dadurch auch Österreichs bei.

Abstract

Cyber-physical systems (CPS) refer to the fusion and connection of software-technical components with mechanical or electronic components that communicate via a data infrastructure. Due to digitalisation and networking, cyber security incidents are unfortunately no longer a rarity in CPS, as Stuxnet or WannaCry, for example, have shown. Examples of CPS include industrial control systems, but also satellite systems, air traffic management and medical technology.
Technical simulation environments can provide a protected space to better understand and prepare for cyber-attacks in CPS. In a simulation environment, the consequences of cyber-attacks can be analysed, new algorithms for detecting attacks can be developed and new, more resilient architectures for CPS can be designed. In addition, these simulation environments can also be used for training and incident exercises and contribute to the long-term building of knowledge and skills of personnel. However, the challenge in implementation is that many technologies for CPS are commercially licensed and only a few open source solutions are available. This and other factors hinder the development of technical simulation environments and thus prevent the generation of shared knowledge in the construction and implementation of technical simulation environments for CPS.
The SHIFT project aims to design and develop safe technical simulation environments for CPS. It aims to address four main aspects: (1) The design and development of technical simulation environments for CPS will be implemented in two application areas, industrial control systems (ICS) and global navigation satellite systems (GNSS) in CPSLabs, a laboratory environment for CPS. (2) The technical simulation of cyber-attacks in ICS and GNSS, which allows to study consequences of attacks and to develop algorithms for detection. (3) Promotion and development of digital competences in the field of CPS for different target groups (e.g. authorities, operators of essential services (OeS)) through e.g. training courses or integration in in-house training tracks. (4) Involving users in the design and evaluation of the CPSLabs through cyber exercises or training to achieve the highest possible acceptance.
Through the CPSLabs, SHIFT supports technology development and simulation in CPS, which are core technologies for OeSs, among others. The CPSLabs support the improvement of knowledge and skills in ICS and GNSS of individual staff members and thereby contribute to the robustness of OeSs and other organisations in Austria. The implementation of SHIFT enables improved preparedness against cyber-attacks and paves the way to strengthening the resilience of OeSs and thereby also Austria.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Universität Wien
- IGASPIN GmbH
- Universität für Weiterbildung Krems
- Bundesministerium für Landesverteidigung
- LINZ NETZ GmbH
- VERBUND AG

- CERT.at GmbH