IHATEC
Innovative
Hafentechnologien

Bundesministerium
für Digitales
und Verkehr

AUTOSEC – Entwicklung und Erprobung von Maßnahmen zur Erhöhung der Sicherheit im digitalisierten Container-Terminalprozess und Implementierung von Schutzmaßnahmen zur Verhinderung und Erkennung von Cyberattacken in der Infrastruktur sowie beteiligten IT-Systemen

Motivation

Lösungen im Umfeld von Industrie 4.0 schaffen die Grundlagen für eine Erschließung großer Effizienzsteigerungspotenziale durch Automati-sierung, Vernetzung und Kommunikation realer Objekte mit virtuellen Systemen zur Planung, Steuerung und Regelung von Wertschöpfungs-systemen. Dies führt jedoch zu einer Vielzahl von Risiken, die einen Einfluss auf die Stabilität der Prozesse (Safety) und auf die IT-Sicherheit durch Cyber-Angriffe (Security) haben. Insbesondere im betrachteten Hafenumschlagsbereich existieren für Automatisierungsvorhaben und den hierfür erforderlichen Systemen und Datenaustausch keine Standards zur Sicherung gegen Cyber-Angriffe sowie zur Überwachung der Systemstabilität.

Projektziel

Das Vorhaben AUTOSEC zielt mit den genannten Projektpartnern aus Forschung, Entwicklung und Endanwender auf die Erhöhung der IT-Sicherheit in den Häfen und Logistikketten sowie die präventive Abwehr von Cyber-Angriffen auf IT-Systeme. Mit dem geplanten Vorhaben soll ein skalierbares Methoden- und Werkzeugset für die Konzeption und Einführung, sowie den Betrieb von Automatisierungsvorhaben in Häfen entwickelt und ebenfalls in Anwendungsfällen prototypisch bei einem See- (Hamburg, Wilhelmshaven) und einem Binnenhafen (Magdeburg) evaluiert werden.

Lösungsansatz

Die Grundlage für die zu entwickelnde Methode besteht in der Definition eines ganzheitlichen Prozessmodells für das Anforderungs- und Veränderungsmanagement sowie das Release und Test Management für alle Prozessbeteiligten. Der zu definierende Prozess muss ein transparentes und abgestimmtes Änderungsmanagement sicherstellen, um Störungen durch nicht abgestimmte Änderungen an Systemen oder Komponenten der Automatisierungslösungen zu verhindern bzw. im Störungsfall, diesen schnell zu erkennen und die Aufwände bei der Fehlersuche einzuschränken und zu minimieren. Zur Abbildung dieses Prozesses und zur nachvollziehbaren Dokumentation soll hierfür ein entsprechendes Werkzeug entwickelt werden, welches an realen Use Cases im EUROGATE Terminal sowie dessen Übertragbarkeit auf kleinere Binnenhäfen im Magdeburger Hafen erprobt und evaluiert wird.

Vorhaben

Zur Umsetzung wurde ein Methoden-Werkzeugset für die Konzeption und Einführung, sowie den Betrieb von Automatisierungsvorhaben in Häfen und in Anwendungsfällen evaluiert. Die Grundlage für die zu entwickelnde Methode besteht in der Definition eines ganzheitlichen Prozessmodells (Cybersecurity Risk Management Process Model) für das Anforderungs- und Veränderungsmanagement sowie das Release und Test Management für alle Prozessbeteiligten. An den EUROGATE-Terminals erfolgt die Prüfung von realen Automatisierungsmöglichkeiten zur Steigerung der Wettbewerbsfähigkeit und Sicherung des Unternehmens. Am Magdeburger Hafen wird überprüft, in wie weit eine Übertragung des Automatisierungskonzeptes mit der zu entwickelnden Methodik und dem Werkzeug für einen kleineren Binnenhafen möglich ist.

Ergebnis

Das Ziel der Partner war, durch die Erkenntnisse aus dem Forschungsprojekt AUTOSEC eine übergreifende Erhöhung der Cyber-Security und einen Standard gegen Cyber Angriffe für den Hafenumschlagsbereich aufzubauen. Zusammenfassend lässt sich feststellen, dass zunächst für cyber-physische Systeme aufgrund Ihrer Eigenschaften sich ergebende Risiken identifiziert und ebenfalls bewertet wurden, jedoch stellt neben der Risikoursachenanalyse auch die Identifikation und Bewer-

IHATEC
Innovative
Hafentechnologien

Bundesministerium
für Digitales
und Verkehr

tung weiterer Risiken eine bestehende Herausforderung für jede implementierte Lösung bestehend aus cyber-physischen Systemen dar. Die im Rahmen der Projektarbeit identifizierten Risiken und Risikoursachen stellen lediglich eine Grundlage dar, während systemspezifische Risiken und Ursachen einerseits systembezogen auf die jeweilige Implementierung sowie auch während des Lebenszyklus des implementierten Systems erfolgen muss. Dies ist insbesondere darin begründet, dass in Systemen immer neue Schwachstellen identifiziert werden. Diese müssen daher anschließend neu bewertet und in die Entwicklung von geeigneten Gegenmaßnahmen münden.

Verbundkoordinator
EUROGATE GmbH & Co. KGaA, KG, Bremen

Projektvolumen
1.490.647,19 €
(davon 66% Förderanteil durch BMVI)

Projektlaufzeit
08/2017 – 12/2020

Projektpartner
- Fraunhofer IFF, Magdeburg
- Magdeburger Hafen GmbH
- METOP GmbH

Ansprechpartner
TÜV Rheinland Consulting
Dr. Silke Marre
Tel.: +49 221 – 806 4174
E-Mail: Silke.Marre@de.tuv.com