FORSCHUNG KOMPAKT

Schutz vor Cyberattacken

Mehr IT-Sicherheit im Hafenterminal

Häfen zählen zu den kritischen Infrastrukturen, da Störungen und Ausfälle immense, nicht nur volkswirtschaftliche Auswirkungen haben können. Dabei sind die möglichen Sicherheitsrisiken vielfältig, insbesondere in digitalisierten Containerterminal-Prozessen, die durch Industrie 4.0 immer mehr an Bedeutung gewinnen. Ein neues Methoden- und Werkzeugset entwickelt von Forscherinnen und Forschern des Fraunhofer-Instituts für Fabrikbetrieb und -automatisierung IFF und seinen Industriepartnern ermöglicht die präventive Abwehr von Angriffen auf automatisierte cyberphysische Systeme und hilft, die Sicherheit entlang der gesamten Logistikkette inklusive der IT-Systemlandschaft zu erhöhen. Gleichzeitig lassen sich Automatisierungsvorhaben effizient planen und einführen.

Eine gut ausgebaute Hafeninfrastruktur ist Voraussetzung, um die Funktionen eines Seehafens zu erfüllen. Mit wenigen Ausnahmen transportieren heutzutage nach wie vor Menschen die Container in den Hafenterminals weltweit mit Fahrzeugen von A nach B. Diesen Prozess wollen die EUROGATE GmbH, die TRANSPORTWERK Magdeburger Hafen GmbH und METOP GmbH, Projektpartner des Fraunhofer IFF, automatisieren. Die Transporter sollen sich künftig beim Be- und Entladen zwischen Schiffen, Lkw und Zügen automatisiert bewegen. Damit werden sie zu cyberphysischen Systemen, die mithilfe von Sensoren auf ihre Umgebung reagieren und mit Aktoren ihre Position im Terminal erkennen und vorgegebene Fahraufträge automatisiert abarbeiten.

Cyberphysische Systeme – das könnten beispielsweise auch Gabelstapler oder Kräne sein – sind hochkomplexe softwaretechnische Systeme, die mit mechanischen und elektronischen Teilen interagieren und damit verschiedensten Risiken wie Hackerangriffen oder physischer Manipulation ausgesetzt sind. Zudem sind sie aufgrund ihrer Komplexität anfällig für systemimmanente Störungen, die die Stabilität beeinträchtigen. »Ein Software-Update auf einem der Fahrzeuge kann schon zu Versionskonflikten und Ausfällen führen. Aber auch Cyberattacken und Hackerangriffe werden in Deutschland zu einer zunehmenden Bedrohung für Hafenunternehmen«, weiß Tobias Kutzler, Wissenschaftler am Fraunhofer IFF in Magdeburg. In enger Zusammenarbeit mit den Projektpartnern etabliert er mit seinem Team und dem Projektpartner METOP GmbH im Verbundvorhaben AUTOSEC (siehe Kasten) Maßnahmen, um die Sicherheit der cyberphysischen Systeme und der IT-Infrastruktur zu erhöhen. Zunächst sollen diese für

Kontakt
Janis Eitner | Fraunhofer-Gesellschaft, München | Kommunikation | Telefon +49 89 1205-1333 | presse@zv.fraunhofer.de
René Maresch | Fraunhofer-Institut für Fabrikbetrieb und -automatisierung IFF | Telefon +49 391 4090-446 | Sandtorstraße 22 | 39106 Magdeburg | www.iff.fraunhofer.de | rene.maresch@iff.fraunhofer.de

die vom Verbundkoordinator EUROGATE betriebenen Hafenterminals umgesetzt werden. Geprüft wird zudem, ob sie sich auf den Magdeburger Binnenhafen, der über deutlich weniger IT-Ressourcen verfügt, übertragen und dort einführen lassen.

Digitaler Zwilling erhöht die Sicherheit und Resilienz kritischer Infrastrukturen

Neu entdeckte Fehler oder spezifische Angriffe können nie ausgeschlossen oder von vornherein komplett verhindert werden (Stabilitätsansatz). Das Ziel der Forscher ist es, einen Ansatz zu finden, der es einerseits erlaubt, auftretende Fehler oder Probleme automatisiert schnell zu erkennen und andererseits die Resilienz zu erhöhen (Resilienzansatz). Das Ziel muss es sein, nicht ein gesamtes System, sondern nur gestörte Teilkomponenten abschalten zu können und weiterhin auch eine schnelle Wiederinbetriebnahme des Gesamtsystems zu ermöglichen, indem die Fehlerursachen schnell ermittelt und auch behoben werden können. Dieser Ansatz lässt sich auf unterschiedlichste Logistikprozesse anwenden. »Mithilfe von Simulationen bauen wir einen Digitalen Zwilling des Hafens auf und gleichen die Prozesse der realen Hafeninfrastruktur permanent mit dem Digitalen Zwilling ab. Verhalten sich beide nicht identisch, liegt ein Problem vor«, erläutert Kutzler die Idee.

Drei-Stufen-Konzept: identifizieren, lokalisieren, beheben

Der Abgleich wird mit einem eigens entwickelten Methoden- und Werkzeugset realisiert, das auf einem Drei-Stufen-Konzept basiert: identifizieren, lokalisieren, beheben. Zunächst wird festgestellt, dass ein Fehler vorliegt. Dies erkennt die Software durch den Abgleich von zu überwachenden Leistungsparametern oder Kennzahlen. »Eine Störung erkennen wir beispielsweise daran, dass die Container nicht mehr in der vorgegebenen Geschwindigkeit bewegt werden«, sagt der Ingenieur. Im nächsten Schritt prüft die Software, wo im System der Fehler vorliegt und um welche Art von Problem es sich handelt. Hier gleicht die Software die überwachten Parameter hinsichtlich ihres historischen Verlaufs mit weiteren Kontextdaten unter Zuhilfenahme von Methoden des Data Mining miteinander ab, um Korrelationen zu erkennen und die Störung punktgenau zu identifizieren. Anschließend wird versucht, die Fehlerursache zu lokalisieren, um zu entscheiden, ob das gesamte System oder nur ein Teil (z.B. ein Fahrzeug) davon abgeschaltet werden muss. »Da es für die Automatisierung der Containerterminal-Prozesse und die Kontrolle der cyberphysischen Systeme bislang keine Standards gibt, fangen wir im Prinzip bei Null an«, so Kutzler. »Mit dem Digitalen Zwilling erhält man zusätzlich die Möglichkeit, die Inbetriebnahme eines Systems in der Simulation mit allen ›realen‹ IT-Komponenten und simulierter Hardware zu erproben und erst dann live zu gehen, wenn es einwandfrei funktioniert. Andererseits können wir mit der gleichen Verfahrensweise auch im Live-Betrieb gegen den Digitalen Zwilling testen. Dadurch sind wir in der Lage, Fehler schnell zu identifizieren, einzugrenzen und das betreffende System abzuschalten.«

In ersten Tests im Wilhelmshavener Hafenterminal und im Binnenhafen Magdeburg von Juli bis Ende September evaluieren die Projektpartner die Lösung prototypisch. In Wilhelmshaven werden zunächst die Position, Fahrtrichtung und Geschwindigkeit von bereits automatisierten Straddle Carrieren, die auf einem Testgelände im Rahmen des Projekts STRADEGY von EUROGATE entwickelt und getestet werden, überwacht. Das sind sehr komplexe Fahrzeuge, die die Container im Terminal umlagern und übereinander stapeln können. »Ein erfolgreicher Hackerangriff oder andere Manipulationen am Logistiksystem würden nicht nur unseren Partner EUROGATE schädigen, sie hätten auch Auswirkungen auf den Verkehr der jeweiligen Hafenstadt, da sich die abzufertigenden Lkws kilometerweit stauen würden«, sagt der Forscher. Die Dringlichkeit des AUTOSEC-Projekts hat der Hackerangriff im Jahr 2017 auf das dänische Unternehmen Maersk deutlich gemacht, das rund 20 Prozent des gesamten Welthandels in seinen Schiffscontainern transportiert. Der Schaden belief sich auf mehrere hundert Millionen Dollar.

Projekt AUTOSEC

AUTOSEC – Entwicklung und Erprobung von Maßnahmen zur Erhöhung der Sicherheit im digitalisierten Containerterminal-Prozess

Projektpartner:
- EUROGATE GmbH & Co. KGaA, Bremen
- Fraunhofer-Institut für Fabrikbetrieb und -automatisierung IFF, Magdeburg
- TRANSPORTWERK Magdeburger Hafen GmbH, Magdeburg
- METOP GmbH, Magdeburg

Förderhinweis:
Das Projekt AUTOSEC wird aus Mitteln des Förderprogramms IHATEC – Innovative Hafentechnologien des Bundesministeriums für Verkehr und digitale Infrastruktur gefördert.

Projektlaufzeit:
8/2017 bis 12/2020

Abb. 1 Automatisierte Straddle Carrier im Containerterminal in Wilhelmshaven – effizient und sicher.

© EUROGATE

Abb. 2 Auch im Magdeburger Hafen werden in der Zukunft Automatisierungslösungen Einzug halten.

© Fraunhofer IFF