Projektträger für das

Bundesministerium
für Verkehr und
digitale Infrastruktur

TÜVRheinland®
Genau. Richtig.

TRANSPORTWERK MAGDEBURGER HAFEN GMBH

AUTOSEC – ABSCHLUSSBERICHT

Förderkennzeichen: 19H17006B

Vorhabensbezeichnung: 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

Zuwendungsempfänger: TRANSPORTWERK Magdeburger Hafen GmbH

Autor: Felix Montag

Inhalt

1 Schlussbericht Teil I 3

1.1 Aufgabenstellung 3
1.2 Voraussetzungen und Durchführungen des Vorhabens 4
1.3 Planung und Ablauf des Vorhabens 5
1.4 Stand der Wissenschaft und Technik 6
1.5 Zusammenarbeit mit anderen Stellen 8

2 Schlussbericht Teil II 10

2.1 Verwendung der Zuwendung und des erzielten Ergebnisses im Einzelnen, mit Gegenüberstellung der vorgegebenen Ziele 10
2.1.1 Arbeitspaket 1 Anforderungsanalyse 10
2.1.2 Arbeitspaket 2.1 – Gesamtarchitektur und Konzepte 11
2.1.3 Arbeitspaket 2.2 – Organisationsmodell und Prozessvorgaben 12
2.1.4 Arbeitspaket 3 – Entwicklung eines Prozessmodells 14
2.1.5 Arbeitspaket 4 – Integration 14
2.1.6 Arbeitspaket 5.2 – Anwendungsfälle und Evaluierung: Use Case Binnenhäfen (Hafen MD) 15

2.2 Wichtige Positionen des zahlenmäßigen Nachweises 16
2.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit 17
2.4 Voraussichtlicher Nutzen, insbesondere Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplans 17
2.5 F&E-Ergebnisse von dritter Seite, die für die Durchführung des Vorhabens relevant sind 17
2.6 Veröffentlichungen 18

3 Literaturverzeichnis 19

1 Schlussbericht Teil I

1.1 Aufgabenstellung

In der Vision der Industrie 4.0 erfolgt eine Vernetzung und Kommunikation der realen Objekte mit den virtuellen Systemen zur Planung, Steuerung und Regelung von Wertschöpfungssystemen (vgl. [1] S. 14). Automatisierte Lösungen im Sinne von Industrie 4.0 steigern zwar die Wettbewerbsfähigkeit von Unternehmen und Infrastrukturbetreibern, stellen sie jedoch vor neue Herausforderungen. Die Fähigkeit, digitale Daten zu verarbeiten, zu speichern und darauf basierende Entscheidungen zu treffen, wird für Unternehmen immer wichtiger. Digitale Vernetzung und ein hoher Grad an Automatisierung führen zu neuen in den Bereichen *Safety* (stabile Prozesse durch ausgereifte Technologie) und *Security* (IT-Sicherheit gegen Cyberangriffe). Da immer mehr Hafeninfrastrukturen als kritische Infrastrukturen eingestuft werden und einen wesentlichen Beitrag zur gesamten Volkswirtschaft leisten, kommt ihnen dabei als Betreibern und Logistikdienstleistern eine wichtige Rolle zu. Höchstmaß an Zuverlässigkeit und Schnelligkeit müssen in reibungslosen Prozessen gewährleistet sein, um die Logistikketten zu schützen und die Wettbewerbsfähigkeit sicherzustellen. Da immer mehr cyber-physische Systeme zur Unterstützung und Erledigung logistischer Aufgaben eingesetzt werden, spielen sie in der Automatisierung zunehmend eine entscheidende Rolle.
Gegenwärtige Standards zum geschützten Datenaustausch gegen Cyberangriffe oder zur Überwachung der gesamten Prozesskette sind für automatisierte Lösungen in kritischen Infrastrukturen sind noch nicht ausgereift. In der Regel werden Netzwerk- oder Angriffserkennungslösungen oder heuristische Methoden verwendet, um Sicherheitsaspekte zu erkennen. Darüber hinaus gibt es keine Ansätze oder Werkzeuge zur Identifikation und Beurteilung potenzieller Bedrohungen von Automatisierungslösungen vor dem Hintergrund der Industrie 4.0. Bestehende Ansätze aus dem Bereich Risikomanagement und IT-Sicherheitsforschung decken nur Teilgebiete ab, jedoch nicht ganze Logistiksysteme und im Allgemeinen auch nicht cyber-physischer Systeme. Darüber hinaus fehlen Möglichkeiten der Skalierung zwischen großen See- und kleineren Binnenhäfen bei der Konzeption.

Das vorliegende Forschungsvorhaben adressiert daher den Schwerpunkt: „Verbesserung der IT-Sicherheit“. Das Vorhaben AUTOSEC zielt auf die Erhöhung der IT-Sicherheit in den Häfen und Logistikketten und die präventive Abwehr von Cyber-Angriffen auf die IT-Systeme. Damit werden zentrale Punkte aus dem Nationalen Hafenkonzept 2015 aufgenommen (Maßnahmen 1.12 “Digitale Infrastruktur verbessern”; 6.2 “IT in den Häfen und den Logistikketten schützen”). Grundsätzlich betont das Nationale Hafenkonzept die hohe Bedeutung der digitalen Infrastruktur und IT für die deutschen Seehäfen. Aufgrund der mit dieser Entwicklung einhergehenden Risiken, fordert das Nationale Hafenkonzept konkrete Weiterentwicklungen im Bereich Sicherheit und Gefahrenabwehr.

Im Vorhaben wird ein skalierbares Methoden- und Werkzeugset für die Konzeption von Automatisierungsvorhaben in Häfen entwickelt sowie ein neuer Ansatz speziell für cyber-physische Systeme in Automatisierungsvorhaben vorgestellt. In einem Seehafen (Hamburg, Wilhelmshaven) und einem Binnenhafen (Magdeburg) wird das Vorhaben prototypisch evaluiert. Dafür werden folgende Anwendungsfälle als Ausgangsbasis genutzt: 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. Die Ergebnisse der Evaluierung fließen in die Entwicklung von Methode und Werkzeug zurück.
Der definierte Prozess muss ein transparentes Änderungsmanagement gewährleisten, um Störungen durch unkoordinierte Änderungen an Systemen und Komponenten zu vermeiden und die Fehlerbehebung bei Störungen einzugrenzen. Spezifikationen für die Überwachung der Sicherheit und des Systemzustands im End-to-End-Betrieb müssen auch für die beteiligten IT-Systeme definiert werden. Neben der konkreten technischen Definition von Automatisierungsspezifikationen müssen auch externe Einflüsse auf das System identifiziert und deren Bedrohungspotential bewertet werden. Bei der Bewertung von Gegenmaßnahmen müssen sowohl quantitative als auch qualitative Variablen berücksichtigt werden.

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 (Lieferanten von Geräten, Automatisierungskomponenten, Software). Der zu definierende Prozess muss ein transparentes, abgestimmtes Änderungsmanagement sicherstellen, um Störungen durch unabgestimmte Änderungen an Systemen/Komponenten des Automatisierungskonzeptes zu verhindern bzw. im Störungsfall die Fehlersuche einzuschränken. Ein entsprechendes IT-Werkzeug zur Abbildung dieses Prozesses und zur nachvollziehbaren Dokumentation1 soll daher entwickelt werden. Dazu sind Vorgaben für prozessbeteiligte Lieferanten von Automatisierungskomponenten zu definieren, die einen Mindestschutz vor Störungen jeglicher Art definieren. Für beteiligte IT-Systeme sind ebenfalls Anforderungen an die Security sowie das Monitoring von Systemzuständen im End-to-End-Betrieb zu definieren. Neben der konkreten technischen Ausgestaltung des Automatisierungskonzeptes sind jedoch auch systemexterne Einflüsse zu identifizieren und auf ihr Bedrohungspotenzial hin zu bewerten. Die Methode und das Werkzeug sollen neben der Analyse auch die Erarbeitung von Gegenmaßnahmen und deren letztendliche Auswahl und Nachverfolgung unterstützen. Bei der Bewertung der Gegenmaßnahmen sind sowohl quantifizierbare (z.B. Kosten) als auch qualitative Größen (z.B. Risikominimierung) zu berücksichtigen.

1.2 Voraussetzungen und Durchführungen des Vorhabens

Die Voraussetzungen für die Durchführung des Vorhabens sind einerseits durch die mit Beantragung dargestellte Motivation der Umsetzung der Projektidee (Erhöhung der IT-Sicherheit in Häfen und deren Logistikketten sowie die präventive Abwehr von Cyber-Angriffen auf IT-Systeme) und andererseits durch die bestehenden Kompetenzen bei den Projektpartnern zur Realisierung des Vorhabens gegeben.

Der Magdeburger Hafen verfügt einerseits durch die Beteiligung an vorangegangenen Forschungsvorhaben über eine Vielzahl an innovativen Lösungen im Logistikbereich und ist gleichzeitig Teil des Galileo Testcenter

[1] Hierbei wird auf Basis des Dokumentationsprototypens des BMBF-Projektes „sprintDoc“ (siehe www.sprintdoc.de) aufgesetzt und eine Weiterentwicklung für den vorliegenden Anwendungsfall vorgenommen. In sprintDoc wird ein Dokumentationswerkzeug für die agile Softwareentwicklung entwickelt, eine Anpassung an die Konzeption und Dokumentation von Automatisierungslösungen für Industrie 4.0 erscheint jedoch notwendig. Die Otto-von-Guericke-Universität (OVGU) Magdeburg zu der seitens Fraunhofer IFF und METOP (An-Institut der OVGU) enge Beziehungen bestehen, ist in das sprintDoc-Projekt eingebunden.

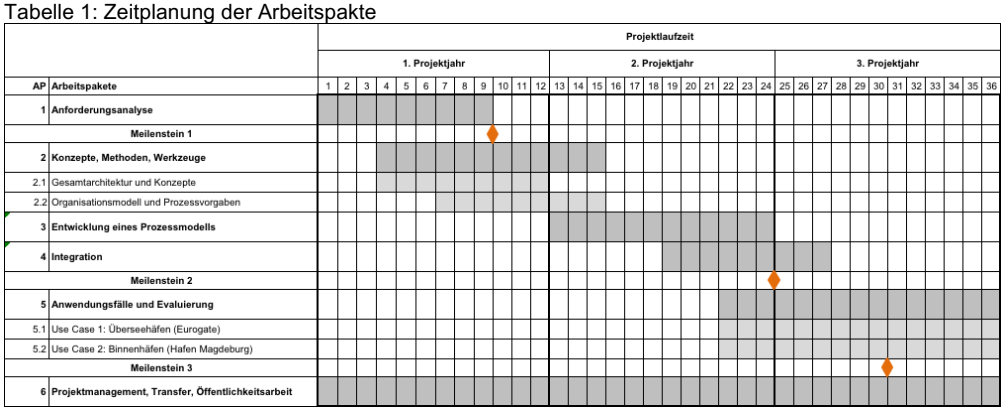
Sachsen-Anhalt der Otto-von-Guericke-Universität Magdeburg, welches über eine Vielzahl moderner Technologien im Logistikbereich wie Ortungs- und Identifikationslösungen verfügt. Der Magdeburger Hafen konnte somit einerseits seine Expertise und Anforderungen an moderne Logistiklösungen sowie andererseits die zur Verfügung stehende Ausstattung in das Vorhaben einbringen.

1.3 Planung und Ablauf des Vorhabens

Basierend auf den geplanten Leistungsinhalten der einzelnen Arbeitspakete ist eine zeitliche Verteilung der Arbeiten vorgenommen worden, die in Tabelle 1 dargestellt ist. Für die Grobeinschätzung der Entwicklung und Erarbeitung von methodischen Ansätzen zur Erhöhung der IT-Sicherheit in den Häfen und Logistikketten sowie die präventive Abwehr von Cyber-Angriffen auf IT-Systeme sowie der Aufbau und die Evaluierung eines Demonstrators, um die spezifisch für cyber-physische System erarbeiteten Konzepte und Methoden zur Anwendung zu bringen und die angestrebte horizontale und vertikale Übertragbarkeit der Ansätze zu überprüfen.

Dem Aufwand entsprechend ist die Anzahl der Mannmonate bereits sehr wirtschaftlich kalkuliert. Für die Durchführung der in den Arbeitspaketen beschriebenen Leistungsinhalte sind die im Teilantrag kalkulierten Aufwände erforderlich.

Tabelle 1: Zeitplanung der Arbeitspakte

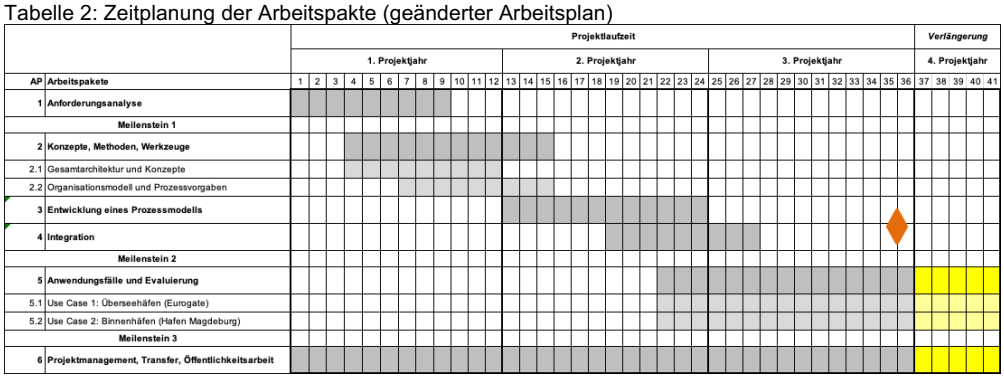


Das Projekt orientiert sich am Vorgehensmodell für Forschungs- und Entwicklungsprojekte und untergliedert sich in den beschriebenen Arbeitspakete. Der Projektstart war der 01. April 2017 bei einer Laufzeit von 36 Monaten Laufzeit. Die einzelnen Arbeitspakete des Gesamtprojekts gliedern sich in zeitlicher Hinsicht wie in Tabelle 1 dargestellt.

Mit Bewilligung ist die Laufzeit des Vorhabens auf 01.08.2017 bis 31.07.2020 festgesetzt worden. Mit Antrag einer kostenneutralen Verlängerung durch alle Projektpartner ist das Projekt um weitere 5 Monate bis zum 31.12.2020 verlängert worden. Der sich hieraus ergebende geänderte Arbeitsplan ist in Tabelle 2 dargestellt.

Das das Projekt kostenneutral verlängert wurde, ist keine Anpassung der Gesamtkosten sowie Kalkulation erforderlich.

Tabelle 2: Zeitplanung der Arbeitspakte (geänderter Arbeitsplan)



1.4 Stand der Wissenschaft und Technik

Das Szenario Software Lifecycle Management umfasst die Verwaltung von Softwareprodukten und in realen kundenspezifischen Systemlandschaften. Organisationen müssen die Systemlandschaften verwalten, indem sie Implementierungsaufgaben durchführen, wie z.B. Änderungen planen, neue Systeme aufbauen, bestehende Systeme kopieren oder die Erstellung und Verteilung von Änderungen in die Systemlandschaft unterstützen.
Aufgrund der Komplexität der heutigen Systemlandschaften und deren Abhängigkeiten zwischen einzelnen Softwarekomponenten, ist die Unterstützung durch Prozessvorgaben und Toolchains für Systemlandschafts-relevante Planungs-, Monitoring-, Wartungs-, Implementierungs- und Aktualisierungsaufgaben unerlässlich. In Szenarien mit starken Sicherheitsbezug kommen Security und Safety Anforderungen hinzu, welche nicht nur Prozessvorgaben und Testszenarien, sondern auch Implementierungs- und Umsetzungsrichtlinien für Soft- und Hardwaresysteme münden ([2] S. 125-134).
Ausgehend von der initialen Integration der beteiligten Komponenten und Systeme bei Eurogate muss anschließend eine für alle Lieferanten und Service Provider bindendes Software Lifecycle Management eingeführt werden. Dabei ist die Bereiche Governance, Development und Operations abzuklären. Allgemein wird diese Betrachtungsweise auch Applikation Lifecycle Management genannt [3].

Der Industrie 4.0 Digitalisierungskontext führt weiterhin zu einer Ausdehnung auf die gesamte Wertschöpfungskette. Die bisher übliche Trennung in Anwendungsbereiche PLM, digitale Fabrik, MES, ERP verhindert die effiziente Nutzung der Digitalisierung im Sinne einer höheren Produktivität. Eine vollständige Integration aller Systeme ist daher einer Grundvoraussetzung [4, 5].
Übergeordnet wird in der Wissenschaft auch noch das Thema System Lifecycle Management (SysLM) betrachtet [6] Dieses Thema soll aber keinen Schwerpunkt des Forschungsvorhabens bilden.
Wissenschaftliche Grundlagen für dieses Vorhaben bilden:

- Security By Design Konzepte,
- System Entwicklungsmodelle und
- Architekturen zur Laufzeitverifikation

Die Folgenden Abbildungen des NIST [6] und [7]zeigt, das Security By Design großen Einfluss auf die Reduktion der Entwicklungskosten hat.

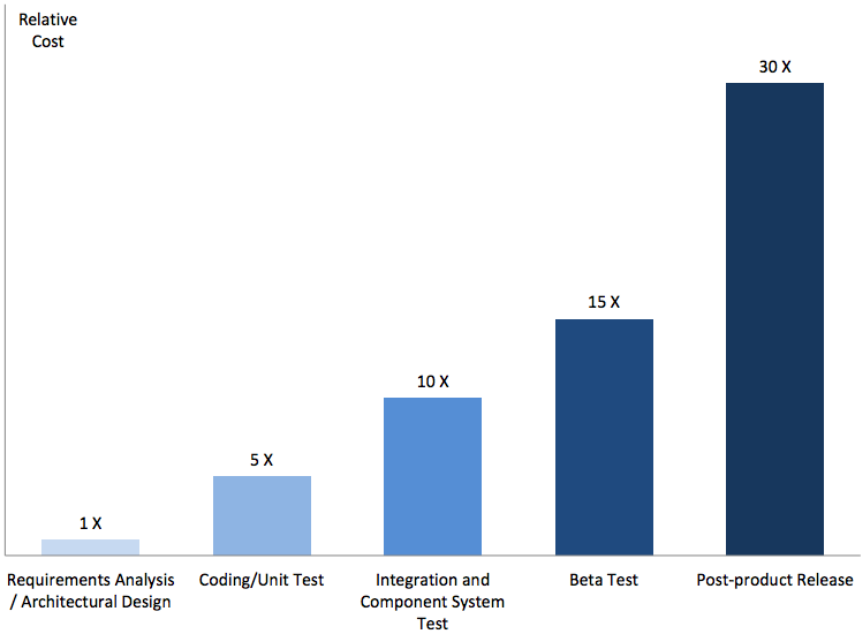


Abbildung 1: relative Kosten zur Behebung von Fehlern in verschiedenen Phasen im Softwarelebenszyklus

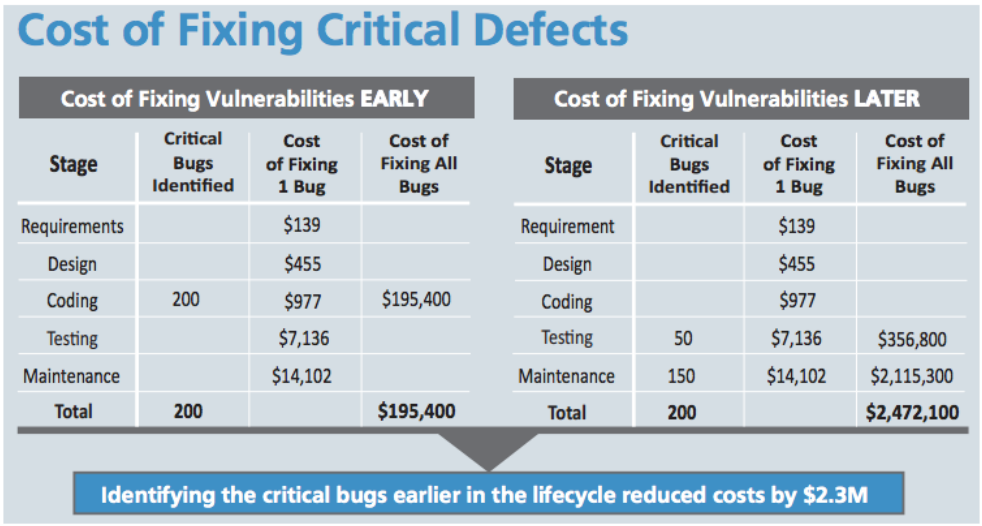


Abbildung 2: Kosten bei der Behebung von kritischen Fehlern in verschiedenen Phasen

In [30] wird der Bedarf von Security by Design bei verteilter Entwicklung und Integration durch entsprechende Vorgaben für Entwicklung und Integration von Systemen beschrieben. Sicherheitsfragen werden bei der heutigen Entwicklung oder Integration von Anwendungssoftware und Hardware entweder überhaupt nicht oder nur unzureichend betrachtet, so dass durch Softwareanwendungen immer wieder neue Ansatzpunkte für Angriffe entstehen. So wird die Sicherheit von Systemen neben der Funktionalität für Anwender und Hersteller immer wichtiger. Die Anwendung neuer praktischer Methoden und das systematische Befolgen von Sicherheitsprozessen sollen Hersteller und Integratoren von Systemen bei der Vermeidung von Sicherheitslücken unterstützen. Die Verbesserung von Entwicklungs- und Sicherheitsprozessen bietet Herstellern auch die Möglichkeit, bei verbesserten Sicherheitseigenschaften Kosten und Entwicklungszeiten von

Systemen zu reduzieren. Folgende Punkte sind dabei aus wissenschaftlicher Sicht relevant und bilden damit das Grundgerüst:

- Standardisierung von wertschöpfungskettenumfassenden Sicherheitsprozessen
- Governance Rahmenframework
- Sicherheit bei der Integration
- Zusicherungen mittels Sicherheitsprozessen

Die Studien und [8] eignen sich für den systematischen Einsatz von Sicherheitsprozessen, die Sicherheit der Systeme signifikant verbessern wurden.
In der Softwareentwicklung sind verschiedenste Software Entwicklungsmodelle und Vorgehensweisen (Paradigmen) für verteilte Entwicklung betrachtet worden. In [9] und [10] wird ein guter Überblick gegeben von Wasserfall-Modell, über V-Modell bis zur agilen Entwicklung.
Interessant für dieses Vorhaben sind aus wissenschaftlicher Sicht Ansätze aus dem DevOps Bereich [11] [12], da diese Ansätze insbesondere das Zusammenspiel aus Entwicklung und Betrieb neu interpretieren. Insbesondere bei der Laufzeitverifikation ist ein gutes Zusammenarbeiten von Betrieb und Entwicklung unumgänglich [35], um die Qualitäts- und Sicherheitsanforderungen nicht zu gefährden.
Grundlage für das Architektur-Framework entsprechender Systeme bilden die Arbeiten von Edward Lee [13] sowie [14], [15] und [16]. Diese Arbeiten widmen sich der Beurteilung von Architekturen im Umfeld von Cyber Physischen Systemen und Service Orientierten Architekturen (SOA). Besonderes Interesse liegt dabei in der Laufzeitverifikation der entsprechenden Systeme.

1.5 Zusammenarbeit mit anderen Stellen

Das Teilvorhaben des Magdeburger Hafens ist in enger Abstimmung mit allen beteiligten Projekpartnern des Gesamtvorhabens AUTOSEC bearbeitet worden.

Im Arbeitspaket 1 sind den Konsortialpartnern METOP und Fraunhofer IFF die Anforderungen eines Binnenhafens zur Verfügung gestellt und mit ihnen gemeinsam definiert worden. Der Magdeburger Hafen hat ebenfalls die Analyse und Bewertung der aufgenommenen Anforderungen sowie im Rahmen der Risikoanalyse der Bedrohungsszenarien begleitet.

Im Arbeitspaket 2 hat der Magdeburger Hafen an der Erarbeitung der Gesamtarchitektur, die von METOP und Fraunhofer IFF koordiniert wurde, mitgewirkt und bezüglich des Organisationsmodells und Prozessvorgaben einerseits eigene Anforderungen eingebracht und andererseits bereits intern Projektergebnisse evaluiert.

Im Arbeitspaket 3 hat der Magdeburger Hafen an der Erarbeitung des Prozessmodells und insbesondere an der Erweiterung des NIST Framework for Cyber Security mitgewirkt und neben der Definition der Anforderungen an das Prozessmodell auch die Untersetzung der zum NIST Framework ergänzten Kategorien und Subkategorien begleitet.

Im Arbeitspaket 4 hat der Magdeburger Hafen automatisierbare Integrations- und Auslieferungsprozesse identifiziert und bewertet. Auf der Grundlage der erarbeiteten Rollenmodelle ist gemeinsam mit den Partner METOP und Fraunhofer IFF eine Bewertung hinsichtlich des geeigneten Rollenmodells für den Magdeburger Hafen vorgenommen worden.

Das Arbeitspaket 5.1 ist in Zusammenarbeit mit dem Fraunhofer IFF vorgenommen worden. Einerseits ist eine praktische Evaluierung der erarbeiteten Systemarchitektur unter Nutzung der kamerabasierten Fahrzeugortung erfolgt und andererseits gemeinsam mit METOP und Fraunhofer IFF Strategien zur Einführung sicherer Automatisierungslösungen evaluiert worden.

2 Schlussbericht Teil II

2.1 Verwendung der Zuwendung und des erzielten Ergebnisses im Einzelnen, mit Gegenüberstellung der vorgegebenen Ziele

2.1.1 Arbeitspaket 1 Anforderungsanalyse

Im Arbeitspaket wurden durch die **TRANS*PORT*WERK** Magdeburger Hafen GmbH (TMHG) die nachfolgenden Teilaufgaben bearbeitet. Zur Darstellung des aktuellen Entwicklungsstands erfolgt eine kurze Darstellung der wesentlichen Ergebnisse.

- Bereitstellung von relevanten Daten und Informationen zur Erstellung der Systemübersicht und Bewertung und Betrachtung der relevanten Systemkomponenten
- Identifikation und Definition von Teilsystemen
- Risikoanalyse
- Aufstellung Anforderungskatalog je Systemkomponente

Zu Beginn des Projektes sind bei der TMHG die existierende Ausstattung, bestehend aus technischen Anlagen und Maschinen sowie die für die operative Planung und Steuerung eingesetzten IT-Systeme und ihre Teilsysteme, ermittelt und dokumentiert worden. Für sämtliche Systeme wurden die jeweiligen Funktionen und Schnittstellen untereinander oder zu anderen Systemen erfasst.
Für die hierbei identifizierten Systeme besteht aktuell ein sehr niedriger Grad an IT-Ausstattung und Durchdringung durch informationstechnische und Automatisierungs-Lösungen. Vorrangig erfolgt die Nutzung von Office-IT in Form eines Excel-basierten Lagermanagements sowie dem Einsatz von SAP für HR, Finanzen und Controlling. Wesentliche Besonderheit der TMHG und Unterschied zum Projektpartner EUROGATE der TMHG ist der Warenumschlag und lagerung unterschiedlicher Produkte (Stück- und Schüttgüter). Vorrangige Aufgabe der TMHG ist dabei die räumliche und zeitliche Vorausplanung bezüglich der zur Verfügung stehenden Ressourcenkapazitäten sowie insbesondere die Einhaltung gesetzlicher Bestimmungen (BImSchG).
Trotz des vergleichsweise geringen Grades an IT-Nutzung und Automatisierung besteht ein Automatisierungspotenzial in verschiedenen Bereichen, aus denen sich Auswirkungen und Risiken ergeben, die gemeinsam mit bereits bestehenden Risiken der schon eingesetzten Systeme dokumentiert worden. Die Risikoanalyse beinhaltete ebenfalls eine Klassifizierung der identifizierten Risiken hinsichtlich der sich ergebenden Auswirkungen (keine Auswirkung, Teilausfall oder Totalausfall) als Grundlage für die Erarbeitung von Bedrohungsszenarien.

Die Infrastruktur lässt sich wie folgt zusammenfassen:

- Glasfaserkabel verbinden alle Terminals und die Hafenverwaltung. Somit haben alle Standorte und Arbeitsplätze eine Verbindung zum unternehmensinternen Netzwerk
- Ergänzend existieren für Mitarbeiter in den Docks, der trimodalen Frachtabwicklung sowie zwischen den Mitarbeitern am Dock und der Verwaltung funkbasierte Kommunikationslösungen
- Viele Terminalstandorte sind mit moderner Videoüberwachung ausgestattet
- In Zusammenarbeit mit dem Galileo Testfeld der Otto-von-Guericke-Universität Magdeburg werden im Hanse-Terminal Prozessmonitoring-Lösungen betrieben, auf deren Basis Forschung und Entwicklung moderner

Prozessmonitoring-Funktionalitäten in einer produktiven Umgebung betrieben und getestet wird
- Office-Anwendungen werden in verschiedenen operativen Tätigkeiten genutzt:
  - Logistik und Betriebsführung
  - Immobilienmanagement
  - Betrieb der Hafenbahn
- Spezielle datenbankbasierte Anwendungen werden zur Unterstützung der Hafenverwaltung genutzt
- Anwendungsspezifische Management-Lösungen, die jedoch nicht in-House sondern extern betrieben werden
- Frachtverwaltung (primär gestützt durch Office-Tools oder unternehmensspezifischer Datenbankanwendung)
- Instandhaltungsmanagementsystem zur Verwaltung der Anlagen, Infrastruktur und Betriebsmittel
- Verkehrsmanagementsystem zur Verwaltung ein- und abgehender Schiffe. Diese Lösung arbeitet autonom und bietet einen Überblick über den Wasserstraßenverkehr innerhalb des Hafengebiets
- Nutzung von SAP-Komponenten für das unternehmensinterne Controlling: Finanzen, Personal und andere unternehmensinterne Belange

Die TMHG hat gemeinsam mit den anderen Konsortialpartnern auf der Grundlage der eigenen IT-Infrastruktur die sich hierdurch ergebenden Risiken in die Risikoanalyse mit eingebracht. Unter anderem sind neben IT-spezifischen und automatisierungsspezifischen Risiken ebenfalls Risikofaktoren aus logistischer Sicht in die Betrachtungen eingeflossen, da diese Faktoren aufgrund ihrer physischen Ausprägungen und Wechselwirkungen ebenfalls eine wesentliche Rolle in der Risikobewertung cyberphysischer Systeme spielen.
Trotz des vergleichsweise geringen Grades an IT-Nutzung und Automatisierung besteht ein Automatisierungspotenzial in verschiedenen Bereichen, aus denen sich Auswirkungen und Risiken ergeben, die gemeinsam mit bereits bestehenden Risiken der schon eingesetzten Systeme dokumentiert worden. Die Risikoanalyse beinhaltete ebenfalls eine Klassifizierung der identifizierten Risiken hinsichtlich der sich ergebenden Auswirkungen (keine Auswirkung, Teilausfall oder Totalausfall) als Grundlage für die Erarbeitung von Bedrohungsszenarien.
Die Bearbeitung der Teilaufgabe „Aufstellung Anforderungskatalog je Systemkomponente“ hat sich primär an der Analyse von Anforderungen für die funktionale Sicherheit von Produktions- und Automatisierungslösungen im Hafenumfeld orientiert. Hierzu sind zunächst typische Anforderungen für CPPS (cyberphysische Produktionssysteme) hinsichtlich Ihrer Eignung für die Anwendung in cyberphysischen Logistiksystemen (CPLS) analysiert worden, deren Anwendung sich auf Systeme, Assistenzsysteme und Anwendungen in logistischen Prozessen zur Erfüllung von Zielen und Aufgaben des Logistikmanagements[1] fokussiert. Wesentlich hierbei ist die Erkenntnis, dass aufgrund der Grundcharakterisitik von cyber-physischen Systemen, dass sie IT-Komponenten und physische Komponenten vereinen und mittels Sensorik und Aktorik
Im Berichtszeitraum sind die Arbeiten des AP1 abschließend bearbeitet und deren Ergebnisse erfasst worden, sodass diese für die weitere Projektarbeit und dem gesamten Projektkonsortium zur Verfügung stehen.

2.1.2 Arbeitspaket 2.1 – Gesamtarchitektur und Konzepte

Im Arbeitspaket wurde durch die **TRANS*PORT*WERK** Magdeburger Hafen GmbH (TMHG) die Teilaufgabe „Analyse der Architekturen“ bearbeitet. Die TMHG hat hier

[1] (Roy, 2017)

primär relevante Architekturen von Logistiksystemen, die cyberphysische Komponenten nutzen, analysiert und hinsichtlich der Anwendbarkeit und Realisierbarkeit untersucht. Der Fokus lag hier bei Lösungen für die Logistik, die zum Tracking, der Identifikation und dem Transport (autonome Transportlösungen) genutzt werden können. Insbesondere sind die auf Kommunikationsebene (Netzwerk, Datenaustausch, Schnittstellen) bestehenden Architekturen und Anforderungen untersucht worden. Hierbei wurde geprüft, welche Anforderungen die TMHG heute schon erfüllen kann. Es wurde festgestellt, dass zwar bereits moderne Kommunikationsinfrastrukturen (Glasfaser, Funk/Mobilfunk (LTE)) und verteilte Systeme (externe Cloud-basierte Management-Lösungen) im Einsatz sind, diese jedoch zusätzlich abgesichert werden müssen – insbesondere da eben durch die physischen Komponenten bzw. Bestandteile (zur Ergänzung zu einem cyberphysischen System) zusätzliche Aspekte in die Betrachtung einfließen müssen. Hier können die ebenfalls die Erkenntnisse bzw. vorliegenden Datengrundlagen aus dem Instandhaltungsmanagement-System der TMHG genutzt werden.

2.1.3 Arbeitspaket 2.2 – Organisationsmodell und Prozessvorgaben

Im Arbeitspaket wurde durch die **TRANS*PORT*WERK** Magdeburger Hafen GmbH (TMHG) die Teilaufgabe „Erstellung von Prozessvorgaben (Rahmenrichtlinie) zur Integration der einzelnen Softwarelebenszyklen“ bearbeitet.
Zur Automatisierung von Prozessen zwischen Softwareentwicklern und IT-Teams hat sich der DevOps-Ansatz (Development (Dev) und IT-Operations (Ops) etabliert, der eine erheblich schnellere, zuverlässigere Entwicklung, Test und Freigabe von IT-Systemen ermöglicht. Die acht Phasen des DevOps sind wie in Abbildung 3 dargestellt:

- Plan
- Build
- Continuous Integration
- Deploy
- Operate
- Continuous Feedback

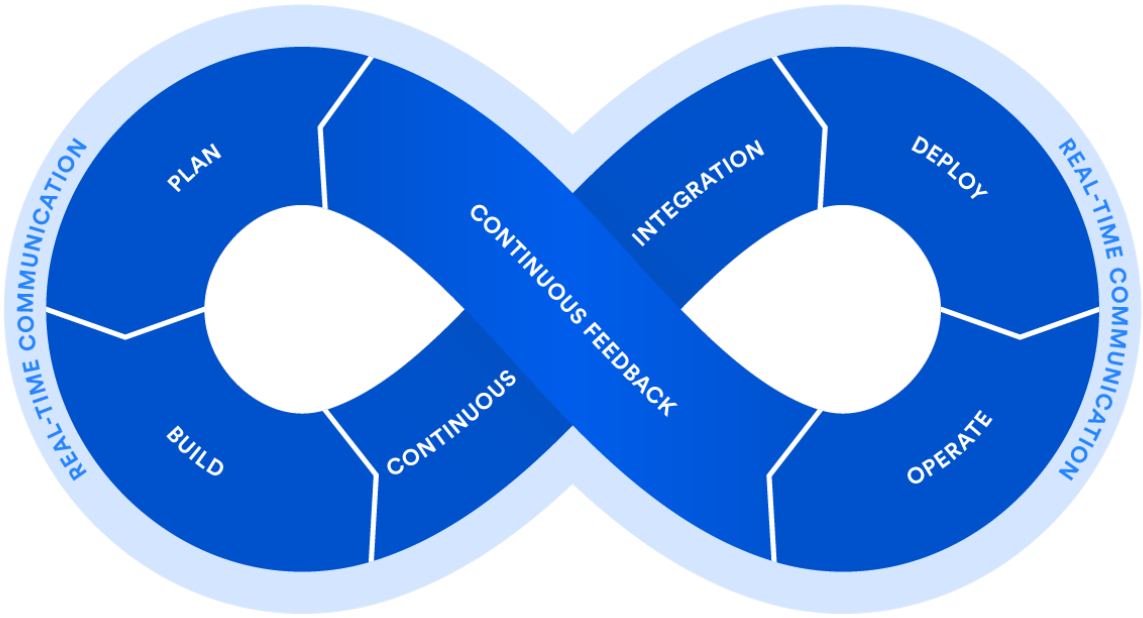
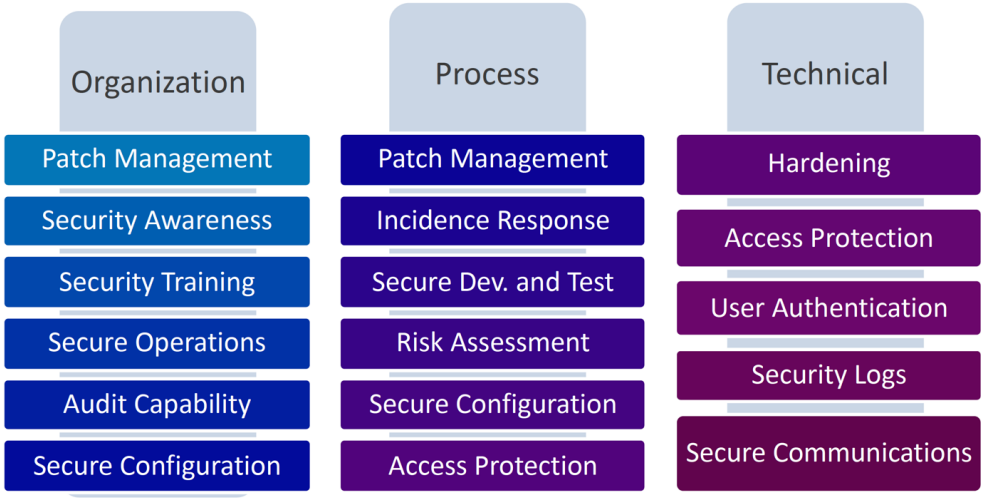


Abbildung 3 - DevOps-Ansatz und dessen Phasen (Quelle: https://de.atlassian.com/devops)

Da die TMHG als Infrastruktur- und Systembetreiber keinerlei Entwicklungskapazitäten vorhält und dies auch nicht vorsieht, sind die Phasen, die auf die Entwicklung abzielen, durch die TMHG nicht selbst abzubilden. Hier ist es erforderlich, dass entweder Systemlieferanten oder -entwickler diese Rolle übernehmen. Die TMHG kann daher nur Aufgaben übernehmen, die dem Operations-Teil zugeordnet werden können. Hierbei entstehen jedoch Besonderheiten und Herausforderungen, die insbesondere bei der Einführung cyberphysischer Systeme sowie deren Absicherung zu beachten sind.
Zunächst gilt es zu klären, wie Fehler festgestellt werden können oder darauf reagiert werden kann oder muss, wenn die TMHG nur Betreiber und nicht Entwickler ist und daher Wissen über die jeweils zugrundeliegenden Architekturen und Systembestandteile nicht bestehen. Es ist somit erforderlich zwischen Systementwickler bzw. -lieferant und dem Systembetreiber (in diesem Fall der TMHG) entsprechende Vereinbarungen zu treffen und Prozesse zu etablieren, die eine integrierte Umsetzung des DevOps-Ansatzes ermöglichen.
Gemeinsam mit den Partnern des Projektkonsortiums wurden hierzu entsprechende Normen und Standards untersucht und aus diesen die erforderlichen Tätigkeiten zur Sicherung cyber-physischer Systeme abgeleitet und gegliedert.



Es ist daher elementar, bei der Einführung cyberphysischer Systeme den einzelnen Aufgaben der Sicherung der Systeme, den Systemkomponenten zuzuteilen und die Verantwortlichkeiten explizit zu definieren. Grundsätzlich lassen sich die Aufgaben wie folgt zuordnen:

- Organization: organisatorische Aufgaben sind (primär) durch den Betreiber durchzuführen/ zu erfüllen.
- Technical: technische Aufgaben sind (primär) durch den Systementwickler bzw. -lieferanten zu gewährleisten
- Process: prozessorientierte Tätigkeiten sind zwischen Systementwickler bzw. -lieferant und dem Betreiber abzustimmen und zuzuordnen. Dies kann durch entsprechende vertragliche Vereinbarungen konkret spezifiziert werden oder durch Dienstleistungsvereinbarungen auch durch den Systemlieferanten übernommen werden.

Die TMHG hat im Speziellen nun diese Tätigkeiten dahingehend geprüft, wie die Ausprägung dieser Tätigkeiten tatsächlich erfolgen könnte und die Anwendbarkeit auf die eigene Organisationsstruktur abgeleitet. Beispielhaft sei hier das „Patch-Management“ genannt, welches die TMHG zwar durchführen kann (Organization). Dessen Planung und die Entscheidung, ob und wann dies durchzuführen ist (Process), kann jedoch nur gemeinsam mit dem Systementwickler bzw. -lieferant spezifiziert werden. „Access Protection“ kann und muss ebenfalls durch die TMHG

realisiert werden. Dies ist jedoch nur auf Prozessebene (Process) z.B. durch Vergabe von Logins zur Zuordnung von Rollen und Rechten möglich, da die Sicherung auf technischer Ebene (z.B. Bereitstellung von Logins oder Authentifizierungsinfrastruktur) wiederum durch den Systementwickler oder -lieferanten bereitzustellen ist. Hierbei ist ebenfalls zu beachten, dass die Zugangssicherung nicht nur aus IT-Sicht gewährleistet ist, sondern auch die physischen Komponenten ebenfalls geschützt werden müssen – Schutz vor Störung/Ausfall (Safety) oder bewusster Beeinflussung (Security).

2.1.4 Arbeitspaket 3 – Entwicklung eines Prozessmodells

Im Arbeitspaket wurde durch die **TRANS*PORT*WERK** Magdeburger Hafen GmbH (TMHG) die Teilaufgaben „Definition des Sollprozesses als ganzheitliches Prozessmodell“ und „Definition der Teilprozesse inkl. Rollenkonzept“ bearbeitet. Wesentlicher Schwerpunkt in diesem Arbeitspaket war die Mitarbeit an der Erweiterung des NIST-Frameworks for Improving Critical Infrastructure Cybersecurity (National Institute of Standards and Technology) zur Erweiterung um spezifische Merkmale von cyberphysischen Systemen (CPS). Der Fokus lag hierbei insbesondere auf der Zuarbeit erforderlicher Kategorien oder Sub-Kategorien sowie der Evaluierung ergänzter Kategorien und Sub-Kategorien.

2.1.5 Arbeitspaket 4 – Integration

In der ersten Teilaufgabe „Bestimmung und Umsetzung automatisierbarer Integrations- und Auslieferungsprozesse“ hat die TMHG insbesondere basierend auf den eigenen Prozessen eine Vielzahl an Schwerpunkten bezogen auf die spezifischen Eigenschaften und Ausprägungen cyberphysischer Systeme bearbeitet. Insbesondere wurden hierbei für die kontinuierliche Integration (Continuous Integration) sowie die Inbetriebnahme (Continuous Delivery) die zu erarbeitenden Prozesse und Rahmenbedingungen definiert. Grundsätzlich wurde hierbei die Anwendung der im Projekt entwickelten Systemarchitektur auf der Basis einer Test-, Staging- und Produktivumgebung verfolgt. Im Wesentlichen hängt dies jedoch von der Art des zu nutzenden Service und darauf basierenden Geschäftsmodells ab. Hierzu sind die folgenden Rollenmodelle erarbeitet worden:

- Rollenmodell 1: der Service Erbringer ist nur der Geräte Lieferant und der Service Nutzer implementiert eigene Services zur Nutzung dieser Hardware
- Rollenmodell 2: der Gerätelieferant bzw. -hersteller ist nicht nur Lieferant der Hardware sondern bietet ein Komplettpaket mit dazugehörigen Services, auf die mittels Schnittstellen die Nutzung der Hardware erfolgen kann

Die TMHG hat basierend hierauf die zweite Teilaufgabe „Evaluierung von einem prototypenhaft automatisiertem Integrations- und Auslieferungsprozess“ bearbeitet und die entwickelten Rollenmodelle hinsichtlich ihrer Eignung und Umsetzbarkeit evaluiert.
Für die TMHG bietet insbesondere das Rollenmodell 2 aufgrund der bestehenden Restriktionen hinsichtlich der nur sehr geringfügigen Ausprägung an unternehmensinterner IT-Ausstattung erhebliche Vorteile, da verschiedenste Vorteile bezüglich Continuous Integration und Continuous Delivery bestehen. So kann durch die Sichtweise, cyberphysische Systeme als Services zu betrachten, die Einbindung in die unternehmensinternen Prozesse sowie die Inbetriebnahme erheblich einfacher erfolgen. Die TMHG hat hierbei Nutzenpotenziale insbesondere darin, dass das Management – und hierzu gehören ebenfalls die sicherheitsbezogenen Aufgaben – in den Service und somit an den Diensterbringer ausgelagert werden können.

2.1.6 Arbeitspaket 5.2 – Anwendungsfälle und Evaluierung: Use Case Binnenhäfen (Hafen MD)

Für den Anwendungsfall Binnenhäfen verfolgte die TMHG primär das Ziel der Evaluierung der vertikalen Übertragbarkeit der Ansätze auf die Rahmenbedingungen eines Binnenhafens. Gemeinsam mit dem Fraunhofer IFF wurde hierbei zur testweisen Integration der Standards, Prozesse und Technologien in die Ablauforganisation ein Anwendungsfall anhand eines Reach Stackers, der auf einem abgegrenzten Gelände des Magdeburger Hafens eingesetzt wird, basierend auf verschiedenen funk- und bildbasierte Tracking-Technologien erarbeitet. Primär dient dies der Evaluierung der Machbarkeit der Detektion von Testszenarien zur Erkennung von Fehlfunktionen des zu überwachenden sowie der Fehleridentifikation des cyberphysischen Systems.
Es sei hier jedoch darauf verwiesen, dass es sich bei dem Reach Stacker in seiner aktuellen Ausprägung und Ausstattung noch nicht um ein automatisiertes Fahrzeug handelt, dieses sich jedoch bestens eignet, die Überwachung der Prozesse des Güterumschlags im Hanse-Terminal des Magdeburger Hafens oder einen Missbrauch oder Fehlfunktion des Reach Stackers selbst zu evaluieren.

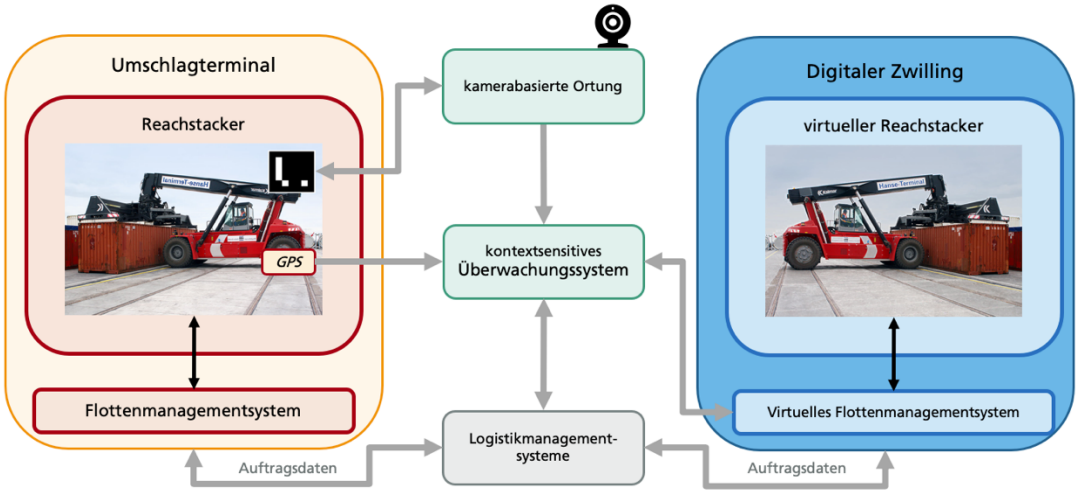


Abbildung 4: Gesamtarchitektur angepasst auf den Magdeburger Hafen[1]

Die Umsetzung des Demonstrators basiert auf den Projektergebnissen aus den Arbeitspaketen 2 bis 4 unter Anwendung des Prozessmodells sowie der Systemarchitektur. Der Magdeburger Hafen hat durch Bereitstellung des Terminals, dessen installierter Technik (Kamerasystem) sowie dem Umschlagsmittel Reach Stacker die Evaluierung der Übertragbarkeit des Automatisierungs- und Sicherheitskonzepts aus den vorherigen Arbeitspaketen unterstützt. Auf dem Hanse-Terminal des Magdeburger Hafens wurde ein Reach Stacker mit einem GPS Tracker des Fraunhofer IFF ausgestattet. Hierbei handelt es sich um eine funkbasierte Lösung, die Bestandteil der Sensorkomponente eines cyber-physischen Systems sein könnte und Informationen über die aktuelle Position des Fahrzeugs gibt.
Das Kameraortungssystem des Fraunhofers, welches Kamerabilder auswertet und somit die Positionsermittlung über ein bildbasiertes Verfahren durchführt, dient als komplementäres Messsystem. Dieses System wurde an das Kameraüberwachungssystem des Hanse-Terminals angebunden, um die

[1] Bild Reachstacker: https://www.magdeburg-hafen.de/umschlag-lagerung/umschlagflaechen-container-wechselbehaelter.html

Kamerabilder an das Ortungssystem zu übermitteln. Ursprünglich war geplant, die Fahrzeuge mit einem spezifischen Marker (ArUco Marker, ähnlich einem QR Code) auszustatten, um diese innerhalb des Kamerabildes zu identifizieren und die Positionsermittlung durchzuführen. Es wurde jedoch in Test festgestellt, dass die Auflösung der installierten Kameras einerseits nicht ausreichend war, um die Marker noch erkennen zu können, andererseits war es nicht möglich, einen Anbringungsort am Fahrzeug zu finden, der für eine Anbringung des Markers geeignet wäre. Unter anderem spielte hier die Sichtbarkeit des Markers aber auch die Größe eine Rolle. Weiterhin musste gewährleistet werden, dass durch eine mögliche Anbringung eines solchen Markers der Betrieb des Fahrzeugs nicht beeinträchtigt wird, da das Fahrzeug im Terminal im Regelbetrieb eingesetzt wurde.
Das Fraunhofer IFF hat hier jedoch zur Lösung dieser Herausforderung das Kameraortungssystem angepasst, in dem die von den Kameras aufgenommenen Bilder hinsichtlich einer Bewegungsanalyse ausgewertet werden und die Bewegungen im Bild mit einer Positionsbestimmung gekoppelt werden. Da bei den Testfahrten lediglich der Reach Stacker als bewegtes Objekt sowie durch seine Farbe deutlich erkennbar war, konnte dies erfolgreich umgesetzt werden.
Somit war es möglich, die Positionsdaten beider Ortungslösungen miteinander zu vergleichen. Das Überwachungssystem des Fraunhofer IFF hat bei Testfahrten kontinuierlich eine Asuwertung der erfassten Daten vorgenommen und bei provozierten Störungen die erwarteten Meldungen hinsichtlich einer möglichen Störung gegeben.
Neben der praktischen Evaluierung wurden weiterhin gemeinsam mit den Projektpartnern METOP und Fraunhofer IFF Strategien zur Systemeinführung evaluiert. Der Fokus lag hierbei auf der Einführung sicherer Automatisierungslösungen, bei denen derartige Strategien Anwendung finden sollten. Der Magdeburger Hafen hat jedoch wie in Arbeitspaket 1 bereits festgestellt aufgrund seiner organisatorischen Restriktionen hinsichtlich seiner Größe und Struktur nicht die Möglichkeiten, unterstützt durch eine eigene IT-Abteilung diese Konzepte umzusetzen. Stattdessen greift der Magdeburger Hafen – auch für die Umsetzung von IT-Lösungen sowie zur Wartung und den Betrieb von IT-Systemen – auf externe Dienstleister zurück. Daher wurde hier als idealer Lösungsansatz die Service Provider Strategie identifiziert. Der Magdeburger Hafen hat dabei gemeinsam mit den beteiligten Projektpartnern die im Projekt vorgenommenen Anpassungen des Organisationsmodells und allgemeinen Vorgaben des BSI evaluiert und einen Entwurf einer Sicherheitsarchitektur erarbeitet. Hierbei wurde festgelegt, welche Leistungen durch den Magdeburger Hafen zu erbringen sind bzw. erbracht werden können und andererseits wie Leistungen mittels Outsourcing an externe Dienstleister vergeben werden.
Als wesentlicher Mehrwert für den Magdeburger Hafen ist neben den Erkenntnissen aus der praktischen Evaluierung sowie Identifikation einer geeigneten Strategie zur Einführung von Automatisierungslösungen der Wissensaufbau hinsichtlich weiterer geeigneter Ansätze und Richtlinien, die zur Anwendung kommen könnten, entstanden.

2.2 Wichtige Positionen des zahlenmäßigen Nachweises

Die wichtigsten Positionen des zahlenmäßigen Nachweises sind:

- 0837 – Personalkosten
- 0838 – Reisekosten

Weitere Kostenpositionen – insbesondere Material oder Anschaffungskosten – sind während des Projekts nicht entstanden. Eine detaillierte Darstellung der

Verwendung der Mittel in den genannten Kostenpositionen kann dem zahlenmäßigen Nachweis entnommen werden.

2.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Basierend auf den geplanten Leistungsinhalten der einzelnen Arbeitspakete ist eine zeitliche Verteilung sowie Aufwandskalkulation der durchzuführenden Arbeiten vorgenommen worden.
Für die Grobeinschätzung der Einsatzmöglichkeiten von der Entwicklung und Erarbeitung methodischer Ansätze zur Erhöhung der IT-Sicherheit in Häfen und deren Logistikketten, die präventive Abwehr von Cyber-Angriffen auf IT-Systeme sowie der Aufbau eines Demostrators sind detaillierte Untersuchungen und Analysen der bestehenden Randbedingungen und ergebenden Anforderungen durchzuführen und zu definieren. Inwieweit sich derartige Ansätze für einen Binnenhafen mit der gegebenen Größe und organisatorischen Strukur integrieren und anwenden lassen, war mit einem gewissen Umsetzungsrisiko im durchgeführten Vorhaben verbunden.

Der Magdeburger Hafen hat primär an der Erarbeitung der Anforderungen in AP 1 mitgewirkt, die eine wesentliche Voraussetzung für die Arbeiten in den Arbeitspaketen 2 und 3 waren, die primär durch die Forschungspartner Fraunhofer IFF und METOP erfolgt ist. Ein weiterer wesentlicher Schwerpunkt der Arbeiten war die Evaluierung der Projektergebnisse im Arbeitspaket 5.2.

Dem Aufwand entsprechend ist die Anzahl der Mannmonate sehr wirtschaftlich kalkuliert worden.

2.4 Voraussichtlicher Nutzen, insbesondere Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplans

Die im Projekt gewonnenen Erkenntnisse hinsichtlich der Entwicklung und Einführung von Automatisierungslösungen werden in die zukünftige Realisierung von Automatisierungslösungen einfließen. Auch wenn der Magdeburger Hafen nicht selbst direkt in die Entwicklung oder auch Betrieb eines derartigen Systems eingebunden ist, so ist der Erkenntnisgewinn bei der Formulierung von Anforderungen sowie der Anwendung der geeigneten Einführungsstrategien von erheblicher Bedeutung. Durch die jeweils definierten Rollen im Prozess- und Organisationsmodell ist klar, welche Rolle(n) durch den Magdeburger Hafen vertreten und auch im Unternehmen etabliert werden müssen.

2.5 F&E-Ergebnisse von dritter Seite, die für die Durchführung des Vorhabens relevant sind

Im Rahmen der Projektbearbeitung sind keine weiteren wesentlichen neuen Erkenntnisse bekannt geworden, die für die weitere Durchführung des Vorhabens relevant sind.

2.6 Veröffentlichungen

- Präsentation des Projekts gemeinsam mit dem Fraunhofer IFF auf der transport logistic 2019 auf dem Gemeinschaftsstand des Landes Sachsen-Anhalt
- Präsentation des Projekts mit einem Vortrag auf dem Messestand des Bundesverbands Öffentlicher Binnenhäfen e.V. (BÖB) am 05.06.2019
- Fraunhofer Forschung kompakt, Ausgabe: September 2020, Titel: Mehr IT-Sicherheit im Hafenterminal,
  Link: https://www.fraunhofer.de/content/dam/zv/de/presse-medien/2020/september/forschungkompakt/iff-mehr-it-sicherheit-im-hafenterminal.pdf
- Internationale Konferenz INCOM2021 - 17th IFAC Symposium on Information Control Problems in Manufacturing: Anmeldung und Einreichung eines Papers bereits im Projektzeitraum und Teilnahme sowie Präsentation im Juni 2021, Titel: Boosting Cyber-Physical System Security
- Fraunhofer IFFocus, Titel: Mehr IT-Sicherheit im Hafenterminal, Link: https://www.iffocus.online/mehr-it-sicherheit-im-hafenterminal/

3 Literaturverzeichnis

[1] M. Schenk, Produktion und Logistik mit Zukunft: Digital Engineering and Operation (VDI-Buch), Springer Vieweg, 2015.

[2] U. Weinreich, "Digitale Sicherheit." Lean Digitization, Berlin Heidelberg: Springer, 2016.

[3] M. Runde, „"Automation Security Risk Assessment."," *atp edition,* pp. 48-55, 2016.

[4] A. D. H. H. R. H. R. S. K. &. V. O. Chughtai, Chughtai, A., Dörnemann, H., Heinold, R., Hubert, R., Salomon, K., & Vogel, O., Springer, 2013.

[5] H. Wannenwetsch, Vernetztes Supply Chain Management: SCM-Integration über die gesamte Wertschöpfungskette, Springer, 2006.

[6] G. Tassey, „The economic impacts of inadequate infrastructure for software testing," NIST (National Institute of Standards and Technology), 2002.

[7] B. R. Vorgang und A. Karry, „Addressing Software Security in the Federal Acquisition Process," 2011. [Online]. Available: https://www.cigital.com.

[8] „Adobe Systems Incorporated: Secure Product Lifecycle," 2013. [Online]. Available: http://www.adobe.com/de/security/splc.

[9] R. R. Dumke, Software Engineering: Eine Einführung für Informatiker und Ingenieure: Systeme, Erfahrungen, Methoden, Tools, Springer, 2013.

[10] A. Janus, „Qualitätsbasierte Bewertung Agiler Entwicklungsmethoden mit dem AMMI," *Softwaretechnik-Trends 32.2 ,* pp. 73-76, 2012.

[11] L. L. B. a. G. C.-S. Zhu, „DevOps and Its Practices," *IEEE Software 33.3,* pp. 32-34, 2016.

[12] M. a. A. S. Callanan, „DevOps: Making It Easy to Do the Right Thing," *IEEE Software 33.3,* pp. 53-59, 2016.

[13] „11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)," in *IEEE*, 2008.

[14] E. Di Nitto, „A software architecture framework for quality-aware DevOps," *Proceedings of the 2nd International Workshop on Quality-Aware DevOps. ACM,* 2016.

[15] N. A. Q. G. a. S. R. Delgado, „A taxonomy and catalog of runtime software-fault monitoring tools," *IEEE Transactions on software Engineering 30.12,* pp. 859-872, 2004.

[16] W.-T. Tsai, „Architecture classification for SOA-based applications," *Ninth IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC'06),* p. 2006.

[17] Atlassian, „What is Continuous Integration," Atlassian, [Online]. Available: https://www.atlassian.com/continuous-delivery/continuous-integration. [Zugriff am 05 02 2019].

[18] N. Pathania, Pro Continuous Delivery, Berkeley: Apress, 2017.

[19] G. Horton, „Ein Beispiel für Servitization: Power by the Hour," Zephram, [Online]. Available: http://www.zephram.de/blog/geschaeftsmodellinnovation/beispiel-servitization/. [Zugriff am 05 02 2019].

[20] Rolls Royce, „Power by the hour - Rolls Royce Total Care," Rolls Royce, [Online]. Available: https://www.rolls-royce.com/media/our-stories/discover/2017/totalcare.aspx. [Zugriff am 06 02 2019].

[21] M. P. Barrett, „Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," National Institute of Standards and Technology, 2018.

Berichtsblatt

1. ISBN oder ISSN	2. Berichtsart Abschlussbericht

3. Titel
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

4. Autor(en): Felix Montag	5. Abschlussdatum des Vorhabens 31.12.2020
	6. Veröffentlichungsdatum 30.06.2021
	7. Form der Publikation Bericht
8. Durchführende Institution(en) (Name, Adresse) TRANSPORTWERK Magdeburger Hafen GmbH Saalestraße 20 39126 Magdeburg	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 19H17006B
	11. Seitenzahl 20
12. Fördernde Institution (Name, Adresse) Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) 53175 Bonn	13. Literaturangaben 21
	14. Tabellen 2
	15. Abbildungen 4

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)
TÜV Rheinland Consulting GmbH, PT IHATEC, Am Grauen Stein 27, 51105 Köln

18. Kurzfassung
Mit dem Einzug von Lösungen im Umfeld von Industrie 4.0 können große Effizienzsteigerungspotenziale durch Automatisierung und digitale Vernetzung erschlossen werden. Die Vernetzung und Automatisierung führt jedoch zu einer Vielzahl von Risiken, die einen Einfluss auf die Stabilität der Prozesse (Safety) und andererseits auf die IT-Sicherheit durch Cyber-Angriffe (Security) haben. Für Automatisierungsvorhaben im Hafenumschlagsbereich existieren aktuell keine Standards zur Sicherung der Automatisierungssysteme und deren Datenaustausch gegen Cyber-Angriffe sowie der Überwachung der Performance in der End-to-End Prozesskette. 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 von Automatisierungsvorhaben in Häfen entwickelt und ebenfalls in Anwendungsfällen prototypisch bei einem See- (Hamburg, Wilhelmshaven) und einem Binnenhafen (Magdeburg) evaluiert werden.

19. Schlagwörter
Cyber-physische Systeme, Risikomanagement, Security und Safety, Cyber-Angriffe, Automatisierung in Häfen, Systemstabilität

20. Verlag Technische Informationsbibliothek (TIB) Hannover, Welfengarten 1B, 30167 Hannover	21. Preis

Document Control Sheet

1. ISBN or ISSN	2. type of document (e.g. report, publication) Report

3. title
AUTOSEC – Development and testing of measures to increase security in the digitized container terminal process and implementation of protective measures to prevent and detect cyber attacks in the infrastructure and the IT systems involved

4. author(s) (family name, first name(s)) Montag, Felix	5. end of project January 31, 2020
	6. publication date June 30, 2021
	7. form of publication Report
8. performing organization(s) (name, address) TRANSPORTWERK Magdeburger Hafen GmbH	9. originator's report no.
	10. reference no. 19H17006B
	11. no. of pages 20
12. sponsoring agency (name, address) Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) 53175 Bonn	13. no. of references 21
	14. no. of tables 2
	15. no. of figures 4

16. supplementary notes

17. presented at (title, place, date)
TÜV Rheinland Consulting GmbH, PT IHATEC, Am Grauen Stein 27, 51105 Köln

18. abstract
Ports are critical infrastructures since disruptions and stoppages can have immense not only economic impacts. The potential security risks are multifarious, especially in digitalized container terminal operations, which are steadily gaining importance through Industrie 4.0. A new method and tool set developed by research scientists at the Fraunhofer Institute for Factory Operation and Automation IFF and its industry partners enables preventive defense against attacks on automated cyber-physical systems and helps increase security along the entire supply chain, including the IT systems landscape. At the same time, automation projects can be planned and implemented efficiently.

19. keywords

20. publisher	21. price