IHATEC – Innovative Hafentechnologien

Schlussbericht

AUTOSEC

Entwicklung und Erprobung von Maßnahmen zur Erhöhung der Sicherheit im digitalisierten Container-Terminalprozess und Implementierung von Schutzmaßnahmen zur Verhinderung und Erkennung von Cyberattacken

Teilvorhaben: Umsetzung Software

Projektlaufzeit: 01.08.2017 - 31.12.2020
Förderkennzeichen: 19H17006D
Kassenzeichen: 81030364100
Mensch Technik Organisation und Planung METOP GmbH

gefördert durch

Bundesministerium für Verkehr und digitale Infrastruktur

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellen Verzeichnis

Teil I

Kurze Darstellung des Vorhabens

1. Aufgabenstellung

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 sollte 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.

1.1 Arbeitsziele des Vorhabens

Die Entwicklungsschwerpunkte des Vorhabens lassen sich wie folgt zusammenfassen:

- ganzheitliches Prozessmodell für das Anforderungs-, Veränderungs-, Release- und Test- Management
- skalierbare Methode für die Bewertung von Gefährdungspotenzialen in den Bereichen Security und Safety[1] sowie die Ableitung und Bewertung von Gegenmaßnahmen als Teil des Risikomanagements
- Dokumentations- und Kollaborationswerkzeug zur Abbildung des Prozessmodells und der Methode welches einerseits durch den Prozess leitet und die Anwendung der Methode un- terstützt und andererseits eine Transparenz und Nachvollziehbarkeit durch Dokumentation sicherstellt
- Pilothafte Evaluierung in einem großen Seehafen- und einem kleinen Binnenhafenautomati- sierungsszenario zur Überprüfung der Anwendbarkeit und Skalierbarkeit sowie zur Identifikation von Anpassungsbedarf (siehe auch nachfolgende Abbildung).

Abbildung 1: Vorgehensweise im Projekt

[1] Unterscheidung: Angriffssicherheit / Datensicherheit / Informationssicherheit (Security) sowie Betriebssicherheit (Safety) (Promotorengruppe Kommunikation der Forschungsunion Wirtschaft – Wissenschaft 2013)

Der wesentliche Schwerpunkt des geplanten Vorhabens war die Entwicklung von Methoden, die eine Erkennung und Bewertung von Gefährdungspotenzialen in den Bereichen Security und Safety ermöglichen, sowie die Ableitung und Bewertung von Gegenmaßnahmen als Teil des Risikomanagements. Hierzu war es zunächst erforderlich, eine Trennung der eigenen und fremden Systeme vorzunehmen, was im Rahmen der Anforderungsanalyse mittels Zerlegung des Komplexen zu betrachtenden Systems in seine Teilkomponenten erfolgte.
Im Ergebnis des Vorhabens entstehen neuartige Methoden sowie Verfahren, wie eine Überwachung der Security und Safety Anforderungen erfolgen kann. Zur Erreichung der Gesamtzielstellung werden eine Vielzahl an Teilzielen mit der Bearbeitung des Projekts aufgeteilt in die im Abschnitt beschriebenen Arbeitspakete angestrebt:

- Gewinnung eines besseren Systemverständnisses mittels Reduktion der Komplexität mittels Zerlegung in Teilsysteme und daraus abgeleitet eine Identifikation von Risiken für das Gesamtsystem
- Erarbeitung einer Gesamtarchitektur bestehend aus Hafen IT-Systemlandschaft und cyber-physischen Systemen (Automatisierung von Straddle-Carriern oder (Teil-)Automatisierung des Güterumschlags im Binnenhafen)
- Ermittlung einzelner kritischer Sicherheits- und Safety-Parameter zur Bestimmung eines Stage Environments sowie der Prozesse des gesamtheitlichen Softwarelebenszyklus in den Automatisierungslösungen
- Erarbeitung eines Prozessmodells inkl. Rollenkonzept als Sollprozess
- Gesamtheitlicher Integrations- und Auslieferungsprozesse über alle beteiligten Partner und IT-Systemlandschaften
- Nachweis der Anwendbarkeit der erarbeiteten Konzepte und Methoden sowie des Prozess-modells

1.2 Voraussetzungen

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 [1].

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 Operation abzuklären. Allgemein wird diese Betrachtungsweise auch Applikation Lifecycle Management genannt [2].

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 [3] [4]. Übergeordnet wird in der Wissenschaft auch noch das Thema System Lifecycle Management (SysLM) betrachtet [5]. Dieses Thema sollte 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.

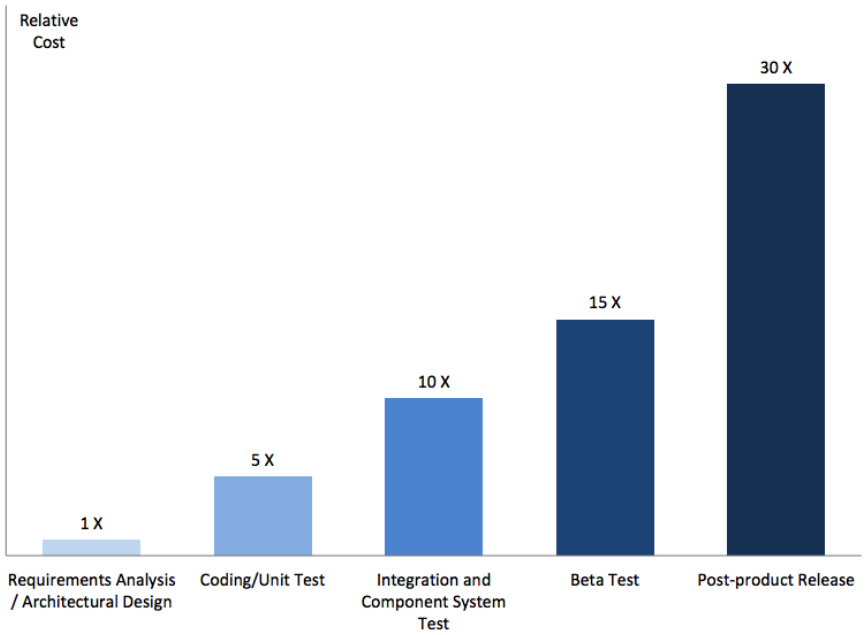


Abbildung 2: relative Kosten zur Behebung von Fehlern in verschiedenen Phasen im Softwarelebenszyklus

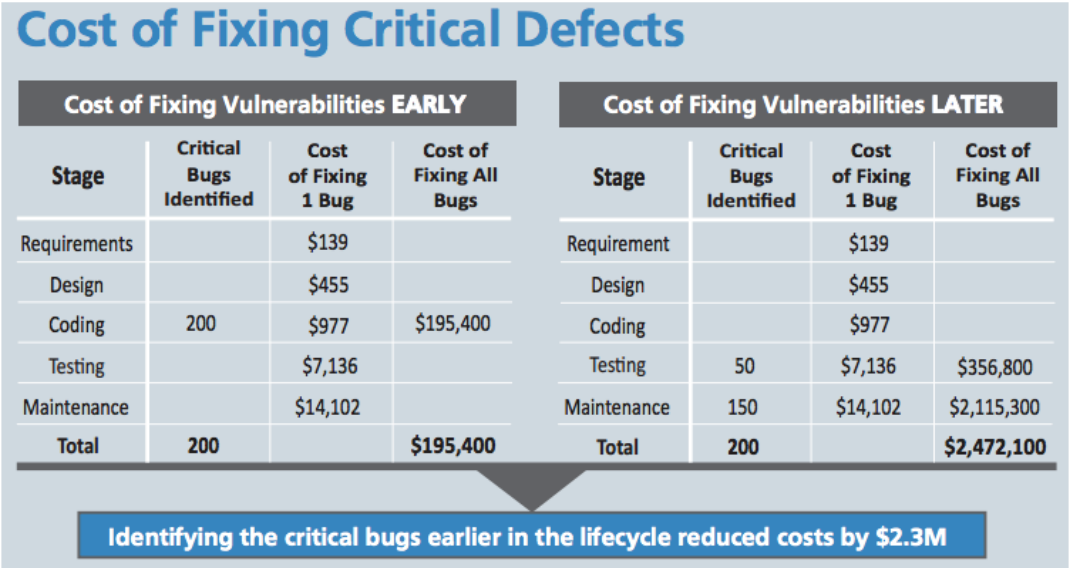


Abbildung 3: Kosten bei der Behebung von kritischen Fehlern in verschiedenen Phasen

Das Konsortium deckt alle für das Vorhaben wesentlichen Kompetenzbereiche ab und führt auf den relevanten Feldern erfahrene wissenschaftliche und industrielle Akteure aus Deutschland in einem leistungsfähigen Verbund zusammen.

Der Containerumschlag im Seehafen ist das Kerngeschäft von EUROGATE. An elf Terminal-Standorten hat die Gruppe im Jahr 2015 mehr als 14,5 Millionen TEU umgeschlagen. Im Jahr 2016 konnte eine Ausschreibung für den Betrieb eines Containerterminals in Limassol, Zypern gewonnen werden.
Als reedereiunabhängige Containerterminal-Gruppe werden, gemeinsam mit dem Schwesterunternehmen Contship Italia, Seeterminals an der Nordsee, im Mittelmeerraum und am Atlantik betrieben. Ein Schwerpunkt liegt auf den deutschen Standorten in Hamburg, Bremerhaven und Wilhelmshaven. Neben dem Containerumschlag bietet EUROGATE zusätzliche Dienstleistungen rund um die "Box", beispielsweise seemäßige

Verpackung oder Container-Depot, -Wartung und -Reparatur. Ein sehr wichtiges Segment innerhalb der Gruppe ist der intermodale Transport. Das Transportnetzwerk verbindet die Seeterminals in Nord- und Südeuropa per Bahn (eigene bzw. Beteiligungen an Operateuren und Eisenbahnverkehrsunternehmen) mit wichtigen europäischen Wirtschaftsregionen. Seit 2015 besteht ebenfalls eine Beteiligung an einem Bahnunternehmen in Brasilien.
EUROGATE strebt mit dem geplanten Vorhaben die unmittelbare Begleitung der Einführung von Automatisierungslösungen im Container-Terminal an und leistet als Federführer und Koordinator des Projektes einen wesentlichen Beitrag zur Zielerreichung durch die Bereitstellung eines Use Cases und einer Testumgebung.

Das Fraunhofer-Institut für Fabrikbetrieb und -automatisierung IFF ist ein eigenständiges Institut im Netzwerk der Fraunhofer-Gesellschaft. Die technologische Ausrichtung des Institutes besteht darin, innovative und kundenorientierte Problemlösungen auf den Gebieten Logistik und Materialflusstechnik, Robotersysteme und Mess- und Prüftechnologie, Prozess- und Anlagentechnik, Virtual Engineering und virtuelles Training zu konzipieren, zu entwickeln und zu realisieren. Das Fraunhofer IFF arbeitet dabei sehr eng mit dem Institut für Logistik und Materialflusstechnik (ILM) der Universität Magdeburg (Institutsleitung in Personalunion) zusammen. Folgende Erfahrungen aus Forschungs- und Industrieprojekten kann das Fraunhofer IFF im Vorhaben AUTOSEC einbringen:

- Risikomanagement: „ValueSec“ (EU, 2011-2014): Entwicklung von Methoden zur Entscheidungsanalyse im Sicherheitsbereich durch Kombination quantitativ-monetärer Werte mit qualitativen Größen
- Dokumentationswerkzeuge/Web 2.0-Technologien: „sprintDoc“ (BMBF, 2015-2017) des ILM: Entwicklung eines Methoden- und Werkzeugsets für die Dokumentation in agilen Softwareprojekten sowie „ICKE 2.0“ (BMBF 2008-2010): Entwicklung eines Enterprise Wikis für KMU
- Konzeption und Durchführung von Industrie 4.0 Check-ups zur Potenzialanalyse für die Einführung von Industrie 4.0 Ansätzen in der Produktion

Die am 18. März 1992 gegründete Magdeburger Hafen GmbH ist ein wesentlicher Motor für den wirtschaftlichen Aufschwung in der Metropolregion Magdeburg und stellt ein wesentliches Bindeglied multimodaler Transportketten entlang der internationalen Wasserstraße Elbe dar. Insbesondere wird dies durch das Leistungsangebot, welches sich von klassischen Hauptaufgaben eines Hafens wie der Vorhaltung von Infrastruktur und Erschließung hafenrelevanter Flächen bis hin zum Logistik-Partner und Systemdienstleister für multimodale Transportketten erstreckt. Der Magdeburg Hafen sieht sich ebenfalls als Vorreiter in der Anwendung neuer Technologien oder der Umsetzung umweltfreundlicher Aktivitäten. Als Greenport hat der Magdeburger Hafen als erster europäischer Binnenhafen eine Hybridlokomotive in den Dienst gestellt und die Energieversorgung des Referenzterminals erfolgt überwiegend mit erneuerbaren Energien.

Die METOP GmbH wurde im Jahre 1995 gegründet und beschäftigt derzeit 30 Mitarbeiter. Das Unternehmen befasst sich seit mehreren Jahren mit innovativen Datenhaltungssystemen und Software-Techniken. Die METOP GmbH steht als An-Institut der Otto-von-Guericke Universität Magdeburg an der Nahtstelle zwischen Forschung und Industrie. In den letzten 20 Jahren konnte diese Position erfolgreich besetzt und durch vielfältige Projekte und Kooperationen mit Unternehmen ausgebaut und ein entsprechend umfangreiches Netzwerk geschaffen werden. Die METOP GmbH fokussiert als forschendes KMU den Transfer von Forschungsinhalten als einen wichtigen Bestandteil des Geschäfts und nutzt das vorhandene Netzwerk in der Industrie, um Forschungsergebnisse erfolgreich zur Marktreife und somit zur Anwendung in der Wirtschaft zu überführen.
Neben Aufträgen und Projekten mit Forschungsfokus ist die METOP GmbH im Geschäftsbereich AI - Angewandte Informatik - als international agierender IT-Beratungs- und Technologie-Dienstleister für die Großindustrie, kleine und mittelständische Unternehmen sowie öffentliche Institutionen aktiv.
Die METOP GMBH war in mehreren Projekten bezüglich Softwareentwicklungsprozessen tätig. Beispielsweise hat die METOP GmbH die Bayer Business Services bei der Entwicklung eines verteilten Entwicklungsprozesses für Anpassungen an einem globalen HR-Softwaresystem beraten (weltweite Entwicklung) und bei der Umsetzung begleitet. Weiterhin wurden bei der regiocom GmbH (Service Dienstleister in der Energiebranche, größter Abrechnungsdienstleiter im deutschsprachigen Raum) die Prozesse der Entwicklungspipeline im Fokus von ITIL und agilen Entwicklungsprozessen analysiert und verbessert.

Im Bereich IT-Sicherheit ist die METOP GmbH derzeit bei zwei forschungsrelevanten Themenkomplexen vertreten:

- methodische Forschung zur Erkennung und Aufklärung von IT-Sicherheitsvorfällen durch die Einführung eines Host Intrusion Detection Systems (HIDS) welches die Vorteile Netzwerk-basierter und Host-basierter Erkennungssysteme kombiniert.
- Ableitung von Anforderungen für IT-Systemlandschaften, um forensische Anforderungen wie Datensicherheit, Korrektheit, lückenlose Nachvollziehbarkeit und Reproduzierbarkeit sicherzustellen.

Für den Punkt 2 hat die METOP GmbH im Jahr 2013 den Hugo Junkers Preis des Landes Sachsen-Anhalt in der Kategorie „Innovativste Projekte der angewandten Forschung“ erhalten. Darüber hinaus leistet die METOP GmbH Gremienarbeit im Bereich der sichernden Kriminaltechnik, woraus Handlungsempfehlungen für IT-gestützte Qualitätssicherung im Verbund von Bund und Ländern hervorging. Weiterführend erfolgt eine regelmäßige Zusammenarbeit mit dem Cyber-Crime-Competence-Center des LKA Sachsen-Anhalt sowie landeseigener Spezialkräfte.
Für die Software-Entwicklung betreibt die METOP GmbH in Zusammenarbeit mit der Universität Magdeburg, Universität Passau, Universität Braunschweig, University of Texas at Austin (USA), Carnegie Mellon University (USA), Federal University of Alagoas (Brazil) und University of Bergamo (Italy) unter Leitung des Prof. Dr. Thomas Leich (METOP GmbH) seit Jahren Forschungsarbeit im Bereich Softwareproduktlinien mit Feature-Oriented-Software-Development. Insbesondere die Erfahrungen im Bereich methoden-basierte algorithmische Komposition und analytischen Dekomposition von IT-Systemen können in diesem Forschungsvorhaben zuträglich sein. Durch die Dekomposition wird das zugrundeliegende Problem verstanden (Zerlegung in Feature) und durch die darauffolgende Komposition als Ganzes zusammengefasst.

2. Planung und Ablauf des Projektes

Das Projekt AUTOSec befasste sich mit den im Folgenden dargestellten Arbeitspaketen. Die Arbeitsplanung orientiert sich an der Gesamtplanung des Projektes und detailliert relevante Aufgabenpakete, wobei die METOP GmbH an den folgenden Teilaufgaben und zu lösenden Problemen arbeitet.

2.1 Arbeitspaket 1 - Anforderungsanalyse

Hauptverantwortlich: Eurogate GmbH

Die Anforderungsanalyse diente dazu, die im weiteren Projektverlauf betrachtete System-Umgebung abzugrenzen. Dazu wurden beteiligte Komponenten (Maschinen, Hardware, Netzwerk-Infrastruktur, Software, etc.) und handelnde Personen (Nutzer, Betreiber, Lieferanten) identifiziert und ihre funktionale Rolle im Gesamtsystem beschrieben.
Auf der Basis einer Risiko-Analyse wurden die globalen Safety- und Security-Anforderungen identifiziert und auf die einzelnen Komponenten runtergebrochen.
Die Anforderungsanalyse stellte die Basis zur Schaffung der erforderlichen Grundlagen zur Überführung des Entwurfsprinzips Security by Design in eine Methode und der Entwicklung eines Prozessmodells für die Implementierung, Support und Maintenance der Systemlösung dar.
Zur Erarbeitung der Anforderungen wurde, die Komplexität eines Systems durch Zerlegung in weniger komplexe Teilsysteme reduziert. Hierbei musste jedoch berücksichtigt werden, dass dabei im Allgemeinen übergeordnete Abhängigkeiten zwischen den Teilsystemen aufgelöst werden, was wiederum zu Anpassungen von fachlichen Anforderungen führte.
„IT-Security“ und „Safety“ sind klassische Beispiele von allgemeinen Anforderungen an eine Systemlandschaft, die Einfluss auf alle Komponenten der Systemlandschaft haben. Dabei spielt der Grad der Zerlegung und auch die reine Überprüfbarkeit der Anforderungen eine wichtige Rolle. Im Rahmen dieses Arbeitspaketes sind ausgehend von übergeordneten Anforderungen, spezifische Anforderungen abgeleitet worden.

Das Arbeitspaket Anforderungsanalyse diente ebenfalls der Ermittlung und Bewertung der für cyber-physische Systeme bestehenden oder ergebenden Bedrohungen, die den fehlerfreien Betrieb stören könnten. Grundsätzlich wurden hierbei die bewusste (Manipulation, Störung etc.) und unbewusste (Fehler, Wechselwirkungen, Ausfälle etc.) Bedrohungen unterscheiden und deren Einfluss auf den Betrieb oder die Erhöhung der Ausfallwahrscheinlichkeit des Gesamtsystems bewertet.

Die METOP GmbH hat innerhalb des Arbeitspaketes die Verantwortung für folgende Teilarbeitspakete übernommen:

- Bewertung der Systemkomponenten bzgl. der Relevanz zur Systemsicherheit
- Identifikation und Definition von Teilsystemen
- Risiko-Analyse

2.2 Arbeitspaket 2 – Konzepte, Methoden, Toolchain

Dieses Arbeitspaket wurde im Laufe des Projektes in zwei Unterarbeitspakete zerlegt und bearbeitet.

2.2.1 Teilarbeitspaket 2.1 - Gesamtarchitektur und Konzepte

Hauptverantwortlich: METOP GmbH

Ausgehend von einer erweiterten Realität, welche sich in diesem Anwendungsszenario durch die Arbeitsprozesse eines Hafens und deren IT-Systemlandschaft zur Steuerung (Leitstand) definiert, wurden Konzepte und Methoden zur Einführung (Development) und Betrieb (Operation) von cyber-physischen Systemen (Automatisierung von Straddle-Carriern) analysiert. Innerhalb dieses Arbeitspaketes wurden zwei grundlegende Probleme mit Bezug auf IT Security und Safety erforscht:

- Die Komplexität des Ereignisraums steigt. Daher ist es theoretisch und praktisch nicht mehr möglich alle Anforderungen zu definieren und zu testen (verifizieren), welche aus der Real-Welt abgeleitet werden können.
- Die Anzahl der beteiligten Systeme und damit die Anzahl von beteiligten Spezialisten steigen. Dieses betrifft die Entwicklung (Development) und den Betrieb (Operation) von cyber-physischen Systemen.

Punkt 1 hatte insbesondere Auswirkungen auf die allgemeine Architektur einer cyber-physischen Entwicklungslandschaft. Das Testen und Verifizieren des Gesamtsystems konnten nicht umgesetzt werden. Weiterhin hat die Architektur starken Einfluss auf die Sicherheit eines Systems (sicherheitstechnische Analysen auf Architekturebene [8], [9])

Ausgehend von dieser Problematik werden Architekturen für die Entwicklungslandschaft benötigt, welche die Überprüfung (Testen und Verifizieren) von IT Security und Safety durch verschiedene Testverfahren, zum Beispiel statische Codeanalyse (z.B. Information Flow Control [8]), Testgeneratoren (z.B. Microsoft Diagnostics und Recovery Toolset DaRT, Mozilla LangFuzz) und Laufzeit Verifikation (z.B. Efficient Hybrid Typestate Analysis [10], Intrusion Detection [11]) ermöglichen.

Ausgangspunkt für dieses Forschungsvorhaben sind Konzepte aus moderner Cloud basierten Architekturen. Abbildung 4: Stage Environment in IT-Infrastruktur zeigt eine derartige Architektur.

Codeanalyse und Testgeneratoren können im Testenvironment abgebildet werden. Das Stage Environment stellt ein virtualisiertes Abbild des Produktions-Environments dar und bildet die Grundlage für Laufzeit Verifikation. Eines der Kernelemente dieses Konzeptes ist die Abbildung der IT Infrastructure als Code (IaC) im Stage Environment. IAC ist eine bestimmte IT-Infrastruktur, die Operations-Teams anstatt manueller Verfahren automatisch per Code verwalten und bereitstellen können. IaC unterstützt Infrastructure-as-a-Service (IaaS)

Ansätze. Weiterführend können IaaS auf industrielle Plattform-as-a-Service (PaaS) Konzepte umgesetzt werden [12].

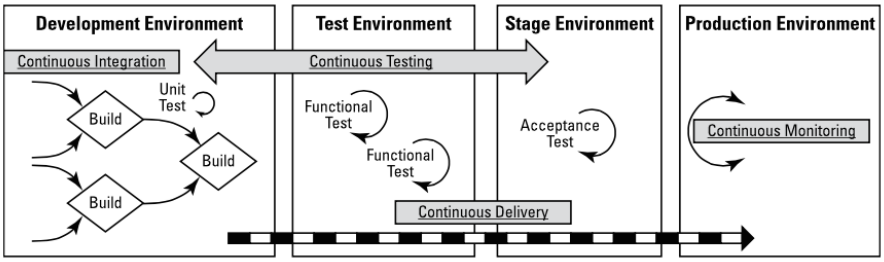


Abbildung 4: Stage Environment in IT-Infrastruktur

Vorgehen: Ausgehend von den Ergebnissen des AP1 sollte ein Architekturkonzept für das Zusammenführen der IT-Systeme der Häfen und der cyber-physischen Systeme (Automatisierung von Straddle-Carriern) erarbeitet werden. Dieses war stark abhängig von den bisher verwendeten Systemen und deren Kopplung.

1. Analyse der Architekturen der IT-Systemlandschaften (Hafen Logistik, automatisierte Straddle-Carrier) in Hinblick IT Security und Safety Anforderungen aus AP1 (Verbund der IT-Systemlandschaften)
2. Erarbeitung einer Gesamtarchitektur bestehend aus Hafen Logistik und automatisierte Straddle-Carrier (Gesamtsystem)
3. Ableitung von zu überwachenden Parametern (Phasenraum) aus den Bedrohungsszenarien des AP1, Erweiterung des Anforderungskataloges für Systemkomponenten um technische Merkmale

Analyse und Überprüfung der Simulationsfähigkeit (Testbarkeit) der gesamtheitlichen IT-Systemlandschaft bestehend aus Hafen und automatisierte Straddle-Carrier (gesamtheitliche Simulation)

Die METOP GmbH hat innerhalb des Arbeitspaketes die Verantwortung für folgende Teilarbeitspakete übernommen:

- Analyse von Architekturen
- Ableitung von zu überwachenden Parametern
- Analyse und Überprüfung der Simulationsfähigkeit

2.2.2 Teilarbeitspaket 2.2 - Organisationsmodell und Prozessvorgaben

Hauptverantwortlich: METOP GmbH

Zielsetzung innerhalb dieses Arbeitspaketes war das Beschreiben des prozessualen Ablaufes des Softwarelebenszyklus unter Berücksichtigung einer Toolchain (z.B. DevOps Toolchain: Code, Build, Test, Package, Release, Configure und Monitor [13]).
Das Ergebnis wurde zu Bestimmung der einzelnen Aufgaben und damit auch der Anzahl der beteiligten Organisationseinheiten verwendet. Darauf basierend wurde ein Entwicklungs- und Betriebsmodell erforscht, welches ein schnelles Eingreifen ermöglichen sollte. Ein schnelles Eingreifen sollte durch die Laufzeit Verifikation durchgeführt werden, da Fehler erst im Betrieb festgestellt werden und damit im Extremfall zum Stillstand im Hafenbetrieb führte. Dieses betrifft in einer groben Übersicht:

- Anforderungsmanagement: Verteilung, Aufsplittung und Überwachung von Anforderungen auf die entsprechenden Organisationseinheiten (Business-, Entwickler-, Test-, QS- und Operationsteams)
- Change-Management: Strategie, Strukturen, Systeme, Prozesse und Priorisierung im Kontext verteilter Entwicklung
- Development (Code, Build): leichtgewichtige entkoppelte Entwicklung von Komponenten

- Test und QS Management (Test): Sicherstellung der grundsätzlichen Funktionalitäten und Ableitung von Überprüfungsregeln zur Laufzeit für nicht test-bare oder unbekannte Ereignisse
- Release und Deployment Management (Package, Release): Continuous Integration (siehe Arbeitspaket 4) und Continuous Delivery
- Operation (Configure und Monitor): Betrieb und Überwachung

Ausgangspunkt für die Bearbeitung dieses Forschungsschwerpunktes bildeten derzeitige Software (Microsoft Security Development Lifecycle [14], SAFECode - Software Assurance Forum for Excellence in Code [15]) und Hardware-Entwicklungsmodelle. Ausgehend von einer Klassifizierung bisheriger Entwicklungsmodelle bezüglich horizontaler und vertikaler Skalierung, wurden leichtgewichtige Entwicklungsmodelle in Zusammenspiel mit der entworfenen Architektur untersucht. Zusätzlich wurde auf Forschungsergebnisse aus dem Bereich virtueller Fabriken und IT Security by Design zurückgegriffen. Dabei wurden aktuelle Forschungsarbeiten aus dem Bereich agiler Softwareentwicklung mit Fokus IT-Sicherheit beachtet [16], [17]. Insbesondere wurden hier Ansätze zur Umsetzung von IT-Security und Safety Anforderungen aus AP1 auf horizontaler und vertikaler Ebene analysiert, welche durch das gewählte Entwicklungsmodell abgearbeitet werden können. Für die Erforschung leichtgewichtiger Entwicklungsprozesse für cyber-physische Systeme wurden Ansätze aus dem Bereich der Service/Mirco Service Entwicklung im Cloud Umfeld wie zum Beispiel DevOps [18] gewählt. Abbildung 5: DevOps Life Cyle mit Shift Left Konzept zeigt den DevOps Life Cyle mit Shift Left Konzept.

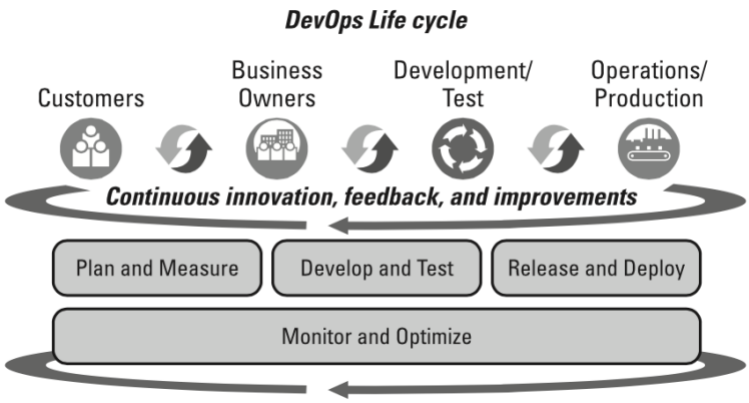


Abbildung 5: DevOps Life Cyle mit Shift Left Konzept

Die METOP GmbH hat innerhalb des Arbeitspaketes die Verantwortung für folgende Teilarbeitspakete übernommen:

- Analyse der Softwarelebenszyklen

2.3 Arbeitspaket 3 – Entwicklung eines Prozessmodells

Hauptverantwortlich: Fraunhofer IFF

Für das Anforderungs- und Veränderungsmanagement sowie das Release und Test-Management wurde ein ganzheitliches Prozessmodell für alle Prozessbeteiligten analysiert und entworfen. Basierend auf den Ergebnissen des AP2, in welchem die Prozessvorgaben sowie die Architektur der Entwicklungs-, Test-, Qualitätssicherungs- und Stage-Umgebungen im Gesamtverbund aller Prozessbeteiligten – also Entwicklern und Anwender – entwickelt wurden, wurde ein Prozessmodell erarbeitet. Im Prozessmodell wurden die zur Realisierung der Sicherung der cyber-physischen Systeme und der IT-Infrastruktur erforderlichen Prozesse sowie die Rollenverteilung, wer für welchen Teilprozess verantwortlich ist, basierend auf der Standardvorgehensweise mittels

- Identifikation von Störungen / Angriffen
- Risikoanalyse: Verifikation und Bewertung der Störung / des Angriffs

- Root Cause Analyse zur Identifikation der gestörten/störenden Komponente bzw. des Angreifers
- Work Around zur übergangsweisen Behebung
- Bugfixing – dauerhafte Behebung

als Sollprozess ermittelt. Diese Sollprozesse dienen in erster Linie zur Sicherstellung eines transparenten und abgestimmten Änderungsmanagements sowie der schnellen Identifikation von potenziellen Fehlerquellen oder im Idealfall der Verhinderung von Störfällen bei der Einführung und dem Einsatz cyber-physischer Systeme im Bereich des digitalisierten Terminal-Prozesses.
Insbesondere werden hierbei Policies, die je nach Unternehmensgröße unterschiedlich ausgeprägt sein können, einen erheblichen Einfluss auf die zu modellierenden Prozesse haben, sodass die mit dem Projekt angestrebte vertikale Übertragbarkeit des Ansatzes auch im Prozessmodell Berücksichtigung findet.

Die METOP GmbH hat innerhalb des Arbeitspaketes keine Verantwortung für ein Teilarbeitspaket übernommen, hat aber das Fraunhofer IFF in der Analyse und Ausarbeitung unterstützt.

2.4 Arbeitspaket 4 – Integration

Hauptverantwortlich: METOP GmbH

Ausgehend von der Problematik der Laufzeit Verifikation, welche in AP1 einen Schwerpunkt darstellte, wurde innerhalb dieses Arbeitspaketes detaillierter auf die Überwachung und die Reaktion im Fehlerfalle eingegangen. Dabei wurde im Allgemeinen davon ausgegangen, dass nicht alle Zustände eines Hafens im Vorfeld emuliert werden können (Komplexität des Gesamtsystems) und damit auch nicht die internen Abläufe in der IT vollständig simuliert werden können. Passend zu dieser Problematik wurde im Umfeld der Softwareentwicklung für komplexe Systeme das Prinzip von Continuous Integration und Continuous Delivery entwickelt.

- Continuous Integration: Prozess der das fortlaufende Zusammenfügen von Komponenten zu einem cyber-physischem Gesamtsystem beschreibt. Das Ziel der kontinuierlichen Integration ist die Steigerung der Gesamtqualität. Typische Aktionen sind das Übersetzen und Linken von Anwendungsteilen und Ausrollen von Hardware, prinzipiell können aber auch beliebige andere Operationen zur Erzeugung abgeleiteter Informationen durchgeführt werden. Üblicherweise wird dafür nicht nur das Gesamtsystem neu gebaut, sondern es werden auch automatisierte Tests durchgeführt und Software Metriken zur Messung der Softwarequalität erstellt.
- Continuous Delivery: bezeichnet eine Sammlung von Techniken, Prozessen und Werkzeugen, die den Systemlieferungsprozess verbessern.

Angewendet auf das autonome Fahren von VAN Carriern ist der Grundgedanke, eine „gutes“ umfängliches Verhalten des Gesamtsystems zu emulieren und die internen IT dabei in einer Stage Environment zu überwachen. Wenn im laufenden Betrieb durch die Laufzeit Verifikation dann ein Fehler entsteht, muss auf diesen schnellstmöglich reagiert werden. Klassischer Weise wird im Service Umfeld dann von einem mindestens 2-stufigen Prozess ausgegangen. Im ersten Schritt wird ein Workaround gesucht, um den Betrieb schnellstmöglich wiederaufzunehmen. Im zweiten Schritt wird dann in Abhängigkeit von der schwere des Fehlers und dessen Häufigkeit entschieden, ob der Workaround ausreichend ist oder ob eine Root-Cause Analyse und anschließend eine Korrektur von IT oder Hardware-Komponenten erfolgen muss.

Folgende Schwerpunkte wurden detaillierter untersucht und analysiert:

- Bestimmung der Integrations- und Auslieferungsprozesse (Hard- und Software)
- Automatisierungs-Potentiale der Integrations- und Auslieferungsprozesse, um schnelle, zuverlässige und wiederholbare Deployments zu ermöglichen
- Prototypenhafte Umsetzung eines automatischen Integrations- und Auslieferungsprozesses

Erweiterungen oder Fehlerkorrekturen können somit mit geringem Risiko und niedrigem manuellem Aufwand in die Produktivumgebung ausgeliefert werden. Continuous Delivery wird primär in Kombination mit agilen

Methoden eingesetzt. Forschungstechnisch wurden bestehende Ansätze aus dem Bericht der Software- und Hardwareentwicklung analysiert und für cyber-physische Systeme erweitert werden [19].

Die METOP GmbH hat innerhalb des Arbeitspaketes die Verantwortung für folgende Teilarbeitspakete übernommen:

- Evaluierung der in Arbeitspaket 2 abgeleiteten Architektur bezüglich Continuous Integration und Continuous Delivery
- Evaluierung des Organigramms aus Arbeitspaket 2 bezüglich Continuous Integration und Continuous Delivery
- Bestimmung und Umsetzung automatisierbarer Integrations- und Auslieferungsprozesse

2.5 Arbeitspaket 5 - Anwendungsfälle und Evaluierung

Hauptverantwortlich: Eurogate GmbH

Für die Validierung des im Projekt erarbeiteten methodischen Ansatzes wurde eine Evaluierung in Form eines Demonstrators/Rollenspiels durchgeführt. Hierbei wurden die spezifisch für das cyber-physische System erarbeiteten Konzepte und Methoden zur Anwendung gebracht und die mit dem Projekt angestrebte horizontale und vertikale Übertragbarkeit der Ansätze überprüft. Da im Projekt zwei Anwendungspartner in ihren jeweiligen Use Cases eine Evaluierung der im Projekt erarbeiteten Ergebnisse durchführten wurde das Arbeitspaket 5 in zwei Use Cases gegliedert:

Use Case 1 - Überseehäfen (Eurogate):
Die Eurogate Gruppe führte parallel zu diesem Forschungsprojekt ein Projekt durch, in dessen Rahmen Automatisierungstechnologien mit selbstfahrenden Container-Transport-Fahrzeugen erprobt, validiert und sukzessive in den Terminals eingesetzt werden. Im Rahmen dieses Projektes wurde die IT- und infrastrukturelle Landschaft des Unternehmens erheblich um eine Vielzahl neuer Komponenten erweitert, die zum größten Teil durch verschiedene und neue Lieferanten beigesteuert wurden. Die im AUTOSEC Projekt entwickelten Ergebnisse (Standards, Prozesse, Technologien) wurden im Rahmen des Automatisierungsprojektes validiert.

Use Case 2 - Binnenhäfen (Hafen MD):
Binnenhäfen zeichnen sich neben der Erreichbarkeit über Binnenwasserstraßen dadurch aus, dass die Größe der meisten Binnenhäfen erheblich kleiner ist als die der großen Überseehäfen in Europa. Somit ergeben sich geringere Umschlagsmengen an Containern, die den erforderlichen Grad an Automatisierung erheblich reduziert. Weiterhin sind die Unternehmensgesellschaften, die die Binnenhäfen betreiben erheblich kleiner, sodass unterschiedliche Voraussetzungen bezüglich der IT – wie weniger Infrastruktur oder weniger IT-Personal – bestehen, sodass bestimmte Anforderungen zur Schaffung einer IT Security und Safety nur bedingt zu erfüllen sind.

Primär dient der Use Case 2: Binnenhäfen, welcher durch den Hafen Magdeburg realisiert wurde, der des vertikalen Transfers der Projektergebnisse, die Konzepte, Werkzeuge und Methoden unter den gegebenen Rahmenbedingungen eines Binnenhafens zu validieren.

Die METOP GmbH hat innerhalb des Arbeitspaketes die Verantwortung für folgende Teilarbeitspakete übernommen:

- Testweise Integration der neuen Standards, Prozesse und Technologien in die Ablauforganisation der beteiligten Bereiche
- Bewertung der Funktionsfähigkeit und praktischen Anwendbarkeit inklusive Dokumentation von Verbesserungen

2.6 Arbeitspaket 6 - Projektmanagement und Ergebnisverbreitung

Hauptverantwortlich: Fraunhofer IFF

Das AP 6.1 beinhaltete die allgemeine Koordination der Zusammenarbeit zwischen den Projektpartnern, die Planung, Organisation und Dokumentation von Projekttreffen, die Kommunikation von Zwischen- und Endergebnissen, die Administration und Berichterstattung sowie die Budgetplanung und -kontrolle.
Als Teilaufgaben des Projektmanagements wurden die Projektkoordination sowie das Qualitätsmanagement durchgeführt. Die Projektkoordination umfasste die Gesamtkoordination des Projektes sowie die Arbeits-, Finanz- und Kostenkontrolle. Primär erfolgten hierbei die Zusammenführung technischer und administrativer Fragestellungen sowie die Kontrolle der Erreichung von Projektzielen und Meilensteinen.
Das Qualitätsmanagement für das Projekt stellte alle notwendigen Aufgaben für die Festlegung der Qualitätspolitik, deren Ziele und Verantwortlichkeiten zur Verfügung. Es stellte weiterhin die Qualität der Ergebnisse sicher und wurde durch eine Qualitätsplanung, Qualitätskontrolle, Qualitätssicherung und Qualitätsverbesserung verwirklicht.

Ergebnisse des Arbeitspaket 6 sind nicht Bestandteil des Abschlussberichtes der METOP GmbH. Die METOP GmbH hat innerhalb des Arbeitspaketes keine Verantwortung für ein Teilarbeitspaket übernommen, hat aber das Fraunhofer IFF bei seinen Arbeiten unterstützt.

2.7 Zeit Planung des Projektes

Das Projekt orientiert sich am Vorgehensmodell für Forschungs- und Entwicklungsprojekte. Die Partner beabsichtigten einen Projektstart zum 01. April 2017 mit einer Laufzeit von 36 Monaten.

		Projektlaufzeit																																	
		1. Projektjahr												2. Projektjahr												3. Projektjahr											
AP	Arbeitspakete	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1	**Anforderungsanalyse**																																				
	Meilenstein 1									◆																											
2	**Konzepte, Methoden, Werkzeuge**																																				
2.1	Gesamtarchitektur und Konzepte																																				
2.2	Organisationsmodell und Prozessvorgaben																																				
3	**Entwicklung eines Prozessmodells**																																				
4	**Integration**																																				
	Meilenstein 2																								◆												
5	**Anwendungsfälle und Evaluierung**																																				
5.1	Use Case 1: Überseehäfen (Eurogate)																																				
5.2	Use Case 2: Binnenhäfen (Hafen Magdeburg)																																				
	Meilenstein 3																														◆						
6	**Projektmanagement, Transfer, Öffentlichkeitsarbeit**																																				

Tabelle 1: Zeitplanung der Arbeitspakete zur Projektbeantragung

Dieser Zeitplan konnte Aufgrund eines Verzögerten Projektstarts 01.08.2017 und der durch die Corona Pandemie verursachten Einschränkungen (Verlängerung um 4 Monate bis 31.12.2020) nicht eingehalten werden. An der grundsätzlichen Aufteilung und Ressourcen Zuordnung wurden aber keine Änderungen vorgenommen.

		Projektlaufzeit																																			Verlängerung				
		1. Projektjahr												2. Projektjahr												3. Projektjahr												4. Projektjahr				
AP	Arbeitspakete	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
1	Anforderungsanalyse																																									
	Meilenstein 1									♦																																
2	Konzepte, Methoden, Werkzeuge																																									
2.1	Gesamtarchitektur und Konzepte																																									
2.2	Organisationsmodell und Prozessvorgaben																																									
3	Entwicklung eines Prozessmodells																																									
4	Integration																																									
	Meilenstein 2																								♦																		
5	Anwendungsfälle und Evaluierung																																									
5.1	Use Case 1: Überseehäfen (Eurogate)																																									
5.2	Use Case 2: Binnenhäfen (Hafen Magdeburg)																																									
	Meilenstein 3																														♦											
6	Projektmanagement, Transfer, Öffentlichkeitsarbeit																																									

Tabelle 2: Zeitplanung der Arbeitspakete nach erfolgreich beantragter Verlängerung

3. Stand der Wissenschaft und Technik vor Projektbeginn

Im Folgenden wird der Stand der Technik, welche bei der Eurogate geplant zum Einsatz kommen sollte, dargestellt. Im Laufe des Projektes wurde dieses als Ausgangslage verwendet und weiter verfeinert. Anschließend wird der Stand der Wissenschaft detailliertere erläutert.

3.1 Stand der Technik

Eurogate betreibt seine Terminals in Deutschland mit Straddle Carriern. Diese übernehmen den horizontalen Transport zwischen dem Lagerbereich im Yard und dem wasser- bzw. landseitigen Ver-, Entladen auf / von Schiffen, LKW oder Zügen sowie den Transport innerhalb der Lagerblöcke inklusive Ein- und Ausstauen.
Diese Transport-Geräte sollen automatisiert werden und zukünftig komplett fahrerlos ihren Weg finden. Ein solches automatisiertes Transport-System gibt es derzeit nur an zwei Terminals in Australien sowie in Long Beach (USA).
Das derzeit einzige automatisierte Terminal in Hamburg Altenwerder benutzt einen vollständig anderen Operationsmodus mit Blockstau und automated guided vehicles (AGV).

Wesentliche Anforderungen an die bei Eurogate angestrebte Lösung sind

- Freie Navigation innerhalb und außerhalb der Lagerblöcke,
- Obstacle detection innerhalb und außerhalb der Lagerblöcke,
- Sicherheitsgerichtet Integration mit den wasserseitigen Containerbrücken sowie den Portalkränen im Bahnbereich,
- Sicherheitsgerichtet Integration Übergabeverfahren von und zu LKWs sowie manuell betriebenen Bereichen des Terminals.
- Fernsteuerung eines Straddle Carriers bei Bedarf (z.B. bei Störung, im LKW-Übergabebereich oder in der Werkstatt)

Das zu implementierende Gesamtsystem muss mit bereits bestehenden Systemen wie dem Terminal Operation System (TOS), dem Instandhaltungssystem und KPI- bzw. BI-Analyse und -Reporting-Tools integriert werden. Es besteht in sich aus mehreren funktionalen Teilkomponenten:

- Fleet Control und Management System (FCMS)
  - Erhält Transportaufträge für Container und meldet Erfüllungsstatus
  - Disponierung der verfügbaren Fahrzeuge auf die Aufträge
  - Steuert die Ausführung der Aufträge durch Berechnung und Optimierung der Fahrtwege sowie vorausschauendes Claiming der benötigten Fahrtstrecke pro Fahrzeug
  - Collision prevention

    - Ständige Interaktion mit allen Straddle Carrieren und Kran-Systemen
- AutoSC Client
    - Steuert den Straddle Carrier auf Basis der Befehle des FCMS (Bremsen, Beschleunigen, Lenken, Container aufnehmen bzw. absetzen)
    - Obstacle detection und Collision prevention
    - Ständige Überwachung und Auswertung der Daten und Signale des an Bord installierten Equipments (Laser, Sensoren, Positionierungssystem, Fernsteuerung, eStop, etc.)
    - meldet den Ausführungsstatus und den Zustand des Fahrzeuges permanent an das FCMS
- Central Remote-Control System (CRCS)
    - Übernimmt die Fernsteuerung von Fahrzeugen z.B. in Störsituationen oder für den letzten Meter im Truck-Übergabebereich
    - Die Fernsteuerung erfolgt von Büro-Arbeitsplätzen ohne Sichtkontakt zum Fahrzeug
- Secure Access Control System (SACS)
    - Übernimmt die sicherheits-gerichtete Kommunikation zwischen FCMS, Straddle Carriern, Kranen, Zugangstoren, Schleusen in den Übergabebereichen zur LKW-Be- und –Entladung sowie zu manuell betriebenen Terminalbereichen etc.
    - Sperrt im Zusammenhang mit dem FCMS bei Bedarf Terminal-Bereiche gegen das Einfahren von Fahrzeugen, wenn Personal den automatisierten Bereich betreten muss
- Lokalisierungssystem
    - Auf dem Straddle Carrier installiertes Positionierungssystem (ähnlich GPS) zur hoch genauen Positionsbestimmung des Straddle Carriers im Terminal
- Crane Instrumentation System (CIS)
    - Kommunikations- und Steuersystem auf den wasserseitigen Kränen (Container-Brücken) sowie den Portal-Kranen im Bahn-Bereich zur Kommunikation und gegenseitigen Absicherung mit den Straddle Carriern (z.B. Claiming der Übergabe-Bereiche unterhalb der Kräne)
    - Die Kommunikation läuft über das FCMS
- Emergency Stop System (eStop)
    - System zur teilweisen oder vollständigen sofortigen Stilllegung der Fahrzeuge in einer Ausnahmesituation.

Das folgende Schaubild stellt schematisch die genannten Komponenten (rot) und ihre Beziehung untereinander sowie zu bestehenden Systemen (blau) in der Eurogate-IT-Landschaft dar.

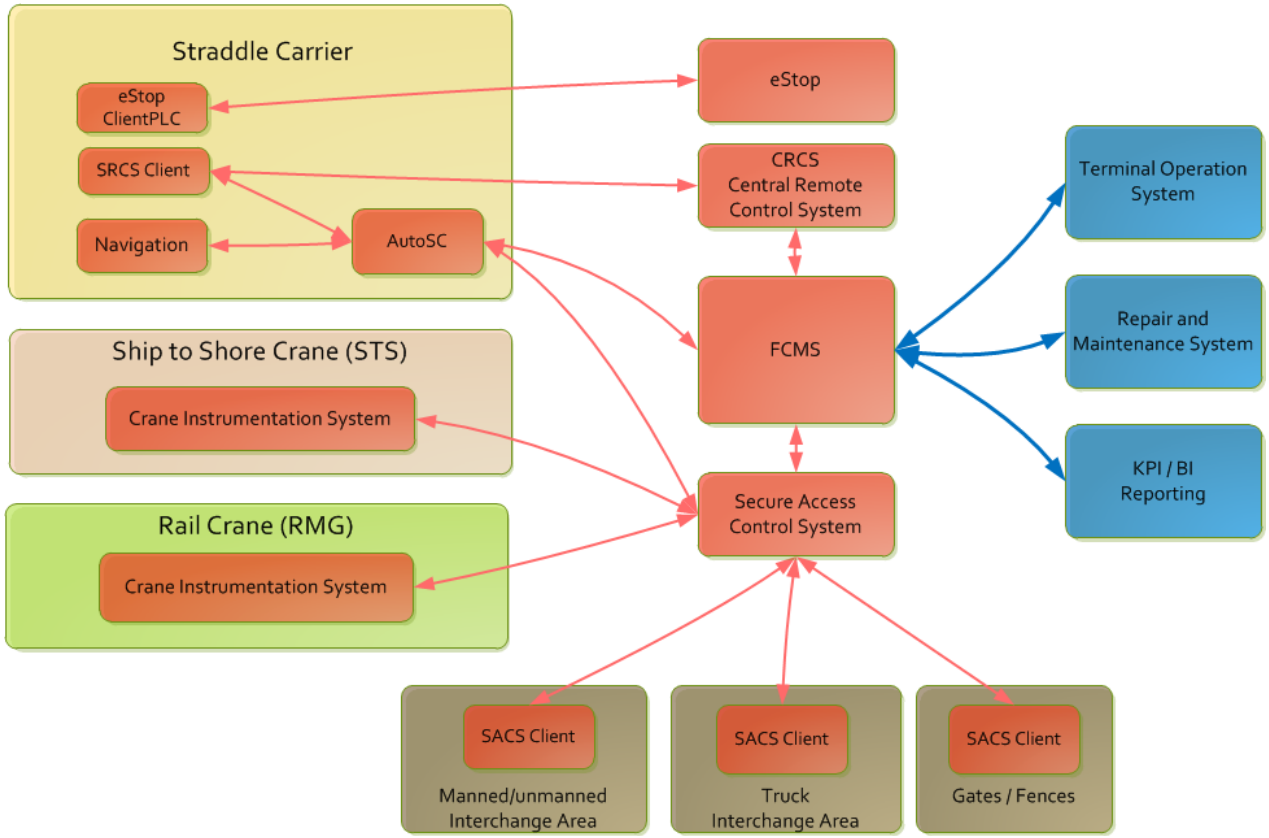


Abbildung 6: Ausgangssituation Eurogate GmbH IT-Systemlandschaft

Die Kommunikation zu den Komponenten auf dem Straddle Carrier erfolgt kabellos. Alle anderen Verbindungen sind kabelgebunden.

3.2 Stand der Wissenschaft

Zusätzlich zu den in den Arbeitspaketen dargestellten wissenschaftlichen Veröffentlichungen sollen hier nochmals einige Aspekte von Security by Design detaillierter dargestellt werden.

In [20] 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 [21] und [22] zeigen, wie durch den systematischen Einsatz von Sicherheitsprozessen die Sicherheit der Systeme signifikant verbessert wurde.

In der Softwareentwicklung sind verschiedenste Software-Entwicklungsmodelle und Vorgehensweisen (Paradigmen) für verteilte Entwicklung betrachtet worden. In [23]und [24]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 [25], [26], 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 [27], um die Qualitäts- und Sicherheitsanforderungen nicht zu gefährden.

Grundlage für das Architektur-Framework entsprechender Systeme bilden die Arbeiten von Edward Lee [28]sowie [27], [29], [30] und [31]. 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.

Teil II

Eingehende Darstellung

4. Verwendung der Zuwendung und des erzielten Ergebnisses im Einzelnen

Der zweite Teil des Berichtes wird zur eingehenden Darstellung der Projektergebnisse verwendet. Als Struktur wird die Aufteilung des Projektes in fünf Arbeitspakete verwendet und die Arbeiten und Ergebnisse entsprechend der Beteiligung der METOP GmbH dargestellt.

4.1 Arbeitspaket 1 – Anforderungsanalyse

Ausgehend von bestehend Report wurde in einem ersten Schritt die allgemeine Bedrohungslage für Cyber-physische Systeme analysiert.

Der VDE (Verband der Elektrotechnik, Elektronik und Informationstechnik) hat 1.350 Mitgliedsunternehmen und Hochschulen der Elektro- und Informationstechnik im Rahmen des VDE-Tec-Reports 2018 [32] befragt. Abbildung 7: Industrie 4.0 - Vernetzung birgt Gefahren zeigt, wo nach Angaben der Industrie und Hochschulen die größten Bedrohungen im Bereich Informationstechnologie liegen.

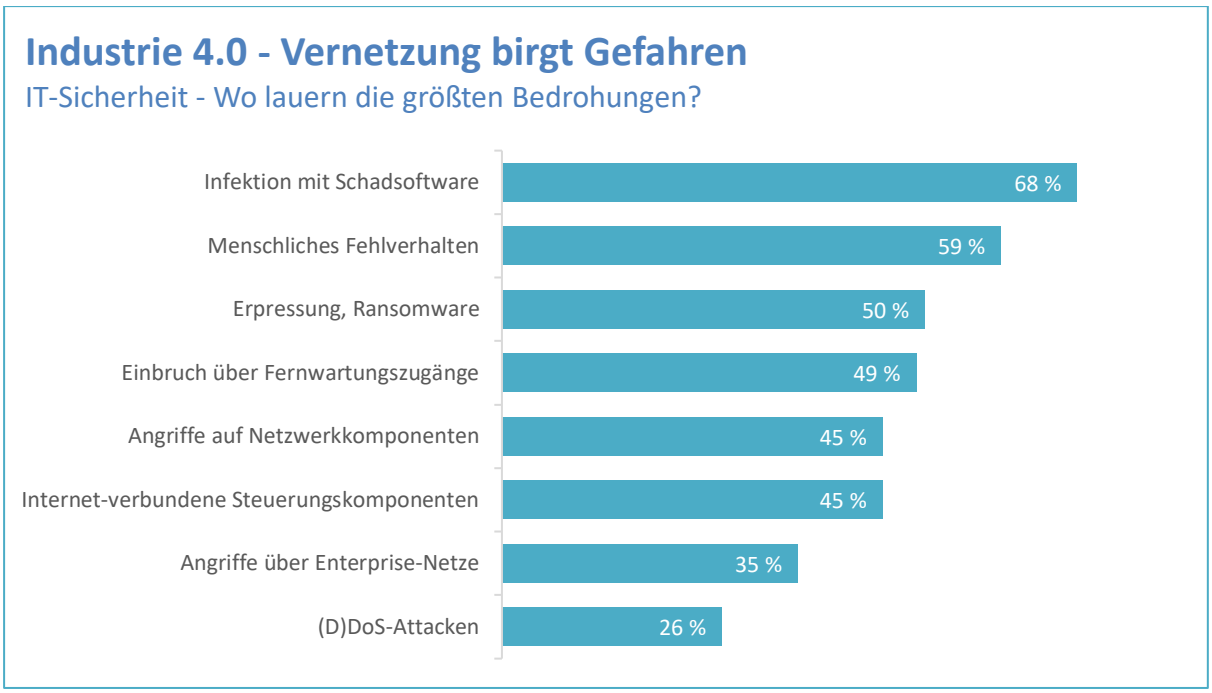


Abbildung 7: Industrie 4.0 - Vernetzung birgt Gefahren

Nach Angaben der Befragten ist die Infektion durch Schadsoftware die größte Bedrohung für Industrie 4.0 – dies nennen 68 Prozent als Bedrohung. Und jedes zweite Unternehmen gibt an, dass speziell die Erpressung mit Hilfe von Ransomware eine Gefahr ist.

Neben dem VDI, hat auch das BSI im Jahr 2019 eine entsprechende Befragung zu den TOP 10 Bedrohungen [33] im Bereich Operation Technologie durchgeführt. Zu den häufigsten Bedrohungen für Unternehmen zählen laut BSI insbesondere Infektionen der IT.

TOP 10 Bedrohungen	Trend seit 2016
Einschleusen von Schadsoftware über Wechseldatenträger oder Hardware	

Infektion mit Schadsoftware über Internet und Intranet	
Menschliches Fehlverhalten und Sabotage	
Kompromittierung von Extranet und Cloud-Komponenten	
Social Engineering und Fishing	
(D)DoS Angriffe	
Internet-verbundene Steuerungskomponenten	
Einbruch über Fernwartungszugänge	
Technisches Fehlverhalten und höhere Gewalt	
Kompromittierung von Smartphones im Produktionsumfeld	

Tabelle 3: Top 10 Bedrohung nach BSI 2019

Die beiden Umfragen zielen inhaltlich auf unterschiedliche Einsatzbereiche ab. Die Bereiche IT (Informationstechnologie) und OT (Operation Technologie) werden nachfolgend detaillierter untersucht und deren unterschiedliche Betrachtungsweisen zu Sicherheit erklärt. Im Großen und Ganzen zeigen die Umfragen aber ein ähnliches Bild bzgl. der Verteilung einzelner Bedrohungen. Bedrohungen aus dem physischen Raum können nur den Punkten „menschliches Fehlverhalten“ (absichtlich, aber auch unabsichtlich) in beiden Umfragen und dem Punkt „Technisches Fehlverhalten und höhere Gewalt“ im Bereich OT zugeschrieben werden. Daraus könnte man schließen, dass die Bedrohungen im Cyber-Raum sowohl im Bereich Informationstechnologie und Operation Technologie als größer eingeschätzt werden.

Diese Schlussfolgerung liegt aber eventuell auch in der Betrachtungsweise des Problems. Der physische Zugriff auf Komponenten ist meist durch entsprechende physische Zugangssperren geregelt. Hier gilt im Allgemeinen das Prinzip des Wegsperrens von Systemen, da bei einem öffentlichen Zugang zu diesen Systemen, ein sicherer Betrieb meist nicht zu gewährleisten wäre.

Beispielsweise sei hier der Versuch der Medienindustrie genannt, entsprechende Medien vor der unordnungsgemäßen Verbreitung mittels Raubkopien zu schützen. Hier wurden Vielzahlen von Varianten entwickelt, um das Kopieren von Informationen zu verhindern. Am Ende musste aber andere Geschäftsmodelle gewählt werden, da die Verbreitung von Raubkopien nicht eindämmt werden konnte. Dieses liegt im Allgemeinen darin begründet, dass durch den physischen Zugriff auf die Daten und die Abspielung dieser auf entsprechenden Endgeräten ein Übergang von digital geschützten Inhalten auf physisch ungeschützte Informationen vorliegt. So können mit entsprechenden Geräten die physischen Daten abgegriffen (beispielweise am Monitor) und in neue digitale ungeschützte Formate überführt werden.

Auch die Manipulation von Steuerungssoftware in Fahrzeugen ist mit entsprechendem physischem Zugang problemlos möglich. Klassische Angebote zum Chiptuning zeigen diese Problematik klar auf.

Auch die Manipulation von Geldautomaten erfolgt meist physisch, Stichpunkt Skimming. So werden entsprechende Geräte eingebracht, welche das Auslesen der Karteninformation inklusive entsprechender Pins ermöglichen.

Arbeiten an der University of Michigan [34] haben weiterhin aufgezeigt das auch physische analoge Backdoors in die Hardware von Prozessoren eingebettet werden können, welche durch klassische Sicherheitsanalysen nicht erkannt werden können. Hier wird also im physischen Raum eine Änderung der Hardware benötigt, welche wiederum durch physische Signale eingeschaltet wird, um anschließend einen Angriff im Cyber-Raum durchzuführen.

Es gibt also auch vielfältige Angriffsmöglichkeiten im physikalischen Raum, nur werden diese derzeit wenig genutzt, da ein physischer Zugang zu den Systemen gewährleistet sein muss. Dieses könnte in Zukunft aber durch Service Mitarbeiter wissentlich oder unwissentlich in den Operation Technologie Bereich eingebracht werden (Stichpunkt manipulierte Hardware).

Weiterhin zeigen Sicherheitsforscher auf, das in komplexen Systemlandschaften Konfigurationsfehler entstehen können. Ein recht aktuelles Beispiel für dieses „menschliches Fehlverhalten“ sind die offen zugängliche Elastic Block Store-Volumes bei einem großen Web-Service-Anbieter, vorgestellt von Ben Morris auf der DEF CON 27 im Jahre 2019 [35]. Tausende Benutzer änderten versehentlich den Status ihrer virtuellen Festplatten von „private“ auf „public“ und ermöglichten so unabsichtlich den komplett öffentlichen Zugriff auf alle Inhalte auf diesen Medien. Dieses Szenario ist im OT Bereich ein bekanntes Problem, da nicht jede physische Reparatur zielführend ist. So werden im Bereich prädiktive Maintenance zwar derzeit viele Ansätze zur genaueren Bestimmung von Fehlerursachen verwendet, aber es ist wohl noch ein weiter Weg bis sichergestellt ist, dass bei allen Reparaturen die ursächlichen Probleme beseitigt wurden und nicht nur die Symptome gelindert werden. Hier liegen also auch Konfigurationsfehler bezüglich der verwendeten physischen Komponenten vor.

Für alle Cyber- und physischen Angriffsmöglichkeiten besteht grundsätzlich das Problem der Detektion. Derzeitige erfolgreiche Attacken werden meist durch Menschen detektiert (z.B. Fehlfunktionen von Systemen) oder gemeldet (z.B. Veröffentlichung von Data Leaks). Zwar gibt es schon Systeme, welche Angriffsmuster automatisch detektieren, aber meist sind diese nur im Anfangsstadium erfolgreich. So kann ein Network-Intrusion System zwar zur Detektion von Angriffen verwendet werden, aber nach einem erfolgreichen Angriff, wird ein derartiges System die Ausnutzung der gebrochenen Schwachstelle nicht viel entgegensetzen können.

Ausgehend von diesen Annahmen wurden Sicherheitsziele ermittelt, welche in der Bewertung mit Berücksichtig werden sollten.

Security („Informationssicherheit“) stellt die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen in Industrie 4.0-Anlagen und -Systemen sicher. Bei Security geht es darum, Gefahren abzuwehren, die auf die Anlage bzw. deren Funktionen einwirken. Insbesondere sind explizite und nicht intendierte Angriffe eingeschlossen. Sicherzustellen ist die Informationssicherheit für alle Funktionalitäten, sowohl für Betriebsfunktionen als auch für Überwachungsfunktionen und Schutzfunktionen (z. B. Safety).
Bei Safety („Funktionale Sicherheit“) für Systeme geht es darum, durch geeignete Maßnahmen sicherzustellen, dass von der Funktion einer Maschine oder Anlage keine Gefahr für Menschen oder Umwelt ausgeht. Safety ist ein Teil der Schutzfunktionen zur Betriebssicherheit.

Für Produkte, Komponenten und Industrie 4.0-Anlagen sind folgende Schutzziele zu berücksichtigen:

- Verfügbarkeit, Integrität und Vertraulichkeit
- Betriebssicherheit
- Know-how-Schutz
- Authentisierung (Identifizierung), Authentifizierung (Authentifikation) und Autorisierung - Der sichere Nachweis und die exakte Verifizierung einer Identität ist bei Industrie 4.0 von besonderer Bedeutung.
- Identitätsmanagement mit eindeutiger Zuordenbarkeit und integrierter Schlüsselverwaltung
- Verbindlichkeit (getätigte Handlungen dürfen nicht abstreitbar sein)
- Zurechenbarkeit (eindeutige Zuordnung einer Handlung zum Handelnden)
- Datenschutz

Wichtige, zu berücksichtigende Aspekte sind:

- Bewertungsverfahren für Bedrohungspotenziale und Risiken inklusive Kosten/Nutzen-Abschätzung von Sicherheitsmaßnahmen
- Schutz von Schnittstellen im Außen- und im Innenverhältnis
- Schutz von Kommunikationssystemen in der Anlage
- Auswirkung von Security-Lücken auf Gefahren für die Betriebssicherheit

- Wechselwirkung mit rechtlichen Vorgaben z. B. zu Datenschutz
- Security-by-Design
- Langzeittauglichkeit von Sicherheitslösungen
- Angriffsdetektion und -analyse
- Grundlegende Differenzierung zwischen böswilligen Angriffen und vorhandener Fehler in den Systemen
- Durch die zunehmende Komplexität und die dynamische Weiterentwicklung von Systemlandschaften (physische Komponenten und Cyber-Komponenten) und speziell die zukünftige Evolution von CPS (zunehmende Komplexität, Wachstum, etc.) birgt die Gefahr von exponentiell wachsender Bedrohungslage bzgl. Fehleranfälligkeit und Angriffen. Dabei sind nicht Angriffe, sondern Fehler immer häufiger die Ursache von Fehlfunktionen bzw. Sicherheitsverletzungen und sollten daher genauer betrachtet werden.
- Erfordernis von hoch dynamischen IT-Operation-Management-Prozessen

Dabei sind folgende Randbedingungen zu berücksichtigen:

- Ausrichtung der Sicherheitsbetrachtung an den betroffenen horizontalen und vertikalen Wertschöpfungsnetzen
- Ausrichtung an konkreten Use-Cases und zeitnahe Übertragung in anwendbare Ergebnisse, die die Praxistauglichkeit beweisen
- Berücksichtigung des „Faktors Mensch”: Transparenz, Usability, Nutzerakzeptanz, Datenschutz
- kontinuierliche Verbesserung (KVP) - Umsetzung von Veränderungen als Ergebnis von Problemen (Plan-Do-Check-Act-Zyklus auch Demingkreis)
- NIST - Cybersecurity Framework
- Identifizierung und Berücksichtigung aller beteiligten und verantwortlichen Personenkreise, wie z.B. IT-Operation, IT-Development

Bereits heute sind vielfältige Standards und Technologien vorhanden, wobei im industriellen Umfeld bisher nur wenig umgesetzt ist. Die Gründe hierfür sind vielfältig, im Wesentlichen ist aber festzustellen, dass der Hauptzweck einer Automatisierungslösung nicht Security Funktionen sind. Für die Anbieter verteuern Security-bezogene Prozesse Entwicklung und Fertigung und erfordern heute häufig nicht vorhandene Kenntnisse. Für die Betreiber stellen Security-Konzepte häufig entsprechende Hürden bzgl. Aufwand und Akzeptanz seitens des Bedienpersonals dar.

Im Zeitalter des Internets der Dinge (IoT) verschwimmen die Grenzen des eigenen Netzwerks immer mehr und ein reiner Perimeterschutz (Firewall, Viren- und Spam-Filter) an den Grenzen des Netzwerks reicht nicht mehr aus. Der daher weitverbreitetste Ansatz ist „Defense in the depth“ (Verteidigung in der Tiefe). Hierbei wird versucht eine vollständige und bestmögliche Isolation der Entitäten innerhalb eines Netzwerks zu erzeugen.
Um eine hohe Akzeptanz aller Parteien zu erreichen, sind Lösungen zu realisieren, die bedienerfreundlich für die Anwender sind, Entwickler durch Tools entlasten und effiziente Methoden zu einer Security-Bewertung bereitstellen.

Folgende Ergebnisse wurden erwartet:

- Einfach handhabbare und benutzerfreundliche Security-Methoden
- Konzepte für Authentisierung und Authentifizierung
- Sicherheitsrichtlinien (IT-Policies) für alle Mitarbeiter
- Skalierbare Security-Infrastrukturen für industrielle Domänen
- Einfach anwendbare Methoden und Bewertungsverfahren hinsichtlich der Security-Eigenschaften einzelner Komponenten und deren Komposition zu einer Industrie 4.0-Anlage
- Maximierung der Verfügbarkeit der Systeme, Verkürzung von Ausfallzeiten durch möglichst flexible, patchbare und konfigurierbare Systemlandschaften
- Einteilung der Fehlerpotentiale nach böswilligen Angriffen und vorhandener Fehler in den Systemen

- Strategien, Prozesse und Anforderungen definieren, um die exponentielle Zunahme der Komplexität und somit auch der Bedrohungslagen aller Art (Fehler und Angriffe) in einem CPS zu analysieren und abzusichern
- hoch dynamische IT-Operation-Management-Prozesse

Zu berücksichtigen sind dabei:

- Bewertung der Systemkomponenten bzgl. der Relevanz zur Systemsicherheit
- Identifikation und Definition von Teilsystemen
- Unterscheidung und Bewertung der bewussten (Manipulation, Störung etc.) und unbewussten (Fehler, Wechselwirkungen, Ausfälle etc.) Bedrohungen, die für cyber-physische Systeme bestehen und den fehlerfreien Betrieb stören könnten
- Risiko-Analyse / Bedrohungsszenarien
- Aufstellung Anforderungskatalog je Systemkomponente
- „Plug & Operate“ und die autonome, dynamische Konfiguration
- Methoden zur dynamischen Ermittlung und Bewertung der Safety-Funktionen einer Anlage unter Berücksichtigung der Wirkung des erzielten Security-Niveaus auf Restrisiken im Sinne von Safety
- Vorbereitung der Security-Standardisierung
- Erstellung geeigneter Maßnahmen-Kataloge für den Eintrittsfall von Sicherheitslücken, z. B. nach CERT-Methode

Ausgehend von diesen Betrachtungen wurde die Systemlandschaft der Eurogate in zwei Bereiche aufgeteilt.

Cyber-Raum oder auch IT-Systemlandschaft: Alle Hard- und Softwaresysteme, welche keine direkten physischen Auswirkungen in der realen Welt besitzen.

Physischer-Raum: Alle Hard- und Softwaresysteme, welche direkte physische Auswirkungen auf die reale Welt haben.

Im Folgenden werden die Systeme des Physischen Raumes als Cyber-physische Systeme bezeichnet. Eine detaillierte Betrachtung ist im nachfolgenden Abschnitt zu finden.

4.1.1 Cyber-physische Systeme

Cyber-physische Systeme (CPS) bestehen aus mechanischen Komponenten, Software und moderner Informationstechnik, die über eine Infrastruktur, wie das Internet oder Firmennetzwerke, kommunizieren. Durch die umfangreiche Vernetzung von Komponenten lassen sich komplexe Infrastrukturen steuern, regeln und kontrollieren. Zu cyber-physischen Systemen gehören sowohl mobile Einrichtungen als auch stationäre Maschinen, Anlagen und Roboter [28]. Das grundlegende Funktionsprinzip basiert auf:

- Sensoren zur Erfassung der realen, physischen Welt
- Aktoren, durch die auf die reale, physische Welt einwirken
- und vernetzter Software.

In Abbildung 8: Abstrahierte Darstellung eines CPS werden die genannten Bestandteile und die Übergänge schematisch dargestellt.

Die Sensorik liefert Messdaten aus der physischen Welt und verteilt diese über das Netzwerk an ein softwarebasiertes Datenverarbeitungssystems weiter, worin sie dann verarbeitet werden können. Die vernetzten Komponenten und deren physische Aktionen werden hierdurch untereinander abgestimmt. Auf diese Weise können sie (teil-)autonom agieren und nutzen die Netzwerkinfrastruktur, um Daten auszutauschen, die für den Betrieb bzw. die Steuerung benötigt werden. Häufig sind die einzelnen Komponenten in eine Cloud-

Architektur eingebunden, sodass typische Vorteile durch die Vernetzung und die Zentralisierung von Teilen der CPS Landschaft bzw. von Diensten genutzt werden können [36] [37].

Der Einsatz von CPS bietet eine Vielfalt an Vorteilen. Die Anpassungs- und Wandlungsfähigkeit sind umfangreich. CPS tragen auf Grund ihrer wirkungsvollen Ressourcennutzung zur Effizienzsteigerung bei. Prozesse, die für die CPS eingesetzt werden, laufen weitgehend autonom und automatisiert ohne den Bedarf des menschlichen Eingriffs ab. Oft erfüllen Menschen nur noch Kontroll- und Steuerungsfunktionen. Abläufe werden über Benutzeroberflächen konfiguriert, gesteuert und kontrolliert. So können Informationen abgerufen und von außen auf das CPS eingewirkt werden. Auf diesem Weg erfolgt eine Verbesserung der Ergonomie sowie eine Erhöhung von (bestimmten Formen) der Sicherheit. Beispielsweise lässt sich u.a. die Arbeitssicherheit steigern.
Die Kopplung und Vernetzung zu komplexen Strukturen ist jedoch hochgradig anfällig und erzeugt diverse Abhängigkeiten, welche sowohl CPS-intern, als auch extern zur Umgebung vorliegen. Insbesondere gilt dies für autonome Systeme, die sich falsch entscheiden können, wenn Fehleinschätzungen erfolgen oder Regeln falsch befolgt werden. Daraus resultieren Gefahren für die Umwelt, sodass Unfälle verursacht und Menschenleben gefährdet werden.
Im Aufbau und im Einsatz eines CPS ergeben sich verschiedene Herausforderungen, die sich u.a. mit Aspekten der Sicherheit beschäftigten. Dazu wird untersucht, inwiefern das mögliche Versagen der cyber-physischen Systeme, etwa durch feindliche Übernahme oder selbstverschuldeten Ausfall, abgesichert sowie verhindert werden kann.

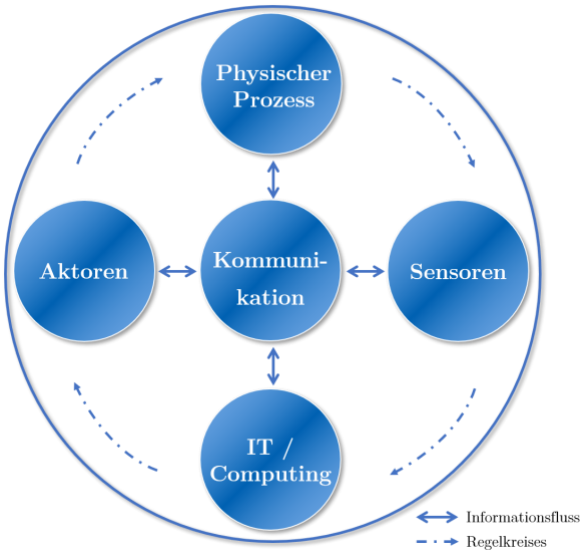


Abbildung 8: Abstrahierte Darstellung eines CPS

4.1.2 Gefahren und Bedrohungen für CPS Systeme

Die grundlegende Struktur und Funktionsweise eines Cyber-physischen System, wie unter 4.1.1 erläutert, bringt zwangsläufig eine massive Erhöhung der Komplexität eines solchen Systems mit sich. Es existieren viele verschiedene Arten von beteiligten Komponenten, wie Sensoren, Aktoren und IT-Systemen, die durch Kommunikationsnetzwerke miteinander in Interkation stehen, meist in Echtzeit, und als Akteur nicht zu vergessen, der Mensch.
Allein die schiere Menge an Komponenten mit verschiedensten Eigenschaften und Bedrohungspotentialen, plus deren permanente Vernetzung, stellt eine enorme Herausforderung an die Absicherung eines solchen Systems dar. Dabei hat ein Sicherheitskonzept in diesem Umfeld nicht nur die Aufgabe Angriffe abzuwehren, sondern es sollte auch gewährleisten, dass die bereits beschriebenen unbewussten Bedrohungen, wie menschliches Fehlverhalten berücksichtigt werden.

Die unbewussten Bedrohungen, zu denen auch Fehler in IT-Systemen besonders in den Softwarekomponenten gehören, werden oftmals unterschätzt. Bei klassischen IT-Systemen gibt es Server, Terminals, mobile Endgeräte und entsprechende Software. Bei einem CPS wir die Systemlandschaft um Sensoren mit Firmware, Aktoren mit Steuersoftware, IoTs mit Embedded Software, usw. erweitert. Wenn man sich vor Augen führt, wie viele Software-Komponenten in einem CPS existieren und miteinander kommunizieren, wird klar, dass „Security-by-Design“ für jedes Unternehmen und jeden Entwickler im Industrie 4.0 Umfeld zum Standard werden sollte/muss. Der Aufwand von Security-by-Design ist um ein Vielfaches geringer, als im Nachhinein Fehler in einem IT-System zu finden und zu reparieren.
Und nicht nur die reine Menge von Software-Komponenten ist entscheidend, sondern auch deren Komplexität und somit deren Anfälligkeit für Fehler. In einem CPS werden immer mehr Produktions- und Geschäftsprozessen fast ausschließlich durch Software gesteuert.
Die Anzahl von Code-Zeilen in einer Software ist natürlich kein 1:1 Gradmesser für deren Komplexität, aber sie können ein gutes Gefühl dafür vermitteln. Diese Art der Komplexität wird nicht weniger werden, sondern steigt permanent immens an. Ein Windows NT Betriebssystem hatte beispielweise ca. 11 Millionen Code-Zeilen, ein aktuelles MacOS Betriebssystem hat bereits ca. 84 Millionen Code-Zeilen.

Folgende grundlegende Klassifizierungen für die Bewertung des Cyber- und physischen Raumes wurden zusätzlich zu den allgemeinen domainübergreifenden Klassifizierung (siehe [38] [39] [40], und Abbildung 11: Bedrohte CPS Komponenten und mögliche Angriffe je Komponentenkategorie nach [40], Abbildung 10: domainübergreifende Klassifizierung nach [39], Abbildung 9: domainübergreifende Klassifizierung nach [38]) definiert:

- *Komplexität:*
  Einführung von Automatisierungslösungen kann zu einer drastischen Erhöhung der Komplexität der Systemlandschaft führen und somit Probleme bei Root-Cause Analysen und beim störungsfreien Betrieb erzeugen.

- *Art des Schutzes:*
  Welche Möglichkeiten bezüglich einer Reaktion auf eingetretene Fehler sind möglich. Hier wird im Folgenden zwischen den Stabilitäts-Ansatz und dem Resilienz-Ansatz unterscheiden.

- *Vernetzung und Erreichbarkeit:*
  Hiermit wird die Einbindung in die bestehende Infrastruktur adressiert und deren Erreichbarkeit. So können Systeme physisch abgeschottet oder öffentlich erreichbar sein. Weiterhin können System über allgemeine Schnittstellen von außen erreichbar sein oder nur über gesicherte überprüfbare Verbindungen (Monitoring des Zugriffes, 4-Augenprinzip)

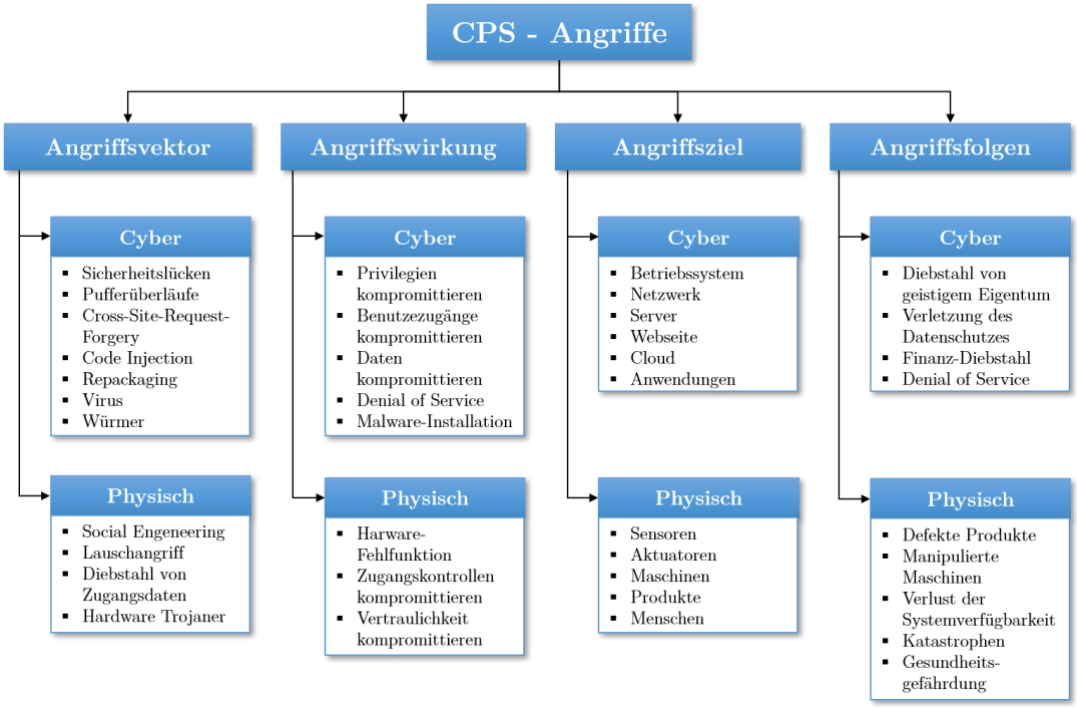


Abbildung 9: domainübergreifende Klassifizierung nach [38]

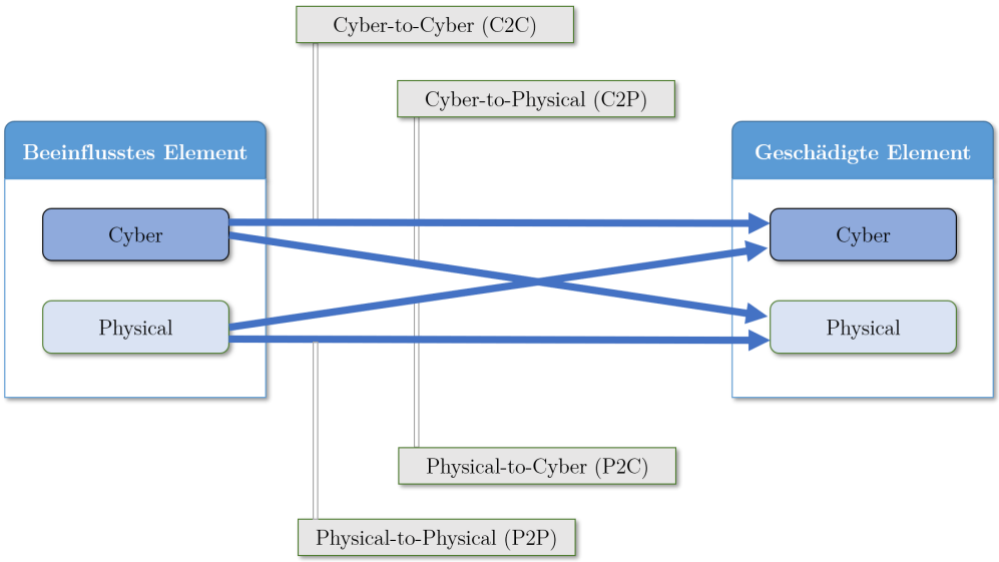


Abbildung 10: domainübergreifende Klassifizierung nach [39]

Abbildung 11: Bedrohte CPS Komponenten und mögliche Angriffe je Komponentenkategorie nach [40]

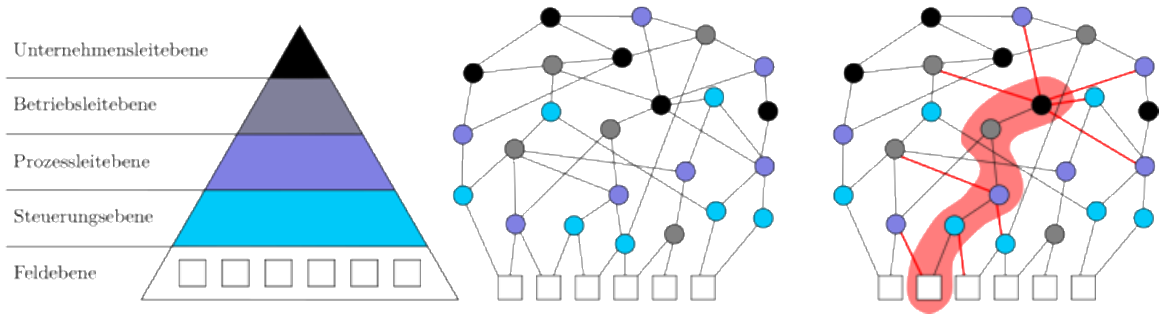
4.1.3 Komplexität von CPS Systemen und Automatisierungslösungen allgemein inkl. Vernetzung

In CPS werden Daten, Dienste und Funktionen dort gehalten, abgerufen und ausgeführt, wo es im Sinne einer flexiblen, effizienten Entwicklung (inkl. Entwurf und Engineering) und Produktion den größten Vorteil bringt. Das wird nicht länger notwendigerweise auf den klassischen Automatisierungsebenen sein. Zum Beispiel könnten Prozessdaten statt über Sensoren auf der Feldebene auch über Dienste in einer sogenannten „Automatisierungs-Cloud“ gewonnen werden. Dies führt zu der Hypothese, dass die heute noch überwiegend existierende Automatisierungspyramide durch die Einführung von vernetzten, dezentralen Systemen schrittweise aufgelöst wird und die verschiedenen Ebenen sowohl für die Struktur der Hardware und Vernetzung als auch für die Informationsverarbeitung und das Engineering nicht weiter existieren werden [5]. Dienste, Daten und Hardwarekomponenten können auf beliebige Knoten des entstehenden Netzes verteilt werden und bilden somit abstrakte funktionale Module, aus denen sich das Automatisierungssystem aufbaut.

Die klassische Automatisierungspyramide zeigt neben der funktionalen Struktur eines Automatisierungssystems die Verdichtung der Daten und Informationen in den einzelnen Knoten. Mit CPS wird die Automatisierungspyramide durch die Möglichkeit der Nutzung und Bereitstellung dezentraler Dienste in den verschiedenen Knoten schrittweise auf ihre funktionale Struktur abstrahiert (Abbildung 12:

Automatisierungspyramide und Automatisierungsnetzwerk). Echtzeitkritische Steuerungen und Regelungen werden hauptsächlich zunächst prozessnah in der Feldebene verbleiben.

Im Zuge der Digitalisierung und der Veränderung der Automatisierung in Richtung von Smart Factories stellen insbesondere Integrationsprojekte eine große Herausforderung dar. Strukturell stellt die klassische Automatisierungspyramide eine typische Ausgangssituation für eine Produktionsanlage dar in die CPS integriert werden sollen. Durch die CPS-Technologie bedingt, wird dieses Strukturierungsmittel und die damit verbundene inhaltlich strikte Trennung sukzessive aufgelöst [41].



Feldebene:	Sensorik, Aktorik, Schnittstelle zum physischen Prozess
Steuerungsebene:	Regelung und Steuerung unter Verwendung SPS
Prozessleitebene:	SCADA (Supervisory Control and Data Acquisition) basierter Überwachung und automatische Steuerung des Produktionsprozesses
Betriebsleitebene:	Produktionsleitung/-datenerfassung, Qualitäts- und Instandhaltungsmanagement (MES - Manufactoing Execution System)
Unternehmensleitebene:	Strategischen und taktischen Unternehmensführung, Ressourcenplanung, Auftragsverwaltung, Produktionsgrobplanung (ERP)

Abbildung 12: Automatisierungspyramide und Automatisierungsnetzwerk

Daher kann zukünftig davon ausgegangen werden, dass die starre, zentralisierte Form durch vernetzte, dezentral organisierte bzw. teilweise selbstorganisierende Dienste ersetzt werden wird [42], [43]. Die feste Struktur wird zukünftig zwar in separate Dienste zerlegt und die strikte Ebenen-Trennung aufgelöst, jedoch bleibt die funktionelle Zugehörigkeit zu einer Ebenen erhalten aufgelöst, jedoch bleibt die funktionelle Zugehörigkeit zu einer Ebenen erhalten [44] [45](siehe Abbildung 7, links und Mitte). Das erhöhte Maß an Vernetzung und die dadurch ermöglichte Kommunikation erlaubt eine Zerlegung von Monolithen zu spezialisierten Diensten, die zur Erfüllung der Aufgaben dezentral miteinander interagieren können, [45]. Dies führt jedoch auch dazu, dass, wie bei CPS üblich, ein erhöhtes Maß an Sicherheit benötigt wird, da sich die mögliche Oberfläche für Angriffe stark vergrößert. Die Steigerung der Vernetzung erschafft aus Sicht der Security
eine Problemlage, die schwer bis nicht mehr zu handhaben ist. Die ursprüngliche Ebenen-Trennung konnten auf Grund der festen Systemgrenzen und Übergänge voneinander isoliert werden, um so eine möglichst geringe Menge an Angriffspunkten zu liefern. Die herkömmliche Ebenen-Trennung geht im Idealfall in eine neuartige netzwerkähnliche Struktur über, in der lose gekoppelte Services miteinander und bis in die Hardware und Sensorik zu kommunizieren und zu interagieren. Für die Einführung von CPS in bestehende Unternehmenslandschaften stellt die Automatisierungspyramide jedoch eine wichtige, strukturelle Orientierungshilfe dar. Durch die verschiedenen Ebenen werden Funktionsbereiche definiert, anhand derer Einführungs- und Integrationsprojekte im Unternehmen, wie sie an dieser Stelle notwendig werden, inhaltlich definiert werden können.

Die Komplexität der eingeführten Lösung sollte aus den oben genannten Gründen daher mit in die Risiko Betrachtung mit aufgenommen werden. Dabei spielt die Einbindung in den Geschäftsprozess auch eine wesentliche Rolle. Die Anzahl der Übergänge in die Automatisierungslösung sollten daher auch berücksichtigt

werden. Es ist anzustreben eine vollständige Isolation der physischen Komponenten zum Cyber-Raum zu erhalten. Hier ist, wie im Abschnitt Architektur ausgeführt wird, eine lose Kopplung zu erreichen.

Folgende Merkmale sollten bezüglich der Komponenten und Komplexität zusätzlich im Risiko Management erfasst werden:

- *Anzahl der Abhängigkeiten getrennt in prozessual und technisch*
- *Komplexität der Automatisierungslösung (High, Medium, Low)*
- *Trennung zwischen physischen und Cyber-Raum (lose, feste Kopplung)*

4.1.4 Art des Schutzes

Die Verfügbarkeit definiert sich nach [34] generell durch: $Verfügbarkeit = \frac{MTTF}{MTTF+MTTR}$.

MTTF *(Mean Time To Failure)*
Ist die durchschnittliche Zeit vom Beginn des ordnungsgemäßen Betriebs eines Systems bis zum Auftreten eines Fehlers.

MTTR *(Mean Time To Recovery)*:
Ist die durchschnittliche Zeit vom Auftreten eines Fehlers bis zur Wiederherstellung des ordnungsgemäßen Betriebs des Systems.

Ziel ist es, die Verfügbarkeit zu maximieren wobei der Höchstwert bei 1 (100 %) liegt. Basierend auf der Formel gibt es zwei Wege dies zu erreichen. Entweder man versucht MTTF zu erhöhen oder MTTR zu verringern. In Abbildung 13: Traditioneller Stabilitäts-Ansatz und Resilienz-Ansatz sind diese beiden unterschiedlichen Ansätze (Stabilitätsansatz und Resilienz-Ansatz) bzgl. der Verfügbarkeit gegenübergestellt.

Der traditionelle Stabilitäts-Ansatz versucht bei der Entwicklung von Systemen die Eintrittswahrscheinlichkeit von Fehlern zu reduzieren. Dabei wird versucht, das Eintreten eines Fehlers möglichst lange hinauszuzögern, d. h. den Wert für MTTF so groß zu machen, dass der Wert für MTTR unbedeutend wird. Das bedeutet i. d. R. einen sehr hohen Aufwand bzgl. der Infrastruktur, z. B. durch redundante Hardware. Je komplexer eine Infrastruktur ist desto aufwändiger gestaltet sich dieser Ansatz.

Im Gegensatz dazu nimmt der Resilienz-Ansatz Fehler als unvermeidbar und teilweise unvorhersehbar hin, sprich MTTF wird als nicht beeinflussbar akzeptiert. Um die Verfügbarkeit dennoch zu erhöhen, versucht man möglichst schnell auf die auftretenden Fehler zu reagieren, sprich MTTR zu minimieren.

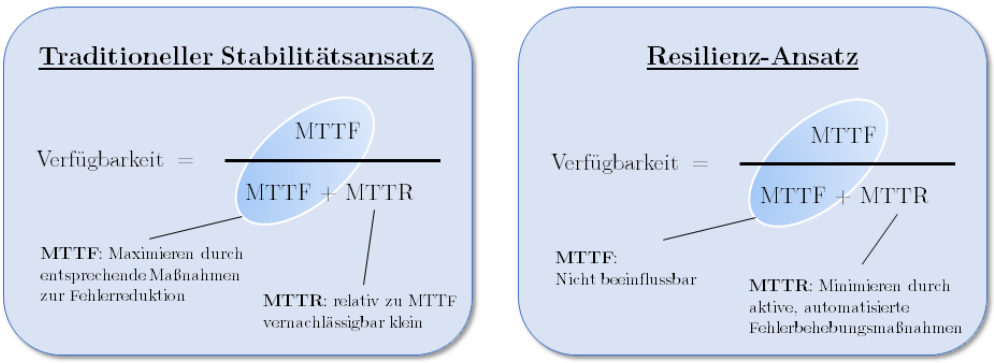


Abbildung 13: Traditioneller Stabilitäts-Ansatz und Resilienz-Ansatz

Bei komplexen, verteilten und stark vernetzten Systemen/Systemlandschaften ist es nicht mehr möglich, entsprechend dem traditionellen Stabilitätsansatz alle erdenklichen Fehler bzw. Fehlerquellen im Vorhinein abzusehen und durch vorbeugende Maßnahmen auszuschließen. Resilienz wird oft als Fähigkeit eines Systems beschrieben. Dabei ist eigentlich die Reaktion gemeint, dass ein System bei negativen Ereignissen, Ausfällen oder Einflüssen nicht vollständig ausfällt, sondern über einen möglichst kurzen Zeitraum wieder selbstständig – ohne menschlichen Eingriff – in seinen optimalen Zustand zurückfindet.

In der Risiko Analyse ist es schwer schon in eventuellen Lösungen zu denken, daher ist es hier ratsam, eher auf allgemeine Faktoren zu fokussieren. Daher ist eine Klassifizierung bezüglich der Fehlerbehebungsmaßnahmen anzuraten.

Folgende Klassifizierung ist empfehlenswert pro Komponente:

Fehlerbehebungsmaßnahmen:

- *manuell:* nach Auftreten eines Fehlers im Event Management des Betriebes, werden manuelle Tätigkeiten eingesetzt den Fehler zu beheben, z.B. Reparatur eines physischen Elementes
- *automatisiert:* nach Auftreten eines Fehlers im Event Management des Betriebes, werden automatisierte Tätigkeiten eingesetzt den Fehler zu beheben, z.B. USV bezüglich der Stromversorgung
- *teilautomatisiert:* nach Auftreten eines Fehlers im Event Management des Betriebes werden, werden manuelle und automatisierte Tätigkeiten eingesetzt den Fehler zu beheben, z.B. händischen umschalten auf redundante Systeme, oder automatisiertes Deployment von neuen Systemen nach händischer Freigabe

4.1.5 Beispielhafte Risikoanalyse bezüglich des WLAN

Drahtlose Netzwerke spielen eine heute eine wichtige, oftmals nicht mehr wegzudenkende Rolle bei der Erreichung einer allgegenwärtigen Kommunikation (Datenaustausch) über weitere aber auch kurze Strecken, in den Fällen, in denen eine kabelgebundene Informationsübertragung nicht umgesetzt werden kann. Diese Netzwerke stellen eine kontinuierliche Konnektivität und Dienste in einer Umgebung mit hauptsächlich mobilen Endgeräten sicher. Da drahtlose Netzwerke räumlich nur schwer oder gar nicht beschränk- und beschütz-bar sind, sind sie naturgemäß ein recht anfälliges CPS-Element für Störungen (Angriffe) in einem Netzwerk. Zu den drahtlosen Netzwerktechniken gehören u.a. WLAN, Bluetooth, NFC, WiMAX und Richtfunk-Techniken.

In drahtlosen Netzwerken werden Informationen mittels elektromagnetischer Funkwellen übertragen. Diese Funkwellen können unbeabsichtigt durch andere elektromagnetische Quellen im selben Frequenzspektrum die drahtlose Kommunikation stören und im Extrem-fall den Betrieb des WLANs verhindern. Dies kann durch andere Funksysteme und Geräte, wie beispielsweise Bluetooth, Mikrowellenherde oder andere WLAN-Netze hervorgerufen werden. Darüber hinaus sind auch beabsichtigte Störungen (Angriffe) wie z. B. Denial-of-Service-Angriffe möglich. Werden beispielsweise bestimmte Steuer- und Managementsignale wiederholt gesendet, kann dies dazu führen, dass das Funknetz nicht mehr verfügbar ist.

Im nachfolgenden Beispiel betrachten wir eine der weitverbreitetsten Art der drahtlosen Netzwerktechnik, das WLAN. WLAN (drahtloses lokales Netzwerk) oder Wi-Fi wird oftmals als allgemeiner Oberbegriff für drahtlose Netzwerke genutzt, meint aber meist nur die Netze basierend auf dem Funknetz-Standards der Normierungsreihe IEEE-802.11x.

Grundsätzlich unterscheidet man zwei Formen der Umsetzung einer WLAN-Architektur, den Ad-hoc-Modus und den Infrastruktur-Modus, u.a. nach dem BSI [36]. Im Ad-hoc-Modus kommunizieren die mobilen Endgeräte (Clients) direkt miteinander. Der Ad-hoc-Modus ist allerdings wesentlich seltener in der Anwendung als der Infrastruktur-Modus. Im Letzteren erfolgt die Kommunikation der Endgeräte nicht direkt, sondern über eine zentrale Funkbrücke, Access Point genannt (AP), siehe Abbildung 14: WLAN-Infrastruktur-Modus.

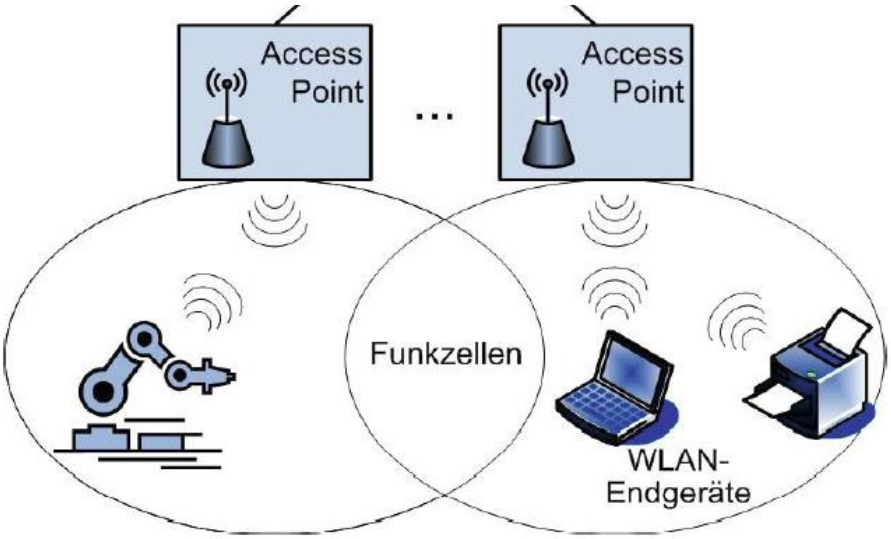


Abbildung 14: WLAN-Infrastruktur-Modus

Die physikalische Übertragung erfolgt beim WLAN, wie bereits erwähnt, auf den Normen IEEE 802.11x. Die verschiedenen Einzelnormen unterscheiden sich hauptsächlich in der Übertragungsgeschwindigkeit und dem ISM-Frequenzband, aktuell 2,4 Ghz und 5 Ghz.

Neben der klassischen Infrastruktur mit autonomen Access Points, welche die WLAN-Funktionen und die Funkübertragung vereinen, kommt zunehmend ein Controller-basiertes WLAN-Design zum Einsatz. Dabei werden zusätzlich zentral positionierte WLAN-Controller benutzt. Diese übernehmen die WLAN-Funktionen und beschränken die Aufgabe der APs ausschließlich auf die reine Funkübertragung, siehe Abbildung 15: Controller-basiertes . Unter WLAN-Funktionen werden in diesem Fall alle „intelligenten“ Funktionen und Dienste (IT/Computing) verstanden.

Um das zu untersuchende WLAN entsprechend der AUTOSEC Taxonomie analysieren und bewerten zu können, betrachten wir in unserem Beispiel ein Controller-basiertes WLAN als eigenständiges CPS. Dazu überführen wir die WLAN-Komponenten in die vorab definierten CPS-Komponenten, siehe Abbildung 8: Abstrahierte Darstellung eines CPS.

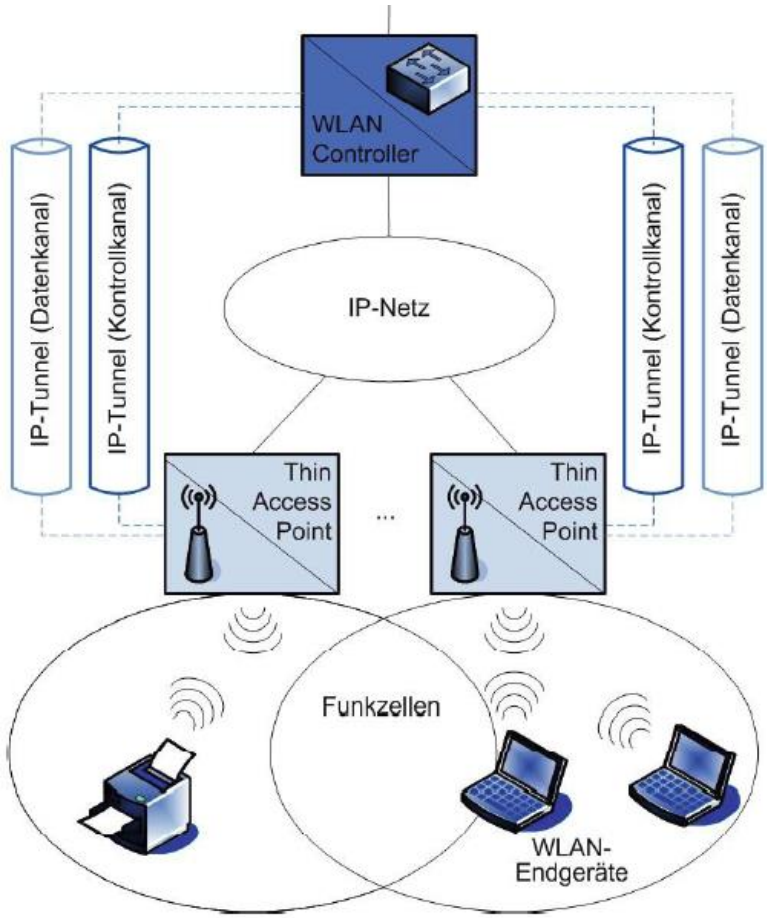


Abbildung 15: Controller-basiertes WLAN-Design

CPS-Komponente (Abb. 11)	WLAN-Komponente (Abb. 14)
1 Physischer Prozess	1 Physische Funkwellen-Übertragung
2 Sensoren	2 Funk-Empfänger: Endgeräte
3 IT/Computing	3 WLAN-Controller
4 Aktoren	4 Funk-Sender: AP
5 Kommunikation	5 IP-Netz

Tabelle 4: Zuordnung WLAN-Komponenten zu CPS-Komponenten

Es gibt verschiedene Arten von unbeabsichtigten Störungen (Angriffen) auf ein WLAN. Im Folgenden gehen wir genauer auf die sehr verbreitete Angriffsart des „Jammings“ ein. Jamming (stören) kann viele Auswirkungen haben, bis hin zu Denial-of-Service-Problemen und weitere daraus folgende Einschränkungen/Problemen. Jamming ist definiert als Unter-brechung und/oder Störung der bestehenden Kommunikation durch Verringern des Signal-Rausch-Verhältnisses auf der Empfängerseite durch Emittieren von störenden Funksignalen. Dies kann auf verschiedenen Ebenen geschehen, wie z. B. Behinderung der Übertragung oder Verzerrung von Paketen innerhalb einer legitimen Kommunikation.

Nach [46] [47] können wir grundsätzlich zwischen zwei Haupttypen von Störsendern unterscheiden, elementar und erweiterte (funktionsbezogene) Störsender unterscheiden. Zudem können elementare Störsender in zwei Untertypen, proaktive und reaktive Jammer, unterteilt werden. Auch die erweiterten Störsender gliedern sich in zwei Untertypen auf, funktions-spezifische und intelligente-hybrid Jammer. Eine Übersicht über die Klassifikation von Störsendern nach [48] zeigt Abbildung 16: Typen von Störsendern WLAN.

Der Störungseffekt eines Störsenders hängt von seiner Funksenderleistung, Lage und dem Einfluss auf das Netzwerk oder den Zielknoten ab.

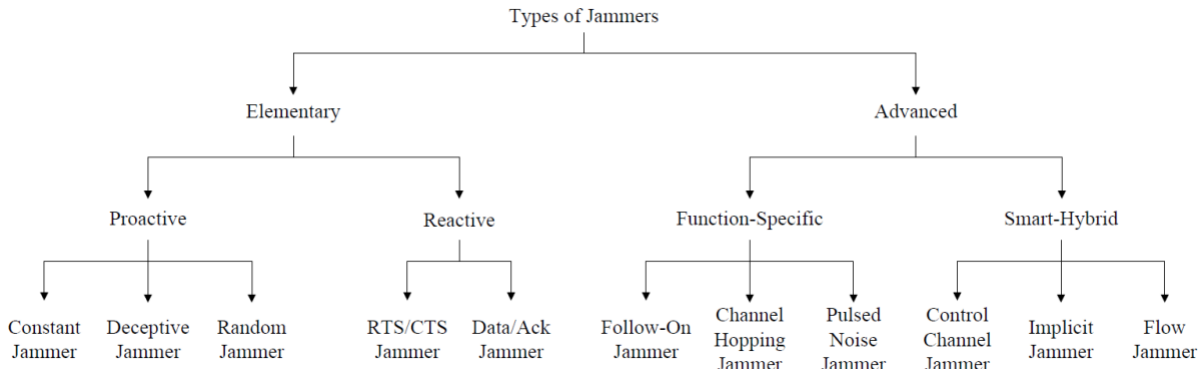


Abbildung 16: Typen von Störsendern WLAN

Bei Störsendern in einem CPS „WLAN“ werden generell nur maximal die drei Schutzziele „Verfügbarkeit“, „Integrität“ und „Zurechenbarkeit“ direkt verletzt. Eine Aufteilung der verletzten Schutzziele je Jammer-Typ zeigt die Tabelle 5: Verletzte Schutzziele durch Jamming

Jammer-Typ	Verfügbarkeit verletzt	Integrität verletzt	Zurechenbarkeit verletzt	Authentizität
Konstanter	X	-	-	-
Täuschender	X	-	X	-
Zufälliger	X	-	-	-
RTS/CTS	X	-	X	-
Data/ACK	X	X	X	-
Follow-on	X	-	-	-
Channel-Hopping	X	-	-	-
Pulsed-noise	X	-	-	-
Control Channel	X	- (X: Steuerkanal)	-	X
Implizit	X	-	-	-
Flow	X	-	-	-

Tabelle 5: Verletzte Schutzziele durch Jamming

Hieraus kann folgende Risikoanalyse abgeleitet werden.

Gesamtbeurteilung für CPS „WLAN“		
Schutzziele	**Eintrittswahrscheinlichkeit**	**Schadenshöhe**
Vertraulichkeit	-	-
Integrität	selten	begrenzt
Verfügbarkeit	sehr häufig	existenzbedrohend
Authentizität und Authentisierung	selten	vernachlässigbar

Zurechenbarkeit	selten/mittel	begrenzt/beträchtlich
Eintrittswahrscheinlichkeit: selten, mittel, häufig, sehr häufig *Potenzielle Schadenshöhe: vernachlässigbar, begrenzt, beträchtlich, existenzbedrohend*		

Tabelle 6: Risikoanalyse für CPS "WLAN"

4.2 Arbeitspaket 2.1 – Gesamtarchitektur und Konzepte

Innerhalb dieses Arbeitspaketes wurde basierend auf den Ergebnissen der Risikoanalyse eine Gesamtarchitektur erarbeitet, dabei wurden insbesondere Konzepte aus modernen Cloud-basierten Architekturen in Zusammenspiel mit DevOps [49] Ansätzen diskutiert. Abbildung 17: Architektur DevOps Systemlandschaft zeigt eine typische Architektur der Systemlandschaft nach DevOps.

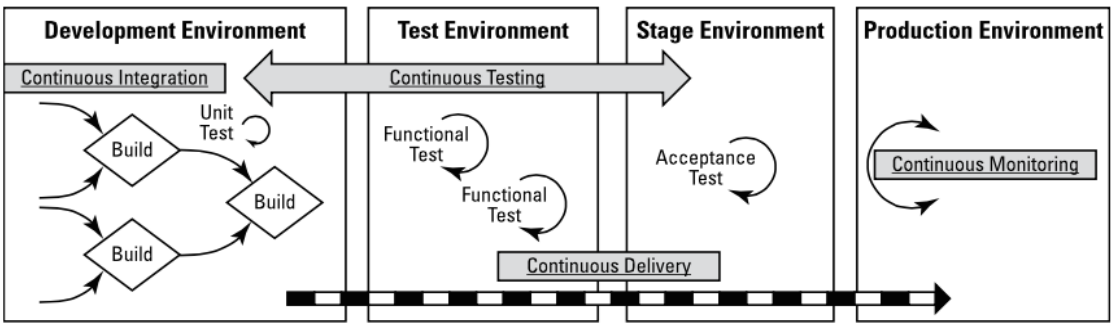


Abbildung 17: Architektur DevOps Systemlandschaft

Dabei wurden folgende Sachverhalte im Projekt ausführlicher diskutiert:

Development Environment: Das das CPS Systems im Normalfall nicht durch die Projektpartner bereitgestellt wird liegt die Entwicklungsumgebung beim jeweiligen Partner, welcher die CPS Systeme zur Verfügung stellt.

Testenvironment: Das Testenvironment bezüglich des CPS Systems zur Durchführung der funktionalen Tests liegt beim Lieferanten des CPS Systems. Im Falle der Eurogate ist dieses Kalmar. Im Falle des Binnenhafens ist dieses nicht ausgeprägt.

Stage Environment: Das Stage Environment liegt bezüglich der Partner zweigeteilt vor. So wird die allgemeine Funktionsfähigkeit durch den Anbieter des CPS Systems dargestellt. Der direkte Einsatz beim Projektpartner wird im Falle der Eurogate im Vorfeld durch Acceptance Test in einem speziellen Testfeld ermittelt. Für den Magdeburger Hafen ist dieses Szenario nicht möglich, da entsprechende Testfelder nur unter sehr hohen Aufwendungen bereitgestellt werden können. Weiterhin besteht bei beiden Partnern das Problem, dass entsprechende Stage Environments der produktiven Umgebung nicht abgebildet werden können. Die Nachstellung eines realen Hafens ist innerhalb eines Stage Environments ist nicht möglich.

Production Environment: Besonderes Augenmerk bezüglich des Production Environments lag innerhalb des Projektes bei dem Continuous Monitoring. Dabei wurde die Beobachtung durch ein kontextsensitives Überwachungssystem diskutiert. Abbildung 18: Kontextsensitives Überwachungssystem zeigt einen möglichen Aufbau eines solchen Systems. Dabei werden Änderungen der physischen Umgebung entlang des nachfolgenden Kreislaufs

- physischen Prozesses
- Datenübertragung (Networking)
- Verarbeitung (Computing)
- Steuerung (Actuation)

untersucht.

Ziel war die Überprüfung des physischen Verhaltens mittels disjunkter oder komplementärer Messmethoden (Zustand des cyber-physischen Systems).

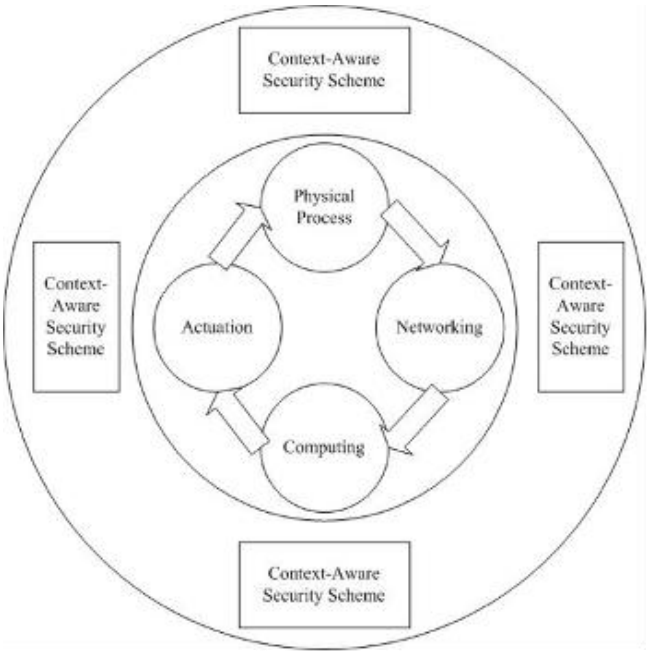


Abbildung 18: Kontextsensitives Überwachungssystem

Hierfür wurde die in Abbildung 19: Systemarchitektur mit digitalem Zwilling zur kontextsensitiven Überwachung dargestellte Architektur gewählt. Diese ermöglicht eine Laufzeitverifikation des Systems und verschiebt damit Teile des Stage Environments in das Production Environment. Ein ähnlicher Ansatz wird auch in [50] beschrieben und kommt zu gleichen Ergebnissen.

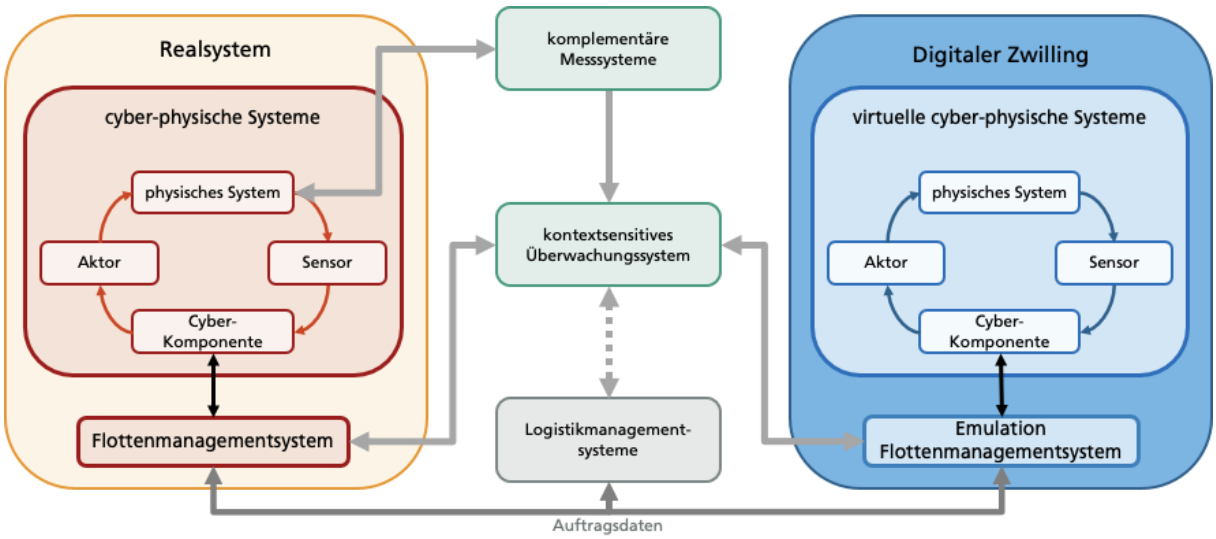


Abbildung 19: Systemarchitektur mit digitalem Zwilling zur kontextsensitiven Überwachung

Daraus können folgende Rückschlüsse bezüglich der zu überwachenden Parameter gezogen werden.
Bedingungen für Eignung CPS

- Parameter wird vom CPS selbst gemessen oder erzeugt.

- Parameter kann überwacht werden.
- Parameter lässt sich ebenfalls mit einem unabhängigen, vom CPS entkoppelten Messsystem mittels unterschiedlicher Messmethodik erfassen.
- Parameter kann simuliert, emuliert oder virtualisiert werden.

Mögliche Quellen:

- Messungen eines Sensors (Observable),
- aggregierte Daten eines Verarbeitungsknotens (Berechnungen) und
- Steuerungsbefehle eines Aktuators

Im Projekt selbst können auf Grundlage des cyberphysischen Logistiksystems neben technischen Kennzahlen auch logistische Kennzahlen Anwendung finden.

Ausgehend von diesen Betrachtungen wurde ein Architekturkonzept für das CPS System entworfen, welches den Security by Design Konzepten der Softwareentwicklung, genauer der Softwareentwicklung von Resilient Systemen entspricht. Dabei wurde insbesondere die Komplexität der Anwendung, welche innerhalb der Risikoanalyse eingeführt wurde, berücksichtigt.

4.2.1 Resilient Design für CPS Systeme

Wie in der Risiko Analyse eingeführt sollten die einzelnen Bestandteile des Geschäftsprozessen sowie des CPS Systems weitestgehend isoliert werden. Daraus lassen sich folgenden Vorteile ableiten:

- Skalierbarkeit
- Autonomie von Subprojekten & Teams
- schnellere Time-To-Market für neue Features
- bessere Wartbarkeit
- technologische Evolutionsfähigkeit

Abbildung 20: Grundprinzip von Resilienz Isolation zeigt die Design Pattern zur Erreichung von Resilienz.

Abbildung 20: Grundprinzip von Resilienz Isolation

Im Zusammenspiel mit dem Risiko eines Ausfalls bei der Eurogate bezüglich der Van Carrier (Stillstand der Logistikkette mit Auswirkungen auf den Hamburger Verkehrsfluss) wurden insbesondere Resilienz Design Pattern näher untersucht. Dabei wurden folgende Pattern näher betrachtet:

- Isolation
  - Bulkheads
  - Complete Parameter Checking
  - Shed Load
- Loose Coupling
  - Asyncronous Communication
  - Location Transparency
  - Event Driven
  - Stateless
- Latency Control
  - Timeouts
  - Fail Fast
  - Bounded Queues
  - Circut Breaker
  - Fan out & Quickest reply
- Supervision
  - Monitor
  - Error Handling
  - Escalation

Ausgehend von diesem Pattern wurde die Aufteilung auf die unterschiedlichen Bereiche bezüglich der Verwendung von Pattern untersucht. Abbildung 21: Vorgehensmodell zur Bestimmung von Design Pattern und deren Einsatz zeigt den schematischen Aufbau.

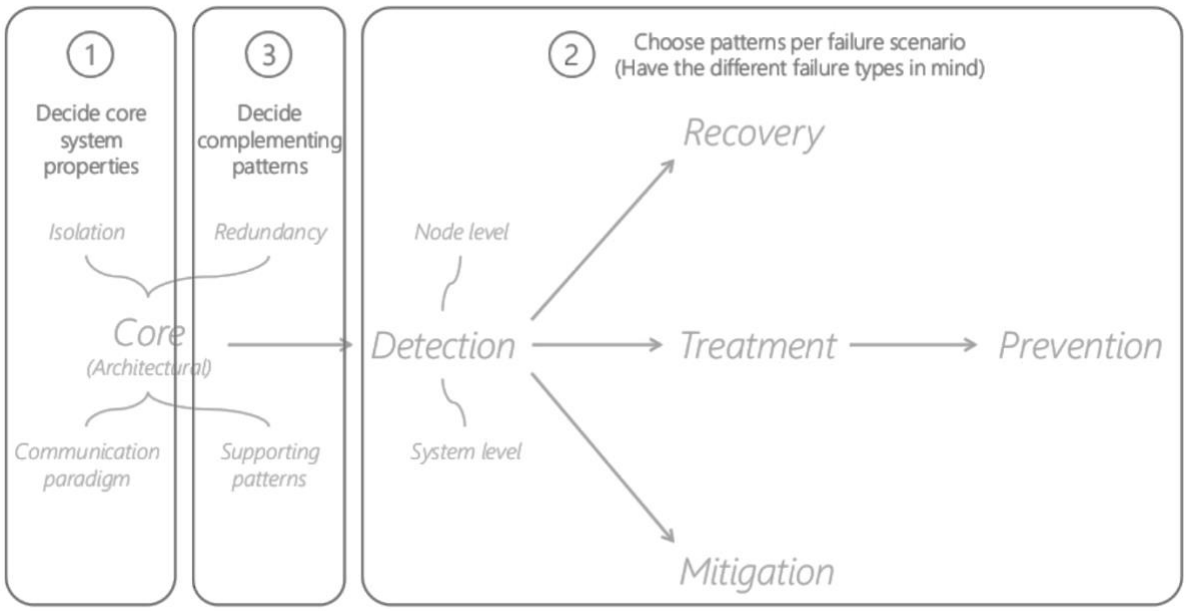


Abbildung 21: Vorgehensmodell zur Bestimmung von Design Pattern und deren Einsatz

Im Folgenden wurden die entsprechenden Lösungsansätze für Fehlszenarien geclustert und erweitert, sowie ihre Anwendbarkeit in Bezug auf CPS Systeme untersucht.

- Recovery
  - Rollback
  - Rollforward
  - Retry
  - Reset
    - Reconnect

        - Restart
        - Data Reset
        - Startup Consistency
    - Failover
    - Read repair
    - Error handler

- Mitigation
    - Shed load
    - Share load
        - statically
        - dynamically
    - Fallback
        - Fail silently
        - Alternative action
    - Queue for resources
    - Marked Data
    - Deferrable work

- Treatment
    - Hot deployments
    - Small releases
    - Let sleeping dogs lie

- Prevention
    - Backup Request
    - Anti fragility
        - Diversity
        - Jitter
    - Anti-entropy
        - Routine Maintenance
        - Spread the news

Damit wurde eine Grundlage geschaffen, die es ermöglicht verschiedene Provider Szenarien (wie z.B. Eurogate und Magdeburg Hafen) zu analysieren und entsprechende architektonische Design Pattern zu wählen. Damit kann ein Schritt hin zu Security By Design abgebildet werden.

Ausgehend von diesen Design Pattern wurden die zu überwachenden Parameter analysiert.

4.2.2 Ableitung zu überwachender Parameter

Innerhalb dieses Arbeitspaketes wurden die architektonischen Design Pattern hinsichtlich der Detection untersucht. Folgende Muster wurden für CPS basierend auf [51] analysiert:

- Node Level
    - Checksum
    - Timeout
    - Circuit breaker
    - Complete parameter checking
- System Level
    - Monitor
    - Watchdog
    - Heartbeat

    - Acknowledgement
- Supporting Patterns
    - Voting
    - Fail Fast
    - Routine checks
    - Leaky bucket
    - Health check

Weiterhin wurden die unterschiedlichen Fehlertypen auf architektonischen Level beschrieben und analysiert [52].

Crash Failure:
Pattern: Failover
Scheme: Active/Passive, Active/Active, N+M Redundancy
Implementations: Load Balancer, Health check, Dynamic routing, Cluster Management

Omisssion Failure
Pattern: Retry, Failover, Backup Request
Schemes: Identical replicas, Failover Schemes for Failover
Implementations: Client based routing, Load Balancer, Leaky bucket + dynamic routing

Timeout Failure
Pattern: Timeout + retry to different replica, Timeout + failover, Backup request
Schemes: Identical replicas, Failover Schemes for Failover
Implementations: Client based routing, Load Balancer, Leaky bucket + dynamic routing

Response Failure
Pattern: Voting, Recovery blocks, Routine exercise
Schemes: Identical replicas, Different replicas
Implementations: Majority based quorum, Adaptive weighted sum, Synthetic computation

Byzantine Failure
Pattern: Voting, Recovery blocks, Routine exercise
Schemes: Identical replicas, Different replicas
Implementations: Majority based quorum, Adaptive weighted sum, Synthetic computation

Entsprechend der gewählten Design Pattern können die zu überwachenden Parameter bestimmt werden. In Zusammenspiel mit dem Arbeitspaket 1.7. wurde der Fokus auf CPS geschärft und für die weitere Betrachtung um die Cyber-to-Cyber Angriff-Szenarien reduziert.

4.2.3 Organisationsmodells

Basierend auf dem DevOps Ansatz wurden innerhalb des Organisationsmodells neue Ansätze der Produktzentrierung dargestellt. Im Gegensatz zu der klassischen Aufteilung in Development und Operations, sollten die Bereiche wie in Abbildung 22: DevOps Organisationsmodell gezeigt, aufgestellt werden. Ausgehend von Abbildung 19: Systemarchitektur mit digitalem Zwilling zur kontextsensitiven Überwachung wurde ein Organisationsmodell mit Digitalen Zwilling entwickelt. Dieses Modell wurde später mit den Ergebnissen der Veröffentlichung [53] abgeglichen.

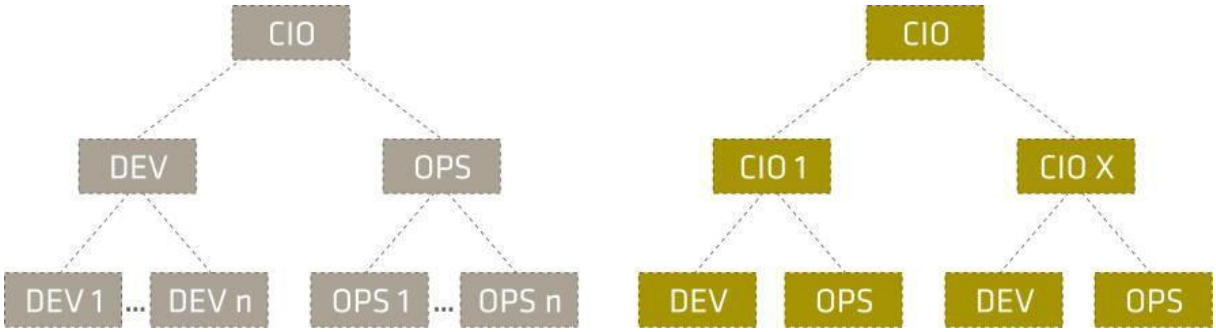


Abbildung 22: DevOps Organisationsmodell

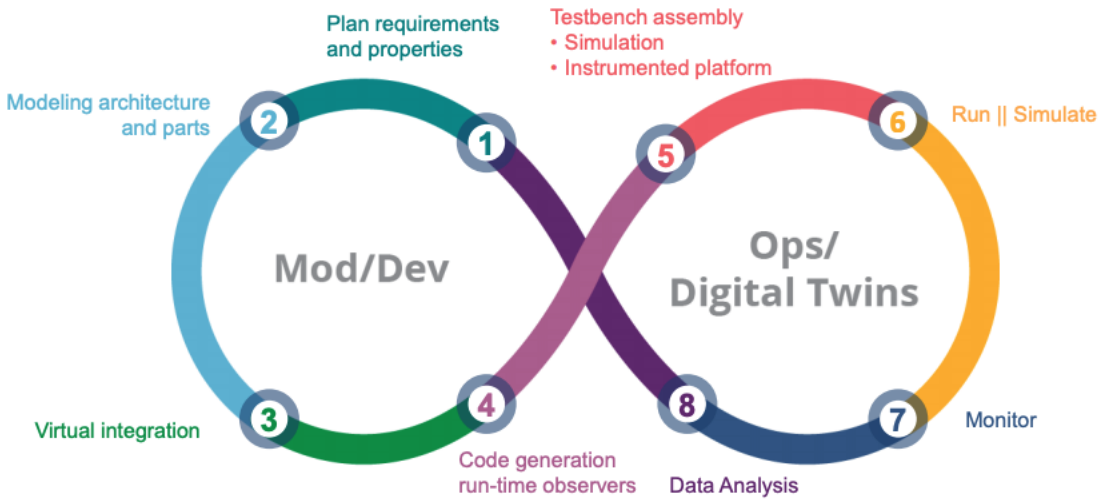


Abbildung 23: TwinOps nach [53]

Weiterhin wurde in diesem Arbeitspaket das Verständnis der Projektpartner im Bereich DevOps erhöht und folgende Bereiche bezüglich der Organisation analysiert.

Folgenden drei Geschäftsziele können mit DevOps bezüglich CPS erreicht werden:

1. Erstens wird die Robustheit des CPS durch ein starkes Bewusstsein der Entwickler für den Verlauf der Wertschöpfungskette und ihren Einflussfaktoren verstärkt.

2. Zweitens sorgen klar strukturierte Abläufe und ein Bewusstsein über diese beim „Fließband“ der agilen Entwicklung für ein schnelles Umsetzen der fachlichen Anforderung und verkürzt damit die Time to Market.

3. Drittens gewährleistet der DevOps-Ansatz die Nachhaltigkeit eines CPS, indem er zukünftigen Entwickler-Teams das Verständnis und die Wiederaufnahme von Arbeiten an diesem Code erleichtert.

Neue Features, kundenspezifische Anpassungswünsche und Hot-Fixes sind typische Beispiele für Elemente, die die Pipeline von der Idee oder der Anforderung und deren Umsetzung in Code-Artefakten bis zum Release bzw. zum Deployment der angepassten Programmversion durchlaufen. Dies gilt ebenfalls für Anpassungen im Rahmen von Security Issues. Zum einen stellt das Schließen von Software-Schwachstellen eine umzusetzende Erweiterung der Software dar, sodass die Code-seitigen Anpassungen automatisiert in der Pipeline verarbeitet werden. Zum anderen können Schwachstellen durch Zusatzbausteine oder Konfigurationsfehler verursacht werden. In solchen Fällen sind Anpassungen innerhalb der Prozessschritte notwendig, um bspw. eine bzgl. Schwachstellen aktualisierte Abhängigkeit zu verwenden oder Anpassungen an Konfigurationseinstellungen

vorzunehmen. Die geschlossenen Sicherheitslücken sind ab dem erfolgreichen Durchlaufen der Pipeline getestet und automatisch Bestandteil in jedem weiteren Release.

Die Pipeline konzentriert sich auf drei Kernthemen, die aufeinander aufbauen und auf vollständige Automatisierung ausgelegt sind (vgl. Abbildung 24: DevOps Pipeline). Das Ziel ist die Minimierung der Zyklen, also die Zeit von der Aufnahme der Anforderungen bis zum Zeitpunkt, an dem die Umsetzung integriert, getestet und bereit zur Auslieferung ist (Continuous Integration) bzw. das Endergebnis erhalten hat (Continuous Delivery).

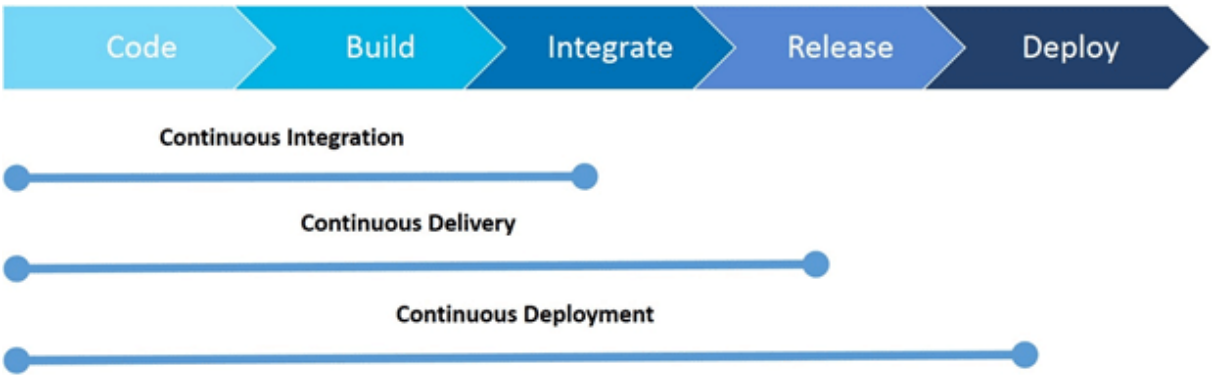


Abbildung 24: DevOps Pipeline

Eine Erweiterung des Continuous Delivery ist das Continuous Deployment, wodurch eine weitere Automatisierung erfolgt und das Produktiv-Deployment ebenfalls ein Teil der Abarbeitungskette wird. Die einzelnen Phasen werden nachfolgend näher erläutert.

Continuous Integration

Der Prozess baut auf die Anwendung klassischer, agiler Software-Entwicklungsmethoden. Auch in großen Projekten arbeiten Entwickler(-teams) an verschiedenen Komponenten, um die Software anzupassen oder zu erweitern. Die Teilschritte des Continuous Integration wird in Abbildung 25 - Continuous Integration dargestellt.

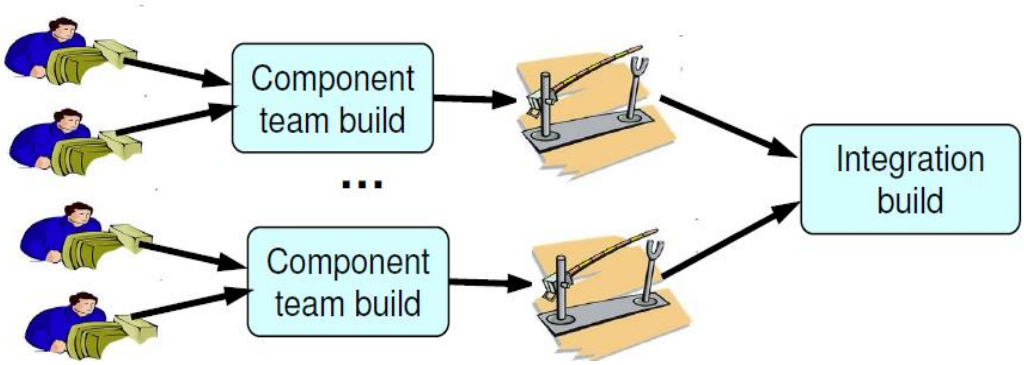


Abbildung 25 - Continuous Integration

Die Entwicklungsergebnisse werden „privat“ je Entwickler gebaut, durch passende Unit-Tests geprüft und bei Erfolg an einen teamübergreifenden Build-Server übergeben. In Kombination mit allen anderen gelieferten Code-Artfakten der gleichen Komponente wird ein integrativer Build für die Team-Komponente erstellt. Übergeordnet erfolgt teamübergreifend die Zusammenführung der einzelnen, erfolgreichen Build-Ergebnisse zu einem systemweiten Integration-Build. Diese Integration führt zu regelmäßigen, am besten täglichen Integrations-Builds, um im Gesamten eine Verifizierung der Arbeiten zu erreichen.

Die kontinuierliche Integration von Softwarekomponenten in die Gesamtcode-Basis eines Programms basiert auf einem immerwährenden Arbeitsfluss in überschaubaren Schritten (Ticketbasierte Abarbeitung, Sprint-Planung).

Dieses Vorgehen ermöglicht eine frühzeitige Fehlererkennung, da durch Testautomatisierung und regelmäßige Integrationstests fortlaufend diverse Prüfungen erfolgen. Bspw. in Form von Unit-Tests, die parallel zur Funktionalität entwickelt werden. Ergänzt werden die Prüfungen durch zusätzliche Testmethoden, wie dem Code Coverage, wodurch die Testabdeckung der Code-Artefakte festgestellt wird. Fehler können auf Basis frühzeitig durchgeführter Checks mit überschaubarem Kosten- und Zeitaufwand behoben werden. In Summe ergeben sich Vorteile bei der Arbeitseffizienz und der Software-Qualität, da die in kleineren Schritten vorgenommenen Änderungen regelmäßig zusammengeführt werden.

Grundkomponenten für den Prozess bilden Code-Repositories, Versionskontrolle und ein darauf aufsetzender, automatisierter Buildprozess. In der Gesamtheit bildet sich so eine Pipeline aus automatisierten sequenziell abzuarbeitenden Teilschritten aus. Der nächste Abschnitt beschäftigt sich mit der Erweiterung des Continuous Integration um automatisierte Auslieferungsschritte.

Continuous Delivery

Das Continuous Delivery ist eine Sammlung von Prozessen, Techniken und Werkzeugen, die den Fokus haben, den Vorgang der Softwareauslieferung durch Automatisierung zu verbessern. Der neue Prozess basiert auf der Weiterentwicklung des Continuous Integration und beinhaltet die bisher erläuterten Schritte. Auf Grundlage dessen wird eine automatisierte Auslieferung an Testing-Umgebung, System-Tests, Staging- und Produktiv-Umgebungen in Form einer gemeinsamen Pipeline ermöglicht. Die Pipeline dient der Validierung aller Änderungen und Schritte und sorgt durch immer wieder neu zu erstellenden Tests und Testumgebungen für eine möglichst hohe Stabilität der Endprodukte.
Im Rahmen der Continuous Delivery Pipeline wird jede Änderung am Programmcode zunächst einmal in der Versionsverwaltung priorisiert, auf den zuständigen Buildserver übertragen und anschließend übersetzt und paketiert. Während dieses Prozesses werden mehrere Tests sowohl automatisiert als auch händisch durchgeführt, um die Lauffähigkeit des Endprodukts zu gewährleisten. Die Tests sind Bestandteil des Prinzips des Continuous Testing, wobei parallel zur Entwicklung begonnen wird solche Tests zu definieren. Neben den Unit- und Integrationstests kann an dieser Stelle frühzeitig damit begonnen werden, Security-Tests in die automatisierte Pipeline zu integrieren.
Abbildung 26 – Verarbeitungspipeline für Continuous Delivery und Continuous Deployment zeigt den typischen Ablauf für die Continuous-Delivery- bzw. Continuous-Deployment-Pipeline in DevOps für eine Applikation von der Entwicklung zur Produktion.

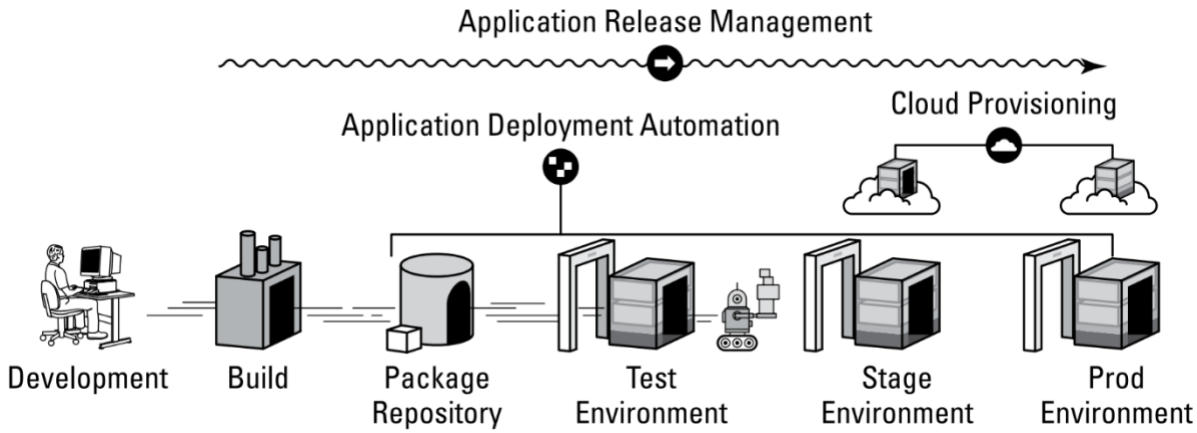


Abbildung 26 – Verarbeitungspipeline für Continuous Delivery und Continuous Deployment

Die Einzelschritte der Pipeline und der Grad der Automatisierung variieren je nach Unternehmen bzw. in einem Unternehmen auch für jedes Projekt. Die Automatisierung kann schrittweise eingeführt werden, wobei der Fokus anfangs auf unternehmenskritischen Phasen liegen sollte. Das Ziel ist die Vollautomatisierung aller Schritte dieses Prozesses. Die erste Ausbaustufe Continuous Integration wird oftmals als Zielzustand erreicht und nicht wieder verlassen, da die Umstellung hinzu einem Continuous Delivery und später Deployment umfangreiche Umstrukturierung in Abläufen und u.a. des Denkens erfordert. Wenn das Deployment nicht automatisiert

funktioniert wird die Geschwindigkeit der Entwicklung zwar schneller, aber der Mehrwert durch neue Features für die Kunden wird nicht unmittelbar weitergegeben.

Development Environment

Die (Weiter-)Entwicklung einer Anwendung findet im Development Environment statt, worin den Entwicklern eine Vielzahl an Werkzeugen bereitgestellt wird, um Code zu schreiben und zu testen. Neben Werkzeugen in Form von integrierten Entwicklungsumgebungen (IDE) sind hierin Werkzeuge zur kollaborativen Entwicklung enthalten. Typische Vertreter sind:

- Quellcodeverwaltung,
- Work-Item-Management,
- Kollaboration,
- Unit-Tests und
- Projektplanung.

Build Phase

Die Build Phase beinhaltet typischerweise den Schritt der Kompilierung der Code-Artefakte. Bedingt durch das Prinzip des Continuous Testing werden die parallel implementierten Unit-Tests verwendet, um die kompilierten Binaries zu überprüfen. In dieser Phase können projekt-spezifisch diverse Build-Tools zum Einsatz kommen, die u.a. auch Cross-Plattform und Cross-Technologie sein können. In Hinblick auf die angestrebte Automatisierung kommen Build-Server zum Einsatz. Hierdurch werden neben der automatischen Erstellung und Unit-Testing, alle Aspekte des Continuous Integration abgebildet.

Package Repository

Alle im Build-Server generierten Binaries werden im Package Repository als zentrales Speicherkonstrukt vorgehalten, nachdem die Unit-Tests und der Test auf die reibungslose Integration durchlaufen wurden. Zusätzlich zum Binary werden alle Artefakte im Repository hinterlegt, die für die weiterführende automatisierte Verarbeitung benötigt werden. Dazu gehören alle zum Deployment der Anwendung benötigten Elemente: Konfigurationen, Infrastructure-as-Code (IaC) Dateien und die Deployment-Skripte.

Testenvironment

Das Testenvironment fasst die Test-Schritte von QA, User-Acceptance und die Entwicklungs- bzw. Testing-Teams zusammen. Der Werkzeugeinsatz kann an dieser Stelle vielfältig und umfangreich ausfallen. Die treibende Kraft ist die Qualitätssicherung, die bestimmt, welche Verfahren und Werkzeuge zum Einsatz kommen.
Folgende Aufstellung beinhaltet Beispiele für QA-spezifische Anforderungen:

- *Test Environment Management:* Tests von Bereitstellung und Konfiguration, u.a. IaC, Cloud und Management Tools
- *Test Data Management:* Für Continuous Testing ist das Datenmanagement für Testdaten essenziell, da hierdurch die Anzahl der Tests und deren Frequenz bestimmt werden.
- *Automatisches Testen von Integration, Funktion, Leistung und Sicherheit:* Dieses Vorgehen konzentriert sich auf die Nutzung von automatisierten Testwerkzeugen, dem organisierten Vorhalten von Szenarien, Test-Skripten/-Konfigurationen und der ermittelten Resultate. Hierdurch können für Defekte unmittelbar Rückschlüsse auf den Code, die Anforderungen usw. gezogen werden.
- *Service Virtualisierungen:* Die Abhängigkeiten in komplexen Systemen können dem Continuous-Gedanken widersprechen, da das multiple Vorhalten und Nutzen nicht möglich oder kostenintensiv sind. Hierfür kommen Service-Virtualisierungen zum Einsatz, die das Verhalten (Funktion und Performanz) simulieren können.

Dabei sind die Bereitstellung der Testumgebung und das Test-Datenmanagement die großen Herausforderungen. Insbesondere für Projekte, die agile Methoden anwenden und kontinuierliche Integration praktizieren. Die einzelnen Bestandteile unterliegen auf Grund dauerhaft stattfindender Zyklen ständigen Änderungen und Erweiterungen. Für Projekte, die die Wasserfallmethode und -tests verwenden, findet diese Phase nur einmal alle paar Monate statt.

Stage- und Produktions-Umgebung

Die Anwendung wird sowohl in einer Stage-Umgebung als auch einer Produktion-Umgebung deployed. Die verwendeten Werkzeuge sind verantwortlich für das Management der Umgebung und für die Bereitstellung. Hier spielen die Infrastructure-as-Code-Tools eine entscheidende Rolle. Durch Virtualisierung und Cloud Technologie inklusive der automatisierten Erstellung der Infrastruktur kann eine Vielzahl an Umgebungen für Stage und Produktion erschaffen werden. Zusätzlich werden passende Monitoring-Tools benötigt, um einen Überblick zu behalten und die Instanzen zu organisieren.

4.3 Arbeitspaket 2.2 - Organisationsmodell und Prozessvorgaben

Ausgehend von den Ergebnissen in Arbeitspaket 2.1 wurde die DevOps Ansätze inklusive der agilen Entwicklungsmethoden für folgende Ansätze untersucht:

Service Provider Sicht: Die Eurogate GmbH setzt CPS Systeme ein, um einen entsprechenden Service selbständig zu erbringen. Dabei fungiert die Kalmar GmbH als Third Level Support und Entwicklungspartner. Dies bedeutet, dass entsprechendes Event Monitoring und der anschließende Incident Management Prozess vollständig bei der Eurogate liegen.

Services Consumer Sicht: Im Gegensatz zur Eurogate GmbH setzt der Magdeburger Hafen entsprechende CPS Systeme als Service ein. Dies bedeutet, dass er die Leistungen, die mittels eines CPS Systems erbracht werden, vollständig von einen Service Provider einkaufen würde. Dieses inkludiert alle Betriebsprozesse. Der Magdeburger Hafen muss aber eine Überwachung der Service Leistung auf dem vereinbarten Service Level übernehmen.

Für die Erbringung der Services würde das ITIL 4.0 Framework analysiert und auf seine Eignung bezüglich der unterschiedlichen Anforderungen der Projektpartner untersucht [54] [55]. Abbildung 27: ITIL 4.0 Prozesse zur Service Erbringung zeigt die Prozesse, welche im Zusammenspiel mit einer Service Erbringung umgesetzt werden müssten.

In Zusammenarbeit mit den Projektpartner wurden die Prozesse des Service Managements bezüglich der Verantwortlichkeit bewertet. Tab zeigt die Ergebnisse dieser Auswertung.

Prozess	Eurogate	Kalmar	Magdeburger Hafen	Service Provider
Availability Management	X	-	-	X
Business Analysis	X	-	X	-
Capacity and Performance Management	X	X	-	X
Incident Management	X	-	-	X
IT-Asset Management	X	-	X	X
Monitoring und Event Management	X	-	-	X
Problem Management	X	X	-	X
Release Management	X	X	-	X

Service Catalogue Management	X	-	-	X
Service Configuration Management	X	-	X	X
Service Continuity Management	X	X	-	X
Service Design	X	X	-	X
Service Desk	X	-	-	X
Service Level Management	X	X	-	X
Service Request Management	X	X	-	X
Service Validation und Testing	X	-	X	X

Tabelle 7: Service Management Prozesse pro Projektpartner

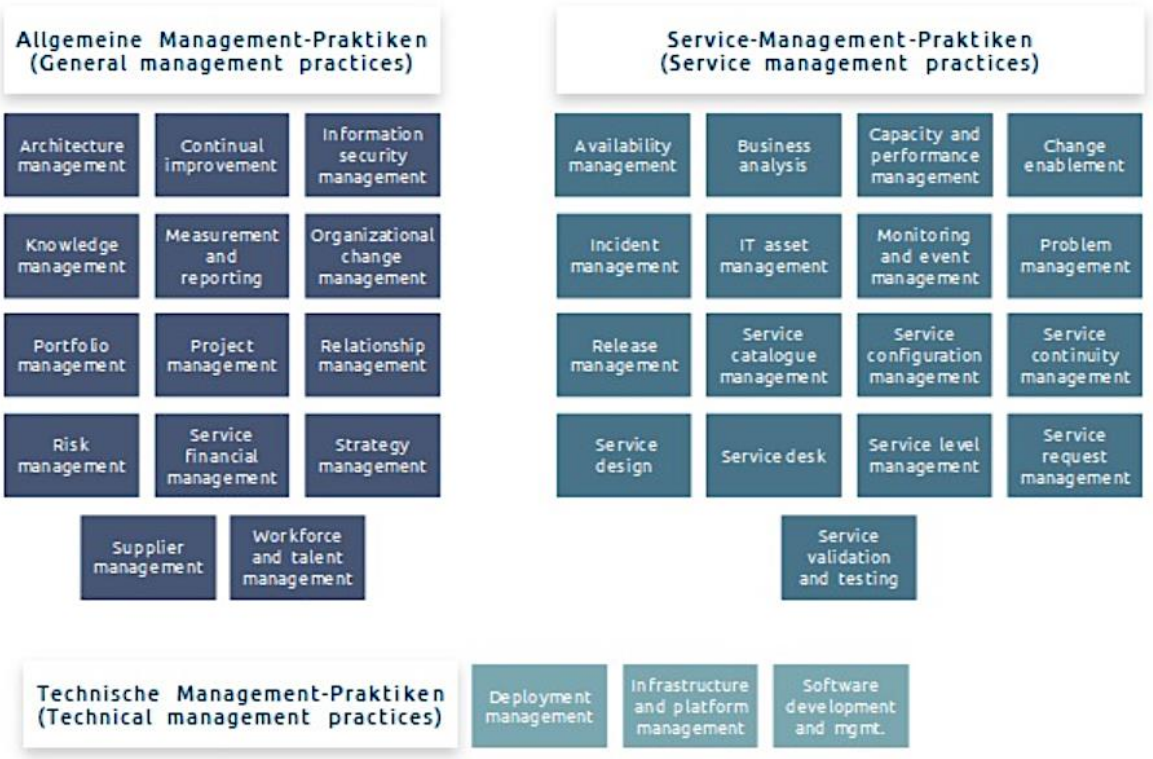


Abbildung 27: ITIL 4.0 Prozesse zur Service Erbringung

Weiterhin wurden die klassischen Risikogruppen aus dem IT-Umfeld auf CPS Systeme erweitert. Dabei wurden die unterschiedlichen Anwendungsszenarien der Projektpartner berücksichtigt. Folgende Risiko Klassen wurden bewertet:

Risikogruppen für CPS Systeme

1. Risikogruppe (abgegrenzte Sicherheitszone): *Partner, mit denen sensible Daten (IT) und Geräte (OT) zum eigenen Vorteil ausgetauscht werden. Das sind zum Beispiel Vertriebsgesellschaften oder Lieferanten. Das Risiko wird auf Grund des wirtschaftlichen Vorteils in Kauf genommen.*

2. Risikogruppe (variable Sicherheitsfaktoren): *Dienstleister wie Werbeagenturen oder Softwareanbieter stellen einen variablen Risikofaktor dar, der von Unternehmen gesteuert werden kann.*

3. Risikogruppen (nicht steuerbare Risiken): Staatliche *Regulierung oder Naturkatastrophen sind nicht-steuerbare Risiken für Unternehmensinformationen. Hier können Unternehmen nur begrenzte Vorkehrungen treffen.*

Auch in diesem Zusammenhang mussten die beiden unterschiedlichen Sichten (Service Provider Sicht, Service Consumer Sicht) bewertet werden.

Service Consumer Sicht: Der Service Consumer übertragt alle sensiblen Daten und Geräte, welche zur Service Erbringung notwendig sind an den Service Provider. Alle Prozessdaten sind je nach Vertragsausführung vertraulich durch den Service Provider zu handhaben. Hier spielen Punkte des Cyberdaten-Souveränität eine wichtige Rolle, da hier der Umgang mit den Daten vertraglich geregelt wird. Beispielsweise kann die Verwendung der Prozess Daten zur Optimierung der eigenen Systeme erlaubt sein, eine übergreifende Verwendung durch den Service Provider kann ausgeschlossen werden (exklusive Nutzungsrechte). Somit sind alle Risikogruppen vom Service Consumer zu bestimmen und entsprechende Regelungen zu verfassen.

Service Provider Sicht: Die Risikogruppe 1 wird auf ein Minimum beschränkt, um eine Abgrenzung zum CPS Produzenten zu erreichen. Der Austausch an Daten ist streng limitiert und sollte nur im Notfall zur Problemlösung und zweckbezogen zur Verfügung gestellt werden. Die variablen Sicherheitsfaktoren in der Risikogruppe 2 sind bestmöglich zu isolieren, um Nichtabstreitbarkeit Problematiken aus dem Integritätsumfeld adäquat zu behandeln.

4.3.1 Rahmenrichtlinie bezüglich der Sicherheitsziele CIA

Ein zu erstellender Sicherheitsprozess ist ein spezieller kontinuierlicher Verbesserungsprozess, welcher für CPS geeignet ist. Er unterteilt sich in fünf wesentliche Schritte, Strukturanalyse, Schutzbedarfsfeststellung, Modellierung des Informationsverbunds (Geltungsbereich des Prozesses), Schutz-Check (Soll-Ist-Vergleich) und die Risikoanalyse. Die im Folgenden beschriebene Reihenfolge ist nicht zwingend. Die Teilaufgaben können je nach Rahmenbedingungen auch unabhängig und gleichzeitig bearbeitet werden.

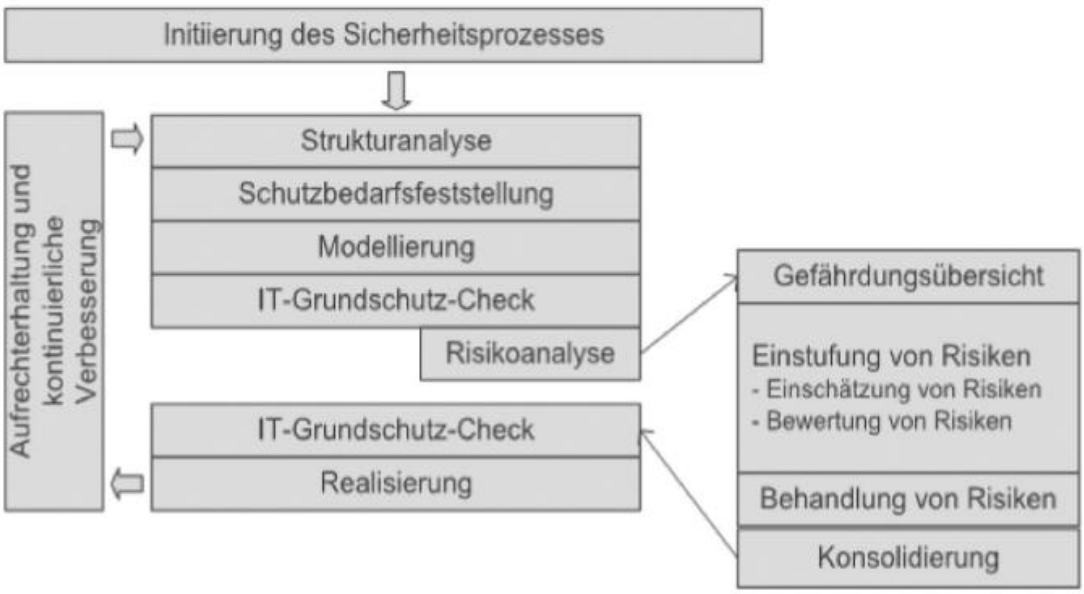


Abbildung 28: Sicherheitsprozess

Zu Beginn eines IT-Sicherheitskonzepts muss festgelegt werden, welcher Bereich der Organisation abgedeckt wird, bzw. der Geltungsbereich abgegrenzt. Dies können z. B. bestimmte Organisationseinheiten oder auch Bereiche sein, die Fachaufgaben oder -verfahren bearbeiten, inklusive der dafür notwendigen IT-Ressourcen, Infrastrukturen und Schnittstellen zu externen Partnern. Dieser Geltungsbereich für die Sicherheitskonzeption wird auch als Informationsverbund bezeichnet.
Ein solcher Informationsverbund wird durch IT-Komponenten, Informationen, organisatorische Regelungen, Aufgabenbereiche und Zuständigkeiten sowie die physische Infrastruktur definiert.

Eine der Vorarbeiten für den Sicherheitsprozess inkl. einer Risikoanalyse ist die Strukturanalyse. Die Hauptaufgabe dieser Teilaufgabe ist das Zusammenspiel der Geschäftsprozesse, der Anwendungen und der vorliegenden Informationstechnik zu analysieren und zu dokumentieren. Es werden grundlegende Informationen, die für den weiteren Sicherheitsprozess benötigt werden, gesammelt. Hierbei geht es um die Erfassung von Geschäftsprozesse, Informationen, Anwendungen, IT- und ICS-Systeme, Räume und Kommunikationsnetze, die zur Betrachtung innerhalb des Sicherheitskonzepts benötigt werden.

Es müssen alle für das Unternehmen wesentlichen Geschäftsprozesse alle geschäftskritischen Informationen und Anwendungen (Software) ermittelt werden. Zudem müssen alle betroffenen IT-, ICS oder IoT-Systeme, Räume und Netze erfasst werden.

Die Strukturanalyse gliedert sich in folgende Teilaufgaben:

- Erfassung von Geschäftsprozesse, Anwendungen und Informationen
- Erhebung von IT-, ICS- und IoT-Systemen und ähnlichen Objekten
- Erfassung der Räume und Gebäude (für den ICS-Bereich sind auch die produzierenden Räumlichkeiten zu berücksichtigen)
- Netzplanerhebung

Aufgrund von Redundanzen oder Menge der Objekte ist es oftmals zweckmäßig, Objekte zu Gruppen zusammenzufassen und nur die Gruppe zu und nicht jedes Objekt einzeln zu erfassen. Die Strukturanalyse bildet den wichtigen Datengrundstock für den gesamten Sicherheitsprozess. Bei der Erfassung alle Einzelobjekte besteht schnell die Gefahr, dass die Ergebnisse durch die Menge und Komplexität im weiteren Prozess nicht mehr händelbar sind. Zusätzlich reduziert eine Gruppenbildung bei technischen Komponenten die Administration, die Anzahl von potenziellen Sicherheitslücken und Sicherheitsmaßnahmen können ohne Unterscheidung verschiedener Schwachstellen umgesetzt werden. Das kommt letzten Endes nicht nur der Sicherheit zugute, sondern es spart Kosten.

Gruppen können gebildet werden, wenn Objekte z.B. vom gleichen Typ sind, ähnliche Aufgaben haben, ähnlich konfiguriert sind, ähnlich ins Netz eingebunden sind, ähnlichen Rahmenbedingungen unterliegen und den gleichen Schutzbedarf benötigen.
Dies gilt natürlich nicht nur für technische Objekte, sondern z.B. auch für Räume und andere Arten von Objekten.

Weitere Ausführungen zu dem Thema Sicherheitsprozess mit entsprechenden Beispielen finden sie im Abschnitt Evaluierung.

Für die Rahmenrichtlinie wurden die Sicherheitsziele Vertraulichkeit, Verfügbarkeit, Integrität und entsprechende Erweiterungen für CPS definiert:

Vertraulichkeit: Bezeichnet die Eigenschaft, dass der Zugriff auf vertrauliche Informationen nur von autorisierten Personen, Entitäten und Prozessen (automatisierter Zugriff) erfolgen darf.

Bei einem Angriff wird die Vertraulichkeit durch unautorisierten/unbefugten Zugriff auf die vertraulichen Informationen verletzt, zum Beispiel durch „Abhören“ eines Funknetzes. Hierbei gibt es zwei grundlegend mögliche Auswirkungen eines Angriffs auf die Vertraulichkeit der vorhandenen Informationen - Datendiebstahl und Datenmissbrauch. Dem Datenmissbrauch geht immer der Diebstahl der Daten voraus.

Es werden jedoch keine Informationen manipuliert, sondern „lediglich“ Informationen aus dem System entnommen. Daher kann der Schaden einer solchen Verletzung der Vertraulichkeit von System zu System sehr unterschiedlich sein. Ausschlaggebend sind dabei die Art, Relevanz und Stufe der Vertraulichkeit der gestohlenen Informationen.

Um die Vertraulichkeit der Informationen in einem CPS zu gewährleisten, müssen daher entsprechende Schutzmaßnahmen sowohl auf der Cyberebene als auch auf der physischen Ebenen ergriffen werden. Mögliche Maßnahmen sind z.B. Zugangskontrollen und Verschlüsselung.

Verfügbarkeit: Die Zeit die ein ganzes CPS, ein Dienst, eine Funktion und Informationen zur Verfügung stehen, wenn sie zur Verfügung stehen sollen/müssen, beschreibt die Eigenschaft der Verfügbarkeit.

I. d. R. ist es Ziel, die Verfügbarkeit so hoch wie möglich zu halten. Je komplexer ein System ist, wie viele systemrelevanten Komponenten existieren und je mehr Verbindungen zwischen diesen Komponenten in einem Netzwerk bestehen, desto höher ist der Aufwand die Verfügbarkeit zu gewährleisten.
Die Verfügbarkeit ist durch Naturkatastrophen, Elementarschäden und zunehmend durch absichtliche Angriffe von Hackern bedroht.

Bei einem Angriff auf die Verfügbarkeit wird durch Manipulation bzw. Sabotage von z.B. Hardware, Software und Informationen versucht die Nutzbarkeit bzw. Funktionstüchtigkeit von Diensten, Funktionalitäten, Informationen, Software, Hardware oder ganzer Systeme zu stören bzw. ganz zum Erliegen zu bringen.

Um die Verfügbarkeit in einem CPS zu gewährleisten, müssen daher entsprechende Sicherheitsmaßnahmen sowohl auf der Cyberebene als auch auf der physischen Ebenen ergriffen werden. Mögliche Maßnahmen sind z. B. Redundanzen in Netzwerken, regelmäßige Datensicherungen, aber auch z. B. auf Personalebene - Vertretungsregelungen.

Integrität: Integrität beschreibt die Eigenschaft, die die Richtigkeit und Vollständigkeit jeglicher „Werte“ gewährleistet und vor Manipulationen schützt. Das gilt sowohl im Cyberbereich als auch im physischen Bereich. Eine Integritätsprüfung einer Information dient der Erkennung jeder unautorisierten und unbemerkten Veränderung/Manipulation dieser Information.

Im Sinne der Integrität können Manipulationen „Werte“ von Informationen, Software, Schnittstellen und Hardware betreffen. Ein Angriff verletzt die Integrität von Informationen durch Manipulation der Informationen indem z. B. Nachrichten, Datensätze, und andere Informationsinhalte verändert, gelöscht, wiederhergestellt oder dupliziert werden. Ein entsprechender Angriff im Sinne der Integrität kann daher einen beträchtlichen materiellen und finanziellen Schaden verursachen.

Um die Integrität der Informationen in einem CPS zu gewährleisten, müssen daher entsprechende Schutzmaßnahmen sowohl auf der Cyberebene als auch auf der physischen Ebenen ergriffen werden. Mögliche Maßnahmen sind z. B. Zugriffskontrolle in Form von Rechten (Schreibrechte) und Verwendung elektronischer Signaturen (Kryptographie).

Authentizität und Authentisierung: Authentisierung beschreibt den Vorgang der zweifelfreien Ermittlung und Prüfung einer Entität, z. B. einer Person. Authentizität wird auch als Echtheit eines Absenders oder einer Information bezeichnet. Anders formuliert bezeichnet die Authentizität die Eigenschaft einer Entität, das zu sein, was sie vorgibt zu sein.
Beispielsweise wird bei einer Benutzerverwaltung jedem Nutzer eine eindeutige Kennung (ID), beispielsweise ein Benutzername zugeordnet, was die Authentizität abbildet. Die Authentisierung erfolgt anschließend durch die Überprüfung der Verbindung der Kennung (ID) und der Nutzeridentität (z. B. durch ein Passwort, welches nur dieser Nutzer kennt). Ist die-se Prüfung positiv, kann davon ausgegangen werden, dass die Kennung (ID) authentisch ist. Da Authentizität sich sowohl auf Informationen (Daten) als auch auf physische Entitäten, wie beispielsweise eine Person bezieht, kann man zwischen Datenauthentizität sowie Instanzauthentizität unterscheiden.

Im Fall eines Angriffs auf die Authentizität gibt sich ein Angreifer durch die Vortäuschung einer gültigen Kennung (ID), welche z.B. durch Social Engineering/Phishing erlangt worden ist als berechtigter Sender aus. Man kann sagen der Angreifer fälscht seine Identität und lässt das System oder andere Personen glauben, er sei jemand anderes. Somit ist die Authentizität nicht mehr gewährleistet.

Um die Authentizität und Authentisierung in einem CPS zu gewährleisten, müssen entsprechende Sicherheitsmaßnahmen sowohl auf der Cyberebene als auch auf der physischen Ebene ergriffen werden. Mögliche Maßnahmen sind beispielsweise Zugangskontrolle durch Login + Passwort (Instanzauthentizität) und Verwendung digitalisierter Signaturen für gesendete Daten (Datenauthentizität).

Zurechenbarkeit: Die Zurechenbarkeit oder auch Verbindlichkeit oder Nichtabstreitbarkeit beschreibt den Vorgang mit dem das Auslösen eines Ereignisses oder einer Aktion zweifelsfrei dem Verursacher zugeordnet und belegt werden kann.
Beispielsweise bezogen auf Daten heißt das, wenn ein Benutzer die Eingabe von Daten in ein EDV-System im Nachhinein nicht abstreiten kann, ist die Zurechenbarkeit in diesem EDV-System gegeben.

Das Schutzziel der Zurechenbarkeit betrifft sowohl die physischen Entitäten als auch die Entitäten im Cyberbereich.

Um die Zurechenbarkeit in einem CPS zu gewährleisten, müssen entsprechende Sicherheitsmaßnahmen sowohl auf der Cyberebene als auch auf der physischen Ebenen ergriffen werden. Mögliche Maßnahmen sind z. B. die Authentifizierung eines Nutzers und deren Protokollierung und den Zugriffszeitpunkt nachzuvollziehen. Aber auch eine eigenhändige Unterschrift auf einem schriftlichen Dokument stellt die Zurechenbarkeit sicher.

Wie in den vorherigen Ausführungen betrachtet, lassen sich Anforderungen zur Erfüllung u. a. der drei Hauptschutzziele Integrität, Vertraulichkeit und Verfügbarkeit definieren. Das in Abbildung 29 - *Schwachstellen gruppiert nach deren Auswirkung* enthaltene Diagramm zeigt die Verteilung der Schwachstellen auf die drei Hauptschutzziele.

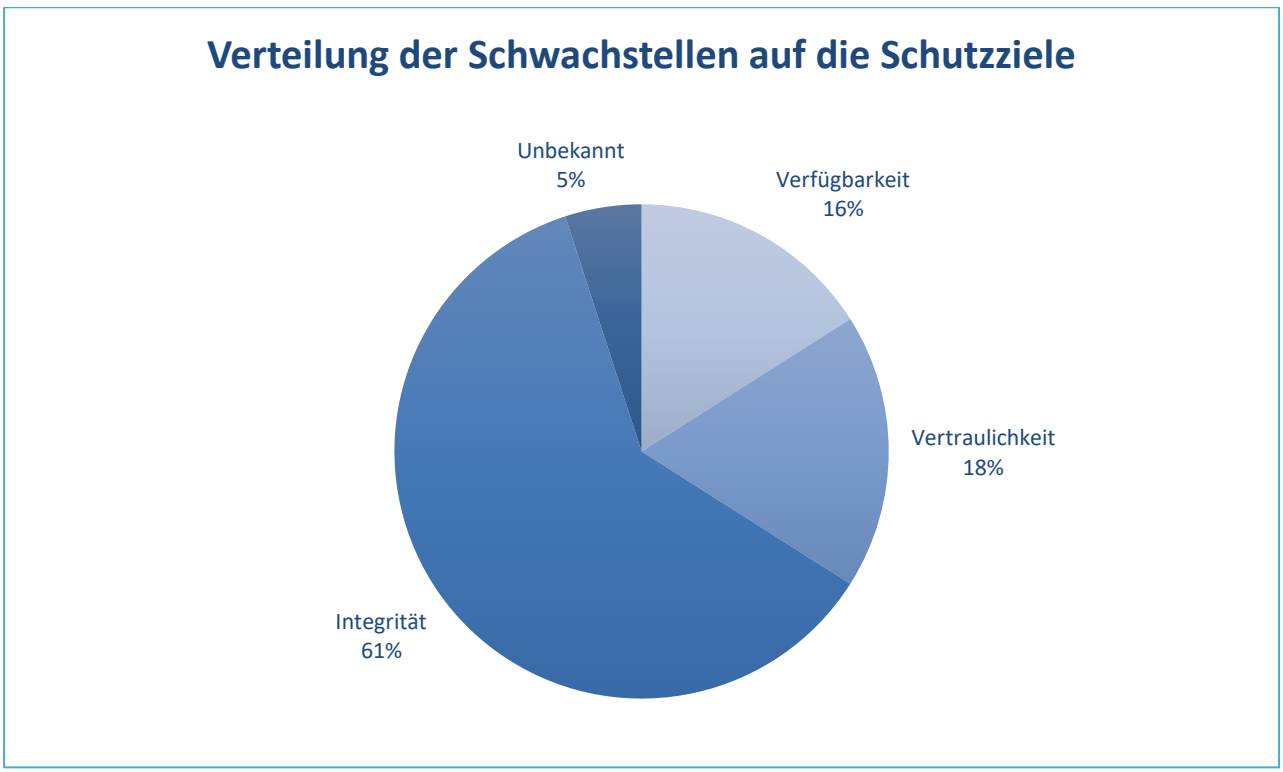


Abbildung 29 - Schwachstellen gruppiert nach deren Auswirkung

Nahezu zwei Drittel der Schwachstellen sorgen dafür, dass die Integrität des betroffenen Systems verletzt wird. Nach „Risk Based Security“ kann dafür ein breites Spektrum von Angriffen verwendet werden. Dazu gehören u. a. die Manipulation von Daten mittels SQL-Injektion oder XSS, um beliebigen Schadcode zur Ausführung zu bringen.

Die Wahrung der Anforderungen ist ein wichtiger Aspekt für AUTOSEC. Die oben gezeigte Aufteilung legt nahe, dass sich eine Priorisierung für den Aufbau von Schutzmaßnahmen als sinnvoll herausstellen kann. Nichtsdestotrotz ist die Wahrung jeder der drei Hauptschutzziele relevant. Denn oftmals verletzt ein Angriff nicht nur eines der Schutzziele. Beispielsweise kann sich ein Angreifer mit einem Sniffer-Programm Zugang zu einem WLAN verschaffen und die Kommunikation „mitlesen“ zu können. Damit ist die Vertraulichkeit verletzt. Erhält der Angreifer dadurch z. B. Zugangsdaten für andere Systeme, hat er die Möglichkeit diese Systeme zu manipulieren und sogar zum Stillstand zu bringen. Somit wären dann auch die Integrität und die Verfügbarkeit verletzt. Daher sollten alle Systeme immer mindestens bzgl. dieser drei Hauptschutzziele analysiert und bewertet werden.

4.3.2 Organisationsmodell

Zur Bestimmung der einzelnen Aufgaben und damit auch der Anzahl der beteiligten Organisationseinheiten wurden als erstes die Entwicklungsprozesse analysiert. Dabei wurde als erstes festgestellt, das keiner der Partner des Projektes aktiv im Entwicklungsprozess für CPS beteiligt ist. Die Eurogate ist noch im Bereich Requirements Engineering tätig, da sie Vorgaben für das CPS System geben kann. Die Entwicklung erfolgt, aber vollständig beim Lieferanten des CPS Systems. Darauf basierend wurde insbesondere das Betriebsmodell erforscht, welches ein schnelles Eingreifen ermöglicht. Die Fokussierung auf den Entwicklungsprozess erfolgte nur bedingt und beinhaltet nur die die klassischen Prozesse des Betriebs bis zum Change-Management. Dieses betrifft folgende Prozesse:

- Capacity and Performance Management
- Incident Management
- IT-Asset Management
- Monitoring und Event Management
- Problem Management
- Release Management
- Service Configuration Management
- Service Continuity Management
- Service Desk
- Service Level Management
- Service Request Management
- Service Validation und Testing

Ein schnelles Eingreifen ist durch die fehlende Möglichkeit eines Stage Environments für das CPS nur durch eine Laufzeit Verifikation möglich, da Fehler erst im Betrieb festgestellt werden und damit im Extremfall zum Stillstand im Hafenbetrieb führen.
Design by Security Ansätze wie im Abschnitt Architektur näher erläutert, können nur als Vorgaben an den Hersteller des CPS übermittelt werden. Security Analysen auf Code-Basis wurden aus diesen Gründen nicht betrachtet. Abbildung 30: Organisationsmodell bezüglich OT- und IT-Informationssicherheit zeigt das im Projekt entwickelte Organisationsmodell bezüglich der Verantwortlichkeiten.

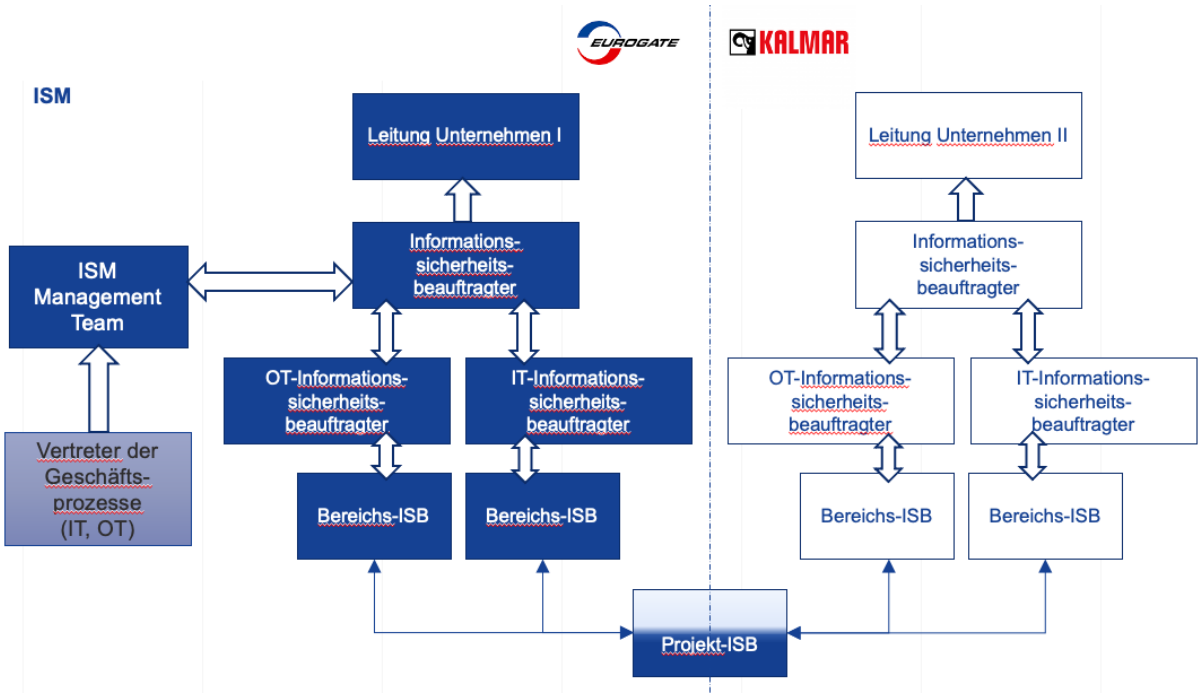


Abbildung 30: Organisationsmodell bezüglich OT- und IT-Informationssicherheit

4.4 Arbeitspaket 3 - Entwicklung eines Prozessmodells

Im Arbeitspaket 3 wurden in Zusammenarbeit mit den Projektpartner folgende Punkte erfolgreich bearbeitet:

- Erarbeitung eines Prozessmodels inkl. Rollenkonzept als Sollprozess
- Entwicklung *Cybersecurity Risk Management Process Model*
- Modell basiert auf:
  - Kernfunktionen des NIST Frameworks
  - Risikoanalyse
  - Konzept des Digitalen Zwillings
    - Definition und Darstellung von Teilprozessen und der jeweiligen Rollen
- Erweiterung der Kategorien und Unterkategorien des NIST-Frameworks für cyber-physische Systeme
  - Identifizierung von Sicherheitsrisiken, Ableiten von Maßnahmen, Erhöhung der Sicherheit erhöhen für cyber-physische Systeme

Ausgangspunkt für diese Arbeiten bildete das NIST National Institute of Standards and Technology [56] [57].

Das „Cyber Security Framework“ (Abbildung 31 - NIST Cyber Security Framework) ist eine Empfehlung der US-Behörde „National Institute of Standards and Technology“ zum Schutz von IT-Infrastrukturen. Ursprünglich war diese Empfehlung für kritische Infrastruktur in den USA gedacht.
Dieses Framework ist eine allgemeine Empfehlung für die gesamten Bereiche der IT-Sicherheit in einem Unternehmen. Es dient als allgemeine Grundlage für die weiteren Betrachtungen im speziellen Anwendungsfall „AUTOSEC“.

In dem Framework werden, auf oberster Ebene, die 5 folgenden Funktionen im Bereich der Cyber-Security unterschieden.

- *Identify (Identifizieren)*

  Identifikation von business-kritischen Systemen, Daten und Funktionen

- Wo befinden sich die Daten?
- Wer nutzt sie?
- Welchen Wert haben sie?
- Wie sind sie derzeit geschützt?
- Sind sie angreifbar, wenn ja, woran liegt das?

- *Protect (Absichern)*

  Entwicklung und Implementierung von Schutzmaßnahmen
  - Zugriffsprozesse und Zugriffsschutz (Berechtigungskonzept)
  - Perimetersicherheit (Firewall, etc.)
  - Verschlüsselung der Daten und Kommunikation
  - Schulung der Mitarbeiter

- *Detect (Aufdecken)*

  Entwicklung und Implementierung von Fähigkeiten zur Aufdeckung/Erkennung von Cyber-Security-Ereignissen
  - Kontinuierliche Sicherheitsüberwachung
  - Anormales Verhalten erkennen

- *Respond (Reagieren)*

  Entwicklung und Implementierung von Aktivitäten/Maßnahmen um auf Cyber-Security-Ereignisse zu reagieren
  - Reaktionsplanung
  - Analyse des Ereignisses und dessen Ursache
  - Kommunikation und Koordination

- *Recover (Wiederherstellen)*

  Wiederherstellung von Systemen und Optimierung für die Zukunft (kontinuierlicher Verbesserungsprozess)

Abbildung 31 - NIST Cyber Security Framework

Weiterhin wurden die Aufgaben in drei Kategorien klassifiziert. hierfür wurden insbesondere folgende Energy Industry Standards and Guidelines analysiert [58]:

- IEC 62351
- IEC 62443/ISA 99
- IEEE 1686
- IEEE C37 240
- NISTIR 7628
- NIST SP800-53
- ISO/IEC 27002/19

Folgende Klassifizierungen wurden dabei vorgeschlagen und mit den Projektpartnern diskutiert:

Organisation: Auf die Organisation bezogen Aufgaben. Insbesondere die Verankerung bezüglich der Verantwortlichkeiten und der Aufnahme dieser Prozesse in Unternehmens Sicherheitsrichtlinien ist notwendig.

Prozesse: Ausgestaltung der Prozesse und Abstimmung mit allen beteiligten Parteien. Hier ist insbesondere das Incident Response und Patch-Management mit dem Hersteller der CPS abzustimmen.

Technical: Hier sind insbesondere technische Verantwortlichkeiten definiert. Wobei diese im OT- und IT-Bereich umgesetzt werden müssen.

Abbildung 32: Klassifizierung von Aufgaben/Prozesse bezüglich Sicherheit für CPS zeigt die einzelnen Aufgaben/Prozesse innerhalb der einzelnen Klassifizierungen.

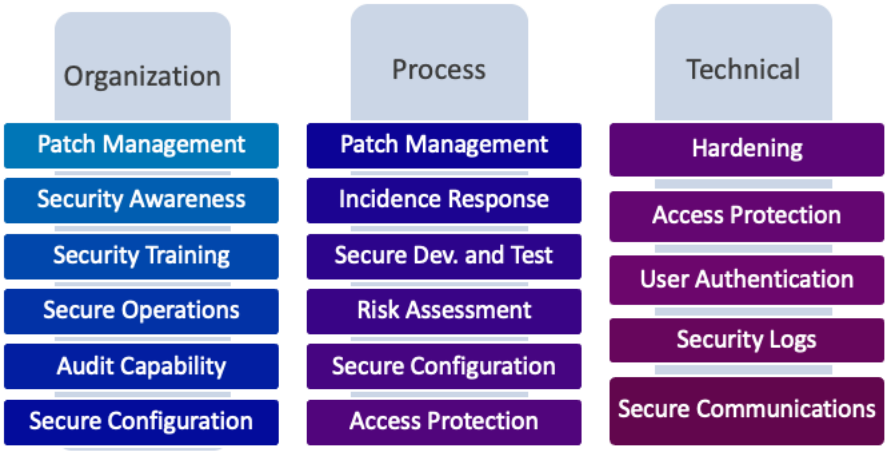


Abbildung 32: Klassifizierung von Aufgaben/Prozesse bezüglich Sicherheit für CPS

Basierend auf diesen Analysen wurde das NIST Modell für CPS Systeme in Zusammenarbeit mit dem Fraunhofer IFF erweitert. Abbildung 33: Erweiterung des NIST Frameworks im Bereich Detect stellt die Detect-Funktion als Beispiel für die fünf erweiterten Kernfunktionen aus dem Prozessmodell dar, die im Projekt AUTOSEC weiterentwickelt werden. Es zeigt nur alle neu eingeführten Kategorien und die entsprechenden Unterkategorien in der Funktion Detect an. Die bereits enthaltenen Kategorien und Unterkategorien wurden nicht erwähnt. Kategorien sind gelb markiert und die entsprechenden Unterkategorien sind grau. Jeder neuen Unterkategorie wurde eine eindeutige Kennung basierend auf der Struktur des NIST-Frameworks zugewiesen.

Alle im erweiterten Prozessmodell speziell für die Sicherheit von Cyber-Physical Systems neu eingeführten Kategorien und Unterkategorien der Detect-Funktion werden im Folgenden zum besseren Verständnis und zur Verdeutlichung kurz erläutert. Jede neue Unterkategorie wurde kurz beschrieben und mit ihren Kernmerkmalen (CA – Kontextbewusstsein, DT – Dynamische Topologie, DS – Verteilte Organisationsstruktur) referenziert. Da Platzbeschränkungen eine Erläuterung bereits vorhandener Kategorien und Unterkategorien ausschließen, wird auf das Framework verwiesen. Alle neuen Einträge sind in Tabelle 8 detailliert beschrieben. Ihre Kategorisierung folgt der vom NIST Framework vorgegebenen Struktur. Die Kurztitel der Unterkategorien sind in Abbildung 33:

Erweiterung des NIST Frameworks im Bereich Detect aufgeführt. Die eindeutigen Identifikatoren in Tabelle 8 verweisen auf die jeweiligen Kurztitel der Unterkategorien in Abbildung 33: Erweiterung des NIST Frameworks im Bereich Detect.

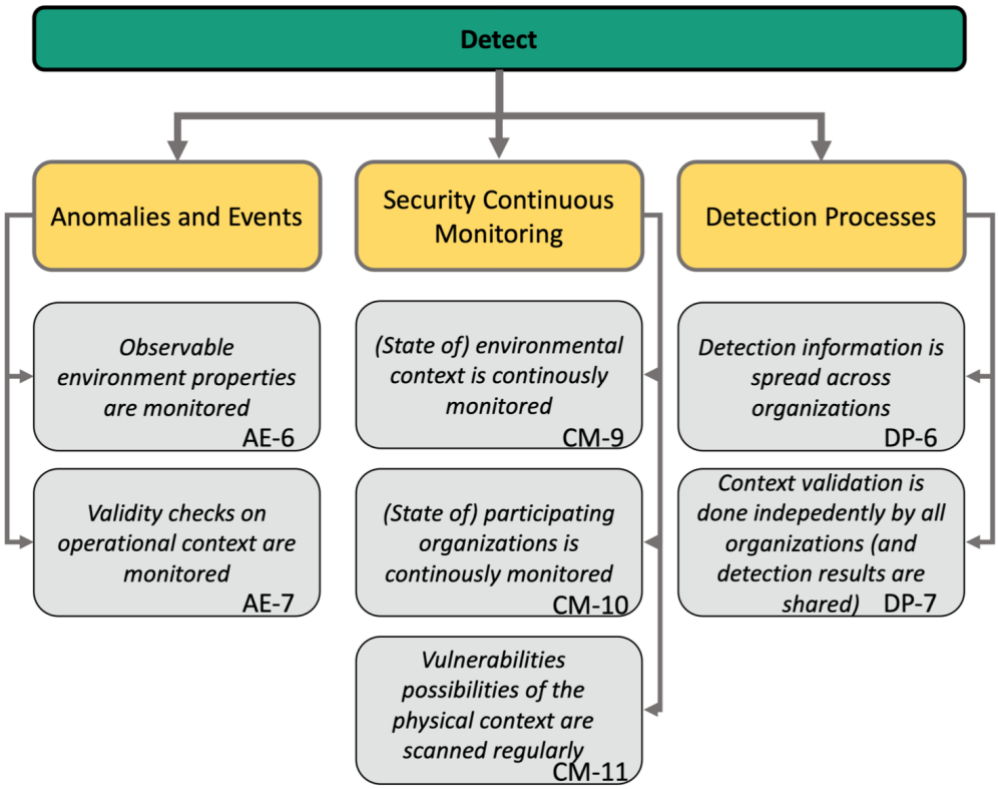


Abbildung 33: Erweiterung des NIST Frameworks im Bereich Detect

Der in diesem Projekt fokussierte Ansatz zur Überwachung der Komponenten eines Cyber-Physical Systems besteht darin, diese mit einem digitalen Zwilling zu modellieren (siehe [59] [60]), ihre Leistungsfähigkeit zu simulieren und Cyberkomponenten zu emulieren. Die realen Komponenten werden mit einer Simulation verbunden und der digitale Zwilling verarbeitet die Zustandsdaten. Darüber hinaus werden die im realen System eingesetzten IT-Systeme in den digitalen Zwilling integriert, allerdings als Emulation oder vom realen System isolierte Umgebung, um den Einfluss des realen Systems zu eliminieren.

Auch die physische Leistungsfähigkeit kann simuliert werden, um mögliche Zustände des cyber-physischen Systems zu ermitteln. Zustände können verglichen werden, um zu bestimmen, ob das cyber-physische System wie erwartet funktioniert. Da Sensoren und Aktoren jedoch zum Vergleich von Zuständen verwendet werden, muss die Richtigkeit der erfassten Sensorwerte und die ordnungsgemäße Übertragung durch die Kanäle ohne physische Manipulation sichergestellt werden.

Da der Digital-Twin-Ansatz Cyber-Physical Systems allein nicht ausreichend schützt, müssen der Systemarchitektur weitere komplementäre Komponenten hinzugefügt werden, mit denen eindeutig nachgewiesen werden kann, dass weder physische Manipulationen noch Störungen aufgetreten sind. In [61] haben Wang et.al. dafür ein kontextbezogenes Sicherheits-Framework für den CPS-Ansatz entwickelt, das kontextbezogene Überwachung basierend auf Veränderungen in der physischen Umgebung entlang der Schleife, bestehend aus physischer Prozessüberwachung, Datenübertragung, Verarbeitung und Steuerung, ermöglicht. Anstatt die Korrektheit der Sensordaten direkt zu verifizieren, ermitteln und verifizieren disjunkte oder komplementäre Messverfahren den Zustand der cyber-physischen Systeme oder des gesamten Logistiksystems. Die komplementären Messsysteme, die die Zustände des Cyber-Physical-Logistik-Systems messen und mit dem kontextsensitiven Monitoring-System abgleichen, verifizieren die Richtigkeit der Zustände. Eine Überwachungsmethode, die die primären erwarteten Zustände des digitalen Zwillings misst und verifiziert, stellt

sicher, dass die Simulation des digitalen Zwillings korrekt und fehlerfrei abläuft. Die Kombination der Ansätze des digitalen Zwillings, des kontextsensitiven Frameworks und eines die Zustände vergleichenden Algorithmus ermöglicht es, ein Cyber-Physical-System digital zu modellieren und damit den Nachweis einer nahezu perfekten Performance zu gewährleisten. Abbildung 18: Kontextsensitives Überwachungssystemzeigt die gesamte entwickelte Architektur, die die Integration von Cyber-Physischen Systemen in eine Systeminfrastruktur beschreibt und die Funktionen der Detect-Funktion beinhaltet.

Identifikation	Core Feature	Beschreibung
Anomalien und Ereignisse		
AE-6	CA	Da die Umgebungsüberwachung ein wirksames Instrument zur Erkennung physikalischer Manipulationen ist, müssen beobachtbare Umgebungsbedingungen spezifiziert und überwacht werden.
AE-7	CA, DT	Die kontinuierliche Validierung des Umgebungskontexts gegen die Systemspezifikation ermöglicht eine frühzeitige Erkennung von physischen Manipulationen.
Security Continuous Monitoring		
CM-9	CA, DT	Der Umgebungskontext, in dem das cyber-physische System arbeitet, muss kontinuierlich überwacht werden. (Voraussetzung für AE-7).
CM-10	CA, DT	Da sich die Prozesse/Regelungen der einzelnen Organisationsstrukturen für Teilkomponenten des Cyber-Physischen Systems jederzeit ändern können, muss der Status aller beteiligten Organisationen ständig überwacht werden.
CM-11	CA, DT	Potenzielle Risiken, die sich aus Veränderungen des physischen cyber-physischen Systemkontextes ergeben, müssen laufend überwacht werden.
Detektionsprozesse		
DP-6	DS	An einem cyber-physischen System können mehrere Organisationseinheiten beteiligt sein. Alle Organisationsstrukturen müssen über jedes festgestellte Ereignis/Anomalie informiert werden, z.B. eine unerwartete Veränderung. Die Entscheidungsbefugnis liegt beim Betreiber bzw. Dienstanbieter des jeweiligen Systems.
DP-7	DS, CA	Da sich der industrielle Kontext eines Cyber-Physical Systems jederzeit ändern kann, sind alle Organisationen angehalten, dies kontinuierlich unabhängig voneinander zu validieren und ihre Erkenntnisse miteinander zu teilen.

Tabelle 8: Beschreibung der Erweiterung spezifischer Unterkategorien für Cyber-Physical Systems

Die entwickelten Ansätze und deren praktische Umsetzung in einem Demonstrator im AUTOSEC-Projekt demonstrierten die Umsetzbarkeit des fortgeschrittenen Vorgehensmodells für Cyber-Physical Systems in kritischen Infrastrukturen (siehe Arbeitspaket Evaluierung).
Der Einsatz ist jedoch nicht auf die hier vorgestellte Detect-Funktion beschränkt. Es kann in allen anderen im NIST Framework spezifizierten Kernfunktionen verwendet werden.

4.5 Arbeitspaket 4 – Integration

Ausgehend von der Problematik der Laufzeit Verifikation, welche in den vorhergehenden Arbeitspaketen motiviert wurde, soll innerhalb dieses Arbeitspaketes detaillierter auf die Überwachung und die Reaktion im Fehlerfalle eingegangen werden. Dabei wird im Allgemeinen davon ausgegangen, dass nicht alle Zustände eines

Hafens im Vorfeld emuliert werden können (Komplexität des Gesamtsystems) und damit auch nicht die internen Abläufe in der IT vollständig simuliert werden können. Dieser Sachverhalt ist im Arbeitspaket Architektur eingeführt worden, da keine geeignete Stage Environment für CPS gestellt werden kann. Ausgehend von dem definierten Test des CPS Lieferanten sind insbesondere im Falle von Patch Management Aufgaben im Betrieb, keine vollständigen Tests möglich.

Grundsätzlich wurden zwei Szenarien diskutiert:

1. Sperrung deduzierter Bereiche des Hafens für Test
2. Laufzeit Verifikation
    a. Hyper Care Phase
    b. dauerhaft

Insbesondere unter der Berücksichtigung von Safety Funktionalitäten, welche eine Grundvoraussetzung für den Betrieb von CPS Systemen darstellen, müssen gepatchte CPS Grundsätzlich alle Tests bezüglich der Safety Anforderungen in einem geschützten Bereich des Hafens durchgeführt werden. Anschließend könnte eine Laufzeitverifikation zur Testierung herangezogen werden. Daraus folgt das bei Feststellungen von Fehlern im Betrieb, schnelle Verfahren zur Fehler Lokalisierung (Root Cause Analysen) und schnelle Verfahren zur Behebung der Fehler benötigt werden.

Dieser Sachverhalt ist unter dem Gesichtspunkt der derzeitigen Entwicklungsgeschwindigkeit derartiges System enorm wichtig, da davon auszugehen ist, dass im IT und OT Bereich die Security von Systemen nur durch entsprechendes Patch Management zur Behebung von physischen und Cyber-Raum Fehlern gewährleistet werden kann. Im Folgenden sollen aber die Prozesse Deployment Automatisierung und Release Management im Bereich Continuous Integration und Continuous Delivery detaillierter dargestellt und bezüglich CPS analysiert werden.

automatisierter Integrations- und Auslieferungsprozess

Das Management des automatisierten Deployments zwischen den einzelnen Pipeline-Phasen erfordert spezialisierte Werkzeuge. Ein Schwerpunkt ist dabei die Deployments der Anwendung in automatisierter Form zu realisieren.
Als erster Punkt wird im weiteren Verlauf ein Ablaufplan für den Deployment-Prozess erläutert, um die verschiedenen Aktivitäten und Zusammenhänge sowie das Vorgehen bei Fehlern oder in kritischen Situationen zu zeigen. Nachfolgend wird das Prinzip von Infrastructure-as-Code betrachtet, wodurch zusätzlich zum Deployment der Anwendung selbst die gesamte Infrastruktur auf Basis von Skripten erschaffen wird. Der dritte Unterabschnitt widmet sich der Verwaltung der Releases, dem Aufbau von Feedback-Schleifen und das Monitoring der Deployment-Pipeline.

Ablaufplan des Deployment-Prozesses

Im Deployment-Prozess wird die Pipeline Schritt für Schritt automatisiert durchlaufen. An verschiedenen Punkten können Fehler festgestellt werden, die dazu führen, dass das Deployment fehlschlägt und entsprechende Korrekturen vorgenommen werden müssen. Die Fehlererkennung basiert sowohl auf automatischen als auch manuellen Tests und wird durch diverse Monitoring-Tests ergänzt.

Der in Abbildung 34: Ablaufplan Deployment-Prozess dargestellte Prozess zeigt fünf Schritte:

1. Versionsverwaltung: Software wird entwickelt oder aktualisiert und dann in den Master-Branch verschoben. In diesem Beispiel konzentrieren wir uns auf Commits, die für die Produktionspipeline geplant sind.

2. Continuous Integration: Um die Software auf Fehler zu prüfen, durchläuft diese automatisiert im Vorfeld angelegte Build-Unit-Tests. Wenn keine Fehler gefunden werden, wird ein Paket erstellt, welches in das initiale Deployment verschoben wird.

3. Testen: (Tests finden am Übergang zu jedem Schritt statt, daher könnte dieser Schritt auch als Haupttest bezeichnet werden.) Es werden erweiterte Akzeptanztests der Kernsoftware und des Pakets ausgeführt. Die Testphase kann auch andere Tests umfassen, z. B. Benutzerakzeptanztests (UAT). Die UAT-Phase ist nicht automatisiert, daher gibt es eine Kontroverse darüber, ob sie in einen echten CI/CD-Prozess gehört. Wenn die Tests bestanden werden, wechselt die Software in den Bereitstellungsstatus.

4. Continuous Deployment: Das Paket kann sofort in die Produktionsumgebung wechseln oder über mehrere Aktualisierungen hinweg warten. In einigen Definitionen von Continuous Deployment muss dieser Schritt automatisiert werden, andere ermöglichen die Freigabe zur Produktion, um den Anforderungen von Business und Service Level Agreement (SLA) gerecht zu werden.

5. Leistungs- oder Bereitstellungstests: Post-Deployment-Tests können ein Rollback auf eine frühere, "bekannt gute" Version (in der Regel ein manueller Schritt) auslösen, gefolgt von einer neuen Entwicklung, um Probleme zu beheben. Usability-Probleme und neue Feature-Anforderungen können dazu führen, dass neue Software entwickelt und bereitgestellt wird, ohne dass ein Rollback erforderlich ist.

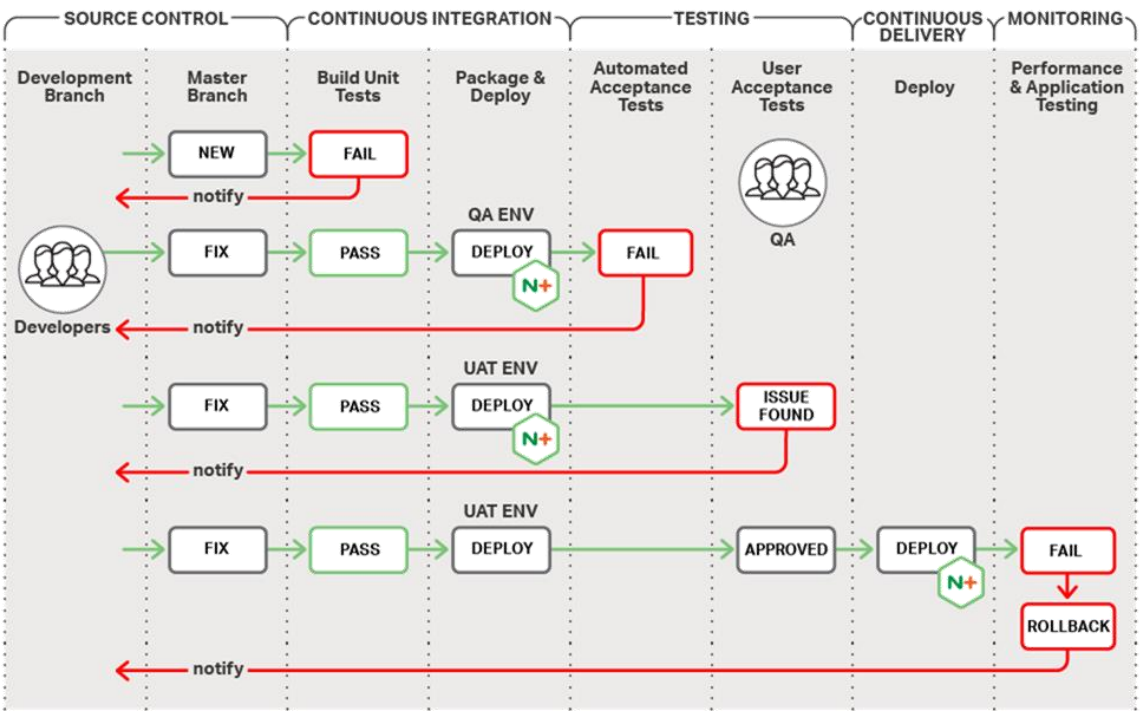


Abbildung 34: Ablaufplan Deployment-Prozess

Es gibt Akzeptanztests für das Verschieben von Software von einer Stufe in die nächste. Ein Fehler bei einem beliebigen Schritt bedeutet, dass sich die Software nicht vorwärtsbewegt, sondern zur Fehlerbehebung und möglichen weiteren Aktualisierung in die Entwicklung zurückkehrt.
Wenn ein Fehler in der bereitgestellten Software auftritt, wird automatisch auf die vorherige nicht-fehlerhafte Version zurückgesetzt und die Aktualisierung wird von dieser Version fortgesetzt. Somit bleibt stets gewährleistet, dass die neuen Versionen sowohl kompatibel als auch lauffähig sind und somit jederzeit in das Release übernommen werden können.
Für Entwickler, die erstmals mit der Continuous Delivery-Pipeline arbeiten und vorher vor allem in Projekten mit langsamen Produktzyklen gearbeitet haben, bedeutet das Vorgehen eine Um-gewöhnung. Bei der Continuous Delivery-Pipeline steht ein jederzeit abrufbares Produkt an oberster Stelle.

In Verlauf des Projekts muss es jederzeit möglich sein, ein vollständiges und fehlerfreies Release zu erhalten, sei es, um Kunden zu überzeugen oder neue Systeme zu testen. Dabei ist es wichtig, den Code frühzeitig zu versionieren, auch wenn er noch nicht für den Endanwender freigegeben wurde.
Durch eine gezielte und professionelle Versionsverwaltung lassen sich die notwendigen Schritte sehr einfach steuern und überwachen, was das Einpflegen neuer Codebestandteile und die Aktualisierung des Codes nach erfolgreichen Änderungen deutlich vereinfacht.
In der Anwendungsentwicklung und -bereitstellung gehören die agilen Methoden wie die Continuous Delivery-Pipeline mittlerweile zum Alltag, da diese eine deutlich höhere Flexibilität versprechen und die Produkte bereits, während der Programmierarbeit umfassend getestet werden. Somit lassen sich Zeitpläne deutlich effizienter organisieren, da lange Korrektur- und Reparaturpausen am Ende eines jeden Release-Zyklus im bisherigen Umfang nicht mehr not-wendig sind.
Applikation Deployment Automation / Infrastructure as Code
Einer der größten Flaschenhälse der Delivery-Pipeline ist das Deployment der Infrastruktur. Der Aufbau von Environments auf Grundlage von Softwaredefinitionen ermöglicht eine schnelle Re-aktion auf sich ändernde Bedingungen und erlaubt es, die Infrastruktur als ein programmierbares und wiederholbares Muster anzusehen. Die Deployment-Geschwindigkeit kann durch IaC enorm gesteigert werden. Eine IT-Infrastruktur kann durch die Operations-Teams anstatt manueller Verfahren automatisch per Code verwaltet und bereitstellt werden.
Zum Beispiel kann IaC unter Verwendung eines IT-Management- und Konfigurations-Tools, einen MySQL-Server installieren und verifizieren, ob MySQL korrekt ausgeführt wird sowie einen Benutzer-Account und das Passwort erzeugen, eine neue Datenbank einrichten und nicht benötigte Datenbanken entfernen. Alle Arbeitsschritte erfolgen auf Basis von Code-Skripten.

Die Nutzung von Code für die Bereitstellung und das Ausrollen von Servern und Anwendungen ist besonders für Softwareentwickler interessant. Anstatt sich bei der Bereitstellung und dem Management operationaler Aspekte einer DevOps-Umgebung auf Systemadministratoren zu verlassen, kann ein Entwickler einen IaC-Prozess für die Qualitätssicherung oder experimentelle Zwecke schreiben.

Trotz der Vorteile birgt IaC auch Nachteile. Zum Beispiel kann die IaC-Codeentwicklung zusätzliche Werkzeuge erfordern, die erst erlernt werden müssen und zu zusätzlichen Fehlern führen können. Jeder Fehler im IaC-Code kann sich außerdem schnell verbreiten, sodass Versionskontrollen und umfassende Pre-Release-Tests notwendig sind.
Wenn Administratoren Serverkonfigurationen ändern, ohne gleichzeitig den IaC-Code anzupassen, verbreiten sich möglicherweise die Konfigurationsveränderungen über die gesamte DevOps-Landschaft hinweg. Es ist daher wichtig, IaC komplett in die Systemadministration, den IT-Betrieb und die DevOps-Prozesse mit gut dokumentierten Richtlinien und Verfahren zu integrieren.

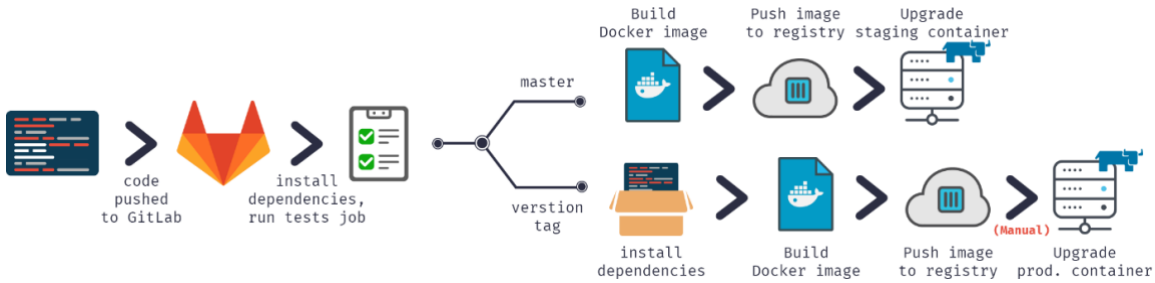


Abbildung 35: Infrastructure-as-Code im Rahmen der Delivery-Pipeline

Abbildung 35: Infrastructure-as-Code im Rahmen der Delivery-Pipeline zeigt die Verwendung von IaC innerhalb der Delivery-Pipeline von DevOps. Code-Änderungen werden in ein zentrales Repository, hier ein Gitlab, eingecheckt. Das IaC erfolgt unter Verwendung von Container-Virtualisierungen, wobei an dieser Stelle Docker-Container zum Einsatz kommen. Die Abhängigkeiten werden aufgelöst, Unit- und Integrations-Tests ausgeführt und schließlich ein neues Docker-Image erstellt. Für QA- und User-Acceptance-Tests wird das Image in eine spezielle Docker-Registry gespeichert, wodurch das Deploy- und Release-Management realisiert wird. Final wird dann ein neuer Container im Staging-System ausgerollt. Nach einem erfolgreichen Absolvieren von QA- und User-

Acceptance-Tests wird eine Release-Version deklariert und in der Quellcodeverwaltung getagt. Für die Release-Version des Containers wird wiederum die gleiche automatisierte Erstellung abgehandelt. Die Abhängigkeiten werden aufgelöst, ein Docker-Image generiert und im Release-Management (Container-Registry) hinterlegt. Im letzten Schritt wird der Container auf dem Produktiv-System eingespielt.

Für das in Abbildung 35: Infrastructure-as-Code im Rahmen der Delivery-Pipeline gezeigte Vorgehen ist ein manuelles Deployment vorgesehen. Mit dem Ziel einer Vollautomatisierung für das Continuous Deployment ist auch der letzte Schritt zu automatisieren.

Deployment Automation

Die Automatisierungswerkzeuge sind eines der Kernthemen von DevOps und betreffen die gesamte Verarbeitungspipeline. Hierdurch werden Deployments untereinander abgestimmt und verfolgt, welche Version an welchem Punkt der Build- und Delivery-Pipeline eingesetzt wird. Zusätzlich werden die Konfigurationen der Environments für alle Phasen, in denen die Applikation deployed werden muss, gemanagt. Deployment Automationswerkzeuge kümmern sich um die:

- zu deployenden Software-Komponenten,
- zu aktualisierenden Middleware-Komponenten und -Konfigurationen,
- die Anpassung der Datenbank-Komponenten sowie
- der Environment-Konfigurationen, wohin Komponenten deployed werden.

Die Überwachung und die Automatisierung dieser Aufgaben ermöglicht die Nachvollziehbarkeit des Deployments und der Konfigurationsanpassungen.
In den einzelnen Phasen kommen diverse Automatisierungswerkzeuge zum Einsatz. Abbildung 36: Beispiele für Werkzeuge entlang der CD-Pipeline enthält eine Auswahl solcher Werkzeuge und zeigt, in welchen Phasen sie verwendet werden können.

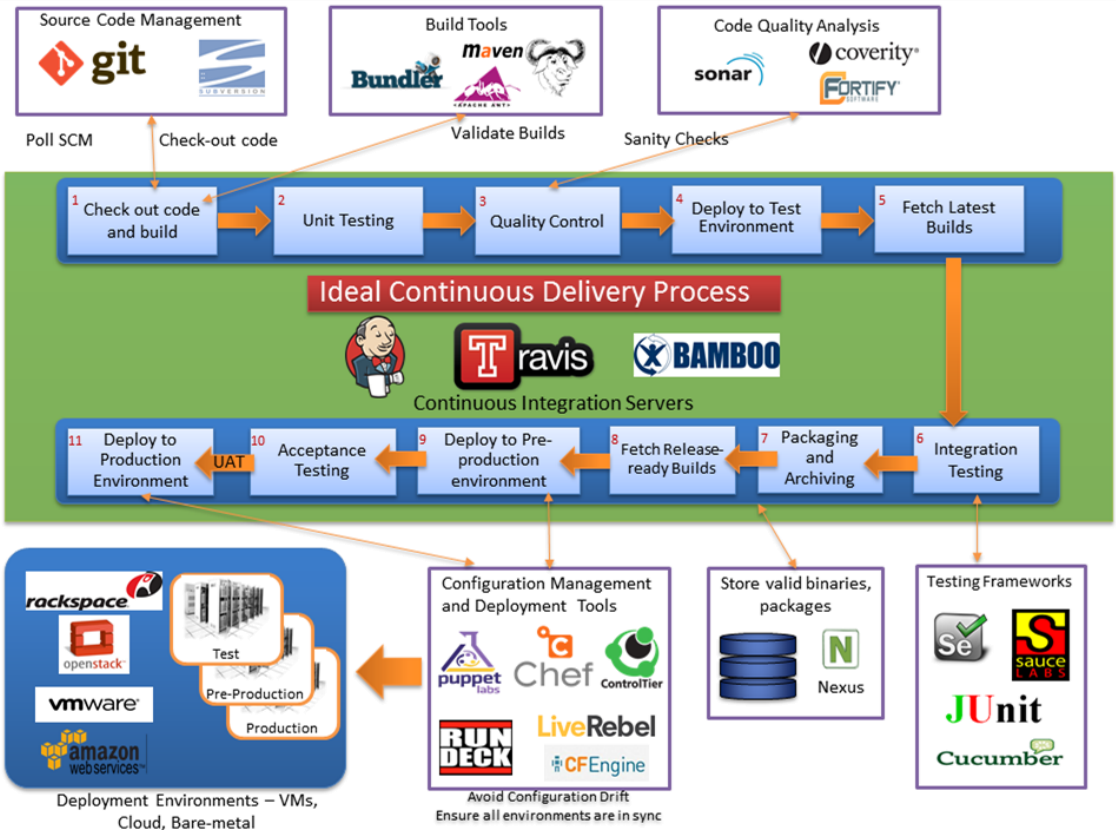


Abbildung 36: Beispiele für Werkzeuge entlang der CD-Pipeline

Release Management

Ein erfolgreiches Zusammenspiel von Release-Plänen und Deployments für jedes Release bedeutet, dass das Business, die Entwicklung, QA und die Operations-Teams koordiniert werden. Mit Hilfe von Werkzeugunterstützung werden Releases geplant und durchgeführt, inklusive der Nachverfolgbarkeit eines Releases und dessen Bestandteile über alle Phasen der Pipeline hin-weg.

Continuous Monitoring (Feedback/Improvement)

In der Produktion ist es die Aufgabe des Ops (Operations)-Teams sicherzustellen, dass die An-wendung die geforderte Performance erfüllt und sich das Environment in einem stabilen Zu-stand befindet (Continuous Monitoring). Eine andere Quelle für Informationen eröffnet sich durch Feedback von Kundenseite (Continuous Feedback). Weiterhin werden die mittels DevOps ausgeprägte Pipeline und der damit erschaffene Prozess im Unternehmenskontext stetig über-wacht und verbessert (Continuous Improvement).

Continuous Monitoring

Monitoring-Daten/-Auswertungen stellen die erste Art an Feedback dar. Für die Erhebung solcher Daten existieren vielfältige Möglichkeiten. Die Rückmeldung kann direkt aus den Phasen der Pipeline bzw. den dort ausgeführten Arbeitsschritten hervorgehen (Development, QA, Produktion). Auch das Environment der Anwendung kann überwacht werden, um bspw. einen Ein-blick in die Performance zu erhalten. Dazu lassen sich typische Metriken nutzen, um das Server-System bzw. die Anwendung zu messen. Eigene Metrik-Module, die direkt in die eigene Anwendung eingebettet werden, stellen ebenfalls eine Option dar.

Continuous Feedback

Das auszuwertende Kundenfeedback nimmt verschiedene Gestalten an (Tickets, formale Änderungsanfragen, informelle Beschwerden und Bewertungen in App Stores). Die dahinterliegenden Prozesse müssen ebenfalls agil und schnell adaptierbar sein, um auf Veränderungen des Marktes oder von Regularien reagieren zu können. Mögliche Datenfluten benötigen wiederum eigene Prozesse, um effektiv das Feedback auf Business-relevante Inhalte zu reduzieren.

Continuous Improvement

Das Monitoring und die Auswertung des Feedbacks tragen dazu bei, Abläufe rund um die Pipeline und im Unternehmen zu optimieren. Die Extraktion und das Anwenden von Verbesserungen sind dauerhafte Aufgaben und können nicht auf einmalige Schritte zu einem singulären Zeit-punkt reduziert werden. Hierfür wird ein interner Prozess erarbeitet und etabliert, um die Verbesserungen zu identifizieren. Die Zuständigkeit hierfür wird meist an speziell geschaffene Teams übergeben.
In Ergänzung zu den Definitionen und Ablaufbeschreibungen wird nachfolgend ein Beispiel verwendet, um die den Deployment-Prozess zu veranschaulichen und auf Strategien für den Über-gang eines neuen Releases in die Produktivumgebung einzugehen.

Bewertung der Architektur bezüglich automatisierter Integrations- und Auslieferungsprozess

Innerhalb dieses Teilarbeitspaketes erfolgte die Bewertung der Architektur bezüglich der Integrations- und Auslieferungsprozesse. Dabei wurden folgende Teilaspekte bearbeitet:

- Geeignete Fehlerdetektion durch den Einsatz von komplementärer Messmethoden inklusive Bestimmung der Überwachungsparameter
- Konzeption der Architektur für die Implementierung der komplementärer Messmethoden zur Verwendung während der Evaluierungsphase

- Bereitstellung von Tools zur gesamtheitlicher Integrations- und Auslieferungsprozesse über alle beteiligten Partner und IT-Systemlandschaften, um schnell und adäquat auf detektierte Fehler zu reagieren

Bezüglich der Bewertung der Architektur für automatisierte Integrations- und Auslieferungsprozesse konnte die EUROGATE nachweisen, dass eine Umsetzung möglich ist. Hierfür wurden ausgewählte Tools des Geschäftsprozess der EUROGATE logisch von anderen Systemen getrennt und nur über definierte Schnittstellen angesprochen. Die Tools wurden anschließend in entsprechende Container überführt und der komplette Infrastrukturbereich konnte als Infrastructure-as-Code umgesetzt werden. Es konnten erfolgreiche Deployments in die Amazon Cloud erstellt werden und damit eine Proof-of-Konzept durchgeführt werden.

Leider könnte das CPS nicht in die aktuellen Betrachtungen mit aufgenommen werden, da eine derartig detaillierte Zusammenarbeit mit dem Zulieferer Kalmar innerhalb dieses Projektes nicht möglich war.

Daher wurde das Konzept auf den Cyber-Raum beschränkt und bei beiden Projektpartner vorgestellt und entsprechende Auswirkungen diskutiert. Insbesondere beim Hafen MD, welcher seine Infrastruktur derzeit lokal im Magdeburger Hafen auf redundanten Systemen betreibt, wurden ausführlich die Auswirkungen bei Umstellung auf Infrastructure-as-Code diskutiert. Dabei konnte abschließend folgende Fragestellungen beantwortet werden:

- Ablösung der lokalen IT-Infrastruktur auf entsprechende Cloud Services
- Ablösung der derzeitigen proprietären IT-System, und Ausarbeitung damit verbundener Change-Management Prozesse innerhalb des Hafen MD
- Vergleich der Sicherheitsaufwendungen von lokal vs. Cloud gehosteten Systemen
    - Definition entsprechender SLA für Cloud Anbieter
    - Definition von Sicherheitsrichtlinien für interne Mitarbeiter und als Vorgaben für den Cloudanbieter
    - Umstellung der internen Verantwortlichkeiten
- Abschätzung der Aufwendungen zur Umsetzung einzelner IT-System auf Container basierte Lösungen, zur Reduktion der angreifbaren Oberfläche

Abschließend bleibt aber festzustellen, dass beide Häfen bezüglich der Infrastruktur sehr unterschiedlich aufgestellt sind. Während die EUROGATE schon cloudbasierten Dienstleistern zusammenarbeitet, arbeitet der Hafen MD mit einem lokalen IT-Service Dienstleister und hostet die IT selbst. Dementsprechend können auch die Ergebnisse interpretiert werden:

- Hafen MD: Abklärung aller Punkte (organisational, prozessual und technisch) für den sicheren Betrieb einer IT-Systemlandschaft in der Cloud mit Infrastructure-as-Code Konstrukten. Keine realen Umsetzungen konnten durchgeführt werden.
- EUROGATE: Umsetzung von Infrastructure-as-Code Konstrukten und erfolgreiches automatisiertes Deployment in die Cloud.

Durch die fehlende Möglichkeit der direkten Zusammenarbeit mit dem Hersteller der CPS wurde auf einen Demonstrator aus Fisher-Technik als CPS zurückgegriffen.

Für die Integration wurden Ansätze aus dem Bereich Continuous Integration CI und Continuous Delivery CD detaillierter untersucht und die Erweiterbarkeit dieser Ansätze für CPS analysiert und auf dem Demonstrator Fisher-Technik implementiert. Dabei wurden, wie in Arbeitspaket 3 DevOps-Ansätze berücksichtigt, die optimale Aufteilung von Aufgabenbereichen bezüglich CI/CD für die Bereiche Entwicklung und Betrieb erprobt.

Im Anwendungsfall automatisierte Transportsysteme wurde auch das Konzept zur automatischen Überwachung der Transportwege mittels Digitalem Zwilling und komplementären Messsystem auf dem Demonstrator umgesetzt. Der Demonstrator wurde auf der Statuskonferenz der IHATEC 19.September 2019 ausgestellt.

Unter Berücksichtigung der resilienten Eigenschaften derartiger Transportsysteme können, durch das automatisierte Überwachungssystem, auch teilgetestete Systeme in die Produktivumgebung übernommen werden. Bei Fehlverhalten der einzelnen Van Carrier würden diese automatisiert gestoppt werden und der Bereich Operation informiert werden. Dabei müssen derartige Ausfälle dokumentiert und deren Fehlerbehebung bis in die Entwicklung gespiegelt werden.

Weiterhin wurden folgende Punkte bearbeitet:

- Verallgemeinerung des Ansatzes für resiliente CPS-Systeme
- Überwachung von Lieferketten bezüglich Hard- und Software Auslieferungen

4.6 Arbeitspaket 5 – Anwendungsfälle und Evaluierung

Folgende Teilaspekte wurden während der Evaluation mit beiden Projektpartnern bearbeitet:

1. Festlegung des Geltungsbereichs (Informationsverbund)

Zu Beginn eines IT-Sicherheitskonzepts wurde festgelegt, welcher Bereich der Organisation abgedeckt wird, bzw. der Geltungsbereich abgegrenzt. Dies können z. B. bestimmte Organisationseinheiten oder auch Bereiche sein, die Fachaufgaben oder -verfahren bearbeiten, inklusive der dafür notwendigen IT-Ressourcen, Infrastrukturen und Schnittstellen zu externen Partnern. Dieser Geltungsbereich für die Sicherheitskonzeption wird auch als Informationsverbund bezeichnet.
Ein solcher Informationsverbund wurde durch IT-Komponenten, Informationen, organisatorische Regelungen, Aufgabenbereiche und Zuständigkeiten sowie die physische Infrastruktur definiert.

2. Strukturanalyse

Eine der Vorarbeiten für den Sicherheitsprozess inkl. einer Risikoanalyse war die Strukturanalyse. Die Hauptaufgabe dieser Teilaufgabe ist das Zusammenspiel der Geschäftsprozesse, der Anwendungen und der vorliegenden Informationstechnik zu analysieren und zu dokumentieren. Es wurden grundlegende Informationen, die für den weiteren Sicherheitsprozess benötigt werden, gesammelt. Hierbei ging es um die Erfassung von Geschäftsprozesse, Informationen, Anwendungen, IT- und ICS-Systeme, Räume und Kommunikationsnetze, die zur Betrachtung innerhalb des Sicherheitskonzepts benötigt werden.

Schritt 1: Geschäftsprozesse und Unterprozesse identifizieren

Schritt 2: Wertigkeit und Bedeutung der Geschäftsprozesse für das Unternehmen abschätzen

Schritt 3: CPS zu Prozess zuordnen

Es wurden exemplarisch für die EUROGATE und Hafen MD wesentlichen Geschäftsprozesse, geschäftskritischen Informationen und Anwendungen (Software) erfasst. Zudem wurden exemplarisch IT-, ICS oder IoT-Systeme, Räume und Netze erfasst.

Die Strukturanalyse gliederte sich in folgende Teilaufgaben:

- Erfassung von Geschäftsprozesse, Anwendungen und Informationen
- Erhebung von IT-, ICS- und IoT-Systemen und ähnlichen Objekten
- Erfassung der Räume und Gebäude (für den ICS-Bereich sind auch die produzieren-den Räumlichkeiten zu berücksichtigen)
- Netzplanerhebung

Aufgrund von Redundanzen oder Menge der Objekte wurde festgestellt, dass es oftmals zweckmäßig ist, Objekte zu Gruppen zusammenzufassen und nur die Gruppe zu und nicht jedes Objekt einzeln zu erfassen. Die

Strukturanalyse bildete einen wichtigen Datengrundstock für den gesamten Sicherheitsprozess. Bei der Erfassung einzelner Objekte wurde festgestellt, dass schnell die Gefahr besteht, dass die Ergebnisse durch die Menge und Komplexität im weiteren Prozess nicht mehr händelbar sind.

Gruppen konnten gebildet werden, wenn Objekte:

- vom gleichen Typ waren,
- ähnliche Aufgaben hatten,
- ähnlich konfiguriert wurden,
- ähnlich ins Netz eingebunden waren,
- ähnlichen Rahmenbedingungen unterlagen oder
- den gleichen Schutzbedarf benötigen.

Dies gilt natürlich nicht nur für technische Objekte, sondern z.B. auch für Räume und andere Arten von Objekten.

4. Geschäftsprozesse, dazugehörigen Informationen und Anwendungen ganzheitlich erfassen und bzgl. der Wertschöpfung bewerten

In diese Teilaufgabe der Strukturanalyse wurde einen Überblick über die für das Unternehmen wesentlichen Geschäftsprozesse oder Fachaufgaben erarbeitet und aufgezeigt was Informationssicherheitsrisiken bzw. IT-Risiken für diese Geschäftsprozesse und somit für die Wertschöpfung des Unternehmens bedeuten können. Dazu war es notwendig einerseits den Bezug zwischen den Geschäftsprozessen und der Wertschöpfung herzustellen und andererseits den Bezug zwischen den Geschäftsprozessen und den beteiligten und schützenswerten Informationen, IT-Systemen, Anwendungen und andere Objekte herzustellen.
Bei der Erfassung war es wichtig eine sinnvolle Granularität zu wählen. Es sind i. d. R. nicht nur Hauptprozesse, sondern auch relevante Unterprozesse zu betrachten. Eine zu detaillierte Auflistung aller Unterprozesse wurde nicht empfohlen und wurde abschließend auch als nicht ratsam eingeordnet. Die Bestimmung der Granularität kann aber nicht verallgemeinert werden und muss in jedem Anwendungsfall neu bestimmt werden.
Weiterhin mussten an dieser Stelle nicht nur Die Geschäftsprozesse, sondern auch die damit zusammenhängenden Anwendungen und Informationen identifiziert und erfasst werden. Auch hier musste auf die sinnvolle Wahl der Granularität geachtet werden.
Wie eine Erhebung und Erfassung von Geschäftsprozessen, Anwendungen und deren Zuordnung aussehen kann, zeigen folgende Beispiele (angelehnt an BSI 200-2):

Strukturanalyse der Geschäftsprozesse					
Bezeichnung	**Beschreibung**	**Prozessart**	**Prozessverantwortlicher**	**Mitarbeiter**	**Wichtigkeit**
GP001	**Produktion:** Text	Kerngeschäft	Leiter Produktion	Alle	sehr hoch
GP002	**Einkauf:** Text	Unterstützender Prozess	Leiter Einkauf	Einkauf	mittel

Tabelle 9: Erfassung der Geschäftsprozesse und der dazugehörigen Information

Zuordnung Geschäftsprozesse zu Anwendungen					
Geschäftsprozess / Anwendungen	**A001**	**A002**	**A003**	**A004**	**A005**
GP001	X		x		
GP002	X				X

Tabelle 10: Zuordnung Geschäftsprozesse zu Anwendungen

6. Netzplanerhebung

Um weitere technische Komponenten identifizieren und analysieren zu können, wurde die Erstellung eines Netzplans exemplarisch durchgeführt. Ein Netzplan ist eine grafische Übersicht über die in der Informations- und Kommunikationstechnik eingesetzten Komponenten und deren Vernetzung. Man kann zwischen physischen und logischen Netzplänen unterscheiden. In der EUROGATE waren die Pläne bereits vorhanden oder wurden während des Projektes in den vorherigen Arbeitspaketen erzeugt. Im Hafen MD wurde das Konstrukt Netzwerkplan eingeführt.
Folgende Komponenten wurden in den Netzplänen identifiziert:

- IT-Systeme, z.B. Client- und Server-Computer, aktive Netzkomponenten (Switches, Router, WLAN Access Points), Netzdrucker usw.
- ICS (Industrial Control System) - und IoT-Komponenten mit Netzanschluss, z.B. Clients, Handscanner, Industriedrucker, Geräte mit speicherprogrammierbarer Steuerung (SPS), Schaltschränke usw.
- Netzverbindungen zwischen den genannten Systemen, d. h. LAN-Verbindungen, WLAN-Verbindungen, Backbone-Techniken (wie ATM - Asynchroner Transfer Mode) usw.
- Verbindungen nach außen, d. h. Einwahlzugänge über ISDN oder Modem, Internetanbindungen oder Router, Funkstrecken oder Mietleitungen zu entfernten Gebäuden oder Liegenschaften usw.

Neben der graphischen Darstellung der Komponenten wurde das Konzept einen Netzplan, ggf. mit zusätzlichen Kataloginformationen anzureichen erörtert. Eine Anzahl von Mindestinformationen, die zu jeder Komponente enthalten sein sollten, sind:

- eine eindeutige Bezeichnung oder ID, Typ und Funktion (Datenbank-Server für Anwendung X),
- die zugrunde liegende Plattform (Hardware-Plattform + Betriebssystem),
- der Standort (Gebäude- und Raumnummer),
- der zuständige Administrator,
- die vorhandenen Kommunikationsschnittstellen (Internetanschluss, Bluetooth, WLAN Adapter, etc.). Bei externen Verbindungen oder drahtlosen Verbindungen (WLAN, UMTS, LTE, ...) sollten zusätzliche Informationen über das externe Netz beschrieben werden
  - Internet,
  - Geschäftspartner,
  - Name des Providers und
  - Art Leitung, z. B. MPLS, Leased Line, VPN)

Die Abbildung 37 enthalt ein Muster aus dem Datenschutz EKD Bereich [62].

7. Erfassung von IT-, ICS-Systemen und anderen Geräten

Die vorhandenen und auch die geplanten IT-Systeme wurden exemplarisch in tabellarischer Form aufgestellt. Unter IT-Systeme zählten hierbei allerdings nicht nur klassische Computer, sondern auch IoT- und ICS-Geräte, aktive Netzkomponenten, Netzdrucker, TK-Anlagen, mobile Endgeräte (Smartphones und ähnliche) und virtuelle IT-Systeme. Die Betrachtung richtete sich bei der Erfassung nicht auf die einzelnen Bestandteile eines der genannten IT-Systeme (Bildschirm, Tastatur, Maus, etc.), sondern die IT-Systeme als Ganzes (Linux-Server, Windows-Client, etc.).
Abschließend wurden die Anwendungen den IT-Systemen zugeordnet, um eine Übersicht über die Zusammenhänge zwischen den wichtigen Anwendungen und den entsprechenden IT-Systemen zu erhalten.

Nachfolgend finden sie Beschreibungen der einzelnen Klassen

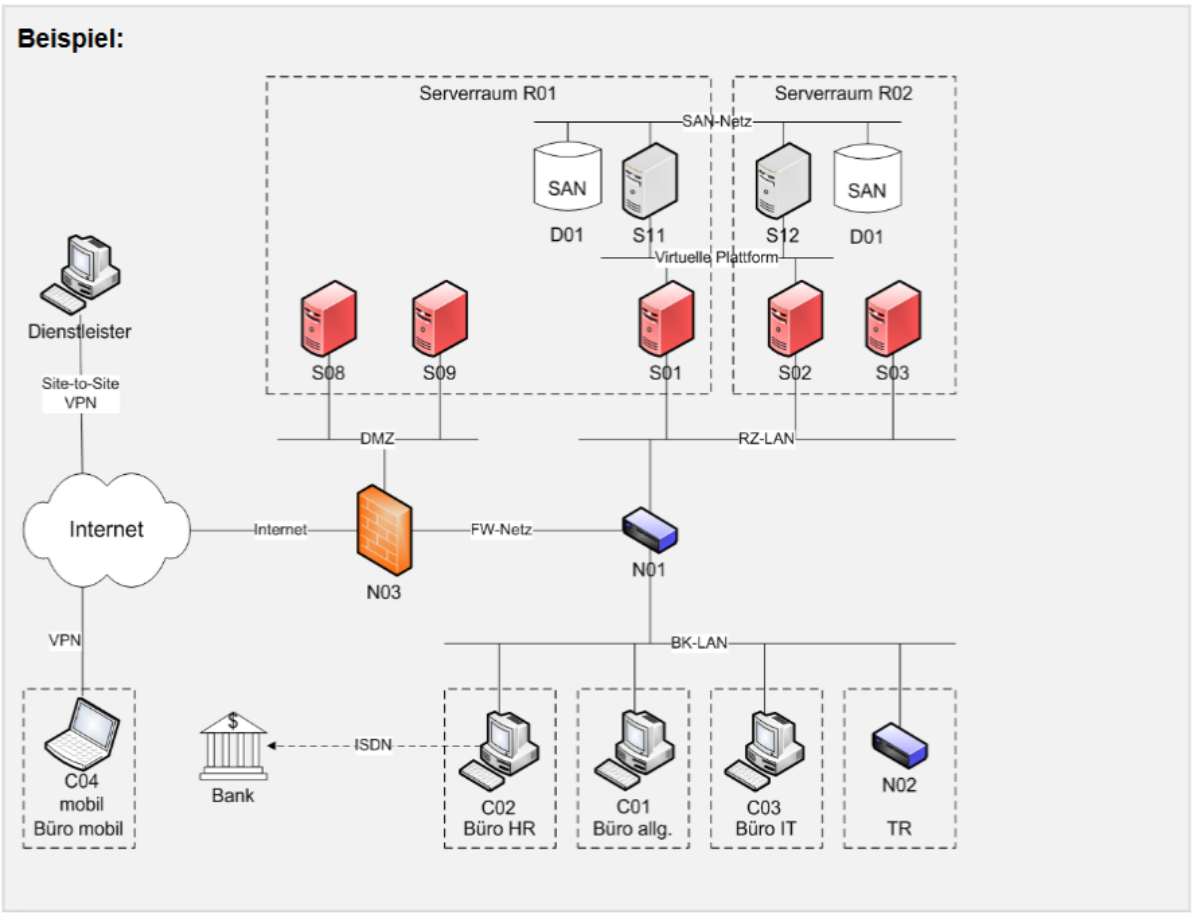


Abbildung 37: Beispiel eines physischen Netzwerkplans

IT-Systeme

Es müssen alle vernetzten und nicht vernetzten IT-Systeme, insbesondere auch die, die nicht im Netzplan erfasst worden sind aufgelistet werden.

Folgende Informationen sollten sich in einer entsprechenden Liste wiederfinden:

- eine eindeutige Bezeichnung der IT-Systeme und die Anzahl bei gruppierten Systemen
- Beschreibung (z. B. Funktion, Typ)
- Plattform (z. B. Hardware-Architektur/Betriebssystem)
- Standort der IT-Systeme (z. B. Ort, Gebäude, Raum)
- Status der IT-Systeme (in Betrieb, im Test, in Planung)
- Benutzer bzw. Administratoren

ICS-Systeme

Speziell in Cyber-physischen Systemen müssen auch die industriellen Steuerungssysteme (ICS) im Rahmen der Strukturanalyse erfasst werden. Unter die Kategorie ICS fallen spezielle Endgeräte, wie z. B. Geräte mit speicherprogrammierbaren Steuerungen (SPSen), WLAN-Module für Maschinen oder selbstfahrende Fahrzeuge.

Folgende Informationen sollten erfasst werden:

- eindeutige Bezeichnung der ICS-Systeme und die Anzahl bei gruppierten Systemen
- Beschreibung (Typ und Funktion)
- Plattform (z. B. Betriebssystem, Art der (Netz-)Anbindung)
- Standort der Geräte (z. B. Gebäude, Halle, Raum)

- Status der ICS-Systeme (in Betrieb, im Test, in Planung)
- Verantwortliche für die ICS-Systeme

Andere Geräte, z.B. IoT Geräte

Neben den klassischen IT- und ICS-Systemen können auch viele andere Arten von Geräten, die oftmals schwer zu identifizieren sind, Einfluss auf die Informationssicherheit haben, z.B. IoT-Geräte, Kaffeemaschinen, Klimaanlagen, Gefahrenmeldeanlagen und viele mehr, auch wenn sie nicht direkt an Geschäftsprozesse beteiligt sind. Ein Kabelbrand kann beispiels-weise Folgeschäden nach sich ziehen, die die Informationssicherheit gefährden können. Für die Modellierung sollten alle vernetzten Geräte mit IoT-Funktionalität erfasst werden, speziell diese, die nicht im Netzplan erfasst wurden.

Folgende Informationen sollten erfasst werden:

- Beschreibung (Typ und Funktion)
- Plattform (z. B. Betriebssystem, Art der Netzanbindung)
- Standort der Geräte (z. B. Gebäude, Halle, Raum)
- Status der Geräte (in Betrieb, im Test, in Planung)
- Verantwortliche für die Geräte

8. Erfassung der Räumlichkeiten (örtlichen Gegebenheiten des Hafens)

Die Geschäftsprozesse des definierten Informationsverbunds werden bei der EUROGATE und dem Hafen MD innerhalb einer räumlichen Infrastruktur durchgeführt. Diese Infrastruktur kann von einem allein genutzten Raum oder Gebäude bis hin zu weitverstreuten Liegenschaften reichen. Oftmals werden auch fremden Räumlichkeiten genutzt, z. B. im Rahmen von Dienstleistungsverträgen.
Alle Liegenschaften, in denen die Geschäftsprozesse betrieben werden, müssen bei der Erfassung berücksichtigt werden. Dazu gehören Betriebsgelände, Gebäude, Etagen, Räume und auch die Wegstrecke zwischen diesen. Auch Räumlichkeiten, die nicht zu den offiziellen Liegenschaften zählen, wie z. B. ein Homeoffice-Arbeitsplatz, sind zu betrachten.
In erster Linie müssen alle Räume erfasst werden, in denen IT-, ICS- oder IoT-Systeme auf-gestellt sind. Dazu gehören Räume, die ausschließlich dem IT-Betrieb dienen (z.B. Server-räume, Datenträgerarchive), aber auch solche in denen IT-, ICS-oder IoT-Systeme betrieben werden (z.B. Büroräume oder Werkhallen). Nicht zu vergessen sind die Wegstrecken, über die Kommunikationsverbindungen laufen.
Zusätzlich müssen alle Räume erfasst werden in denen schutzbedürftige Informationen aufbewahrt werden. Die Form der Aufbewahrung spielt hier keine Rolle. Auch eine nicht elektronische Aufbewahrung (z.B. Akten, Mikrofilme) ist hier zu berücksichtigen.

Folgende Informationen sollten erfasst werden:

- Beschreibung (Typ und Funktion)
- Plattform (z. B. Büroraum, Lagerhalle)
- Ort, Gebäude, Raum, Anzahl
- Status der Räume (in Betrieb, in Planung)
- Verantwortliche für die Räume

9. Schutzbedarf-Feststellung

Zweck der Schutzbedarfsfeststellung war es, zu ermitteln, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu wurden beispielhaft für einzelne Geschäftsprozess, Anwendung, und verarbeiteten Informationen der Schutzbedarf bzgl. einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit ermittelt. Der Schutzbedarf leitet sich aus der Anzahl und dem Ausmaß möglicher Schäden ab, die durch die Beeinträchtigung von Anwendungen oder anderer Objekte und somit auch dem verbundenen Geschäftsprozess entstehen können. Für die bessere Vergleichbarkeit bat sich eine Einteilung Schutzbedarfskategorien, z.B. „normal“, „hoch“ und „sehr hoch“ an.

10. Auswahl von Maßnahmen

Die Informationen über die Struktur und den Schutzbedarf der relevanten Objekte (Entitäten) wurde in den zuvor beschriebenen Teilaufgaben ermittelt und dokumentiert. Um geeignete Sicherheitsanforderungen und umzusetzende Maßnahmen für den betrachteten Informationsverbund (Unternehmensbereich oder Teilaufgaben) identifizieren zu können, mussten die Bausteine des IT-Grundschutz-Kompendiums auf die Zielobjekte und Teilbereiche abgebildet werden. Dabei konnte festgestellt werden, dass der IT-Grundschutz zwar eine gute Ausgangsbasis bildet, diese aber durch die Partner Hafen MD und EUROGATE stark erweitert werden müssten, ohne dass diese Informationen übergreifend zu Verfügung stehen.

11. Schutz-Check (Soll-Ist-Vergleich)

Der Schutz Soll Check wurde bei der Evaluierung nicht durchgeführt.

Der Schutz-Check soll einen schnellen Überblick über das vorhandene Sicherheitsniveau (IST-Zustand) bieten. Dieser Katalog des „Status quo“ kann an dieser Stelle des Prozesses mit der zuvor durchgeführten Schutzbedarfsanalyse verglichen werden. Durch die Identifizierung von noch nicht oder nur teilweise erfüllten Anforderungen werden Verbesserungs-möglichkeiten für die Sicherheit der betrachteten Geschäftsprozesse und der Informations-technik aufgezeigt.

12. Risikoanalyse

Die Risikoanalyse wurde schon in den vorhergehenden Arbeitspaketen entworfen und wir hier nur für allgemeine Komponenten beschrieben.

Bei einem hohen oder sehr hohen Schutzbedarf kann es sinnvoll sein, zusätzlich zu den zu-vor beschriebenen Teilaufgaben des Sicherheitsprozesses, zu prüfen, ob zusätzliche oder ersatzweise höherwertige Sicherheitsmaßnahmen erforderlich sind. Dies gilt auch, wenn besondere Einsatzbedingungen vorliegen oder wenn Komponenten verwendet werden, die nicht mit den existierenden Bausteinen des IT-Grundschutz-Kompendiums abgebildet wer-den können. In diesen Fällen ist eine Risikoanalyse durchzuführen. Sie sollte in regelmäßigen Abständen aktualisiert werden, damit auch geänderte Gefährdungslagen schnell erkannt werden können.

Bei der Risikoanalyse müssen Bedrohungen, Schadenspotenziale und Eintrittshäufigkeiten eingeschätzt und die daraus resultierenden Risiken bewertet werden. Individuelle Werte für Schäden und Eintrittshäufigkeiten im Detail zu ermitteln, stellt sich in der Praxis jedoch meist als schwierig, aufwendig und fehleranfällig dar. Daher empfiehlt sich, für die Eintrittshäufigkeit und auch für die potenzielle Schadenshöhe mit qualitativen Kategorien zu arbeiten, z. B.:

- Eintrittswahrscheinlichkeit: selten, mittel, häufig, sehr häufig
- Potenzielle Schadenshöhe: vernachlässigbar, begrenzt, beträchtlich, existenzbedrohend

Die Granularität, auf der solche Bewertungen im Rahmen der Risikoanalyse durchgeführt werden können, ist je Anwendungsfall zu entscheiden. Der Grundschutzkatalog des BSI bietet hierfür Übersichten, Beispiele und konkrete Empfehlungen.

Jede Risikoanalyse sollte die folgenden Schritte umfassen [63]

- zu schützenden Informationen und Geschäftsprozesse identifizieren
- relevante Bedrohungen für die zu schützenden Informationen und Geschäftsprozesse ermitteln
- eventuelle Schwachstellen/Sicherheitslücken analysieren
- potenzielle Schäden durch den Verlust der definierten Schutzziele, z.B. Vertraulichkeit, Integrität oder Verfügbarkeit abschätzen
- möglichen Auswirkungen auf die Aufgabenerfüllung oder die Geschäftstätigkeit untersuchen

- Risiko, durch Sicherheitsvorfälle Schäden zu erleiden, bewerten

Im Folgenden wird die Risikoanalyse auf der Ebene der zuvor definierten CPS-Komponenten-Kategorien, Computerressourcen (IT-Systeme), Sensoren, Aktuatoren und Kommunikation durchgeführt. Dabei werden je Kategorie die Gefährdung der einzelnen Schutzziele bzgl. Eintrittswahrscheinlichkeit eines Angriffs und die potenzielle Schadenshöhe bewertet.

Eintrittswahrscheinlichkeit: selten, mittel, häufig, sehr häufig
Potenzielle Schadenshöhe: vernachlässigbar, begrenzt, beträchtlich, existenzbedrohend

Schutzziele	**Eintrittswahrscheinlichkeit**	**Schadenshöhe**
Vertraulichkeit		
Integrität		
Verfügbarkeit		
Authentizität und Authentisierung		
Zurechenbarkeit		
Eintrittswahrscheinlichkeit: selten, mittel, häufig, sehr häufig *Potenzielle Schadenshöhe: vernachlässigbar, begrenzt, beträchtlich, existenzbedrohend*		

Tabelle 11: Schutzziele, Eintrittswahrscheinlichkeit, Schadenshöhe

Eintrittswahr-scheinlichkeit	**Hoch**	Mittleres Risiko	Hohes Risiko	Hohes Risiko
	Mittel	Niedriges Risiko	Mittleres Risiko	Hohes Risiko
	Niedrig	Niedriges Risiko	Niedriges Risiko	Mittleres Risiko
		Niedrig	**Mittel**	**Hoch**
		Schadenshöhe		

Abbildung 38: Risikomatrix [62]

4.6.1 Anwendungsfälle und Evaluierung: Use Case Übersee-Häfen (EUROGATE)

Durch das Projekt STRADegy (BMVI, Programm IHATEC) wurden im Testfeld Wilhelmshaven selbstfahrende Container-Transport-Fahrzeuge bereitgestellt. Hierfür wurden entsprechende Testszenarien entworfen und mit der EUROGATE und dem FHG-IFF abgestimmt. Tests bezogen sich auf die automatisierte Testbarkeit ausgehend von Daten eines Digitalen Zwillings. Weiterhin wurden Planspiele mit der Entwicklung und dem Betrieb zur Überprüfung der Prozesse und Organisationsmodelle durchgeführt.

Durch das FHG-IFF wurde hierfür eins automatisierten Überwachungssystems entworfen, implementiert und erste funktionale Tests durchgeführt. Leider konnte das System durch die Auswirkungen der Corona Pandemie nur begrenzt im auf dem Testfeld in WIlhelmshaven erprobt werden. Grundsätzlich konnte aber die Möglichkeit des Abgleichs von Produktion Daten mit einem komplementären Messsystem aufgezeigt werden. Die METOP GmbH begleitet diese Tests und hat bei der Testvor- und Testnachbereitung unterstützt.

Eine Evaluierung des allgemeinen Vorgehens (Prozess- und Organisationsmodell bezüglich Sicherheitsprozess) erfolgte entlang des BSI Leitfadens unter Berücksichtigung der neuen CPS Anforderungen. Anschließend erfolgen die Validierung und Bewertung der Übertragbarkeit des Ansatzes.

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

Im Gegensatz zum Arbeitspaket 5.1, in welchem die praktische Evaluierung im Vordergrund stand, wurde im Arbeitspaket 5.2 in Zusammenarbeit mit dem Hafen MD die Einführung und der Betrieb von CPS-Systemen an einem abstrakten CPS-System evaluiert.

Dabei sind im ersten Schritt insbesondere Problemstellungen der vertikalen Skalierung adressiert. Dabei standen in der Analyse service-orientierte Ansätze bezüglich der vollständigen Erbringung von automatisierten Logistiklösungen im Fokus. Hierfür wurden mit dem Hafen MD daraus resultierende Anforderungen an die Entwicklung und den Betrieb evaluiert.

5. Wichtigsten Positionen des zahlenmäßigen Nachweises

Die wichtigste Position des zahlenmäßigen Nachweises sind die Personalkosten für die beschäftigten Mitarbeiter. Weitere Ausgaben betreffen Dienstreisen, die getätigt wurden, um Veranstaltungen im Bereich Cyber-Security zu besuchen. Die nachstehende Tabelle 12 dokumentiert die personellen Aufwände für AUTOSec.

Arbeitspaket	**PM**
AP1: Anforderungsanalyse	9 PM
AP2.1: Gesamtarchitektur und Konzepte	8 PM
AP2.2: Organisationsmodell und Prozessvorgaben	7 PM
AP3: Entwicklung eines Prozessmodells	10 PM
AP4: Integration	9 PM
AP5.1: Use-Case 1: Überseehäfen (EUROGATE)	11 PM
AP5.2: Use-Case 2: Binnenhäfen (Hafen MD)	6 PM
AP6.1: Projektmanagement	5 PM
AP6.2: Ergebnisverbreitung	3 PM

Tabelle 12: personellen Aufwände für AUTOSEC

6. Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die durchgeführten Arbeiten, wie zum Beispiel:

- systematische Literatur-Recherche
- Forschung
- Konzepterstellung
- Methodenerstellung
- Prozesserarbeitungen
- Organigramm Erstellung
- Evaluierung
- CPS Architektur und Design

im Verbundprojekt AUTOSec sowie die dafür aufgewandten Ressourcen waren notwendig und angemessen, da sie der im Projektantrag formulierten Planung entsprachen und alle wesentlichen im Arbeitsplan formulierten Aufgaben erfolgreich bearbeitet wurden.

Bei den geplanten Kosten für Reisen wurden Mittel eingespart und für eine verbesserte Evaluierung unter den COVID19 Pandemiebedingungen für die Erweiterung der Personalkosten genutzt. Darüber hinaus waren keine zusätzlichen Ressourcen für das Projekt notwendig.

7. Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse im Sinne des fortgeschriebenen Verwertungsplans

Die grundlegenden Forschungsarbeiten und Konzepte, Methoden und allgemeine Vorgehensweise bzw. Leitlinien bieten eine Vielzahl von Verwertungsmöglichkeiten. Vor dem Hintergrund der innerbetrieblichen und gesellschaftlichen Bedeutung von Sicherheit von CPS werden folgende wesentlichen Anknüpfungspunkte gesehen.

7.1 Wirtschaftliche Erfolgsaussichten

Die wirtschaftlichen Erfolgsaussichten wurden mit der Entwicklung der Konzepte, Methoden und Tools zur Sicherung von cyberphysischen und IT-Systemen sowie dem zur Einführung und Umsetzung erforderlichen Prozessmodells, bestehend aus Sollkonzept und Rollenkonzept, bewertet und sind in der technischen und organisatorischen Anwendbarkeit sowie Umsetzbarkeit begründet. Diese Konzepte und Methoden lassen sich auf vielfältige Industriepartner transferieren.

In Zusammenarbeit mit dem Forschungsinstitut FHG-IFF, welches einen wesentlichen Beitrag in Form von Ergebnissen auf dem neusten Stand der Forschung und Entwicklung in den Bereichen der Logistik leistete, sowie durch die METOP, welches als An-Institut der Otto-von-Guericke Universität Magdeburg an der Nahtstelle zwischen Forschung und Industrie als erfahrener Partner im Bereich der Entwicklung von innovativen Datenhaltungssystemen und Software-Techniken arbeitet, konnten praxisrelevanten, wissenschaftlichen Ergebnissen erzeugt werden, die in laufende oder zukünftige Forschungs- und Entwicklungsvorhaben einfließen und in Folgeprojekten umgesetzt und weiterentwickelt werden. Teile der Ergebnisse fließen durch die enge Kooperation mit der Otto-von-Guericke Universität Magdeburg und der Hochschule Harz auch in die akademische Ausbildung ein. Wissenschaftlich relevante Ergebnisse wurden/werden auf nationalen und internationalen Kongressen präsentiert und veröffentlicht.

Neben den im Projekt als Basis für die Evaluierung herangezogenen Use-Cases zur Automatisierung der Straddle Carrier im Container-Terminal der Eurogate sowie der (Teil-)Automatisierung des Warenumschlags im Magdeburger Hafen ergeben sich zahlreiche weitere Anwendungsfälle, die ebenfalls durch die Integration und Nutzung cyberphysischer Systeme oder IT-Systeme allgemein, von der Anwendung der Projektergebnisse partizipieren können. Hiermit wird insbesondere die Consulting Tätigkeit in den Bereichen strategische IT-Beratung unter dem Gesichtspunkt Sicherheit und Projektbegleitung bei der Einführung von (Teil)automatisierten System gestärkt.

Ausgehend von den Arbeiten in AUTOSec ergeben sich für die METOP die im Folgenden dargestellten wirtschaftlichen Erfolgsaussichten.

Kurz- und mittelfristig

- Beratung von Unternehmen bezüglich des Aufbaus innerbetrieblicher Verfahrensweisen und Anwendungen zur Vermeidung von Sicherheitsvorfällen unter Berücksichtigung von Datenschutz und innerbetrieblicher Complaints Richtlinien
- Übertragung der Projektergebnisse bezüglich der CPS Systemen in der Logistik in andere Industriebreichen
- Aufbau einer Forschungskooperation mit FHG-IFF zur Gestaltung von Sicherheitsprozessen und Maßnahmen für die Sicherheit von CPS Systemen

Langfristig

- Aufbau einer Forschungskooperation mit FHG-IFF zur verhaltensbasierten Überwachung von CPS mit komplementären Messsystemen und Digitalem Zwilling
- Beratung von Unternehmen bei der Planung und Aufbau von automatisierten Prozessen in den Bereichen
  - Continuous Delivery
  - Continuous Integration

  für CPS und Teil(automatisierte) Systeme

Für die METOP ergeben sich weiterhin folgende wissenschaftlich sowie technischen Erfolgsaussichten.

Kurz- und mittelfristig

- Ausbau und weitere Erforschung von Methoden und Konzepten zur schnellen Ermittlung von Ursache–Wirkung Beziehungen bezüglich von Sicherheitsvorfälle, unter Berücksichtigung von Datenschutz und Complaints-Regelungen in innerbetrieblichen Anwendungen
- Zusammenführung der bestehenden Forschungsergebnisse auf dem Gebiet der Sicherheit von CPS Systemen
- Einbindung der Forschungsergebnisse in die Vorlesung „IT Security and Risk-Management an der Hochschule Harz“

Langfristig

- Ausbau und weitere Erforschung von Potentialen des digitalen Zwillings und der digitalen Shadow Ansätze zur Identifikation und Vermeidung von Sicherheitsvorfallen bei CPS
- Ausbau der forschungsnahen Beratung und Expertise des Anwendungsforschungsspektrums der METOP GmbH

7.2 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

Im Ergebnis wurde ein Modell und Methodenset zur Unterstützung der Konzeption und Architektur von Automatisierungslösungen für Industrie 4.0. auf Basis von Design Pattern erschaffen. Diese Expertise wir in eine wirtschaftliche Verwertung überführt

Die ersten Vertriebsaktivitäten werden bereits innerhalb des Projektes gestartet, sind aber auf den Cyber Raum beschränkt. Erste Kontaktaufnahmen mit Herstellern von CPS waren dagegen sehr unbefriedigend, da das Thema Security derzeit für Hersteller von CPS nicht relevant erscheint. Hier wird eine stärke Fokussierung auf den Bereich Safety durch die METOP notwendig sein. Diese Fokussierung wurde auch in einem Anschlussprojekt mit der IB Sachsen-Anhalt angegangen.

Innerhalb der Projektlaufzeit wurde bereits ein erster Transfer von einem großen Überseehafen zu einem kleinen Binnenhafen angewandt. Dabei aufgetretene Probleme hinsichtlich der vertikalen Skalierung müssen aber weiter untersucht werden, um ein durchgängiges Model zu erzeugen. Derzeit wird die wirtschaftliche Verwertung in zwei voneinander getrennten Bereichen weiterentwickelt:

Service Provider: Bereitstellung und Betrieb von CPS
Service Nutzer: Einsatz von CPS zur Automatisierung von Geschäftsprozessen
werden.

Über diese Punkte hinaus gehend bieten sich der METOP GmbH folgende Möglichkeiten der Anschlussfähigkeit.

Kurz- und mittelfristig

- Grundlagenforschung: Weiterführende Arbeit als Netzwerkpartner in dem Verbund Wirtschaft und Wissenschaft mit den Verbundpartnern und auch anderen Forschungs- und Anwendergruppen, um das Portfolio im Bereich Sicherheit von CPS zu schärfen.
- Erweiterung des Portfolios um das neue Forschungsthema und Ausbau des Geschäftszweiges: digitaler Zwilling, digitaler Shadow und Sicherheit von CPS in Zusammenarbeit mit dem Partner FHG-IFF
- Übertragung von DevOps Ansätzen auf die Entwicklung von CPS

Langfristig

- Technische Begleitung und Unterstützung bei strategischen Entscheidungen innerhalb von IT-Projekten im Bereich Sicherheit von CPS
- Anwendungsgetriebene Forschung im Bereich der Sicherheit von CPS

8. Fortschritt auf dem Gebiet des Auftrags bei anderen Stellen

Es konnten keine relevanten Fortschritte von anderer Stelle festgestellt werden.

9. Gesamtliste der Veröffentlichungen und Vorträge

1) Veröffentlichung inkl. Vortrag auf der Konferenz INCOM 2021, 7-9 June 2021 Budapest Conference
Topic: Information Control in the cyber-physical enterprise: technological breakthrough vs. cultural revolution

Boosting Cyber-Physical System Security

Tobias Kutzler * **Alexandra Wolter** ** **Andy Kenner** ***
Stephan Dassow ****

* *Fraunhofer Institute for Factory Operation and Automation IFF, Sandtorstr. 22, 39106 Magdeburg, Germany (e-mail: tobias.kutzler@iff.fraunhofer.de)*
** *Fraunhofer Institute for Factory Operation and Automation IFF, Sandtorstr. 22, 39106 Magdeburg, Germany (e-mail: alexandra.wolter@iff.fraunhofer.de)*
*** *METOP GmbH, Sandtorstr. 23, 39106 Magdeburg, Germany (e-mail: andy.kenner@metop.de)*
**** *METOP GmbH, Sandtorstr. 23, 39106 Magdeburg, Germany (e-mail: stephan.dassow@metop.de)*

Abstract: Automation and digital connectivity can be used to tap a great potential to boost efficiency as solutions are being introduced in the Industry 4.0 environment. Automation and connectivity spawn a multitude of risks arising from cyberattacks, which affect process stability (safety) and IT security (security), though. Automation projects currently lack standards for the protection of automated systems, the exchange of data, and performance monitoring in the end-to-end process chain (e.g. container terminals) in critical infrastructures. This paper describes the process model developed in the AUTOSEC research project, which was employed to derive actions and security mechanisms that boost IT security and fend off cyberattacks on IT-systems. The approach developed in this project was prototyped and evaluated in a demonstrator in an automated solution.

Keywords: Cyber-Physical Systems, Risk Management, Security, Safety, Automated Guided Vehicles (AGV) Monitoring, Resilience, Physical Internet

2) angenommene Veröffentlichung, Konferenz 25th ACM International Systems and Software Product Line Conference, 6-11 September 2021, Leicester, United Kingdom
Topic: Safety, Security and Configurable Software Systems: A Systematic Mapping Study

Safety, Security, and Configurable Software Systems: A Systematic Mapping Study

Andy Kenner
METOP GmbH & Otto-von-Guericke University Magdeburg, Germany
andy.kenner@metop.de

Richard May
Harz University Wernigerode, Germany
rmay@hs-harz.de

Jacob Krüger
Otto-von-Guericke University Magdeburg, Germany
jkruger@ovgu.de

Gunter Saake
Otto-von-Guericke University Magdeburg, Germany
saake@ovgu.de

Thomas Leich
Harz University Wernigerode & METOP GmbH, Germany
tleich@hs-harz.de

ABSTRACT

Safety and security are important properties of any software system, particularly in safety-critical domains, such as embedded, automotive, or cyber-physical systems. Moreover, particularly those domains also employ highly-configurable systems to customize variants, for example, to different customer requirements or regulations. Unfortunately, we are missing an overview understanding of what research has been conducted on the intersection of safety and security with configurable systems. To address this gap, we conducted a systematic mapping study based on an automated search, covering 10 years (2011–2020) and 65 relevant (out of 367) publications. We classified each publication based on established security and safety concerns (e.g., CIA triad) as well as the connection to configurable systems (e.g., ensuring security of such a system). In the end, we found that considerably more research has been conducted on safety concerns, but both properties seem underexplored in the context of configurable systems. Moreover, existing research focuses on two directions: Ensuring safety and security

ACM Reference Format:
Andy Kenner, Richard May, Jacob Krüger, Gunter Saake, and Thomas Leich. 2021. Safety, Security, and Configurable Software Systems: A Systematic Mapping Study. In *Proceedings of 25th ACM International Systems and Software Product Lines Conference (SPLC'21).* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Safety and Security (S&S) are important quality attributes of any software system, particularly in the context of safety-critical domains in which harms to the system, its users, or the surrounding environment must be avoided. For instance, automotive systems (e.g., self-driving cars) must prevent accidents and injuries [22], cloud-computing systems must ensure data availability and privacy [27], or cyber-physical systems must assure the safety of involved humans [17]. Consequently, various software-engineering process models and standards (e.g., ISO 26262) in such domains explicitly involve S&S concerns.

3) Industrial Research Track Paper

Questionnaire on the Subject: Security and Safety in Cyber Physical Systems

Introduction & Terms

With this questionnaire, we aim to collect information to scope future projects in the field of Cyber Physical Systems (CPSs). In this context, we emphasize especially the aspects of security and safety protection objectives, which we aim to consider from different perspectives. Regarding security and safety, we assume that CPSs pose novel challenges that require a joint effort of various stakeholders and integration into/of various components. It is not sufficient anymore to analyze and guarantee these two protection objectives independently, since they are interacting with each other, humans, and their environment, each of which may involve unforeseen changes.

In Zusammenarbeit mit der OvGU Universität Magdeburg und dem LIT Cyber-Physical Systems Lab in Innsbruck wird dieses Thema weiterführend bearbeitet. Leider ist ein entsprechendes Feedback aus der Industrie auf Workshops nicht zielführend gewesen, da das Thema Security durch die Industrie derzeit nicht fokussiert wahrgenommen wird.

10. Literaturverzeichnis

[1] U. Weinreich, „Digitale Sicherheit," *Lean Digitization. Springer Berlin Heidelberg,* pp. 125-134, 2016.

[2] Runde, Markus, et al., „Automation Security Risk Assessment," *atp edition 58.01-02,* pp. 48-55, 2016.

[3] Chughtai, A., Dörnemann, H., Heinold, R., Hubert, R., Salomon, K., & Vogel, O., Software Management: Beherrschung des Lifecycles., G. Versteegen (Ed.): Springer-Verlag, 2013.

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

[5] U. Sendler, „Industrie 4.0–Beherrschung der industriellen Komplexität mit SysLM," *Industrie 4.0. Springer Berlin Heidelberg,* pp. 1-19., 2013.

[6] G. Tassey, „The economic impacts of inadequate infrastructure for software testing. NIST (National Institute of Standards and Technology)," *Planning Report 02-3,* 2002.

[7] Vorgang, Blair R.; Karry, Alec, „Addressing Software Security in the Federal Acquisition Process," *Cigital White Paper https://www.cigital.com,* 2011.

[8] Bauhaus-Projekt, „Software-Architektur, Software-Reengineering und Programmverstehen," 2013. [Online]. Available: http://www.iste.uni-stuttgart.de/ps/projekt- bauhaus.html.

[9] Bunke, Michaela; Sohr, Karsten, „An architecture-centric approach to detecting security patterns in software," *Engineering Secure Software and Systems. Springer,* p. 156–166, 2011.

[10] E. Bodden, „Efficient Hybrid Typestate Analysis by Determining Continuation-Equivalent States," *ICSE '10: International Conference on Software Engineering,* p. 5–14, 2010.

[11] L. Pimendis, „Beobachten von Netzwerken – Überwachung der Sicherheit," *MISC Magazin. ,* Bd. Ausgabe 01/2006, 2006.

[12] Rostyslav Zabolotnyi, Philipp Leitner, Waldemar Hummer, and Schahram Dustdar, „JCloudScale: Closing the Gap Between IaaS and PaaS," *ACM Trans. Internet Technol. 15,* pp. 5-20, 2015.

[13] M. Httermann, Devops for Developers (1st ed.), Berkely, CA, USA: Apress, 2012.

[14] Howard, Michael; Lipner, Steve, „The Security Development Lifecycle," *Redmond, WA, USA : Microsoft Press,* 2006.

[15] SAFECode, „Software Assurance Forum for Excellence in Code: SAFECo-de," 2007. [Online]. Available: http://www.safecode.org/index.php.

[16] Christoph Pohl, Hans-Joachim Hof, „Secure Scrum: Development of Secure Software with Scrum," *SECURWARE The Ninth International Conference on Emerging Security Information, Systems and Technologies,* Bde. %1 von %2Venice, Italy, 2015.

[17] Rene Esteves Maria, Luiz Antonio Rodrigues, Jr, and Nelson Alves Pinto, „ScrumS: a model for safe agile development," *Proceedings of the 7th International Conference on Managment of computational and collective intelligence in Digital EcoSystems,* 2015.

[18] M. Shahin, „Architecting for DevOps and Continuous Deployment. In , , and M," *Proceedings of the ASWEC 2015 24th Australasian Software Engineering Conference (ASWEC ' 15 Vol. II),* Bde. %1 von %2ACM, New York, pp. 147-158, 2015.

[19] Ståhl, Daniel, and Jan Bosch, „Modeling continuous integration practice differences in industry software development," *Journal of Systems and Software 87,* pp. 48-59, 2014.

[20] Waidner, Michael, Michael Backes, and Jörn Müller-Quade, „Entwicklung sicherer Software durch Security by Design," *Technical Report SIT-TR-2013-01, Fraunhofer-Institut für Sichere Informationstechnologie, Darmstadt, Germany.*

[21] Microsoft, „SDL Helps Build More Secure Software," Microsoft, 2013. [Online]. Available: http://www.microsoft.com/security/sdl/learn/measurable.aspx.

[22] A. S. Incorporated, „Secure Product Lifecycle," 2013. [Online]. Available: http://www.adobe.com/de/security/splc/.

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

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

[25] Zhu, Liming, Len Bass, and George Champlin-Scharff, „DevOps and Its Practices," *IEEE Soft-ware 33.3,* pp. 32-34, 2016.

[26] Callanan, Matt, Alexandra Spillane, „DevOps: Making It Easy to Do the Right Thing," *IEEE Software 33.3,* pp. 53-59, 2016.

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

[28] E. A. Lee, „Cyber physical systems: Design challenges," *11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC). IE-EE,* 2008.

[29] Delgado, Nelly, Ann Q. Gates, and Steve Roach, „A taxonomy and catalog of runtime software-fault monitoring tools," *IEEE Transactions on software Engineering 30.12,* pp. 859-872, 2004.

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

[31] Cardenas, Alvaro A., Saurabh Amin, and Shankar Sastry, „Secure control: Towards survivable cyber-physical systems.," *System 1.a2,* 2008.

[32] Verband der Elektrotechnik Elektronik Informationstechnik e. V., „Auszug aus VDE Tec Report 2018: Digitalisierung und Cyber Security," VDE Pressemittei-lung:, [Online]. Available: https://www.vde.com/de/presse/pressemitteilungen/tec-report-cyber-security.

[33] Bundesamt für Sicherheit in der Informationstechnik, „Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen 2019.," 2019. [Online]. Available: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_005.pdf.

[34] K. Yang, M. Hicks, Q. Dong, T. Austin and D. Sylvester, „A2: Analog Malicious Hardware," *IEEE Symposium on Security and Privacy (SP),* Bd. SP.2016.10. 10.1109, pp. 18-37, 2016.

[35] B. Morris, „More Keys Than A Piano Finding Secrets In Publicly Exposed Ebs Volumes," *DEFCON-27,* 2019.

[36] M. Broy, „Cyber-Physical Systems: Innovation durch softwareintensive eingebettete Systeme," *acatech, Springer Berlin Heidelberg,* 2011.

[37] „Was ist ein Cyber-physisches System (CPS)?," 2018-02-16. [Online]. Available: https://www.bigdata-insider.de/¬was-ist-ein-cyber-physisches-system-cps-a-668494.

[38] Yampolskiy, Mark & Horvath, Peter & Koutsoukos, Xenofon & Xue, Yuan & Sztipanovits, Janos, „Taxonomy for description of cross-domain attacks on CPS.," *Proceedings of the 2nd ACM international conference on High confidence networked systems,* pp. 135-142, 2013.

[39] Mingtao Wu, Young B.Moon , „Taxonomy of Cross-Domain Attacks on Cyber Manufacturing System," *Procedia Computer Science Volume 114,* pp. 367-374, 2017.

[40] Rasim Alguliyev, Yadigar Imamverdiyev, Lyudmila Sukhostat, „Cyber-physical systems and their security issues," *Computers in Industry,* Bd. 100, pp. 212-223, 2018.

[41] M. Foehr, J. Vollmar, A. Calà, P. Leitão, S. Karnouskos, and A. W. Colombo, „Engineering of Next Generation Cyber-Physical Automation System Architectures," *Multi-Disciplinary Engineering for Cyber-Physical Production Systems,* pp. 185-206, 2017.

[42] A. A. F. Saldivar, Y. Li, W.-n. Chen, Z.-h. Zhan, J. Zhang, and L. Y. Chen, „Industry 4.0 with cyber-physical integration: A design and manufacture perspective," *21st International Conference on Automation and Computing (ICAC). Glasgow, United,* pp. 1-6, 2015.

[43] A. W. Colombo, S. Karnouskos, and T. Bangemann, „Towards the Next Generation of Industrial Cyber-Physical Systems," *Industrial Cloud-Based Cyber-Physical Systems,* Nr. Springer Internation Publishing, pp. 1-22, 2014.

[44] J. Jiang, „An improved Cyber-Physical Systems architecture for Industry 4.0 smart factories," *International Conference on Applied System Innovation (ICASI),* pp. 918-920, 2017.

[45] Vogel-Heuser, Birgit & Kegel, Gunther & Bender, Klaus & Wucherer, Klaus, „ Global Information Architecture for Industrial Automation," *Automatisierungstechnische Praxis (atp),* pp. 108-115, 2009.

[46] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, „A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys & Tutorials,* Bd. 11, Nr. 4, pp. 42-56, 2009.

[47] Dong Y., Zhou P., „Jamming Attacks Against Control Systems: A Survey," *Intelligent Computing, Networked Control, and Their Engineering Applications. ICSEE ,* Bde. %1 von %2Communications in Computer and Information Science, vol 762. Springer, 2017.

[48] Kanika Grover, Alvin Lim, and Qing Yang, „Jamming and anti-jamming techniques in wireless networks: a survey," *Int. J. Ad Hoc Ubiquitous Computing,* Bd. 17, p. 197–215, 2014.

[49] C. Ebert, G. Gallardo, J. Hernantes and N. Serrano, „DevOps," *IEEE Software,* Bd. 33, pp. 94-100, 2016.

[50] Ugarte, Miriam & Etxeberria, Leire & Sagardui, Goiuria, Towards a DevOps Approach in Cyber Physical Production Systems Using Digital Twins, 2020.

[51] Al-Obeidallah, Mohammed & Petridis, Miltos & Kapetanakis, Stelios, „A Survey on Design Pattern Detection Approaches," *International Journal of Software Engineering,* Bd. 7, Nr. 3, pp. 41-59, 2016.

[52] Haider, S., Nazir, B. , „Fault tolerance in computational grids: perspectives, challenges, and issues," *SpringerPlus 5,* 2016.

[53] Jerome Hugues, Anton Hristosov, John J. Hudak, and Joe Yankel, „TwinOps - DevOps meets model-based engineering and digital twins for the engineering of CPS.," *In Proceedings of the 23rd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems: Companion Proceedings,* pp. 1-5, 2020.

[54] J.Q. Cao, S.H. Zhang, „ITIL Incident Management Process Reenginieering in Industry 4.0 Environments," *Proceedings of the 2nd International Conference on Advance in Mechanical Engineering und Industria Informatics (AMEII),* 2016.

[55] A. Limited, ITIL Foundation: ITIL 4.0 Edition, TSO; 4th Edition, 2019.

[56] Margot J. Hutchins, Raunak Bhinge, Maxwell K. Micali, Stefanie L. Robinson, John W. Sutherland, David Dornfeld, „Framework for Identifying Cybersecurity Risks in Manufacturing," *Procedia Manufacturing,* Bd. 1, pp. 47-63, 2015.

[57] P. Mell, and T. Grance, „Recommendations of the National Institute of Standards and Technology," *US Department of Commerce National Institute of Standards and Technology,* 2011.

[58] Ruland, K.C., Sassmannshausen, J., Waedt, K. et al., „Smart grid security – an overview of standards and guidelines," *Elektrotech. Inftech.,* Bd. 134, p. 19–25, 2017.

[59] Yang, W., Tan, Y., Yoshida, K., and Takakuwa, „Digital Twin-Driven Simulations for a Cyber Physical System in Industry 4.0," *DAAAM International,* p. 227 – 234, 2017.

[60] Uhlemann, T.H.J., Lehmann, C., and Steinhilper, R., „The digital twin: Realizing the cyber-physical production system for industry 4.0.," *Procedia CIRP,* Bd. 61, p. 335 – 340.

[61] Wang, E.K., Ye, Y., Xu, X., Yiu, S.M., Hui, L.C.K., and Chow, K.P, „Security issues and challenges for cyber physical system," *IEEE/ACM Int'l Con- ference on Green Computing and Communications Int'l Conference on Cyber, Physical and Social Computing,* 2010.

[62] „Muster IT SIcherheitskonzept für mittlere und grosse Einrichtungen," 09 2015. [Online]. Available: https://datenschutz.ekd.de/wp-content/uploads/2015/09/B_Muster-gro%C3%9F.pdf.

[63] „Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge: 14. Ergänzungslieferung," 2014-2021. [Online]. Available: Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge: 14. Ergänzungslieferung 2014. https://gsb.download.bva.bund.de/BSI/ITGSK/IT-Grundschutz Kataloge_2014_EL14_DE.pdf. .

Berichtsblatt

1. ISBN oder ISSN geplant	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht

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

Teilvorhaben: Umsetzung Software

4. Autor(en) [Name(n), Vorname(n)]

Dassow, Stephan
Kenner, Andy
Leich, Thomas

5. Abschlussdatum des Vorhabens
31.12.2020

6. Veröffentlichungsdatum
30.06.2021

7. Form der Publikation
Schlussbericht

8. Durchführende Institution(en) (Name, Adresse)

Mensch-Technik-Organisation-Planung GmbH (METOP GmbH)
Sandtorstraße 23
39106 Magdeburg

9. Ber. Nr. Durchführende Institution

10. Förderkennzeichen
19H17006D

11. Seitenzahl
80

12. Fördernde Institution (Name, Adresse)

Bundesministerium für
Verkehr und digitale Infrastruktur (BMVI)
53175 Bonn

13. Literaturangaben
63

14. Tabellen
12

15. Abbildungen
69

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)

18. Kurzfassung

Mit dem Einzug von Lösungen im Umfeld von Industrie 4.0 können große Effizienzsteigerungs-Potenziale 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 zielte mit den 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.

Ausgangsbasis für das Vorhaben AUTOSEC bildeten aktuelle Tendenzen im Bereich Infrastructure-as-Code und damit verbundene Architekturen und Sicherheitstendenzen im Bereich Resilienz. Für die Erhöhung der Resilienz, Prozesssicherheit und organisatorische Vorgaben von Automatisierungslösungen im Hafenumschlagsbereich wurden daher das Thema Isolation zur Erhöhung der Resilienz im Bereich Architektur Design Pattern (Security-by-Design), das Thema DevOps Entwicklungs- und Betriebsmodelle im Bereich Organisation und Prozesse, sowie der Informationssicherheitsprozess des BSI und NIST Framework für Automatisierungslösungen auf Basis von CPS erweitert werden. Im Ergebnis konnten architektonische Vorgaben für den Aufbau der Systemlandschaft, Prozesse zur schnellen Entwicklung und sicherem Betrieb, sowie Organisationsmodelle erarbeitet und erfolgreich evaluiert werden.

Die Anwendungsmöglichkeiten der Forschungsergebnisse lassen sich auf Automatisierungsvorhaben im Hafenumschlagsbereich und allgemein für den sicheren Betrieb von CPS anwenden. Die Erweiterung des NIST Frameworks auf CPS und die damit verbundene Überwachung der physischen Systeme mit einem digitalen Zwilling ist allgemein anwendbar.

19. Schlagwörter

IT Security, CPS Security, DevOps Security, Container Security, Informationssicherheitsprozess, Resilienz, NIST Framework

20. Verlag	21. Preis

Document Control Sheet

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

Sub-project: implementation of software

4. author(s) (family name, first name(s)) Dassow, Stephan Kenner, Andy Leich, Thomas	5. end of project 31.12.2020
	6. publication date 30.06.2021
	7. form of publication Final report
8. performing organization(s) (name, address) Mensch-Technik-Organisation-Planung GmbH (METOP GmbH) Sandtorstraße 23 39106 Magdeburg Germany	9. originator's report no.
	10. reference no. 19H17006D
	11. no. of pages 80
12. sponsoring agency (name, address) Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) 53175 Bonn	13. no. of references 63
	14. no. of tables 12
	15. no. of figures 69

16. supplementary notes

17. presented at (title, place, date)

18. abstract

With the introduction of solutions in the field of Industry 4.0, great potential for increasing efficiency can be tapped through automation and digital networking. However, networking and automation lead to a large number of risks that have an impact on the stability of the processes (safety) and, on the other hand, on IT security through cyber-attacks (security). For automation projects in the port handling area, there are currently no standards for securing the automation systems and their data exchange against cyber-attacks, as well as for monitoring the performance in the end-to-end process chain. The AUTOSEC project, together with project partners from research, development, and end users, aimed to increase IT security in ports and logistics chains as well as preventive defence against cyber-attacks on IT systems. With the project, a scalable set of methods and tools for the conception and introduction of automation projects in ports was developed and evaluated prototypically in use cases at a seaport (Hamburg, Wilhelmshaven) and an inland port (Magdeburg).

The starting point for the AUTOSEC project was formed by current trends in Infrastructure-as-Code area and the associated architectures and security trends in the resilience area. To increase resilience, process security and organizational requirements of automation solutions in the port handling area, the topic of isolation to increase resilience in the architecture design patterns (security-by-design) area, the topic of DevOps development and operating models in the organization and processes area, as well as the information security process of the BSI and NIST framework for automation solutions based on CPS are expanded.

As a result, the specifications for the structure of the system landscape, processes for rapid development and secure operation as well as organizational models were developed and successfully evaluated.

The possible applications of the research results can be applied to automation projects in the port handling area and generally for the safe operation of CPS. The extension of the NIST framework to CPS and the associated monitoring of the physical systems with a digital twin is generally applicable.

19. keywords

20. publisher	21. price