TRANSACT

Sachbericht

DLR e. V.

Berichtszeitraum: 01.01.2022 – 30.06.2024

Version	1.2
Editor	DLR e. V.
Förderkennzeichen	16MEE0209
Erstellungsdatum	12.12.2024

Gefördert durch:
Bundesministerium für Bildung und Forschung
aufgrund eines Beschlusses des Deutschen Bundestages

Dokumenteninformation

Autoren

Die im Folgenden genannten Personen haben an der Erstellung dieses Dokuments mitgewirkt. Durch den Übergang des Bereichs „Verkehr“ des OFFIS in das DLR Institut Systems Engineering für zukünftige Mobilität waren diese Personen teilweise zuvor beim OFFIS e. V. und anschließend beim Deutschen Zentrum für Luft- und Raumfahrt e. V. beschäftigt.

Dr.-Ing. Eike Möhlmann

Dr. rer.-nat. Astrid Rakow

Sebastian Vander Maelen

Thomas Strathmann

Arnold Akkermann

Kontakt

DLR e. V.

Escherweg 2

26121 Oldenburg

Deutschland

Phone: +49 441 770507 400

Email: andre.bolles@dlr.de

Beteiligte Partner:

Partnername	Abkür-zung
Philips GmbH	PFLH
AVL Software and Functions GmbH	AVL
Eclipse Foundation Europe GmbH	ECL
Denso Automotive Deutschland GmbH	DENSO
Fraunhofer IESE	IESE
OFFIS E.V.	OFFIS

DLR Institute Systems Engineering für zukünftige Mobilität	DLR

Sowie weitere internationale Partner siehe Anhang A.

Revisionslog

Version	Datum	Kommentar	Autor	Partner
0.1	19.01.2022	Initialer Entwurf	Sebastian Vander Maelen	OFFIS
0.11	03.02.2022	Vervollständigung	Sebastian Vander Maelen	OFFIS
1.0	13.05.2022	Letzte Anpassungen	Sebastian Vander Maelen	OFFIS
1.1	11.10.2024	Aktualisierung des Sachberichts für OFFIS für das DLR	Eike Möhlmann Arnold Akkermann Astrid Rakow	DLR
1.2	6.12.2024	Finale Überarbeitung	Eike Möhlmann	DLR

Inhaltsverzeichnis

1 KURZBERICHT

1.1 Aufgabenstellung

Im Projekt TRANSACT wurde ein universell anwendbares Lösungsarchitekturkonzept, Framework und Methodik für die Transformation von sicherheitskritischen cyber-physische Systeme (CPS) in verteilte sicherheitskritische CPS-Lösungen entwickelt. Das TRANSACT-Architekturkonzept bringt CPS-Geräte am Rande des Netzwerks mit mehreren Edge-Geräten (sowohl Low-End- als auch High-End-Geräte) und Cloud-Computing-Einrichtungen zusammen, die mehrere Anwendungen mit unterschiedlichen Kritikalitäten hosten. Ein Schlüsselelement des TRANSACT-Konzepts ist, dass die Edge- und Cloud-Infrastrukturen anwendungsübergreifend, geräteübergreifend, mandantenfähig, skalierbar und interoperabel sind und nicht-funktionale Qualitätseigenschaften wie z.B. Performance, technische Betriebssicherheit und Datensicherheit garantieren. Anwendungen können über diese verteilte Architektur flexibel eingesetzt werden. Neuartige Dienste und Anwendungen können die TRANSACT-Infrastruktur gemeinsam nutzen, Domänen-Dienste wiederverwenden und im Allgemeinen schneller entwickelt, getestet und unabhängig vom sicherheitskritischen Gerät selbst freigegeben werden. Dieses neue verteilte Architekturkonzept wird neue Geschäftsmodelle ermöglichen, indem es Systemhersteller in Lösungsanbieter verwandelt. Die Evaluierung erfolgt im Rahmen von fünf Fallstudien aus verschiedenen technischen Bereichen.

Zusammenfassend wurden in TRANSACT die folgenden fünf Ziele verfolgt:

1. Nutzung von Edge- und Cloud-Technologien für sicherheitskritische CPS,
2. Umsetzung von Konzepten für kontinuierliche Entwicklung und Updates von Anwendungen und Diensten,
3. Sicherstellung von Performance und technischer Sicherheit,
4. Gewährleistung von Datensicherheit und Datenschutz im Device-Edge-Cloud-Kontinuum,
5. Befähigung zur schnellen Entwicklung, Integration und Betrieb von Innovationen mit neuartigen Dienstleistungen und Produkten.

1.2 Planung und Ablauf des Vorhabens

Das Projekt gliederte sich in sechs Arbeitspakete (Abbildung 1), in denen Lösungen für fünf in AP1 und AP5 entwickelte Anwendungsfälle aus den Bereichen Gesundheit, Automotive und Schifffahrt erarbeitet und validiert wurden.

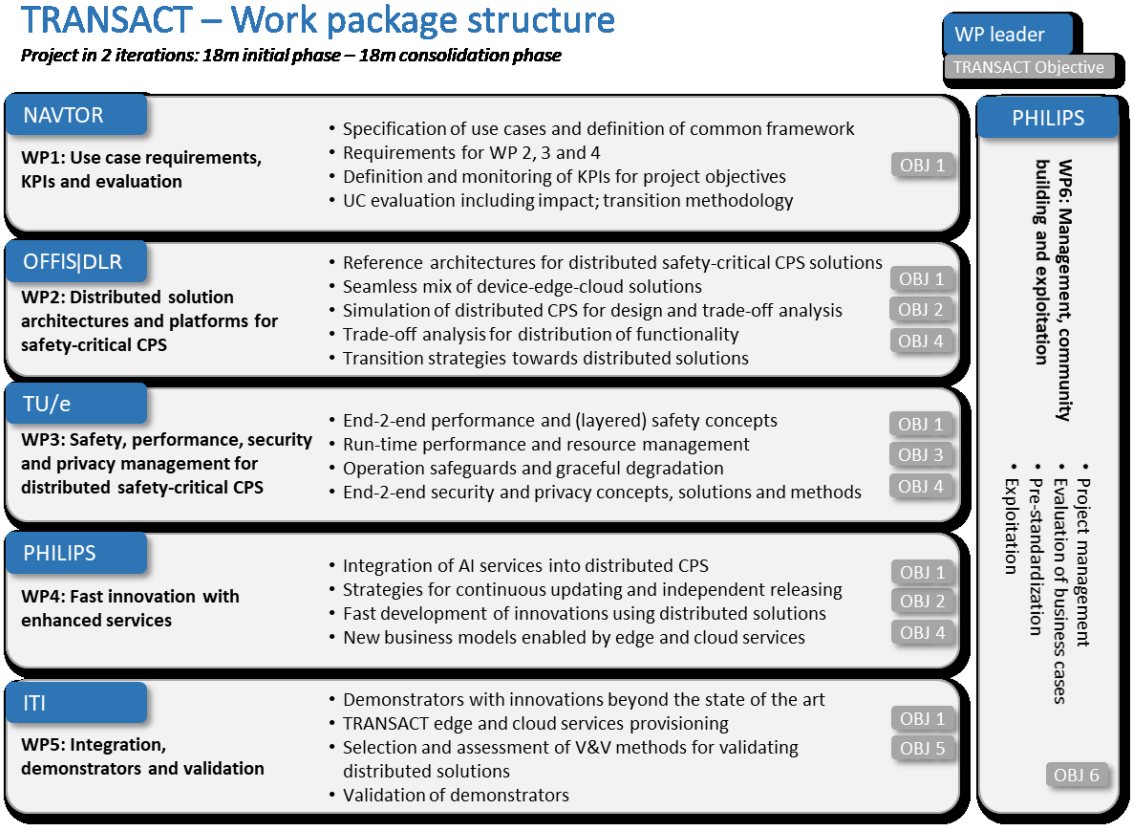


Abbildung 1: TRANSACT Arbeitspaketstruktur

AP2 betrachtete Architekturen und Analysenmethoden, AP3 beschäftigte sich mit Laufzeitlösungen und AP4 beschäftigte sich mit der Weiterentwicklung von sicherheitskritischen CPS. Die operative und technische Steuerung und Kommunikation sowie Ergebnisverwertung fand in AP6 statt.

DLR übernahm die Arbeiten von OFFIS an den technischen Arbeitspaketen AP1, AP2, AP3 und AP5 beginnend mit dem Projektmonat 6.

Der Arbeitsschwerpunkt von DLR in TRANSACT waren die Sicherheitsbewertung von Architekturen bei der Transformation von klassischen Systemen bei denen alle Funktionen auf dem System durchgeführt werden hinzu Systemen bei denen Funktionen in die Edge oder sogar in die Cloud ausgelagert wurden. Dies betrifft insbesondere Funktionen die mittelbar oder unmittelbar mit der sicherheitskritischen Anwendung des Systems verknüpft sind. Konkret sollen Methoden zu Analyse der Systeme, ihrer Architektur und Komponenten entwickelt werden, welche insbesondere die Auswirkung der Funktionsauslagerung betrachten. Darunter fallen Möglichkeiten zum Update und Upgrade aber auch Latenzen und reduzierte Verfügbarkeit.

1.3 Wissenschaftlicher und technischer Stand vor Beginn des Projekts

Der Stand von Wissenschaft und Technik bezieht sich auf die gestellten 5 Projektziele:

Das Ziel 1 (Nutzung von Edge- und Cloud-Technologien für sicherheitskritische CPS) wurde zu Beginn des Projektes in der Forschung durch verschiedene Konzepte und Technologien adressiert. Zum einen wurden Referenzarchitekturen für Edge- und Cloud-Computing entwickelt, welche die Besonderheiten verteilter nicht sicherheitsrelevanter Systeme und einen optimalen Betrieb gemäß der Qualitätsanforderungen [1] [2] [3] ermöglichen. Cloud-Plattformen wie AWS und Azure sind insbesondere auf nicht sicherheitskritische Anwendungen ausgerichtet. Edge Computing bietet nicht die Verlässlichkeit, die für sicherheitskritische CPS erforderlich ist [4] [5] [6] [7]. Daneben sind viele Produkte und Dienste mit ihren Sensor-, Planungs-, und Steuerungsfunktionen nicht für den Betrieb im Edge-Cloud-Kontinuum ausgelegt [3] [5] [6]. Flexible Transitionsstrategien fehlen hier. Das TRANSACT-Projekt deckte genau diese Lücke ab.

Bezüglich des Ziels 2 (Umsetzung von Konzepten für kontinuierliche Entwicklung und Update von Anwendungen und Diensten) umfasst der Stand von Wissenschaft und Technik zu Projektbeginn zum einen Ansätze zum modellbasierten Entwurf und Exploration von neuen Anwendungen und Diensten. Die zu diesem Zeitpunkt aktuellen modellbasierte Entwurfsansätze und -werkzeuge fokussierten entweder auf Funktionalität oder auf Zeitaspekten und Performance, aber niemals auf beide Aspekte [8] [9]. Verteilte CPS mit gemischt-kritischen, d.h. sicherheitsrelevanten und nicht sicherheitsrelevanten, Diensten und Komponenten wurden selten adressiert [10]. Ein weiterer Punkt ist die Integration, Freigabe und das Deployment von neuen Anwendungen und Diensten. Die damalige Over-the-Air-Update-Mechanismen konzentrieren sich auf das Einspielen und Rückgängigmachen der Updates. Sie berücksichtigen aber nicht die Safety-Aspekte in Systemen mit gemischtem Betrieb von Diensten und Komponenten in verschiedenen Versionen [11] [12]. Micro-Services und serviceorientierte Architekturen fokussieren auf die Zerlegung der Gesamtfunktion in kleinere, wartbare Dienste, berücksichtigen aber nicht die Besonderheiten der technischen Sicherheitsanforderungen.

Das Ziel 3 (Sicherstellung von Performance und technischer Sicherheit) wurde durch verschiedene Themen in den Forschungs- und Entwicklungsarbeiten adressiert. Zum einen wurden monolithische und statische Konzepte zur Sicherstellung von Performance und Safety-Eigenschaften entwickelt, wie bspw. fail-operational, fail-safe und Betriebsmodi mit abgestufter Funktionalität [13] [14]. Darüber hinaus gibt es Ansätze zum modellbasierten Safety Engineering von komplexen software-basierten Ökosystemen. Die Konzepte adressieren das Monitoring von Safety- und Performance-Eigenschaften und modellbasierte Entwurfs- und Analyseansätze für safety- und performance-kritische Systemarchitekturen [15] [16]. Des Weiteren gibt es aktuelle Lösungen zum Run-time Management beider Qualitätsattribute, bspw. durch Steuerungsansätze zur Laufzeit und Quality-of-service Methoden [17].

Das Ziel 4 (Gewährleistung von Datensicherheit und Datenschutz im Device-Edge-Cloud-Kontinuum) wurde im damaligen Stand der Wissenschaft und Technik durch verschiedene Ende-zu-Ende Absicherungen für die Datensicherheit adressiert. Zum einen gab es diverse branchenspezifische Standards, Vorschriften und Security Policies, wie bspw. ISO/SAE 21434 “Road vehicles–Cybersecurity engineering”, IEC 62443 “Security

for industrial automation and control systems", welche aber nur unvollständig die Besonderheiten von CPS berücksichtigen. Diese werden in Richtlinien wie dem NIST Security Framework und dem SAE J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" adressiert. Daneben gab es verschiedene Technologien für Datensicherheit und Datenschutz, welche datensichere Updates und Rollbacks ermöglichen, fremdes Eindringen erkennen oder Verhaltensmuster von Nutzern und Komponenten analysieren [18] [19] [20] [21]. Die Datensicherheit von CPS durch geeignete Entwurfsmethoden und Architekturen wurde damals in Forschung und Entwicklung nicht betrachtet.

Das Ziel 5 (Befähigung zur schnellen Entwicklung, Integration und Betrieb von Innovationen mit neuartigen Dienstleistungen und Produkten) wurde durch diverse Ansätze in der Forschung und Entwicklung adressiert. Zum einen erfordert die Integration und Absicherung von CPS mit KI-basierten Komponenten damals wie auch heute neue Konzepte und Technologien [22]. Für die Integration, die Freigabe und das Deployment wurden virtuelle Entwicklungs- und Absicherungslösungen entwickeln, wie bspw. AVL ModelConnect. Diese Lösungen berücksichtigten aber nur unzureichend die Herausforderungen von Edge- und Cloud-basierten Architekturen [23] [24]. Darüber hinaus mussten geeignete Geschäftsmodelle entwickelt werden, welche die Vorteile des TRANSACT Ansatzes voll ausschöpfen. Damalige Geschäftsmodelle fokussierten meist auf monolithischen Software-Systeme und deren Entwicklungs- und Freigabekosten und unterstützen keine flexible Definition von Geschäftsmodellen und Business Partner Ecosystems [25] [26].

1.4 Wesentliche Ergebnisse

Das DLR hat im Berichtszeitraum die folgenden Projektergebnisse erreicht bzw. aktiv an ihrer Erreichung mitgewirkt:

1. Ein **Vorgehensmodells zur Erhebung technischer Anforderungen** sowie die Koordinierung der Anforderungserhebung aller TRANSACT Use Cases und die Durchführung der Erhebung für UC2.
2. Die erhobenen Anforderungen wurden als Basis für die entwickelte **TRANSACT Referenzarchitektur** genutzt.
3. Ein **V&V Vorgehen**, welches speziell für den UC 2 angepasst und die Anwendbarkeit im UC2 demonstriert wurde.
4. Eine **Transition & Validation (T&V) Methodik**, welche für den Entwurf und die V&V von SCDCPS bestehende Methoden und Werkzeuge integriert und bei der Transition von SCCPS in ein SCDCPS unterstützt.

1.5 Zusammenarbeit mit anderen Stellen und Forschungseinrichtungen

Im Rahmen des Projektes arbeitete das deutsche Teilkonsortium eng mit Industrie- und Forschungspartnern des internationalen Projektkonsortiums zusammen. Der Austausch fand hier beispielsweise hinsichtlich der Erhebung der Anforderungen für die TRANSACT

Referenzarchitektur statt. Zuvor hat das OFFIS wesentliche Unterstützung bei der Erhebung der Anforderungen aus den fünf Anwendungsfällen heraus geleistet. Hier kam es insbesondere zum Austausch mit Fleetonomy, NAVTOR, AVL, Philips und DAM.

Zunächst OFFIS und später DLR waren zu dem in die Planung der Aktivitäten im maritimen Anwendungsfall involviert. Hierbei kam es zu einer engen Zusammenarbeit mit den norwegischen Partner NAVTOR.

Mit AVL kam es hinsichtlich des Anwendungsfalls des Batteriemanagementsystems zu einem Austausch hinsichtlich von Prozessen und Methoden für sichere (Safe&Secure) Updates. AVL hat im Rahmen dieses Anwendungsfall Methoden zum Update der Parameter des Batteriemanagementsystems bearbeitet. Zuvor hatte OFFIS und im Berichtszeitraum dann das DLR seine Expertise zu dieser Thematik, welche unter anderem im Projekt Step-Up!CPS [27] gesammelt wurde, geteilt.

2 EINGEHENDE DARSTELLUNG

2.1 Verwendung der Zuwendung und erzielte Ergebnisse

In den folgenden Unterkapiteln werden die vom DLR bearbeiteten Arbeitsthemen und die erreichten Ergebnisse beschrieben. Die Arbeitsstände wurden mit dem Übergang des Bereichs Verkehr vom OFFIS an das DLR Institut Systems Engineering für zukünftige Mobilität vom OFFIS übergeben und im DLR zu Ende geführt.

2.1.1 Arbeitspaket 1

Ziel von Arbeitspaket 1 war es, die Anwendungsfälle und Demonstratoren, die lokale, eigenständige CPS verwenden, zu definieren und die Anforderungen für die Umwandlung der CPS in verteilte sicherheitskritische CPS-Lösungen über ein Device-Edge-Cloud-Kontinuum zu beschreiben.

Das DLR hat im Rahmen von Arbeitspaket 1 die Ergebnisse von OFFIS bezüglich des Vorgehensmodells zur Erhebung der technischen Anforderungen per Anwendungsfall sowie der Durchführung übernommen und als wissenschaftliche Veröffentlichung verbreitet. Um den Herausforderungen und Risiken der Erstellung und Ableitung natürlich sprachlicher Anforderungen in Technische Anforderungen zu begegnen, wurde ein Spiralmodell als einheitlicher Prozess zur Ableitung der funktionalen und nicht-funktionalen Anforderungen aus den End User Requirements (EURs) der Use Case entwickelt und etabliert. Dieses Modell verbindet die Idee der iterativen Entwicklung mit den systematischen, kontrollierten Aspekten des Wasserfallmodells. Es ist eine Kombination aus einem iterativen Entwicklungsprozessmodell und einem sequentiellen linearen Entwicklungsmodell. Es ermöglicht die inkrementelle Ableitung von Anforderungen oder inkrementelle Verfeinerungen durch jede Iteration entlang der Spirale. Im Rahmen des Liefergegenstandes D 1.3 wurde für den UC 2 eine umfassende Risikoanalyse über die Verwendung von AIS-Daten für die Routenvorhersage von Schiffen durchgeführt. Diese Analyse basiert auf den Bedrohungen, Schwachstellen und Risiken (TVR) eines Systems. Im Rahmen dieser Analyse liegt das Risiko in der alleinigen Verwendung von AIS-Daten für die Vorhersage von Schiffsrouten und einer gewissen Anfälligkeit/Unzuverlässigkeit der AIS-Daten. Aufgrund des Fehlens von Sicherheitsvorkehrungen innerhalb der AIS-Daten, wie z.B. Quality of Service (QoS), ist eine Manipulation der AIS-Daten von außen möglich. Im Rahmen der Analyse wurden 7 Gegenmaßen zur Risikominimierung vorgeschlagen. Gemeinsam mit dem UC2-Partner SNG trug das DLR zum Teilergebnis D1.4 bei, indem es eine Gefährdungsermittlung und -bewertung für Überwachungs- und Beratungsdienste sowie eine Sicherheitsrisikobewertung auf der Grundlage des Mappings von Bedrohungen und anwendbaren Schutzmaßnahmen durchführte.Zudem hat das DLR die Deliverables D1.3 und D1.4 gereviewed.

2.1.2 Arbeitspaket 2 und 5

2.1.2.1 Zielsetzung der Arbeitspakete

Ziel von Arbeitspaket 2 war der Entwurf und die Entwicklung von Architekturen und Plattformen für verteilte Lösungen, die sich durch Flexibilität bei der Bereitstellung von Anwendungen und der Verteilung von Aufgaben auszeichnen. Das Arbeitspaket hat

architektonische Herausforderungen in Bezug auf Sicherheit in verteilten Systemen gesammelt und Architekturmuster bereitgestellt, die diese Herausforderungen lösen oder erleichtern. Zudem hat AP2 auch die Mittel für die Spezifikation und simulationsbasierte Analyse der Dienste eines solchen verteilten Systems bereitgestellt.

Arbeitspaket 5 zielte auf das Design, die Implementierung, das Testen und die Integration von industriellen Demonstratoren ab, wählte V&V-Methoden für die Validierung von verteilten sicherheitskritischen CPS-Lösungen aus und führte die eigentliche Validierung der Demonstratoren durch. AP5 verband die Bemühungen der Innovations- und Entwicklungsaktivitäten mit den Bedürfnissen der Industrie durch reale Demonstratoren, die die TRANSACT-Innovationen über den Stand der Technik hinaus präsentieren. Arbeitspaket 5 fungierte als Bindeglied zwischen den Innovations- und Verwertungsaktivitäten (Arbeitspaket 6). Am Ende des Projekts wurden die Ergebnisse von industriellen Pilotanwendern validiert und im Hinblick auf die Gesamtergebnisse und Auswirkungen des Projekts bewertet.

2.1.2.2 Arbeiten des DLR

Im Rahmen des Berichtzeitraumes hat das DLR die Leitung von AP 2 übernommen und regelmäßige Meetings organisiert, um die Koordination der involvierten Tasks sicherzustellen.

Im Rahmen von Task 2.1 wurde der „Wissenschaftliche Stand“ von „Architectures for distributed safety-critical CPS solutions“ in Zusammenarbeit mit den Projektpartnern erhoben. Dieser wurde als Grundlage zur Auswahl geeigneter Architekturpattern für verteilte Systemarchitekturen mit Cloud Anbindung im weiteren Rahmen des Projektes dienen. Das DLR hat zum Deliverable D2.1 einen Beitrag über „Safe and Secure Modular Updates“ beigetragen. Für die Domänen Automotive, Maritime und Industrie 4.0 wurde der Stand der Wissenschaft und Technik hinsichtlich von Updates Over The Air (OTA) zusammengetragen. Es wurden bestehende Standards und Best Practices als auch laufende wissenschaftliche Projekte berücksichtigt.

Das DLR koordinierte die Arbeit in AP2. Für AP2 wurden monatliche Treffen organisiert, um die Arbeit zwischen den Aufgaben im Arbeitspaket zu synchronisieren. Das DLR nahm als Vertreter von AP2 an Ad-hoc-Sitzungen und Projektleitungssitzungen teil.

Das DLR organisierte die Arbeit in Task 2.2 und organisierte regelmäßige Treffen, um die Arbeit mit den beteiligten Partnern zu koordinieren. Der Schreibprozess für den Beitrag D27 (D2.2) wurde organisiert und die T&V-Methodik für die Entwicklung von SCDCPS wurde für den Beitrag ausgearbeitet.

Das DLR hat ein Konzept für die V&V des in UC2 entwickelten Beratungsdienstes und der Autorouten für Seeschiffe erarbeitet. Dieses Konzept beinhaltet die Identifizierung geeigneter Routen zur Validierung des Beratungsdienstes und der Navigationssicherheit der vorgeschlagenen Routen. Für die Identifizierung dieser Routen wurde ein Konzept ausgearbeitet, das auf der Analyse historischer AIS-Daten basiert. Diesem Konzept folgend wurden 458 Routen identifiziert, die für die simulationsbasierte Validierung des

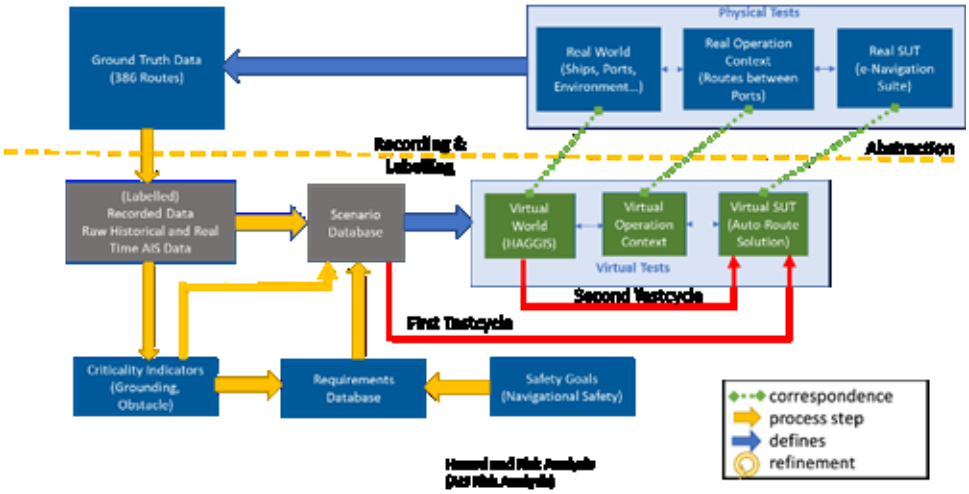
Beratungsdienstes verwendet werden können. Für den Teil dieser Routen, für den Seekarten oder ENCs verfügbar waren, wurde ein Sicherheitscheck durchgeführt, um die Navigationssicherheit in Bezug auf die Qualität der Autorouten zu überprüfen.

Außerdem wurden 159 Routen aus dem Satz von etwa 458 Routen ausgewählt und mit identischen Routen aus verschiedenen historischen AIS-Datenbanken verglichen. Ziel war es, festzustellen, ob die Autorouten relativ kurze Routen darstellen und ob sie für bestimmte Schiffe/Schiffsklassen prinzipiell befahrbar sind. Um dies zu erreichen, muss die Referenzroute von bemerkenswert hoher Qualität und Zuverlässigkeit sein. Diese Eigenschaften werden durch die Verwendung verschiedener mathematischer Modelle zur Erstellung der Referenzroute erreicht, die voneinander unabhängig sind und sich teilweise überschneiden. Darüber hinaus wurden verschiedene Modelle für dieselbe Aufgabe verwendet und ihre Ergebnisse mit den neuesten Techniken verglichen und bewertet. In einem ersten Schritt müssen die verfügbaren historischen AIS-Daten aus denjenigen Daten extrahiert werden, die für eine Route zwischen 2 Häfen relevant sind.

Die nachstehende Abbildung veranschaulicht den implementierten Rahmen für die Durchführung von V&V. Die Grundlage der Szenarien für die Durchführung dieser Aktivitäten sind die 458 Routen zwischen den weltweit verteilten Häfen der statistischen Analyse. Statistisch gesehen decken diese Routen die im Durchschnitt am häufigsten befahrenen Routen ab und bilden die Ground-Truth-Daten, die durch die bereinigten und verarbeiteten AIS-Daten untermauert wird. Die resultierenden virtuellen Routen werden zusammen mit den virtuellen Häfen und Schiffen als Szenarien in der Szenario-Datenbank gespeichert. Die folgenden Kriterien wurden als Sicherheitsziele definiert, um die Navigationssicherheit der generierten NAVTOR Auto-Routen für Schiffe zu bewerten:

- Die Route muss über den Beratungsdienst zugänglich sein und der Route zwischen den beiden angegebenen Häfen folgen.
- Die zur Herstellung der Navigationssicherheit verwendeten Blocker müssen funktionieren.
- Die Autoroute muss die jeweils vorgeschriebenen TSS enthalten und diese müssen in der richtigen Richtung geplant sein.
- Die Route muss die entsprechenden vorgeschriebenen Tiefwasserrouten enthalten, wenn der Tiefgang des Schiffes dies erfordert, und diese müssen in der richtigen Richtung geplant werden.
- Die Route des Schiffes muss den Fahrwassern in der richtigen Richtung folgen. Der Auftrieb muss gemäß den Vorschriften beachtet werden.
- Die generierte NAVTOR Autoroute sollte nicht mehr als 10% von der am häufigsten verwendeten Referenzroute für einen bestimmten Schiffstyp abweichen (Einsparung von Treibstoff und Reduzierung von CO2-Emissionen).
- Der Beratungsdienst sollte stabil und zuverlässig sein.

- Ein Ausfall des Beratungsdienstes sollte dem Benutzer deutlich angezeigt werden.



Besonders kritische Indikatoren sind das Vermeiden von Grundberührungen und der Kontakt mit Objekten wie Bojen oder Verankerungen. Unser System ermöglicht die Durchführung von zwei Testzyklen (siehe Abbildung oben): Im ersten Testzyklus wird die NAVTOR Autoroute manuell mit der Referenzroute eines bestimmten Schiffes und der am häufigsten genutzten Route zwischen den beiden jeweiligen Häfen verglichen. Dieser Vergleich erfordert die Verfügbarkeit von aktuellen Papierseekarten oder ENCs. Der Hauptzweck dieses Testzyklus besteht darin, die Anforderungen zu verifizieren. Im zweiten Testzyklus wird die maritime Simulation HAGGIS des Deutschen Zentrums für Luft- und Raumfahrt verwendet, um die generierten NAVTOR Autorouten zu validieren. Die virtuelle Co-Simulationsinfrastruktur von HAGGIS umfasst KI-basierte Umwelt-, Verkehrs- und Schiffssimulatoren. Diese werden verwendet, um die Risiken, die Effizienz und die Navigationssicherheit der Autorouten für Schiffe während der Produktentwicklung zu bewerten.

In Task 2.2 wurde außerdem die Simulationsumgebung HAGGIS erweitert, um eine Sicherheitsüberprüfung für eine simulierte Strecke durchführen zu können. Zu diesem Zweck hat das DLR ein Konzept zur Durchführung einer Sicherheitsprüfung in HAGGIS entwickelt, das derzeit umgesetzt wird. Die Sicherheitsprüfung beinhaltet unter anderem die Überprüfung der Tiefeninformationen der befahrenen Route in Bezug auf den Tiefgang des Schiffes.

In Arbeitspaket 5 hat das DLR die Simulationsaktivitäten in UC2 vorbereitet, indem es die maritime Simulationsumgebung HAGGIS eingerichtet hat. Die technischen Details des Zugriffs auf den Beratungsdienst von NAVTOR wurden diskutiert und vereinbart.

Da die Erweiterungen an der HAGGIS-Simulation noch nicht vollständig abgeschlossen sind, wurden sowohl die Generierung der beiden Referenzrouten als auch ihr Vergleich mit der NAVTOR-Autoroute manuell durchgeführt. Die bisher erzielten Ergebnisse sind:

1. die Berechnung der NAVTOR Autoroute ist stabil. Änderungen können sich aufgrund von ENC-Aktualisierungen ergeben.

2. die Blocker, die zur Herstellung der Navigationssicherheit verwendet wurden, funktionieren einwandfrei.
3. mit den gesetzten Blockern wird der Zielhafen erreicht.
4. auch bei der Verwendung mehrerer Blocker wird der Zielhafen erreicht.
5. der Anpassungsaufwand für die bordeigene Navigation in vielen Fällen > 70% ist, als wenn die Route manuell mit einer NavStation oder anderen Navigationsgeräten geplant werden müsste.
6. einige der berechneten NAVTOR Autorouten sind länger als die am häufigsten befahrene Referenz-Route zwischen den beiden angegebenen Häfen. Die Entfernungsunterschiede bei großen Entfernungen (10.000 nm) sind jedoch sehr gering. Diese Referenzroute enthält Schiffe mit geringerem Tiefgang. Dies zieht die am häufigsten befahrene Referenzroute näher an die Küsten heran. Teile der Referenzroute sind für das angegebene Schiff unsicher.
7. die meisten NAVTOR Autorouten sind kürzer als die Referenz-Route des angegebenen Schiffes zwischen den beiden Häfen.
8. insgesamt macht NAVTOR Autoroute trotz fehlender Wetterinformationen in den durchgeführten Tests einen sehr guten, effizienten Eindruck und ist geeignet, den Kraftstoffverbrauch und den CO2-Ausstoß zu reduzieren. Die Wetterinformationen wurden zwischenzeitlich in das Framework integriert.

In sehr seltenen Fällen kann die NAVTOR Autoroute aus navigatorischer Sicht optimiert werden, um die bestehende Route zu verkürzen und so den Treibstoffverbrauch und die CO2-Emissionen des Schiffes zu reduzieren. Zu diesem Zweck hat das DLR konkret spezifizierte Routen mit Wegpunkten, Kursen, etc. erstellt und NAVTOR vorgeschlagen.

Was die Bewertung des abnormalen Verhaltens von Schiffen betrifft, so wurden 10 Dateien, die vom Partner Simula generiert wurden, analysiert und bewertet. Zur Durchführung dieser Bewertung wurde ein spezieller Bewertungskatalog mit 13 Kriterien entwickelt und dem Partner zur Verfügung gestellt.

Außerdem hat das DLR einen Beitrag zum Ergebnis D5.4 UC2 Demonstrator geleistet, indem es eine Beschreibung der durchgeführten Risikobewertungen lieferte.

2.1.3 Arbeitspaket 2 und 3

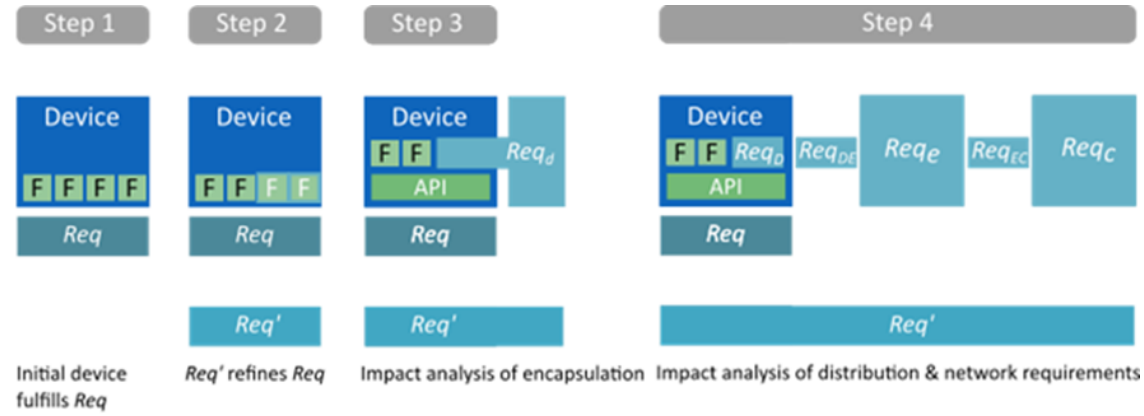
Ziel von AP3 war die Entwicklung von Konzepten und Lösungen, die sicherstellen, dass verteilte sicherheitskritische CPS-Systeme über die notwendigen Mittel verfügen, um sicher, leistungsfähig und unter Wahrung der Privatsphäre zu arbeiten und gleichzeitig von Edge- und Cloud-Diensten zu profitieren. Auf der Grundlage der in AP1 ermittelten Anforderungen wurden diese Konzepte und Lösungen entwickelt und mit der in AP2 unter Beteiligung des DLRs entwickelten TRANSACT-Referenzarchitek-

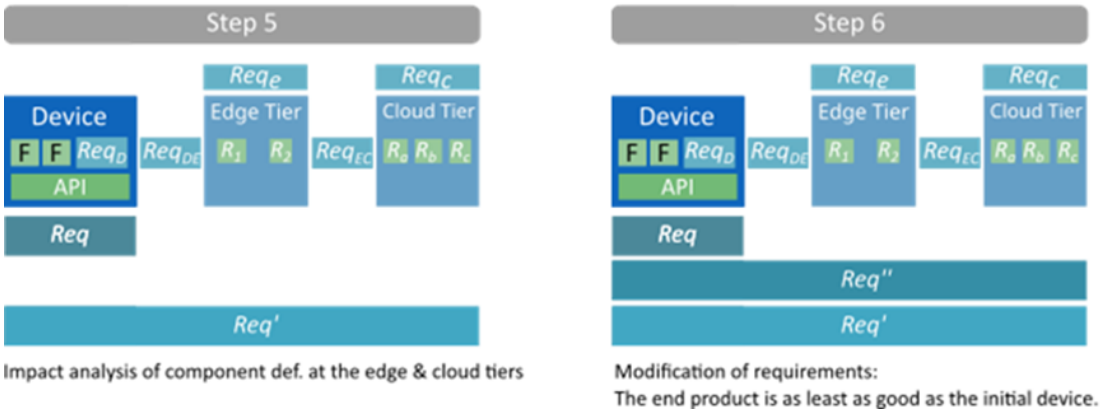
tur abgeglichen. Die Spannungen und Wechselwirkungen zwischen Konzepten und Lösungen für Sicherheit und Leistung und Sicherheit und Datenschutz werden ebenfalls ermittelt.

Das DLR hat das Deliverable D3.3 gereviewed.

Das DLR arbeitete an einer Methodik für die Umwandlung eigenständiger Systeme in das Device-Edge-Cloud-Kontinuum (Transition & Validation Methodology). Die Methodik zielt darauf ab, die Herausforderungen zu bewältigen, die sich aus den Auswirkungen dieser Transformation auf die Anforderungen des Systems ergeben. Das vertragsbasierte Design wird als Grundlage verwendet, um die Systemanforderungen zu formulieren und die schrittweise Verfeinerung des Systems während der Transformation zu unterstützen. Die ersten Ergebnisse dieser Methodik wurden im Kontext des maritimen Anwendungsfalls (UC2) angewandt.

Das DLR hat diese Transition & Validation Methodology für den Entwurf und die V&V von SCDCPS definiert , um die Integration der einzelnen von den Partnern entwickelten Methoden in ein gemeinsames Konzept für die simulationsbasierte Analyse von sicherheitskritischen verteilten CPS-Lösungen voranzutreiben.





Die in der obigen Abbildung skizzierte T&V-Methodik wurde als Rahmen formuliert, in den alle einzelnen V&V-Lösungen integriert werden können, wenn ein SCCPS in ein SCDCPS umgewandelt wird.

2.1.4 Arbeitspaket 4

Es waren keine Arbeiten in diesem Arbeitspakt geplant.

2.1.5 Arbeitspaket 6

Der Zweck von AP6 ist es, eine reibungslose Projektdurchführung und eine angemessene Nutzung und Verbreitung der Projektergebnisse zu gewährleisten, vor allem durch den Aufbau einer Open-Source-Community.

Das DLR hat die Pläne für die Verbreitung, Nutzung und Standardisierung angepasst und verfolgt. Das DLR leitete AP2 und organisiert die Arbeit in diesem Arbeitspaket. Das DLR hat den Beitrag D3.3 überprüft.

Während des Berichtszeitraums hat das DLR drei Publikationen eingereicht, wobei zwei Publikationen bereits veröffentlicht sind und die dritte im Dezember 24 veröffentlicht werden soll. Das DLR nahm an der HIPEAC 2023 und 2024 Konferenz teil. 2023 wurde dort eine Präsentation zum Thema "User-driven Requirements Engineering - Challenges and possible solutions in natural language derivations" abgehalten und 2024 ein Vortrag zum Thema „A methodology for transforming a local safety-critical cyber-physical system into a distributed safety-critical solution” gehalten.

2.2 Zahlenmäßiger Nachweis

Der zahlenmäßige Nachweis wird in einem separaten Dokument zur Verfügung gestellt.

2.3 Notwendigkeit der Zuwendung

Die Ziele von TRANSACT, insbesondere die erreichten Ergebnisse, wären ohne ein Konsortium wie in TRANSACT gebildet nicht vorstellbar. Erst durch das Projekt ergab sich die Möglichkeit, mit einer Vielzahl von Forschungs- und Industriepartnern zusammenzuarbeiten, die durch gemeinsame Ziele verbunden und offen waren, in verschiedenen Teams und an verschiedenen Fragestellungen zusammenzuarbeiten. TRANSACT hat dadurch den Rahmen geschaffen, der es ermöglichte, sich zur Entwicklung von Lösungen zusammenzufinden.

Durch eine enge Zusammenarbeit mit NAVTOR einem führenden Unternehmen für die Entwicklung von e-Navigationslösungen war es möglich konkrete Anforderungen für den im Projekt vorhandenen maritimen Anwendungsfall zu erheben. Diese Anforderungen bilden die Grundlage für den im Projekt zu erarbeitenden Architekturentwurf einer Plattform, welche die Auslagerung von Cloud Funktionalitäten sicherheitskritischer Anwendungen ermöglicht hat. Die während TRANSACT entwickelte Autorouten Funktion ist als Produktivsystem marktverfügbar und in der Nutzung.

Das Projekt TRANSACT hat eine besondere Bedeutung für die weitere Stärkung von Schlüsselindustrien in Deutschland und Europa im Rahmen der fortschreitenden Vernetzung, steigenden Komplexität und flexiblen Anpassung von technischen Systemen. Die Projektergebnisse werden in verschiedenen Fallstudien aus den Domänen: Automotive Systeme, Maritime Systeme, Medizintechnik und Automatisierungssysteme angewendet und validiert.

Bei dem Projekt handelt es sich um ein technologieübergreifendes, anwendungsbezogenes und risikoreiches industrielles Forschungs- und vorwettbewerbliches Entwicklungsvorhaben („high risk/high gain“ Projekt) mit hoher gesellschaftlicher Relevanz. Dieses Risiko kann von den beteiligten Unternehmen nicht ohne eine staatliche Förderung getragen werden.

2.4 Voraussichtlicher Nutzen, insbesondere Verwertbarkeit der Ergebnisse

Da der in TRANSACT involvierte Bereich Verkehr des OFFIS vollständig in das DLR Institut Systems Engineering für zukünftige Mobilität übergegangen ist, findet die Verwertung ausschließlich dort statt. Es wurden durch OFFIS und später das DLR vier wesentliche Ergebnisse produziert: 1. Vorgehensmodel zur Anforderungserhebung und Anwendung dieses auf den UC2, 2. TRANSACT Referenzarchitektur, 3. V&V Vorgehen, und 4. Transition & Validation Methodik.

Diese Ergebnisse werden vom DLR Institut Systems Engineering langfristig über die Forschungsplattformen gepflegt und bereitstellt. Darüber wird eine nachhalte Weiterentwicklung und Nutzung sichergestellt. Überdies werden die Ergebnisse darüber auch in zukünftige Forschungs-, Beratungs- und Entwicklungsdienstleistungen für industrielle Kunden eingebracht.

Auch sollen die gewonnenen Forschungsergebnisse in Lehrveranstaltungen eingebettet werden, die an der Carl von Ossietzky Universität Oldenburg angeboten und durch das DLR Institut Systems Engineering für zukünftige Mobilität unterstützt werden. Die in TRANSACT erzielten Forschungsergebnisse hinsichtlich Design und Bewertung von sicherheitskritischen Systemen mit Funktionen in der Cloud/Edge sind zukunftsweisende Themen, die in diese Vorlesungen eingebettet werden sollen.

2.5 Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Die im Verlauf des Projekts erzielten Ergebnisse Dritter auf dem Gebiet des Vorhabens wurden durch das Konsortium im Rahmen der Recherche zum wissenschaftlich-technischen Stand im Rahmen der Arbeiten am Deliverable D2.1 erfasst und dokumentiert. Es sind dabei keine Arbeiten identifiziert worden, welche eine Änderung der Zielsetzung hätten notwendig gemacht.

2.6 Veröffentlichungen

Innerhalb des Berichtszeitraumes wurden die folgenden wissenschaftlichen Publikationen oder Dissemination-Aktivitäten auf Konferenzen, Workshops und anderen öffentlichen Events durchgeführt:

Titel	Autoren	Typ	Herausgeber	Jahr	DOI/ISSN
Application of a Simulation-Based V&V Approach to Automatic Voyage Planning	Arnold Akkermann und Bjorn Age Hjollo	Paper	10th International Conference on Artificial Intelligence & Applications (ARIA 2023)	2023	DOI: 10.5121/csit.2023.131909
A methodology for transforming a local safety-critical cyber-physical system into a distributed safety-critical solution	Oborzynski, Krzysztof und Rakow, Astrid	Vortrag	EUCloud-EdgeIoT.eu initiative	2024	

Titel	Autoren	Typ	Herausgeber	Jahr	DOI/ISSN
A methodology for transforming a local safety-critical cyber-physical system into a distributed safety-critical solution	Oborzyski, Krzysztof und Rakow, Astrid	Vortrag	ENHANCE Workshop. Enabling Technologies and Dependability in Cyber Physical Systems, workshop associated with HiPEAC	2024	
User-driven requirements engineering - challenges and possible solutions in natural language derivations	Akkermann	Vortrag	HiPEAC	2023	
User-driven requirements engineering - challenges and possible solutions in natural language derivations	Arnold Akkermann und Bjorn Age Hjollo	Paper	TechRxiv	2023	DOI: 10.36227/techrxiv.22093874.v1
Scenario based Verification and Validation of Automated driving Vessel	Arnold Akkermann	Paper	WSC 24	2024	ACM and IEEE digital libraries

Anhang A. Liste aller TRANSACT Partner

Partnername	Abkür-zung	
Philips Medical Systems B.V.	PMS	NL
FEops NV	FEops	BE
Technische Universität Eindhoven	TUE	NL
TNO-ESI	TNO	NL
PS-Tech BV	PST	NL
Philips GmbH	PFLH	DE
AVL Software and Functions GmbH	AVL	DE
Eclipse Foundation Europe GmbH	ECL	DE
Technische Universität Graz	TUG	AT
DAC Spolka Akcyjna	DAC	PL
Politechnika Gdanska	GUT	PL
CISC Semiconductor GmbH	CISC	AT
Denso Automotive Deutschland GmbH	DENSO	DE
Fraunhofer IESE	IESE	DE
Depuración de Aguas del Mediterráneo	DAM	ES
Instituto Tecnologico de Informatica	ITI	ES
NUNSYS S.L.	NUN	ES
Kumori Systems	KUM	ES
Singlar Innovation S.L.	SNG	ES
Fundació per a la Universitat Oberta de Catalunya	UOC	ES
NAVTOR AS	NVT	NO
OFFIS E.V.	OFFIS	DE
Simula Research Laboratory AS	SRL	NO
DLR Institute	DLR	DE
Fleetonomy.ai Oy	FLEET	FI
Teknologian tutkimuskeskus VTT Oy	VTT	FI
Nodeon Finland Oy	NOD	FI
F-Secure	FSC	FI
Vinotion BV	VIN	NL
Danmarks Tekniske Universitet	DTU	DK
Toitware ApS	TW	DK

Referenzen

[1] S. Taherizadeh, V. Stankovski und M. Grobelnik, „A capillary computing architecture for dynamic internet of things: Orchestration of microservices from edge devices to fog and cloud providers.," *Sensors*, 2018.

[2] S. K. Datta, C. Bonnet und J. Haerri, „Fog computing architecture to enable consumer centric internet of things services.," *International Symposium on Consumer Electronics (ISCE) . IEEE*, pp. (pp. 1-2).

[3] C. C. Byers, „Architectural imperatives for fog computing: Use cases, requirements, and architectural techniques for fog-enabled iot networks.," *IEEE Communications Magazine*, pp. 14-20, 2017.

[4] J. Gubbi, S. M. R. Buyya und M. Palaniswami, „Internet of things (IoT): a vision, architectural elements, and future directions," *Future Generation Computer Systems, vol. 29, no. 7*, p. pp. 1645–1660, 2013.

[5] „AWS Internet of Things," [Online]. Available: http://aws.amazon.com/iot.

[6] „Azure IoT Suite - IoT Cloud Solution," [Online]. Available: http://www.microsoft.com/en-us/internet-of-things/azure-iot-suite.

[7] „Google IoT Core," [Online]. Available: http://cloud.google.com/iot-core.

[8] D. Broman, E. Lee, T. S und T. M., „Viewpoints, formalisms, languages, and tools for cyber-physical systems.," *Proceedings of the 6th International Workshop on Multi-Paradigm Modeling*, 2012.

[9] P. Hehenberger, B. Vogel-Heuser, D. Bradley, B. Eynard, T. Tomiyama und S. Achiche, „Design,modelling, simulation and integration of cyber physical systems.," *J Comput Ind.*, pp. 273-289, 2016.

[10] M. Zeller und M. Prehofer, „Timing constraints for runtime adaptation in real-time, networked embedded systems.," *7th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS). IEEE*, pp. (pp. 73-82), 2012.

[11] E. Geisberger und B. M., „agendaCPS - Integrierte Forschungsagenda Cyber-Physical Systems (acatech STUDIE)",," Deutsche Akademie der Technikwissenschaften, 2012.

[12] P. Oliveira Antonino, J. Jahic, B. Kallweit, A. Morgenstern und T. Kuhn, „Bridging the Gap between Architecture Specifications and Simulation Models.," in *International Conference on Software Architecture (ICSA) Companion*, 2018.

[13] A. Armoush, „Design patterns for safety-critical embedded systems, Ph.D. dissertation, Aachen University," 2010.

[14] T. Bijlsma und T. Hendriks, „ A fail-operational truck platooning architecture.," in *2017 IEEE Intelligent Vehicles Symposium (pp. 1819-1826). IEEE*, 2017.

[15] M. Jakovljevic, C. C. Insaurralde und A. Ademaj, „ Embedded cloud computing for critical systems.," in *2014 IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC) (pp. 4A5-1). IEEE.*, 2014.

[16] K. D. Foster, J. J. Shea, J. B. O. T. W. Michael, L. Peitso und M. T. Shing, „Cloud computing for large-scale weapon systems.," in *2010 IEEE International Conference on Granular Computing (pp. 161-166). IEEE.*, 2010.

[17] K. D. Foster, J. J. Shea, J. B. Michael, T. W. Otani, L. Peitso und M. T. Shing, „ Cloud computing for large-scale weapon systems.," in *2010 IEEE International Conference on Granular Computing (pp. 161-166). IEEE.*, 2010.

[18] O. Cassetto, „How UEBA Overcomes 5 Hurdles to Achieving Effective Security and Incident Response.," [Online]. Available: https://www.exabeam.com/ueba/ueba-incident-response/. [Zugriff am 2018].

[19] J. Kuusijärvi, R. Savola, P. Savolainen und A. Evesti, „Mitigating IoT Security threats With a Trusted Network Element.," in *Proceedings of the 11th International Conference for Internet Technology and Secured Transactions (ICITST)*.

[20] A. Al-Hasnawi, I. Mohammed und A. Al-Gburi, „Performance Evaluation of the Policy Enforcement Fog Module for Protecting Privacy of IoT Data," in *IEEE International Conference on Electro/Information Technology (EIT)*, 2018.

[21] A. Giaretta, N. Dragoni und F. Massacci, „Protecting the Internet of Things with Security-by-Contract and Fog Computing," in *IEEE 5th World Forum on Internet of Things (WF-IoT 2019)*, 2019.

[22] „Siliconangle," [Online]. Available: https://siliconangle.com/2019/07/28/hardware-still-matters-era-cloud-computing/.

[23] M. Brettel, n. Friederichsen, M. Keller und M. Rosenberg, „How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective,," in *International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering Vol:8, No:1*, 2014.

[24] A. Model.CONNECT. [Online]. Available: https://www.avl.com/-/model-connect-.

[25] H. Van Houten, „Five ways in which healthcare innovation has changed over the past 15 years,“ https://www.linkedin.com/pulse/five-ways-which-healthcare-innovation-has-changed-over-van-houten/.

[26] A. I. Association, „Embedded Intelligence: Trends & Challenges book release.,“ https://artemis-ia.eu/news/embedded-intelligence-trends-challenges-book-release.html., 2019.

[27] Step-Up!CPS, „Step-UP!CPS,“ 15 12 2021. [Online]. Available: https://stepup-cps.de/.

[28] W. Zhou, Y. Jia, A. Peng, Y. Zhang und P. Liu, „The Effect of IoT New Features on Security and Privacy: New Threats,ExistingSolutions,andChallengesYettoBeSolved.,“ in *IEEEInternetThings*, 2019.