Schlussbericht

zum Teilvorhaben **ContainIT EADS**

(Entwurf einer vernetzten standardisierten IKT Architektur sowie Entwurf von Konzepten / Methoden zur Optimierung der physischen Sicherheit und des integrierten Risikomanagements)

im Rahmen der

Bekanntmachung des BMBF zur **Sicherung der Warenketten**

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

im Verbundvorhaben **ContainIT**

(Containersicherheit durch vernetzte IT-Systeme)

Zuwendungsempfänger	EADS Deutschland GmbH, EADS Innovation Works Germany
Förderkennzeichen	13N11006
Teilvorhabensbezeichnung	ContainIT EADS - Entwurf einer vernetzten standardisierten IKT Architektur sowie Entwurf von Konzepten / Methoden zur Optimierung der physischen Sicherheit und des integrierten Risikomanagements
Schlagwörter	Container, Sicherheit, Informations- und Kommunikations-Technologie (IKT), Risiko-Profiling, Risiko-Management, Multi-Layer-Ansatz, tri-modale Logistik, Telematik
Laufzeit des Vorhabens	01.08.2010 – 31.12.2012
Berichtszeitraum	01.08.2010 – 31.12.2012
Ausgabedatum	30.08.2013
Dateiname	ContainIT_EADS_BMBF_FKZ-13N11006_Schlussbericht_V1.docx
Status	Endversion
Vertraulichkeit	nicht vertraulich

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bedeutung
AIS	Automatic Identification System
ASP	Application Service Provider
ATLAS	Automatisiertes Tarif- und Lokales Zoll-Abwicklungs-System
BAFA	Bundesamt für Ausfuhrkontrolle
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BKA	Bundeskriminalamt
BPMN	Business Process Modelling Notation
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
EADS	European Aeronautic Defence and Space Company
EADS IW	EADS Innovation Works
EDI	Electronic Data Exchange
EU	European Union; Europäische Union
EC	European Commission, Europäische Kommission
EMEA	Europe Middle East and Africa
ESP	Elektronisches-Stabilitäts-Programm
FPGA	Field Programmable Gate Array
FSR	Freight Security Requirements der TAPA
GefPot	Gefährdungspotentiale
GESA	German European Security Association
GPO	German Port Order
HW	Hardware
ID	Identification Number
IKT	Informations- und Kommunikations- Technologie
Incoterms 2000	International Commercial TERMS 2000
IMO	International Maritime Organisation
ISO	International Standardisation Organisation
ISPC	Institute for the Protection and Security of the Citizen; ein Institut am JRC
ISPS Code	International Ship and Port Facility Security Code
JRC	Joint Research Centre of the European Commission
LKA	Landeskriminalamt
LKW	Lastkraftwagen
OBU	On-Bord-Unit
OLAF	Office de Lutte Anti-Fraude; Antibetrugsbehörde der EU
RAND	Research ANd Development
SCOR	Supply-Chain-Reference-Operations Model
SMS	Short Message Service
SSCC	Serial Shipping Container Code
STORM	Secure Transportation Operations Reference Model
SW	Software
TAPA EMEA	Transported Asset Protection Association, Section for Europe, Middle East and Africa

TEU	Twenty Foot Equivalent Unit; Standardcontainer mit 20 Fuss Länge
TACSS	Tapa Air Cargo Security Standards der TAPA
THW	Technisches Hilfswerk
TSR	Truck Security Requirements der TAPA
UN	United Nations
UN/EDDIFACT	United Nations Electronic Data Interchange For Administration, Commerce and Transport
USA	United States of America
VBA	Visual Basic Application
VHDL	Very high speed integrated circuit Hardware Description Language
VTS	Vessel Traffic System
WCO	World Customs Organisation; Welt-Zoll-Organisation
XML	eXtensible Markup Language
ZKA	Zollkriminalamt

1 Kurze Darstellung

1.1 Aufgabenstellung

Im Zuge der Globalisierung hat sich der Warenhandel ebenso zu einem weltweiten agierenden System entwickelt. Hiervon ist nicht nur der eigentliche Warentransport, sondern auch der entsprechende Informations- und Datenaustausch betroffen. Für den Informations- und Datenaustausch hat sich ein komplexes internationales Netzwerk entwickelt, über den die Akteure den weltweiten Warenhandel abwickeln.

Aufgrund des stetig steigenden internationalen Handelsvolumens sind mittlerweile nicht nur die agierenden Unternehmen sondern auch die einzelnen Volkswirtschaften abhängig von funktionierenden Warenketten, um die Versorgung der Bevölkerung mit Gütern zu gewährleisten. Doch auch der Export von Waren, vor allem für Deutschland als größte Exportnation, sind funktionierende Warenketten lebensnotwendig für die Wirtschaft.

Der Großteil dieses weltweiten Warenhandels wird mittels Containern abgewickelt, welche mit Containerschiffen über weite Strecken auf See transportiert werden, als auch per Bahn, LKW oder Binnenschiffen im Zuliefer- bzw. Verteilerverkehr bewegt werden.

Das Ziel des Gesamtvorhabens ist die Entwicklung eines IKT-basierten Multi-Layer-Ansatzes (IKT = Informations- und Kommunikations- Technologie) zur Steigerung der Sicherheit im Bereich der Logistik von Containertransporten, von der Gestellung und Beladung bis zur Entladung und Ablieferung des leeren Containers im Depot. Der Multi-Layer-Ansatz deckt hier alle drei Teilbereiche der Logistikkette ab, d.h. einerseits die physische Handhabung der Container über den Umgang mit den Container begleitenden Dokumenten bis hin zum IKT-basierten Datenaustausch entlang der Logistikkette.

Hierzu sind einzelnen heute existenten IKT Inseln für übergreifendes Risiko-Profiling zu vernetzen, d.h. für ein sicherheitstechnisches Evaluieren aller verfügbaren Daten und gleichzeitig der Schutz der vernetzten IKT Systeme gegen das Eindringen, Manipulieren oder Stören.

Basierend auf einer solchen vernetzten und geschützten IKT Architektur wird es möglich sein, alle verfügbaren Einzelinformationen übergreifend durch ein Risiko-Profiling auszuwerten und zu klassifizieren als auch mittels einem entsprechenden Risikomanagement für auftretende Ausnahmesituationen sofort entsprechende Handlungsmaßnahmen einzuleiten.

Im Teilvorhaben ContainIT-EADS der EADS gibt es zwei wesentliche Hauptziele, welche wesentliche Elemente im Verbundvorhaben ContainIT darstellen:

- Erweiterung bestehender IKT (Teil-) Architekturen bzw. der Entwurf eines standardisierten IKT Architekturmodells für einer lückenlose IKT Gesamtarchitektur in Verbindung mit einem generisches Datenmodell zum Datenaustausch innerhalb der gesamten Transportkette.

und

- Entwurf von Konzepten bzw. Methoden zur Optimierung der physischen Sicherheit als auch für ein für ein integriertes Risikomanagement z.B. durch Risiko-Profiling von Containertransporten.

Die Konzeption einer standardisierten IKT Architektur in Verbindung mit einem generischen Datenmodell bildet die Grundlage einer zukünftigen Vernetzung der derzeit existenten IKT Systeme der Akteure.

Basierend auf der Vernetzung IKT Systeme können die wesentlichen Einzeldaten der Akteure wie z.B. die Transportdokumente, die Zustandsdaten eines Containers oder eines Transportmittels (Schiff, LKW oder Bahn) zentral zur Verfügung gestellt werden.

Mittels der Konzepte und Methoden zur Optimierung der physischen Sicherheit können diese zentral erfassten Daten zusammenhängend und übergeordnet durch z.B. spezielle Risiko-Profiling Algorithmen analysiert und bewertet und für das nachfolgende Risikomanagement aufbereitet und weiterverarbeitet werden, wie z.B. zur Intervention von Sicherheitskräften oder zur Alarmierung von Behörden genutzt werden.

1.2 Voraussetzungen

Bei der Containerlogistik handelt es sich um ein komplexes Gebilde, in dem die Akteure geographisch Global verteilt und prozesstechnisch miteinander vernetzt sind. Für einzelne Akteure ist es somit nahezu unmöglich systemrelevante Änderungen alleine entscheidend zu beeinflussen oder gar zu steuern. Somit ist es notwendig die relevanten Akteure der Prozesskette, Software- und Systemanbieter zur Containerlogistik, Forschungseinrichtungen, Nutzervereinigungen sowie Behörden und in einem entsprechenden Konsortium zu vereinen um die Problematik zu diskutieren, analysieren und Konzepte für richtungweisende Neuerung zu entwickeln bzw. um solche Konzepte auch im Markt einzuführen.

Es ist gelungen ein entsprechendes Konsortium mit maßgeblichen Konzerne und marktführenden mittelständischen Firmen, die zum Teil im direkten Wettbewerb miteinander stehen, sowie Forschungsinstitutionen, Nutzer, Behörden und Standardisierungsorganisationen/Dachverbände auf nationaler, europäischer und globaler Ebene zusammenzuschließen, um gemeinsam innovative IKT-basierte Sicherheitslösungen im Logistikbereich zu entwerfen und im Rahmen von neuen Standards und Regulierungen die Marktvoraussetzungen für den wirtschaftlichen Erfolg zu schaffen:

Die DAKOSY AG und dbh Logistics AG vertreten die beiden mit Abstand größten deutschen Seehäfen Hamburg und Bremen/Bremerhaven und bilden mit deren Hafenkommunikationssystemen sowie anderen Softwarelösungen wie z.B. für die komplette Zollabwicklung deren IKT Plattform.

EADS Astrium und Bosch Sicherheitssysteme sind technologisch führende Systemanbieter für Containertelematiksysteme für z.B. sensorbasierte Containerüberwachung inklusive Tracking und Tracing Funktionalitäten für Container.

Die Funkwerk Eurotelematik ist ein führender Hersteller und Betreiber von Telematiksystemen für LKW-Flotten.

Mit SAPPER ist ein europaweit führender Hersteller und Betreiber einer Softwarelösung für Compliance-Prüfung und Risiko-Profiling im Projekt vertreten.

Aus dem Bereich der Universitäts-, Instituts- und Industrieforschung sind die Technische Universität Hamburg-Harburg für IT-Sicherheit, die Technische Hochschule Wildau für die Logistikprozesskette, das Fraunhofer Institut SIT aus Darmstadt für System- und Kommunikationssicherheit sowie EADS Innovation Works als industrieller Forschungspartner von EADS Astrium für Kommunikationstechnologie und Risiko-Profiling.

Weiter hat EADS Innovation Works (EADS IW) die Rolle der Konsortialführung von ContainIT übernommen.

Zur Komplettierung des Expertenwissens des Konsortiums wurden assoziierte Partner in das Projekt mit Partner eingebunden als auch während des Projektverlaufs Experten aus der realen Wirtschaft sowie Behörden in Form von Interviews und Workshops integriert, auf welche später in Kapitel 1.5 nochmals eingegangen wird.

Im Rahmen der der BMBF Bekanntmachung „Sicherung der Warenketten“ sind das Vorhaben ContainIT mit dem zuvor dargestellten Konsortium als auch das Teilvorhaben ContainIT EADS am 1. August 2010 gestartet und hatten 29 Monate Laufzeit (inklusive kostenneutraler Verlängerung von 5 Monaten) bis zum 31. Dezember 2012.

Entsprechend der BMBF Bekanntmachung „Sicherung der Warenketten“ stehen das Gesamtvorhaben ContainIT insbesondere aber das Teilvorhaben ContainIT EADS thematisch im Fokus der Untersuchung und Entwicklung von Konzepten und Methoden um die Störung bzw. den Ausfall des Warentransports und somit den Einfluss auf die Sicherheit als auch der Versorgungssicherheit auf die Bevölkerung zu minimieren bzw. zu verhindern.

Die Projektziele sind direkt ausgerichtet auf Prävention und Früherkennung von Gefahrensituationen welche sich durch einen Missbrauch der Warenkette des Containertransports für kriminelle oder terroristische Zwecke als auch durch Sabotage zu einem Sicherheitsrisiko der Bevölkerung entwickeln könnten.

Wie auch schon im Jahre 2003 von Experten in der RAND[1] Studie festgestellt haben, gibt es erhebliche Sicherheitsdefizite im globalen Seecontainer Schifffahrtssystem. Hierbei wurden insbesondere die Gefährdung durch terroristische Aktionen, die Mängel an Transparenz, Verfolgbarkeit, Verfügbarkeit sicherheitsrelevanter Daten oder die fehlende Standardisierung genannt.

Zu Beginn des Vorhabens kann die Lage im Umfeld der Containertransporte wie folgt zusammengefasst werden:

Die allgemeine Gefahrenlage für Containertransporte lässt sich u.a. an den folgenden Punkten ableiten, d.h. die stetig wachsende Anzahl an Containertransporten von ca. 500 Millionen TEU (Twenty Foot Equivalent Unit) im Jahre 2010[2] und der vorhandenen komplexen Netzwerke der beteiligten Akteure bringen direkt und indirekt unzählige Abhängigkeiten und Sicherheitsrisiken mit sich. Weiter gibt es eine seitens der USA getriebene Sicherheitsinitiative der mit Forderung eines 100% (d.h. jeder Container) bildgebenden Röntgen-Scanning von Containern mit Ziel USA bis Anfangs 2013, dann ausgesetzt bis 2015. Dieses Scanning bringt eine große zeitliche, technologische und finanzielle Herausforderung mit sich, welche zu Lasten der Versender-Staaten wie z.B. Deutschland, als der größte Versender aus dem EU-Raum in die USA, gehen. In ContainIT hat somit der Schutz der Warenketten unter Berücksichtigung deutscher Wirtschaftsinteressen eine besondere Bedeutung.

Als übergeordnete Ziele des Vorhabens ContainIT können somit folgende Punkte aufgezeigt werden:

- Die Prävention und Früherkennung von Gefahrensituationen durch ein umfassendes Risiko Profiling unter Einbezug der bereits jetzt bei den Akteuren vorhandenen Informationen.
- Der Schutz der Lieferketten vor terroristischen und kriminellen Bedrohungen, durch Früherkennung von Gefahrensituationen und entsprechend rechtzeitiger Intervention.
- Die Reduktion des geforderten 100% Container-Scanning durch das Risiko-Profiling auf möglichst ausschließlich als verdächtig eingestufte Container (sowie z.B. stichprobenweise Untersuchungen wie bisher).

Aufgrund der damals stattfindenden europäischen und transatlantischen Diskussionen sahen die deutschen Bedarfsträger und Sicherheitsanbieter die Notwendigkeit sich umgehend aufzustellen, um sich im sowohl europäischen als auch im internationalen Wettbewerb optimal positioniert zu sehen. Aus diesem Grunde wurde im Vorhaben ContainIT eine Laufzeit von ursprünglich 24 Monaten vorgesehen.

1.3 Planung und Ablauf des Vorhabens

Die Idee zum Vorhaben ContainIT entstammt EADS Innovation Works.

Während der Planungsphase für die Projektskizze war die Bildung des bereits beschriebenen Konsortiums einer der wesentlichen Arbeitsschritte als Fundament für ein erfolgreiches Forschungsprojekt.

Die Koordination als auch die Anfertigung von Projektskizze und Gesamtvorhabensbeschreibung wurden von EADS Innovation Works mit Unterstützung des Konsortiums durchgeführt.

Im Zeitraum zwischen Bewilligung des Vorhabens durch den Fördergeber und dem ersten Projekttreffen, dem KickOff-Meeting, wurde ein Kooperationsvertrag (Konsortialvertrag) zwischen den allen Partnern des Konsortiums vereinbar, welcher die vertragliche Grundlage zur Zusammenarbeit im zwischen den Partnern während des Vorhabens dienst. Es sind u.a. Punkte wie die offene Zusammenarbeit zwischen den Partnern, der Umgang mit vertraulichen Informationen oder der Umgang mit bestehenden als auch neuen Schutzrechten geregelt. Er bildet das wesentliche Fundament für die Zusammenarbeit der Partner im Vorhaben ContainIT.

[1] Quelle: RAND – „Research ANd Development“, eine gemeinnützige Institution zur Politikverbesserung und Entscheidungsfindung durch Forschung und Analyse

[2] Quelle: Drewry Shipping Consultants (2011)

Die Abbildung 1 zeigt Zeitplan mit den drei Hauptarbeitspaketen sowie deren Unterarbeitspaketen inklusive der Meilensteine des Projektträgers zum Übergabezeitpunkt (halbe Projektlaufzeit) sowie ein Abbruchmeilenstein (evtl. notwendiger vorzeitiger Stopp des Vorhabens seitens des Fördergebers).

		1. Aug. 2010	1. Sep. 2010	1. Okt. 2010	1. Nov. 2010	1. Dez. 2010	1. Jan. 2011	1. Feb. 2011	1. Mrz. 2011	1. Apr. 2011	1. Mai. 2011	1. Jun. 2011	1. Jul. 2011	1. Aug. 2011	1. Sep. 2011	1. Okt. 2011	1. Nov. 2011	1. Dez. 2011	1. Jan. 2012	1. Feb. 2012	1. Mrz. 2012	1. Apr. 2012	1. Mai. 2012	1. Jun. 2012	1. Jul. 2012	1. Aug. 2012	1. Sep. 2012	1. Okt. 2012	1. Nov. 2012	1. Dez. 2012
Projektmonat		**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**
AP 1	**IKT-Architekturen**																													
AP 11	Hafen-IT																													
AP 12	Logistik-IT & Schnittstelle Zoll-IT																													
AP 13	Flottentelematik (Land)																													
AP 14	Profiling-IT (Compliance, Ship-Profiling …)																													
AP 15	Buchungsplattform (IT-Frontend)																													
AP 16	Control/Operation-Center (IT-Backend)																													
AP 17	IKT-Standardisierung																													
AP 2	**Integriertes Risikomanagement**																													
AP 21	IKT-Bedrohungsanalyse																													
AP 22	IKT-Sicherheit																													
AP 23	physische Bedrohungsanalyse & Intervention																													
AP 24	Sensortechnologie Sicherheit																													
AP 25	physische Sicherheit																													
AP 26	Risiko Profiling (Compliance, Ship-Profiling …)																			AP26.2: Erweiterung Sapper zu Risiko-Profiling										
AP 27	Untersuchung typischer Transportketten																													
AP 3	**Kosten/Nutzen Modelle & Demonstrator**																													
AP 31	Buchungsplattform (IT Frontend)																													
AP 32	Control/Operation-Center (IT Backend)																													
AP 33	Innovation für Endnutzer																													
AP 34	Prüfung & QM der Geschäftsmodelle																													
AP 35	Demonstrator																													

		Projektmonat	**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**
Meilensteine																															
M12	Übergabepunkt													X																
M18	Abbruchmeilenstein																		X											

Abbildung 1: Zeitplan mit Arbeitspaketen und Meilensteinen

In Abbildung 2 ist die Struktur des Vorhabens in drei Hauptarbeitspakete

- AP1 - IKT Architektur
- AP2 - Integriertes Risikomanagement
- AP3 - Kosten/Nutzen-Modelle und Demonstrator

dargestellt, sowie die für die einzelnen Arbeitspakete verantwortlichen Partner.

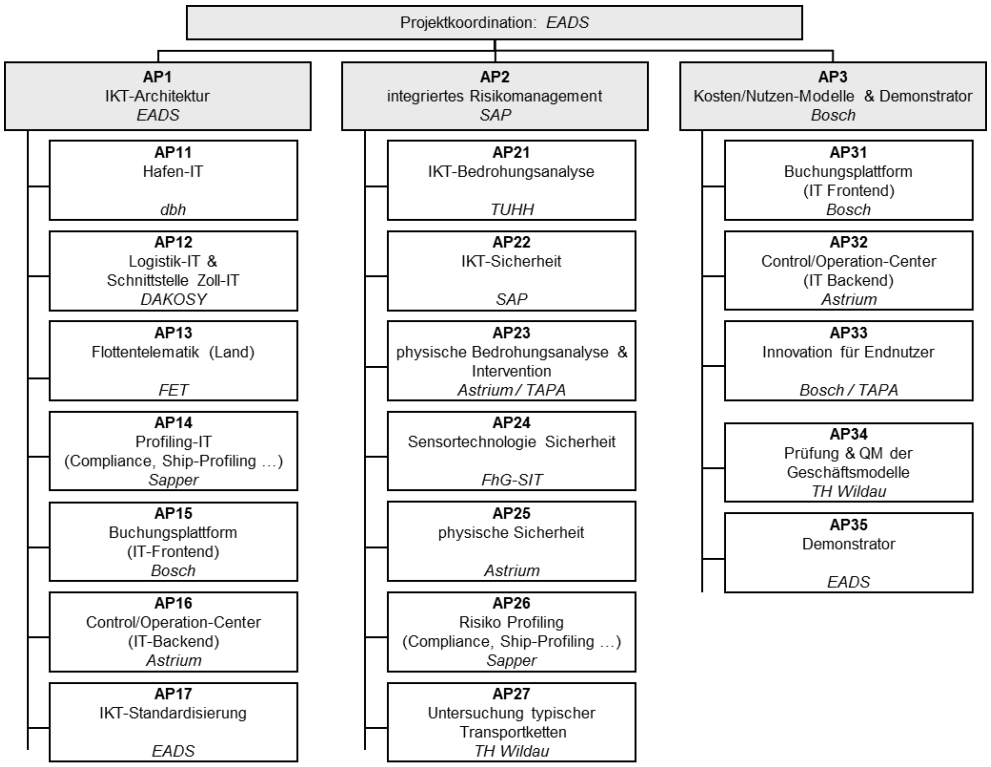


Abbildung 2: Arbeitspaketstruktur

EADS Innovation Works hatte neben der Rolle zur Koordination des Gesamtvorhabens ContainIT auch die Leitung für das Hauptarbeitspaket AP1 für IKT Architektur.

Die wesentliche fachliche Arbeit wurde seitens EADS Innovation Works in den Unterarbeitspaketen

- AP17 - IKT Standardisierung (inklusive Leitung des Arbeitspakets)
- AP25 - Physische Sicherheit
- AP26 - Risiko Profiling
- AP35 – Demonstrator (inklusive Leitung des Arbeitspakets)

durchgeführt.

Verschiedene weitere Arbeitspakete wurden von EADS Innovation Works unterstützt.

Das erste Projekttreffen, das KickOff-Meeting, fand am 16. September 2010 bei EADS in Ottobrunn bei München statt.

Ab diesem Zeitpunkt gab es regelmäßige Treffen mit allen Partnern des Konsortiums, im ca. halbjährigen Zyklus auch unter Teilnahme des Projektträgers VDI-TZ. Weiter wurden im 14-tägigen Zyklus Telefonkonferenzen mit allen Partnern des Konsortiums durchgeführt. Bei Bedarf wurden im kleineren Kreis der Partner Treffen einberufen oder Telefonkonferenzen durchgeführt.

Während der Abarbeitung der verschiedenen Arbeitspakete wurden mehrere Workshops und Interviews mit den nicht im Vorhaben involvierten Akteuren aus dem operativen Geschäfts der Containertransporte wie z.B. Spediteure, Hafen- und Bahnterminalbetreiber, Zoll- und Sicherheitsbehörden, Versicherungen oder auch mit einer Datenschutzorganisation durchgeführt. Somit war sichergestellt, dass die Aspekte und Sichtweisen alle an Containertransporten beteiligten Akteure mitberücksichtigt werden konnten.

Zum Ende des Projekts wurde eine komplexe Projektdemonstration entworfen und aufgebaut, welche die Projektidee darstellt, d.h. einer vernetzten IKT Infrastruktur, der dadurch ermöglichten Zusammenführung von Informationen aus den verschiedensten bestehenden IKT Systemen der Akteure, der Fusion der Informationen für ein integriertes und umfassendes Risiko-Profiling mit einem

nachfolgendem Risikomanagement bis hin zur finalen Intervention. Die Projektdemonstration wurde an einem speziellen Mustertransportszenario, welches alle relevanten und typischen Prozesse eines Containertransports abbildet, interaktiv veranschaulicht und dargestellt.

Auf der Projektabschlussveranstaltung am 5. Dezember 2012 war neben der Vorstellung des Gesamtkonzepts von ContainIT die Projektdemonstration war einer der wesentlichen Hauptbestandteile, neben der Veranschaulichung von Vorgehensweise und vor allem der Projektergebnisse als auch weitere Fachbeiträge wie z.B. von der World Customs Organisation (WCO). Der breite Teilnehmerkreis bestand aus u.a. aus dem Projektträger, dem Projektkonsortium, den assoziierten Projektpartnern Transported Asset Protection Association Section for Europe, Middle East and Africa (TAPA EMEA) und dem Joint Research Centre (JRC) of the European Commission (Institut for the Protection and Security of the Citizen - ISPC). Weiter waren Vertreter von Behörden wie z.B. dem Bundesamt für Ausfuhrkontrolle (BAFA; Referat für Proliferations- und Exportkontrolle), der WCO und des United Nations Office on Drugs and Crime (UNODC). Außerdem waren Vertreter weiterer vom BMBF geförderter Containersicherheitsprojekte vertreten.

1.4 Wissenschaftlicher und technischer Stand

Auf dem internationalen Feld der Containertransporte und der Containersicherheit haben sich zum Zeitpunkt der Projektplanung weltweit verschiedene Initiativen gebildet, die ihren Schwerpunkt in der administrativ-organisatorischen Abwehr von Bedrohungen sehen. Ein Auszug der aktuellen Initiativen ist nachfolgend kurz aufgeführt:

- CSI: Die „Container Security Initiative“[3] (CSI) des Heimatschutzministeriums der USA, zum Schutz der USA durch Profiling, Container Scanning, Versiegelung, 24-Stunden-Lademanifestvoranmeldung in die Ausgangshäfen.
- C-TPAT: Das „Customs-Trade Partnership Against Terrorism” (C-TPAT) der USA für die Sicherheit in der Lieferkette definiert Anforderungen an US-Importeure. Die C-TPAT ist äquivalent zum europäischen Zugelassenen Wirtschaftbeteiligten[4].
- s.a.f.e: In Deutschland hat sich in die „Schutz- und Aktionsgemeinschaft zur Erhöhung der Sicherheit in der Spedition“ (s.a.f.e) etabliert. s.a.f.e. unterstützt ihre Teilnehmer durch ein ganzheitliches Sicherheitsmaßnahmenpaket, das auf die Sicherheit der individuellen Infrastruktur am Logistikstandort in den Bereichen Stückgut, Umschlag, Lager, Kommissionierzonen und Transport abgestimmt werden kann[5].
- TAPA: Die „Transported Asset Protection Association“[6] (TAPA) ist eine Vereinigung von Sicherheitsexperten und Geschäftspartnern aus Industrie und Transport, um die Sicherheitsbedrohungen in den gefährdeten Branchen zu adressieren. TAPA bietet neben einem Forum zum Informationsaustausch auch die Erarbeitung einheitlicher Frachtsicherheitsstandards sowie eine zentrale Datenbank, die z.B. kriminelle Vorkommnisse und Unfälle der betroffenen TAPA Mitglieder erfasst.
- ISO-Normen[7]: Unter anderem die ISO27001 zur Einrichtung von Sicherheitsmanagementsystemen in Unternehmen, die ISO28000 für Sicherheitsmanagementsysteme in der Lieferkette (orientiert an TAPA-Empfehlungen) oder die ISO18185 für elektronische Containersiegel.
- ISPS Code: Der „International Ship and Port Facility Security Code“ (ISPS Code) besteht aus einem umfangreichen Paket von Maßnahmen zur Gefahrenabwehr bei Schiffen und Häfen. Damit dient der ISPS-Code der Sicherheit in der Lieferkette. Diese Vereinbarung wurde 2002 unter der Federführung der International Maritime Organisation (IMO)[8] geschlossen.

Neben den prozessbezogenen Initiativen gibt es weitere Anstrengungen im technischen Umfeld, um die Sicherheit im Containertransport durch die Einführung elektronischer Siegel zu erhöhen. In den Anfängen steckt noch die auf Sensoren basierende Technologie, um mobile Geräte im Container

[3] Quelle: www.cbp.gov/xp/cgov/trade/cargo_security/csi/
[4] Quelle: www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/
[5] Quelle: www.safe-spediteure.de/
[6] Quelle: www.tapaonline.org/
[7] Quelle: www.iso.org
[8] Quelle: www.imo.org/

einzusetzen, die neben der Türprüfung auch andere relevante Umgebungsparameter (Erschütterung, Feuchtigkeit ...) erfassen. Die Analyse zur Containersicherheit in 2007[9] ergab u.a., dass der Markterfolg bzgl. der elektronisch abgesicherten, physischen Sicherheit im Wesentlichen von zwei Faktoren abhängig ist:

- Den notwendigen internationalen Regularien und
- Dem Preis derartiger Systeme im Vergleich zu konventionellen, mechanischen Lösungen.

Obwohl bereits der Standard ISO18185 für elektronische Siegel existiert, gibt es für die kommunikationstechnische Anbindung an Track-Trace-Monitoring Systeme bislang keine verbindlichen Standards. Dabei werden an solche - am Container montierten - Systeme erhebliche technische Anforderungen gestellt, z.B. sichere Datenkommunikation, Positionsbestimmung, Sensorfunktionalitäten, hohe Zuverlässigkeit usw. Hier sind derzeit noch klare technische Grenzen gesetzt, insbesondere bei Energieversorgung, Miniaturisierung und Sensorintegration. Im Rahmen verschiedener Forschungsprojekte TRACK[10] und E-Cab[11] erforscht u.a. die EADS Innovation Works neue Technologien für Track-Trace-Monitoring Systeme.

Im Bereich des Risiko-Profiling befinden sich intelligente IT-Systeme um anhand den Boykott- und Anti-Terrorlisten der Europäischen Union (EU), Schweiz, USA etc. eine Compliance-Prüfung der Frachtdaten im Rahmen der Exportkontrolle und CSI / C-TPAT durchzuführen. Firma Sapper ist in Europa Marktführer und verwendet statt Soundex[12]- und Fuzzy-Logik-Algorithmen hier ein in-house entwickeltes Verfahren, das auf einer Vorfeldformatierung der Sanktionslisten und Matching auf Silbenebene aufsetzt. Prototypisch wurde am europäischen Forschungszentrum JRC in Zusammenarbeit mit der Anti-Korruptionsbehörde OLAF die Ship-Profiling Software ConTraffic[13], entwickelt, welche sich als Datenbasis öffentlich zugänglicher Schiffsmeldungen durch „Vessel Traffic System“ (VTS) und „Automatic Identification System” (AIS) bedient (Schnittstelle zu eCustoms). Um Manipulationen am AIS zu entdecken forscht EADS an der automatisierten Auswertung von Radarbildern[14].

Als Voraussetzung für eine Verbesserung der Sicherheitslage sind die Bereitstellung und Verfügbarkeit von Informationen zwingend notwendig, um eine End-to-End Überwachung von Warenketten und damit ein Risko-Profiling zu ermöglichen. Dies setzt die Nutzung von vernetzten Netzwerken voraus. Eine solche Vernetzung kann jedoch dazu führen, dass sich die involvierten Netzwerke durch diese selbst wiederum in einer gemeinsamen Bedrohungslage befinden und der Gefahr von Angriffen auf Rechner, Programme und Daten ausgesetzt sind. Durch die hohe Anzahl von beteiligten Rechnern in der komplexen Warenkette besteht ein großes Potenzial, dass Sicherheitslücken bei einzelnen Beteiligten entstehen, die letztlich das gesamte Netzwerk gefährden. Als schwächstes Glied der Sicherheitskette erweist sich zunehmend der externe Informationsschutz[15]. Im Rahmen des Echtzeit-Trackings von Containern wurde bereits der Einsatz von sicheren leichtgewichtigen Kanälen zur Kommunikation dediziert untersucht[16, 17]. Andere Ansätze für die logische Sicherung von Containertransporten sind agenten-[18] als auch event-basiert[19]. Der Austausch von Daten in Containertransportketten bedarf sicherer und vertraulicher (im Sinne von Privatheit)

[9] Quelle: „Container Security - A Market Analysis“, N15C-16, Frost & Sullivan, 2007

[10] „TRACK”, ein Förderprojekt des BMBF; Förderkennzeichen: 16SV2033

[11] „E-Cab“, ein Förderprojekt der EU; Vertragsnummer: AIP5-CT-2006-030815

[12] „Soundex“, ein phonetischer Algorithmus zur Indizierung von Wörtern und Phrasen nach ihrem Klang

[13] Ship-Profiling Software „ConTraffic“, http://contraffic.jrc.it; http://masure.jrc.ec.europa.eu

[14] R&D-Verbund DeMARINE (ShipDetec, Parol und DEKO) von u.a. Astrium: Schiffsdetektion mittels Satellitenrader (TerraSAR-X) und automatischer Schiffsdetektion (AIS)

[15] Quelle: Deloitte "Treading Water - The 2007 Security Survey", http://www.deloitte.com/dtt/cda/doc/content/TreadingWater.pdf

[16] Quelle: J. O. Lauf, D. Gollmann, V. Turau: “MASC - Monitoring and Security of Containers”, Tagungsband Informatik 2007, GI, Bremen, 2007

[17] Quelle: J. O. Lauf, H. Sauff: “Secure Lightweight Tunnel for Monitoring Transport Containers”, Proceedings SecureComm 2007, Nizza

[18] Quelle: S. Werner "Agent-Based Container Security Systems - An Interdisciplinary Perspective", DIGMA, 7. Jahrgang, Heft 4, Dezember 2007

[19] Quelle: R. Müller "Developing a Security Event Management System for Intermodal Transport", DIGMA, 7. Jahrgang, Heft 4, Dezember 2007

Methoden, insbesondere was die Up- bzw. Down-Stream Kommunikation zwischen Warenkettenpartnern angeht[20].

In Bezug auf das Teilvorhaben ContainIT EADS werden zum einen die aktuelle IKT Architektur als auch die aktuellen Bewertungsmethoden zur physischen Sicherheit der Containerlogistikkette betrachtet.

Bei den verschiedenen Akteuren der Containerlogistikkette existieren mehrheitlich eigenständige IKT Insellösungen nebeneinander, wie schematisch in Abbildung 3 dargestellt ist. Diese Inseln sind nicht bzw. nur teilweise (oft nur proprietär) miteinander vernetzt, so dass ein nahtloser Datenaustausch untereinander zwischen den Akteuren bzw. zu den Behörden nahezu unmöglich ist. Einzig innerhalb weniger Teilprozesse der Logistikkette wie z.B. zwischen Reedern, Schiffen, Hafenterminals, Spediteuren oder Zollbehörden werden in begrenztem Umfang einige spezielle Daten wie z.B. transportbegleitende Dokumente ausgetauscht.

Dies mag ein Grund dafür sein, warum aktuell verfügbare Risiko-Profiling Lösungen nur ein Gebiet abdecken, wie z.B. das Matching von Frachtdokumenten mit Sanktionslisten.

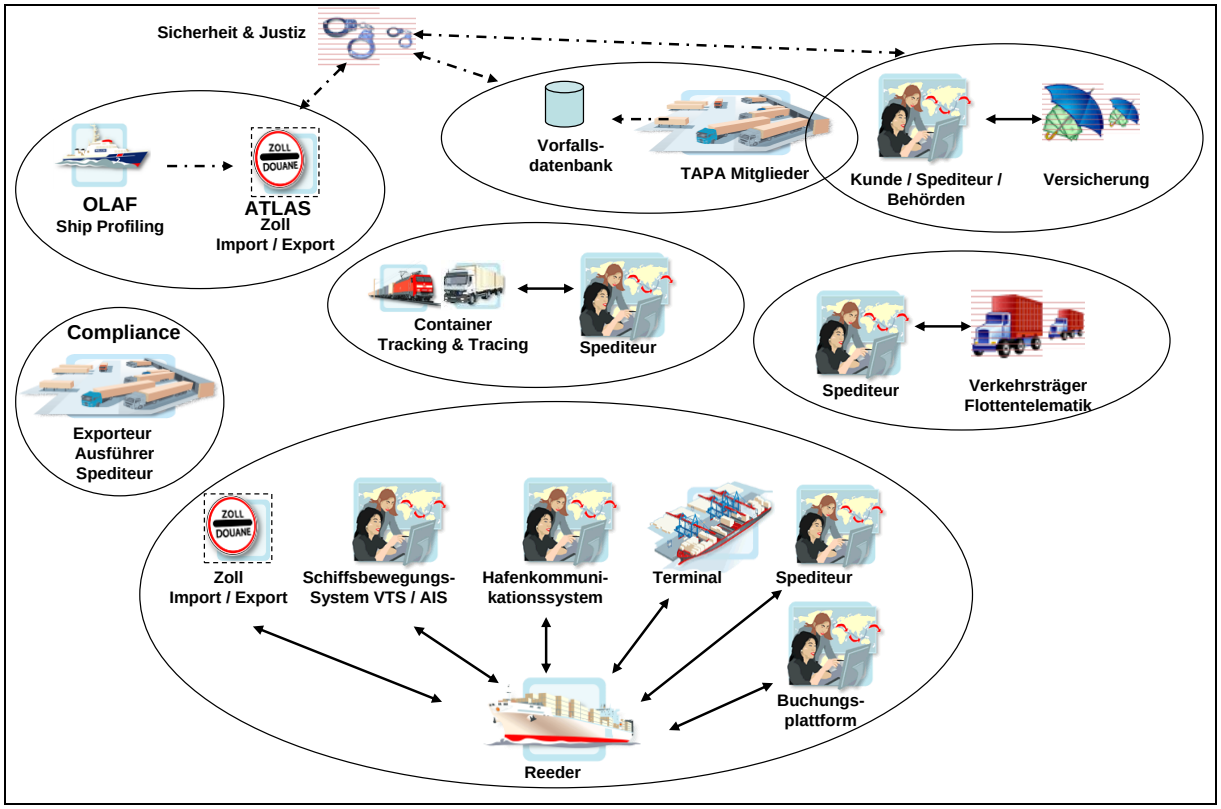


Abbildung 3: IKT Insellösungen innerhalb der Containerlogistikkette

1.5 Zusammenarbeit mit anderen Stellen

Im Vorhaben ContainIT waren mehrere assoziierte Partner eingebunden, welche zum ergänzenden Informationsaustausch sowie zur Diskussion fachlicher Inhalte, Ideen und Ergebnissen ins Projekt eingebunden waren. Die assoziierten Partner wurden im Laufe des Projekts von einzelnen oder mehreren Projektpartnern immer wieder kontaktiert, entweder telefonisch, per Email oder auch durch persönliche Treffen.

[20] Quelle: Florian Kerschbaum “Building A Privacy-Preserving Benchmarking Enterprise System”, Enterprise Information Systems 2 (4), 2008

Das Joint Research Centre (JRC) der European Commission (EC) als auch das Office de Lutte Anti-Fraude (OLAF), die Antibetrugsbehörde der European Union (EU), waren als assoziierte Partner involviert. Für das Projekt waren die Arbeiten am vom JRC entwickelten ConTraffic System von Interesse, welches sich bei OLAF im Einsatz befindet. Das System erweitert die derzeitigen Sicherheitsmechanismen für seegehende Containertransporte, durch die Möglichkeit der automatischen Erfassung und Analyse von globalen Containerbewegungen auf See und identifiziert dadurch potentiell verdächtige Lieferungen und unterstützt somit die Risikoanalysen von Zoll (Schnittstelle zu eCustoms) und Häfen.

Die Transported Asset Protection Association (TAPA) als assoziierter Projektpartner, ist eine Organisation, welche sich mit der Sicherheit in der kompletten Lieferkette befasst. In dem Regionalbereich EMEA (Europe Middle East and Africa) mit über 255 Mitgliedern aus Europa, dem Mittleren Osten und Afrika begegnen der Herausforderung zur Aufrechterhaltung der Sicherheit in der Lieferkette gemeinsam. Zu den Initiativen der TAPA zählen insbesondere:

- Herausgabe von Frachtsicherheits-standards wie z.B. Freight Security Requirements (FSR), Truck Security Requirements (TSR) oder Tapa Air Cargo Security Standards (TACSS).
- Eine zentrale Datenbank, die z.B. kriminelle Aktivitäten gegen TAPA Mitglieder erfasst.

Im Rahmen der fachlichen Arbeiten wurden mit verschiedenen Akteure aus der Containertransportkette einzelne Interviews oder auch mit mehreren Workshops durchgeführt. Nachfolgend ein Auszug der Veranstaltungen mit projektexternen Firmen und Organisationen an denen EADS wesentlich beteiligt war:

- Im Oktober 2011 fand in Kiel beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein ein Treffen zum Thema Datenschutz in Bezug zum Konzept von ContainIT statt.
- Ebenso fand im Oktober 2011 ein Treffen mit einem Vertreter des SMART-CM Projekts (im 7. Rahmenprogramm der EU gefördert) statt. Für eine Studie im Bereich der “Container Security & Tracking Devices” konnte ContainIT Beitrag leisten, im Gegenzug gab es Informationen aus der Studie, welche für ContainIT hilfreich waren.
- Mit Unterstützung der German European Security Association (GESA) wurde ein Workshop mit Behörden organisiert, auf welchem die Bedürfnisse und Anforderungen von Sicherheitsbehörden in Bezug auf Containersicherheit als auch das Systemkonzept von ContainIT diskutiert wurden. Seitens der Behörden waren Vertreter der Bundespolizei, der Wasserschutzpolizei, des Bundesministeriums für Verkehr, Bau und Stadtentwicklung sowie vom Zollfahndungsamt vertreten.

2 Eingehende Darstellung

2.1 Verwendung der Zuwendung und erzielte Ergebnisse

Wie in Kapitel 1.1 schon beschrieben, waren die Arbeiten der EADS fokussiert auf zwei wesentliche Hauptziele, welche auch als zwei Kernpunkte im Verbundvorhaben ContainIT betrachtet werden können:

- Erweiterung bestehender IKT (Teil-) Architekturen bzw. der Entwurf eines standardisierten IKT Architekturmodells für einer lückenlose IKT Gesamtarchitektur in Verbindung mit einem generisches Datenmodell zum Datenaustausch innerhalb der gesamten Transportkette.
- Entwurf von Konzepten bzw. Methoden zur Optimierung der physischen Sicherheit als auch für ein für ein integriertes Risikomanagement z.B. durch Risiko-Profiling von Containertransporten.

Die Arbeiten am ersten Hauptziel, an der **IKT Architektur**, waren gebündelt im Hauptarbeitspaket AP1, wobei die Unterarbeitspakete AP11 bis AP14 zur Erfassung des Status Quo der bei den verschiedenen Akteuren der Containertransportkette derzeit verwendeten IKT Systeme fokussieren. Im Rahmen der Unterarbeitspakete AP15 und AP16 wurde ein Konzept für eine Frontend-Struktur als auch für eine Backendstruktur entworfen, zum einen die Schnittstelle zum Benutzer, d.h. zu den Akteuren und zum anderen die Hardwarestruktur zur Verarbeitung der Daten aus den Containertransporten. Innerhalb der Unterarbeitspakete AP11 bis AP16 hat EADS den anderen entsprechend verantwortlichen Projektpartnern zugearbeitet.

In Unterarbeitspaket AP27, geleitet vom Projektpartner TH Wildau, wurden ergänzend zum Arbeitspaket AP1 noch typische Transportketten untersucht, d.h. welcher Akteur interagiert z.B. beim multimodalen Güterverkehr mit wem und welche Prozesse werden dabei durchlaufen und welche IKT Technologien werden dabei verwendet. Weiter wurde ein Mustertransportszenario entworfen, welches im gesamten Projektverlauf als Leitfaden für übergreifende Betrachtungen herangezogen wurde.

In AP17 wurden von EADS die Ergebnisse aus den Unterarbeitspaketen AP11 bis AP16 konsolidiert, um anschließend ein Konzept für eine übergreifende IKT Architektur zu entwerfen, welche es erlaubt die Idee von ContainIT, d.h. der IKT basierten Containersicherheit, umzusetzen.

Für das zweite Hauptziel, letztendlich von EADS dem Entwurf einer **Methodik für ein Risiko-Profiling** basierend auf den unterschiedlichen Informationen kommend von verschiedenartigen IKT Systemen, wurde im Rahmen der Unterarbeitspakete AP25 und AP26 durchgeführt. Die Arbeiten in den Unterarbeitspaketen AP25 und AP26 wurden von den Projektpartnern Astrium und Sapper geleitet. Hierzu waren die Vorarbeiten zur IKT Architektur aus dem Arbeitspaket AP1, als auch aus dem Arbeitspaket AP2 seitens der Sicherheits- und Risikoanalysen zu den IKT Systemen und der Prozesse erforderlich.

Hierzu ergänzend hat EADS die Arbeiten in den Unterarbeitspaketen AP21, AP22 und AP23 zur Untersuchung verschiedener Musterangriffsszenarien mit „terroristischer und krimineller Motivation“ basierend auf dem Mustertransportszenario, welche die Basis zur Bearbeitung der entsprechenden Arbeitspakete und weitere Betrachtungen im Projekt waren, wie z.B. in AP22 durch generelle Evaluierung der Methodik oder Verifikation durch beispielhafte Bewertungsdurchläufe für die Risikobewertung sowie in AP31/AP32 als Randbedingungen für wirtschaftliche Betrachtungen zur sekundären Nutzung der ContainIT Plattform als Unterstützung für die an der Plattform beteiligten Akteure z.B. durch transparentere Transportprozesse, unterstützt.

Als übergreifender wie auch als abschließender dritter Arbeitsschwerpunkt ist das Unterarbeitspaket AP35 mit der **Projektdemonstration** aufzuführen, welches von EADS koordiniert als auch maßgeblich von EADS mit der Veranschaulichung des Risiko-Profiling unterstützt wurde.

2.1.1 IKT Architektur

In AP11 bis AP14 fokussierten sich die unterstützenden Arbeiten seitens EADS auf die Erfassung des aktuellen Zustands der IKT Architekturen der verschiedenen Beteiligten Akteure eines Containertransports.

Als Koordinator des Hauptarbeitspakets AP1 hat EADS maßgebend daran gearbeitet, dass die Erfassung IKT Architekturen innerhalb der einzelnen Unterarbeitspaketen möglichst einheitlich und vergleichbar erfolgt und vor allem, dass für die nachfolgenden Arbeiten in AP17 und für AP2 alle notwendigen Aspekte berücksichtigt wurden.

Hierzu hat EADS federführend - mit Unterstützung der Projektpartner - an der Ausarbeitung einer Dokumentvorlage zur arbeitspaketübergreifenden einheitlichen Erfassung und Beschreibung der aktuellen der IKT Architekturen erarbeitet. Die Dokumentvorlage beinhaltet die Beschreibung der Akteure, der detaillierten Prozesse, der den Prozessen zugehörigen IKT Systeme sowie vorbereitend für die Risikoanalysen im Hauptarbeitspaket AP2 die entsprechend relevanten Sicherheitskriterien. Bzgl. der Sicherheitskriterien wurde ebenso zusammen mit den Projektpartnern eine Methodik zur Beurteilung und Klassifizierung der Gefährdungspotentiale durch den Menschen, der Sicherheitsmechanismen sowie der Prozesse entwickelt. Hiermit konnten bereits in den Unterarbeitspaketen AP11…AP16 die Gefahrenpotentiale der unterschiedlichen IKT Systeme einheitlich für spätere Arbeiten erfasst und beschrieben werden.

Nachfolgend zeigt Abbildung 4 die Struktur der Dokumentvorlage zur Veranschaulichung des Inhalts und der Vorgehensweise zur Erfassung des aktuellen Zustands der IKT Architekturen.

Inhaltsverzeichnis

Abbildung 4: Struktur der Dokumentvorlage zur Erfassung des IKT Istzustands

Ein wesentlicher Punkt der Vorlage war die Beschreibung der Prozesse. Hierzu wurde das anhand des von bestehenden Beschreibungsmodellen vom Projektpartner TH Wildau abgeleitete „Secure

Transportation Operations Reference Model“, das sogenannte STORM-Referenzmodell, genutzt, um die Hierarchisierung des betrachteten Prozess des Akteurs grafisch darstellen zu können.

Das STORM Modell wurde abgeleitet von dem als Managementansatz bekannten „Supply Chain Reference Operations“ (SCOR) Model des Supply Chain Council[21].

Die nachfolgende Abbildung 5 zeigt das STORM Modell zur Beschreibung der Prozesse bei den Akteuren.

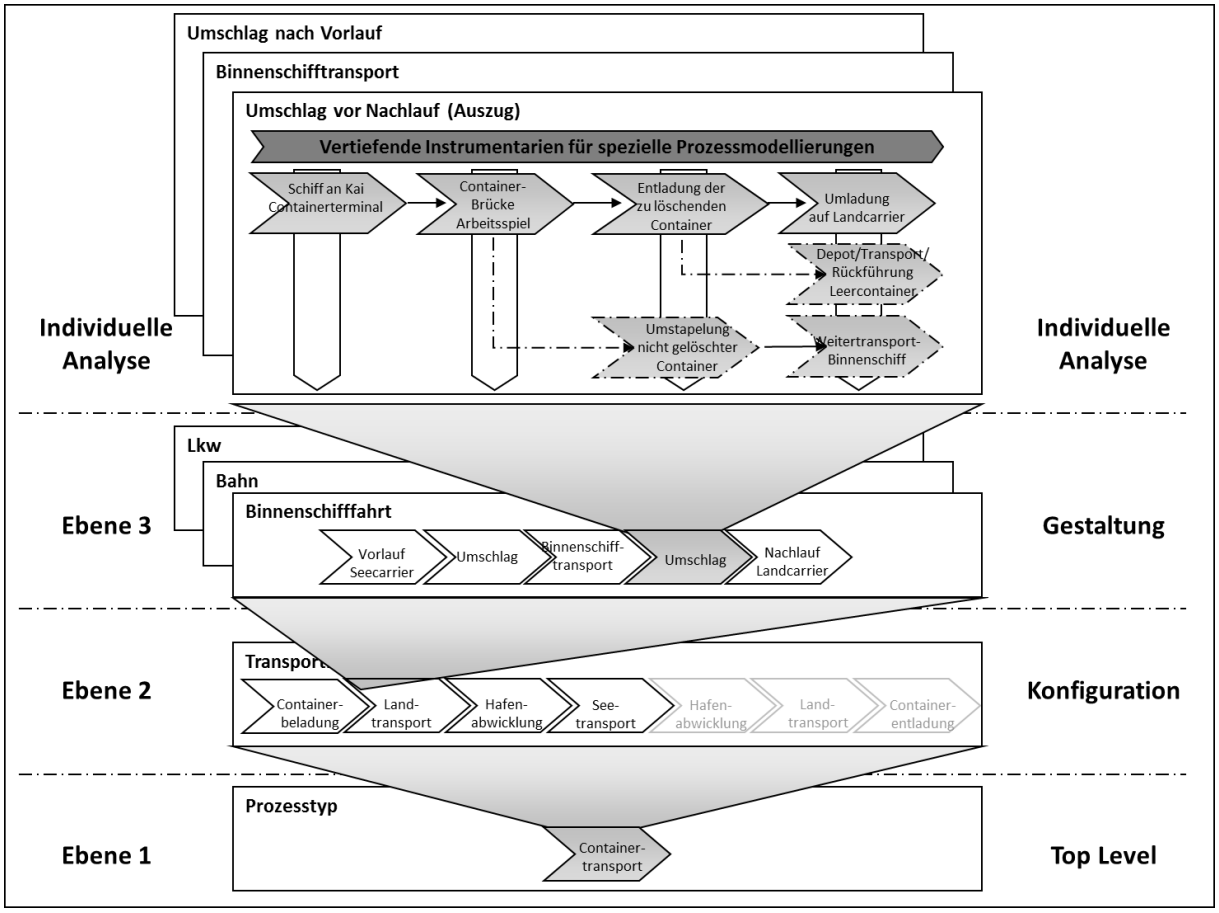


Abbildung 5: Beschreibung der Prozesse beim Akteur nach dem STORM Modell

Durch die Anpassung ermöglicht STORM einen durchgängigen Vergleichslevel zwischen den beteiligten Entitäten und Prozessen der unterschiedlichen Darstellungsebenen und soll für eine operationalisierende Visualisierung der zu analysierenden containergestützten Transportkette in ContainIT eingesetzt werden.

Innerhalb von ContainIT werden die Prozesse für STORM mit Hilfe einer IT-gestützten Lösung visualisiert. Hierzu wird auf die Software BizAgi Process Modeler[22] zurückgegriffen, die den untersuchten grafischen Modellierungsansatz Business Process Modelling Notation (BPMN) benutzt.

Beispielhaft zeigt Abbildung 6 die grafischie Beschreibung des Prozesses basierend auf BPMN mittels der BizAgi Software.

[21] Quelle: http://supply-chain.org; Supply Chain Council, 1996 gegründete Non Profit Organisation

[22] Quelle: http://www.bizagi.com/; BizAgi kostenfreies BPMN Modellierungswerkzeug zur grafischen Darstellung von Geschäftsprozessen

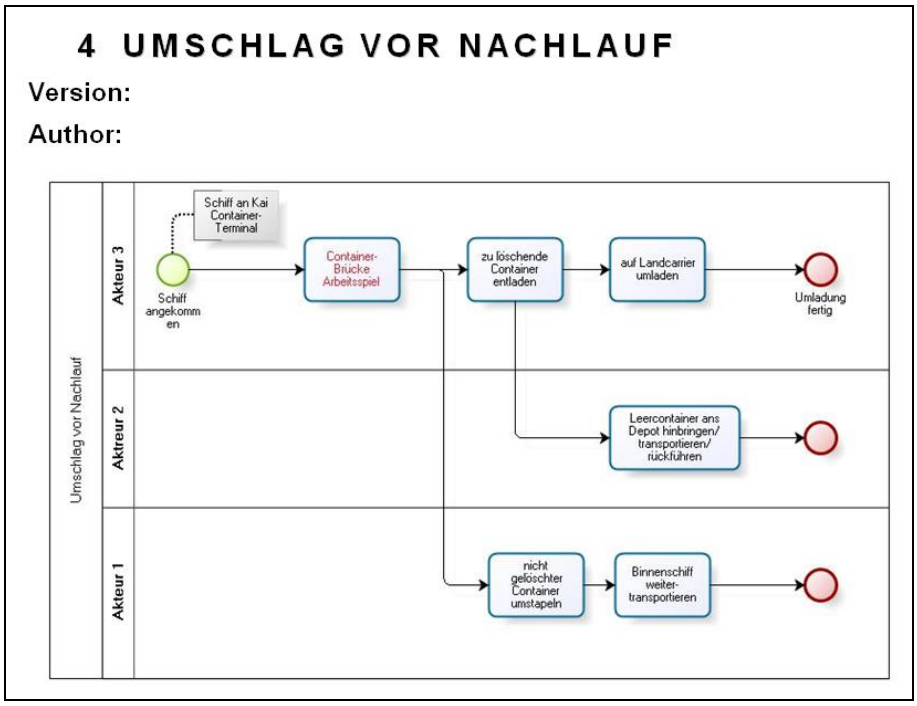


Abbildung 6: Beschreibung der Prozesse bei den Akteuren entlang der Transportkette mit BizAgi

Ergänzend zur grafischen Darstellung werden die Prozesse textuell beschrieben, wie nachfolgend in Tabelle 1 dargestellt.

Informationsfluss	eingesetzte Netzwerktopologien	Medienbrüche	Normen, Regularien, Standards, Best Practices	Sicherheitsaspekte, Risiken, Auswirkungen	Probleme, Optimierungsbedarf
• Input & Output von Daten / Dokumenten sowie Methoden zur Handhabung, Datenaustausch-Format, Dokumententyp/Inhalt	• auf Systemebene; Medien, Infrastruktur, Technologien und Methoden, …	• Fax/Papier, Telefon, Web, eMail, …	• auch intern	• Vertraulichkeit, Authentizität der Daten, Auswirkung von Datenmanipulation, …	
• Awendungs- und Verantwortungs-wechsel • Anforderungen an Verfügbarkeit und Integrität der Daten	• VPN • Zertifikate	• Anwendungs- und Verantwortungs-wechsel	• ISO Zertifizierung	• Handhabung vertraulicher Dokumente • Sicherheitsrelevante Prozess-Elemente • Systemanalyse • Prozesse/ Mechanismen für Daten-Verfügbarkeit/Integrität • Bedrohungsanalyse/-Aspekte • Sensibilität der Daten • Auswirkungen möglicher Fehlfunktionen (Todesfall, …)	• verzögerter Daten/Dokumentenfluss → verzögerte Abwicklung • Was kann schief gehen? z.B. auch bei Verzögerungen? • Bedrohungen / Zwischenfälle

Tabelle 1: Ergänzende textuelle Beschreibung der IKT des jeweiligen Prozesses beim Akteur

Weiter werden auf Ebene 2 des STORM Referenzmodells die Gefährdungspotentiale Mensch (GefPot M), Sicherheitsmechanismen (GefPot S) und Prozess (GefPot P) untersucht, eine entsprechende Bewertung durchgeführt und das gesamte Gefährdungspotential für den jeweiligen

Prozess beim Akteur berechnet. (Bei der Erstellung Methodik zur Bewertung der Gefährdungspotentiale hat EADS unterstützend mitgewirkt.)

Für jedes der drei Elemente des gesamten Gefährdungspotentials gilt:

- Berechnung bei einer einheitlichen Gewichtung von 20% je Bewertungsfaktor bei 5 Bewertungsfaktoren, in Summe 100%
- es ergibt sich eine Kennzahl von 0 Punkte = 0% Sicherheit bis zu 3 Punkte = 100 % Sicherheit

Das gesamte Gefährdungspotential setzt sich aus der Summe der drei Elemente des Gefährdungspotentials zusammen:

- Gefährdungspotential = GefPot M + GefPot S + GefPot P
- es ergibt sich eine Kennzahl von 0 Punkte = 0% Sicherheit bis zu 9 Punkte = 100 % Sicherheit

Die nachfolgende Tabelle 2 zeigt exemplarisch die Tabelle zur Bewertung der Sicherheitsmechanismen GefPot S.

		Bewertungsfaktoren GefPot S				
	Gewichtung	20%	20%	20%	20%	20%
Level / Punktzahl	Logik	Zugang	Überwachung	System (Verfügbarkeit / Ausfallsicherheit)	Datenübertragung (Verfügbarkeit / Ausfallsicherheit)	Widerstandsfähigkeit (zeitlich)
0	Hohes Gefährdungspotential = niedriges Sicherheitsniveau	- öffentlich zugänglich	keine	Sehr niedrig z.B.: - nur Stand-alone System - kein Backup verfügbar	Sehr niedrig z.B.: - nur 1 Datenkanal - keine Verschlüsselung	Sehr niedrig: Angreifer kann ohne Zeitverlust eindringen
1		- alle Mitarbeiter / Firmenangehörige, die Zutritt zu Gebäude oder Bereich haben	passive Überwachung / einfach zu umgehen z.B. - Überwachung beschränkt auf bestimmte, sehr kritische Bereiche - bei Gebäuden z.B. Einbruchmeldeanlage (EMA) - bei IT Systemen Firewall vorhanden - bei mobilen Objekten z.B. Türalarm	Niedrig z.B.: - Systeme teilweise redundant ausgelegt z.B. Datensicherung auf separatem Server aber kein separates Operativsystem als Backup	Niedrig z.B.: - nur 1 Datenkanal aber mit Fallback z.B. GPRS -> GSM	Niedrig: Angreifer wird kurzfristig aufgehalten, geringe Gefahr der Entdeckung
2		- getrennter Bereich, Freischaltung / Bevollmächtigung notwendig	passive Überwachung / schwerer zu umgehen z.B. - Überwachung sehr umfangreich und dicht - bei Gebäuden z.B. Einbruchmeldeanlage (EMA) - bei IT Systemen Firewall vorhanden - bei mobilen Objekten z.B. Türalarm	Mittel z.B.: - Kritische Systemkomponenten redundant cold-standby - Notfallkonzept vorhanden - regelmäßige Wartungen	Mittel z.B.: - nur 1 Datenkanal aber mit Fallback z.B. GPRS -> GSM - Datenverschlüsselung	Mittel: Angreifer wird eine gewisse Zeit aufgehalten; es besteht für ihn eine erhöhte Gefahr der Entdeckung
3	Niedriges Gefährdungspotential = hohes Sicherheitsniveau	- ausschließlich Sicherheitspersonal	aktive Überwachung: - bei Gebäuden z.B. Wächter- bzw. Videorundgänge - bei IT Systemen z.B. regelmäßige Virenscanns - bei mobilen Objekten z.B. regelmäßige Positionsmeldung und Gebietsüberwachung	Hoch z.B.: - System redundant ausgelegt - hotstandby - Notfallkonzept vorhanden - USV vorhanden - regelmäßige Wartungen	Hoch z.B.: - mind. 1 Backup für Datenkanal z.B. GSM + Iridium oder Telefonanbindung über 2 TK-Knoten - Datenverschlüsselung	Hoch / lang: Ein potentieller Angreifer würde für einen Einbruch so lange benötigen, dass Einbruchsversuch höchst wahrscheinlich erfolglos bleibt bzw. Angriff an anderer Stelle erfolgt
	Beispiele - nicht ausschließlich Kann sich beziehen auf:	- Orte: Lager, Parkplatz, Bahnhof, Hafen... - IT Systeme: Buchungssysteme, Disposysteme, Ortungssysteme & Überwachungssysteme, Einbruchmeldesysteme, Videoüberwachungssysteme ,... - Transportmedien: LKW, Bahn, Schiff,...	- Orte: Lager, Parkplatz, Bahnhof, Hafen... - IT Systeme: Buchungssysteme, Disposysteme, Ortungssysteme & Überwachungssysteme, Einbruchmeldesysteme, Video überwachungssysteme ,... - Transportmedien: LKW, Bahn, Schiff,...	- IT Systeme: Buchungssysteme, Disposysteme, Ortungssysteme & Überwachungssysteme, Einbruchmeldesysteme, Videoüberwachungssysteme ,... - Kommunikationsmedium Mail, Brief, Fax, SMS... - kann sich befinden an einem Orte: Lager, Parkplatz, Bahnhof, Hafen oder auf einem Transportmedien: LKW, Bahn, Schiff,...	- IT Systeme: Buchungssysteme, Disposysteme, Ortungssysteme & Überwachungssysteme, Einbruchmeldesysteme, Videoüberwachungssysteme ,... - Kommunikationsmedium Mail, Brief, Fax, SMS... - kann sich befinden an einem Orte: Lager, Parkplatz, Bahnhof, Hafen oder auf einem Transportmedien: LKW, Bahn, Schiff,...	- Bezieht sich auf alle Vorkehrungen oder Systeme, die einen Angreifer abhalten z.B. mechanische Sicherungen (Zäune, Schößer, Türen), elektronische Sicherungen (Firewall, elek. Türschlösser)

Beispiel Berechnung bei einer einheitlichen Gewichung von 20% je Bewertungsfaktoren bei 5 Bewertungsfaktoren, in Summe 100% :

Kennzahl GefPot S = Level Zugang x Gewichtungsfaktor + Level Überwachung x Gewichtungsfaktor ...

Min. Punktzahl = 0x0,2 + 0x0,2 + 0x0,2 + 0x0,2 + 0x0,2 = **0**, entspricht 0/3=0% Sicherheit

Max. Punktzahl = 3x0,2 + 3x0,2 + 3x0,2 + 3x0,2 + 3x0,2 = **3** entspricht 3/3= mathematisch 100%, aber reale 100% Sicherheit gibt es nicht

Bewertbar sein sollten:

- Prozesse (Beladen, Ausladen, Verladen, Transport, Lagern,...)
- somit auch Orte (Parkplatz, Hafen, Lager ...)
- somit auch Transportmedien (LKW, Bahn, Schiff,...)
- somit auch IT Systeme

Tabelle 2: Bewertungsschema für Gefährdungspotential Sicherheitsmechanismus

Weiter werden wie in Tabelle 3 dargestellt die verwendeten IKT Systeme noch technisch beschrieben.

	System A	System B	System C	…
Name	SAP	Logistik IT	Buchungsplattform	
Anwendungstyp	ERP	Speditionstool	?	
internes/externes System	Intern (SW läuft auf eigenem Server))		extern (Web-Zugriff)	
Verwendungszweck	Warenmanagement	Disposition		
Funktionen	Lagerplanung, Warenzusammenstellung, …	Einsatzplanung, Routenplanung		
Nutzer (Abteilungen)	Lagerhaltung, QMM, Versand	Dispositionsplanung, Operative		
Nutzungsverhalten	Batch-Prozess	Zyklisch		
Eingabemedien	PC, Handheld, Terminal	PC		
Zugriffstechnologie	Internet, Netzwerk	Netzwerk		
Verschlüsselung (Datentransport)	VPN	keine		
Autorisierung	Passwort	Kartenleser		
weitere Sicherheitsmechanismen	4-Augen-Prinzip	Fingerabdruck		
Ausgabemöglichkeiten	Excel Report	HTML		
Datenverfügbarkeit	95%	97%		
Datenaktualität	täglich	stündlich		
Datenintegrität	kann nicht zu 100% garantiert werden			
Protokollierung	?			
Fehlerbehandlung (Wiederanlauf eines Prozessabbruchs, …)	?			

Tabelle 3: Beschreibung der beim Akteur eingesetzten IKT Systeme

Aus dieser Basis wurden innerhalb der einzelnen Unterarbeitspakete in AP1 mit entsprechenden Akteuren Interviews durchgeführt um eine möglichst umfassende Beschreibung des aktuellen Zustands der IKT Architekturen d.h. der verwendeten IKT Systeme als auch der angewandten Prozesse zu erhalten.

Wesentliche der zuvor beschriebenen Elemente, wie z.B. die Bewertung der Gefährdungspotentiale wurden unter Mitwirkung von EADS im Unterarbeitspaket AP27 zusammen mit der TH Wildau entwickelt.

Weiter hat EADS in AP27 die Untersuchung und Beschreibung der typischen Transportketten unterstützt, durch z.B. die Evaluierung und Auswahl von Prozess-Sprachen und -Methoden für die Modellierung mittels der zuvor bereits genannten Software BizAgi Process Modeler und deren grafischen Modellierungsansatz Business Process Modelling Notation (BPMN).

Ein wesentliches Ergebnis aus AP27 mit maßgeblicher Beteiligung von EADS ist das sogenannte Mustertransportszenario (dargestellt in Abbildung 7 und Abbildung 8), welches im gesamten Verlauf von ContainIT als Untersuchungsgegenstand für alle übergreifenden Betrachtungen der Containertransportkette als auch für die finale Projektdemonstration herangezogen wurde. Das Mustertransportszenario wurde mit BizAgi erstellt.

Die Erstellung des Mustertransportszenarios basiert auf der notwendigen Fokussierung des Untersuchungsgegenstands in ContainIT, welche einen multimodalen Containertransport (LKW, Bahn und See-Schiff) und die zugehörige Export-Zollabwicklung für einen grenzüberschreitenden Transport in Richtung USA abbildet. Der dargestellte Prozess wurde dabei so generisch gehalten, dass damit z.B. auch eine Import-Zollabwicklung oder andere grenzüberschreitende Verkehre mit anderen Verkehrsträgern darstellbar sind.

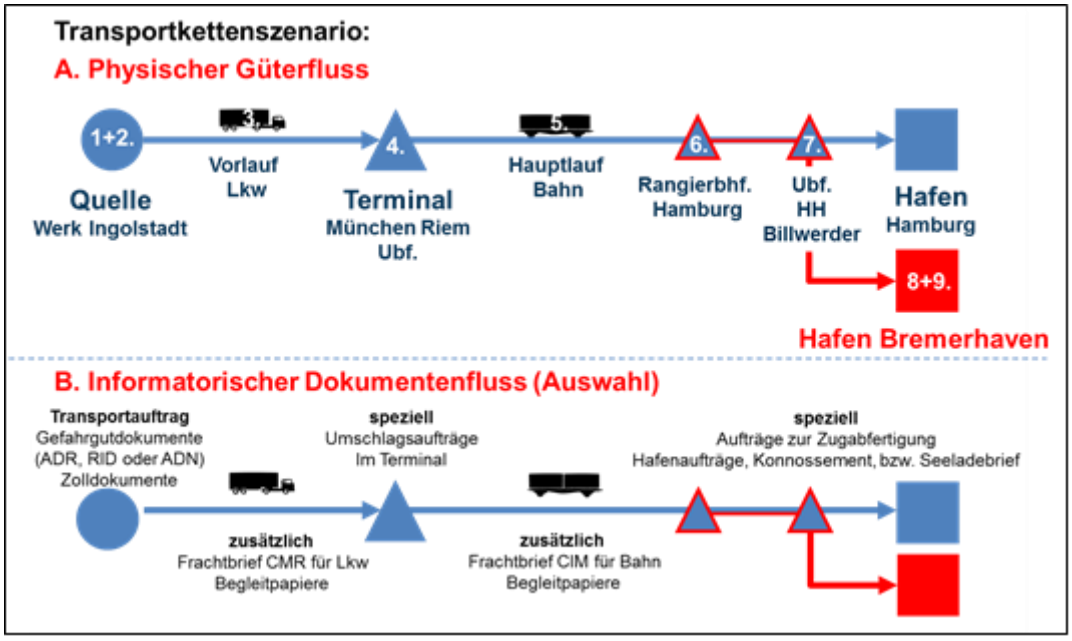


Abbildung 7: Mustertransportszenario als Untersuchungsgegenstand für ContainIT

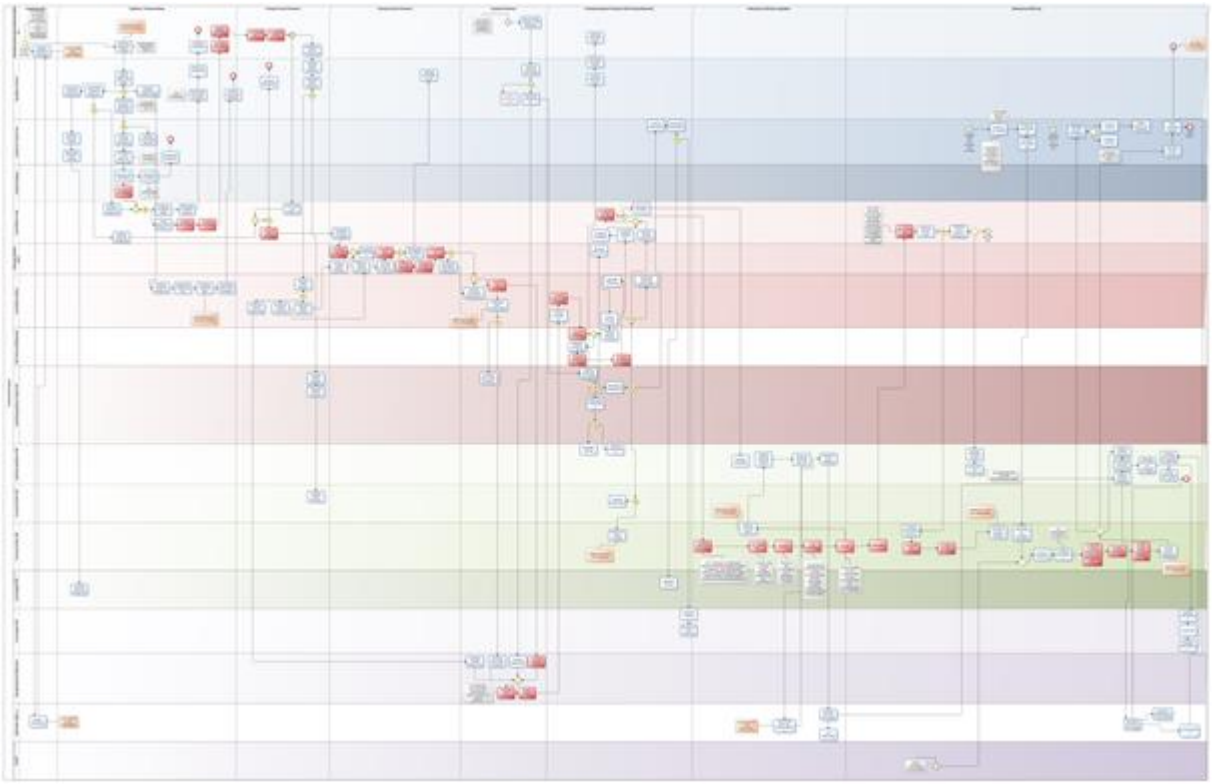


Abbildung 8: Prozesse des Mustertransportszenarios mit BizAgi modelliert

Innerhalb des Arbeitspakets AP1 hat EADS übergreifend die Recherchen und Ausarbeitungen, zu den nachfolgend dargestellten grafischen und tabellarischen Ergebnissen, durchgeführt. Die Recherchen bilden eine essentielle Grundlage zum Gesamtverständnis über die Prozesse ind Interaktionen zwischen den Akteuren bei einem Containertransport als auch über den jeweiligen Daten- bzw. Dokumentenaustausch zwischen den IKT Systemen der verschiedenen Akteure während

eines Containertransports. Die Ergebnisse wurden als Grundlage für die Arbeiten der Projektpartner, als auch für die eigenen Arbeiten in den Unterarbeitspaketen AP17 und AP25/AP26 genutzt.

Die Tabelle 4 zeigt eine Übersicht der möglichen Transportbeteiligten bzw. deren Rolle während eines Containertransports, sowie in Abbildung 9 deren Interaktion innerhalb der Containertransportkette inklusive des Daten- und Dokumentenaustauschs. Es ist zu beachten, dass im realen Containertransportgeschäft typischerweise mehrere der aufgezeigten Rollen durch den selben Transportbeteiligten übernommen und selbst ausgeführt bzw. weiterbeauftragt werden. Es ist nicht immer sofort zu erkennen, welcher Transportbeteiligte welche Rollen übernommen hat bzw. ob er sich letztendlich für diese sich verantwortlich zeigt. Diese von Transport zu Transport teils unterschiedliche Rollenverteilung zwischen den Transportbeteiligten sorgt nicht immer für die notwendige Klarheit im Prozess bzgl. Verantwortung und Sicherheit.

Transportbeteiligte bei Containerbehandlung und -transport	
• Frachtführer See	• Frachtführer (Inland)
• Linienagent / Reedereivertreter	• Eisenbahnunternehmen
▪ Stauzentrale	• LKW Transportunternehmen
• Container Frachtführer	• Binnenschiffsunternehmen
▪ Containerdepot	• Leasingunternehmen
▪ Container Terminal	• Schadensbesichtiger
▪ Container Fracht Station (CFS)	• Containerwartung & Reparatur
▪ Stauer	• Hafenbehörden
▪ Ladungskontrolleur	• Zoll
▪ Feeder Services (Küstenschifffahrt)	• Exporteur / Importeur
▪ Spediteur (Verschiffungs- / Fob-)	• Werk (Hersteller / Lieferant)

Tabelle 4: Beschreibung der beim Akteur eingesetzten IKT Systeme

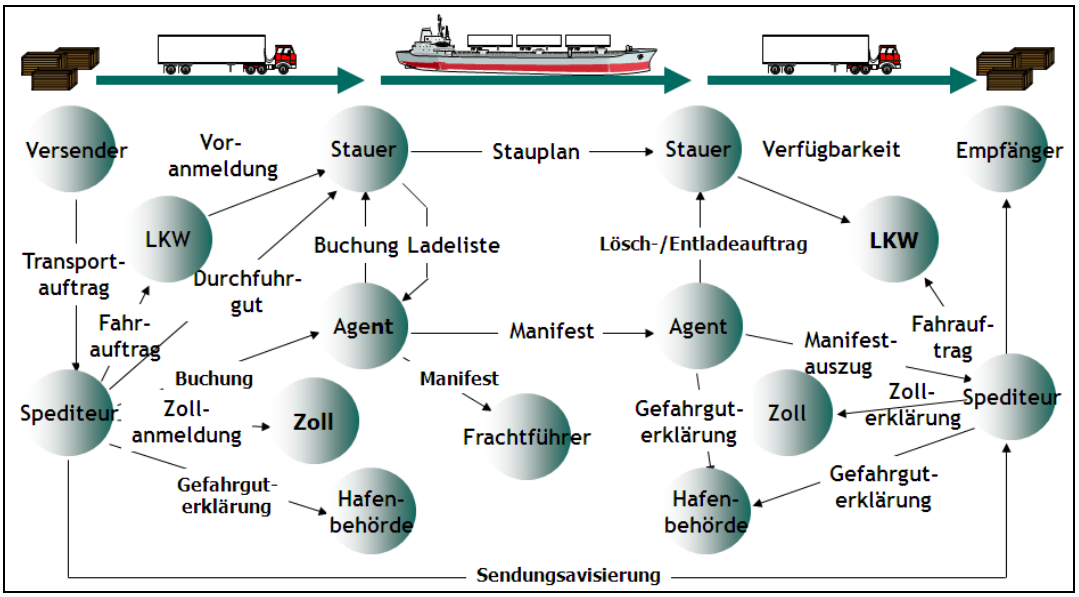


Abbildung 9: Auszug aus dem Daten- und Dokumentenaustauschs entlang der Containertransportkette

In Abbildung 10 ist beispielhaft ein typischer Export Prozess sequentiell aufgezeigt, d.h. den Interaktionen und Handlungsablauf der beteiligten Akteure sowie die zur Datenkommunikation verwendeten „United Nations Electronic Data Interchange For Administration, Commerce and Transport“ (UN/EDIFACT) Nachrichten, einem branchenübergreifenden internationalen Standard für das Format elektronischer Daten im Geschäftsverkehr.

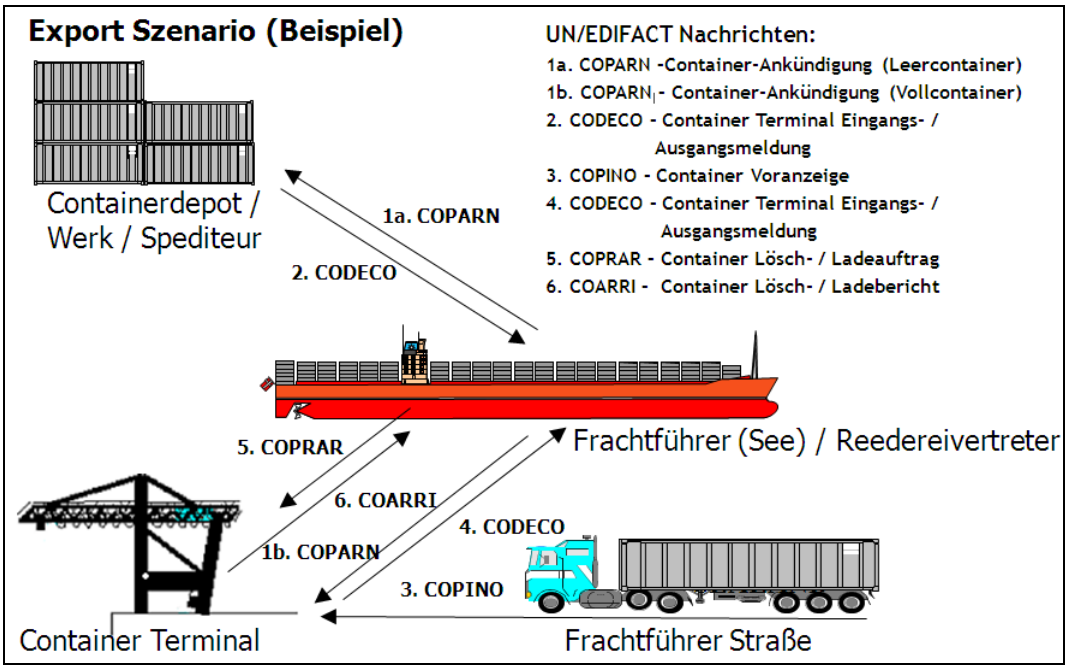


Abbildung 10: Typischer Export Prozess mit Transportbeteiligten und verwendeten UN/EDDIFACT Nachrichten

In Abbildung 11 erfolgt die Beschreibung eines typischen internationalen Containertransports bzw. Auslandsgeschäfts in detaillierter sequentieller Form inklusive der dafür notwendigerweise zwischen den beteiligten Akteuren erstellten und ausgetauschten Dokumente.

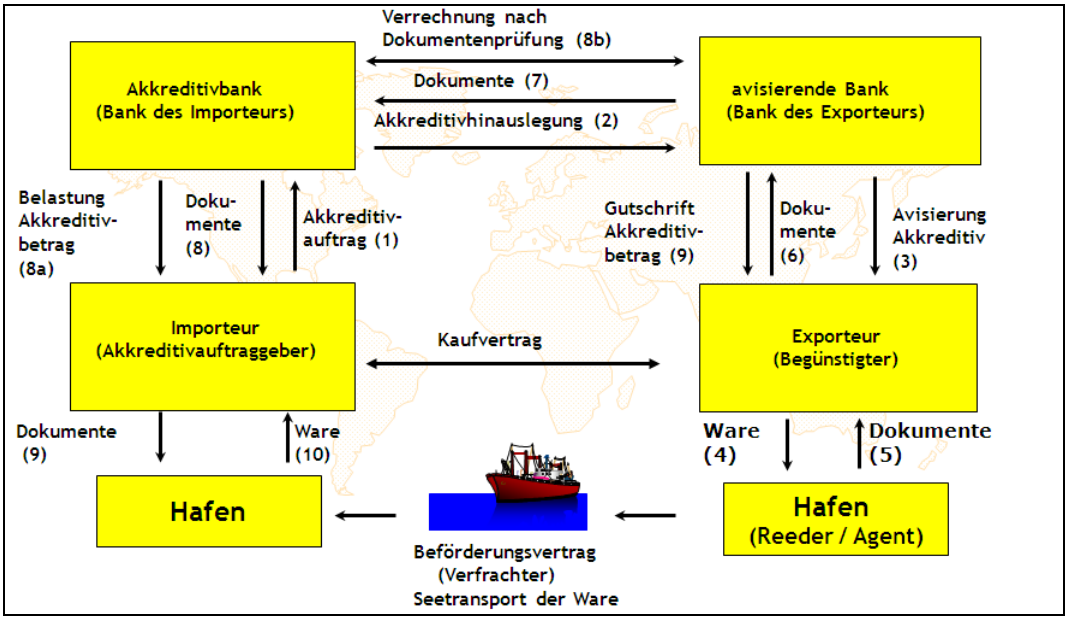


Abbildung 11: Auslandsgeschäft ausgetauschte Dokumente im internationalen Seetransport

Ein Auszug der Beschreibung der „INternational COmmercial TERMS 2000“ (Incoterms 2000) zur Beschreibung der Verantwortlichkeiten bei einem Containertransports zeigt Tabelle 5. Die Darstellung zeigt die verschiedenen Möglichkeiten bzgl. des Übergangs der vertraglichen Verantwortlichkeit beim Containertransport zwischen den verschiedenen Transportbeteiligten.

E-TERMS		F-TERMS	
EXW	Ab Werk	FCA	Frei Frachtführer
		FAS	Frei Längsseite Schiff
		FOB	Frei an Bord
C-TERMS		**D-TERMS**	
CFR	Kosten und Fracht	DAF	Geliefert Grenze
CIF	Kosten, Versicherung und Fracht	DES	Geliefert ab Schiff
CPT	Frachtfrei	DEQ	Geliefert ab Kai
CIP	Frachtfrei versichert	DDU	Geliefert unverzollt
		DDP	Geliefert verzollt

Tabelle 5: Auszug aus der Dokumentation der Incoterms 2000

In Abbildung 12 ist die Beschreibung der Containerabfertigung in einem Containerterminal inklusive des Import- und Exportvorgangs dargestellt. Die verschiedenen dargestellten Vorgänge beschreiben umfassend das Handling eines Containers von Beginn an im Containerdepot, über das Beladen als Teilladung oder Komplettladung eines Containers über den Transport, des Entladen bin wieder zurück ins Containerdepot.

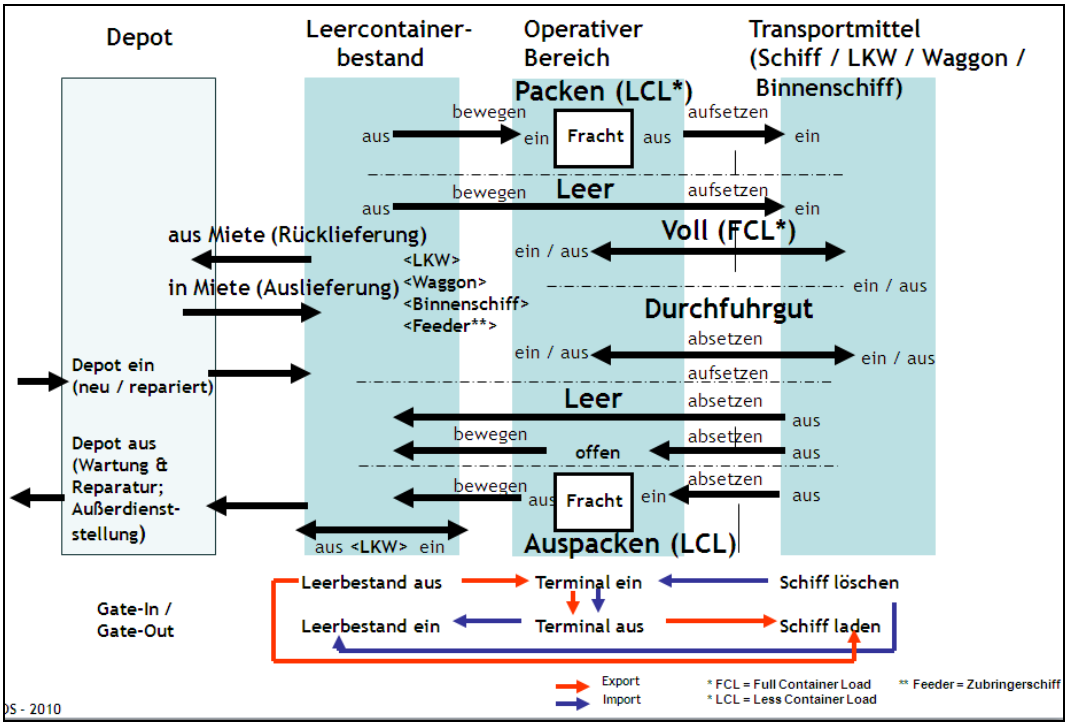
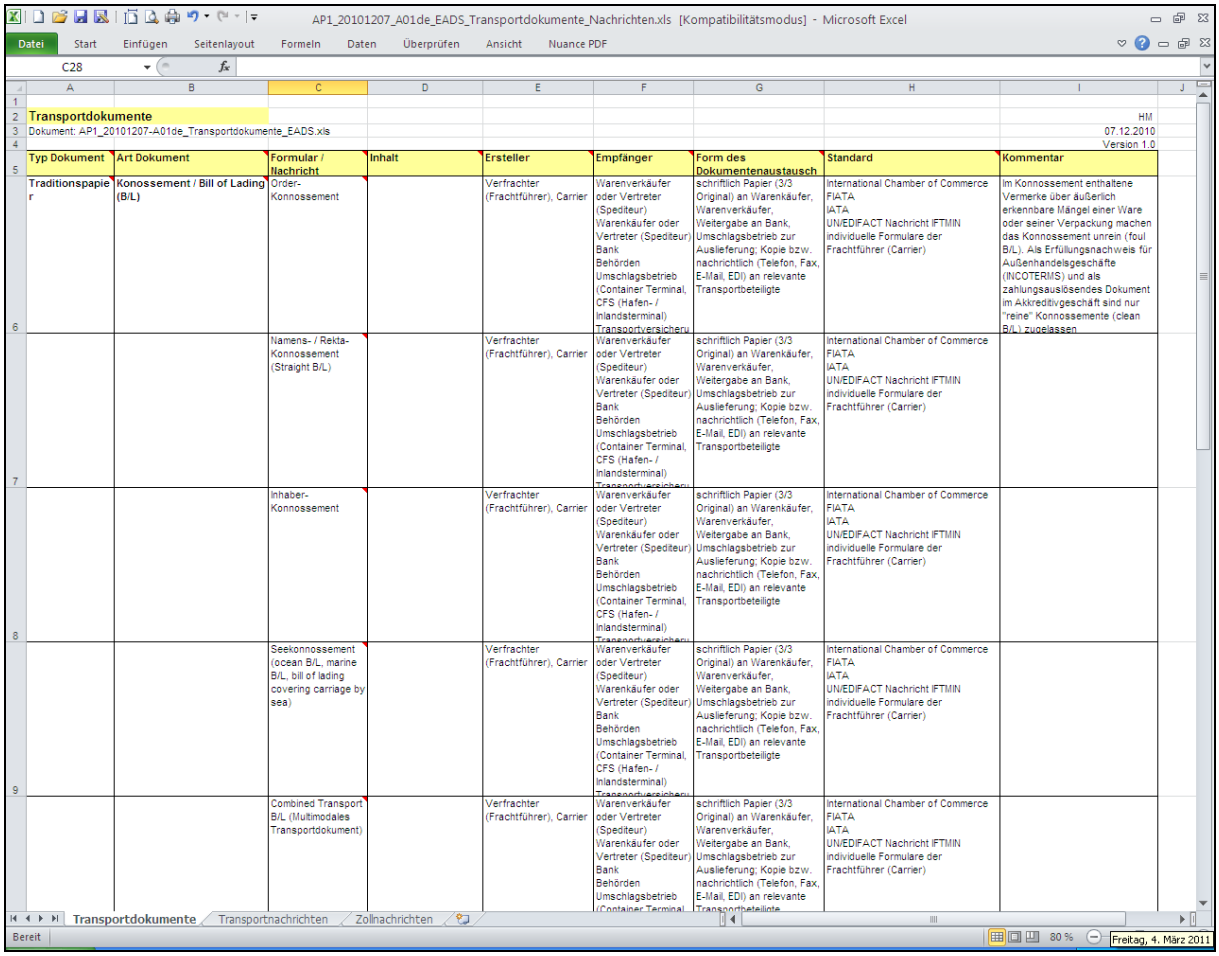


Abbildung 12: Abwicklung Container Export / Import am Container Terminal im Hafen

Die Tabelle 6 zeigt eine detaillierte Beschreibung aller während eines Containertransports ausgetauschten Transportdokumente, Transportnachrichten und Zollnachrichten. Hierbei wurden Parameter wie Dokumententyp, Dokumentart, Ausprägung des Dokuments (Formular/Nachricht), Inhalt, Ersteller, Empfänger, Form des Dokumentenaustauschs, verwendete Standards für das Dokument und dessen Übermittlung sowie zusätzliche ergänzende Informationen (Kommentare) erfasst und beschrieben.



Transportdokumente

Dokument: AP1_20101207-A01de_Transportdokumente_EADS.xls

HM
07.12.2010
Version 1.0

Typ Dokument	Art Dokument	Formular / Nachricht	Inhalt	Ersteller	Empfänger	Form des Dokumentenaustausch	Standard	Kommentar
Traditionspapier	Konossement / Bill of Lading (B/L)	Order-Konnossement		Verfrachter (Frachtführer), Carrier	Warenverkäufer oder Vertreter (Spediteur) Warenkäufer oder Vertreter (Spediteur) Bank Behörden Umschlagsbetrieb (Container Terminal, CFS (Hafen- / Inlandsterminal) Transportversicheru	schriftlich Papier (3/3 Original) an Warenkäufer, Warenverkäufer, Weitergabe an Bank, Umschlagsbetrieb zur Auslieferung; Kopie bzw. nachrichtlich (Telefon, Fax, E-Mail, EDI) an relevante Transportbeteiligte	International Chamber of Commerce FIATA IATA UN/EDIFACT Nachricht IFTMIN individuelle Formulare der Frachtführer (Carrier)	Im Konnossement enthaltene Vermerke über äußerlich erkennbare Mängel einer Ware oder seiner Verpackung machen das Konnossement unrein (foul B/L). Als Erfüllungsnachweis für Außenhandelsgeschäfte (INCOTERMS) und als zahlungsauslösendes Dokument im Akkreditivgeschäft sind nur "reine" Konnossemente (clean B/L) zugelassen
		Namens- / Rekta-Konnossement (Straight B/L)		Verfrachter (Frachtführer), Carrier	Warenverkäufer oder Vertreter (Spediteur) Warenkäufer oder Vertreter (Spediteur) Bank Behörden Umschlagsbetrieb (Container Terminal, CFS (Hafen- / Inlandsterminal) Transportversicheru	schriftlich Papier (3/3 Original) an Warenkäufer, Warenverkäufer, Weitergabe an Bank, Umschlagsbetrieb zur Auslieferung; Kopie bzw. nachrichtlich (Telefon, Fax, E-Mail, EDI) an relevante Transportbeteiligte	International Chamber of Commerce FIATA IATA UN/EDIFACT Nachricht IFTMIN individuelle Formulare der Frachtführer (Carrier)	
		Inhaber-Konnossement		Verfrachter (Frachtführer), Carrier	Warenverkäufer oder Vertreter (Spediteur) Warenkäufer oder Vertreter (Spediteur) Bank Behörden Umschlagsbetrieb (Container Terminal, CFS (Hafen- / Inlandsterminal) Transportversicheru	schriftlich Papier (3/3 Original) an Warenkäufer, Warenverkäufer, Weitergabe an Bank, Umschlagsbetrieb zur Auslieferung; Kopie bzw. nachrichtlich (Telefon, Fax, E-Mail, EDI) an relevante Transportbeteiligte	International Chamber of Commerce FIATA IATA UN/EDIFACT Nachricht IFTMIN individuelle Formulare der Frachtführer (Carrier)	
		Seekonnossement (ocean B/L, marine B/L, bill of lading covering carriage by sea)		Verfrachter (Frachtführer), Carrier	Warenverkäufer oder Vertreter (Spediteur) Warenkäufer oder Vertreter (Spediteur) Bank Behörden Umschlagsbetrieb (Container Terminal, CFS (Hafen- / Inlandsterminal) Transportversicheru	schriftlich Papier (3/3 Original) an Warenkäufer, Warenverkäufer, Weitergabe an Bank, Umschlagsbetrieb zur Auslieferung; Kopie bzw. nachrichtlich (Telefon, Fax, E-Mail, EDI) an relevante Transportbeteiligte	International Chamber of Commerce FIATA IATA UN/EDIFACT Nachricht IFTMIN individuelle Formulare der Frachtführer (Carrier)	
		Combined Transport B/L (Multimodales Transportdokument)		Verfrachter (Frachtführer), Carrier	Warenverkäufer oder Vertreter (Spediteur) Warenkäufer oder Vertreter (Spediteur) Bank Behörden Umschlagsbetrieb (Container Terminal,	schriftlich Papier (3/3 Original) an Warenkäufer, Warenverkäufer, Weitergabe an Bank, Umschlagsbetrieb zur Auslieferung; Kopie bzw. nachrichtlich (Telefon, Fax, E-Mail, EDI) an relevante Transportbeteiligte	International Chamber of Commerce FIATA IATA UN/EDIFACT Nachricht IFTMIN individuelle Formulare der Frachtführer (Carrier)	

Tabelle 6: Auszug aus der Beschreibung der ausgetauschten Transportdokumenten, Transportnachrichten und der Zollnachrichten

Die Abbildung 13 zeigt eine schematische Darstellung der Funktionalität des Zoll-Systems ATLAS (Automatisiertes Tarif- und Lokales Zoll-Abwicklungs-System), welches von den deutschen Zollbehörden den Akteuren bereitgestellt und letztendlich zur Zollabwicklung genutzt wird.

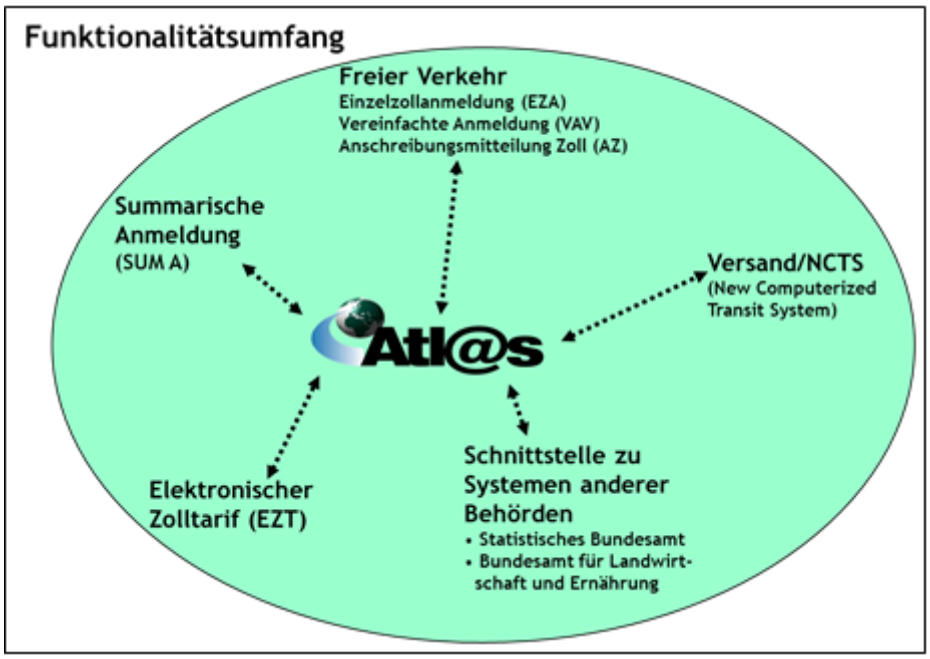


Abbildung 13: Schematische Darstellung der Funktionalität des Zoll-Systems ATLAS

Der große Arbeitsschwerpunkt seitens EADS lag innerhalb Arbeitspaket AP1 in der Ausarbeitung einer IKT Architektur in Unterarbeitspaket AP17.

Hierbei war der Arbeitsgegenstand fokussiert auf

Analyse und Bewertung sowie prozessbezogene Definition der Anforderungen der sicherheitsorientierten Informations- und Kommunikationsarchitekturen sowie der entsprechenden Technologien. Definition und Entwicklung einer lückenlosen und sicherheitsorientierten IKT Gesamtarchitektur. Analyse und Definition eines generischen Datenmodells zum durchgehenden Datenaustausch.

Anforderungen zur IKT Architektur

Die Anforderungen an die ContainIT IKT Architektur basieren im Wesentlichen auf den heute existenten Strukturen der IKT Systeme der Akteure von Containertransporten, d.h. die heute meist als nur als teilvernetzte Insellösungen vorhandenen IKT Systeme sollen durch ContainIT miteinander vernetzt werden.

In Deutschland z.B. verfügen viele Transportbeteiligte (Im-/Exporteure, Ablader, Produzenten in Industrie, Handelsunternehmen, Speditionen, Frachtführer, Umschlagsbetriebe, Behörden etc.) besonders in der Abwicklung von Containertransporten über IKT-gestützte Systeme und Anwendungen, die auch teilweise untereinander vernetzt sind bzw. miteinander elektronisch kommunizieren können. In aller Regel handelt es sich dabei um Anwendungen zur Erfassung, Aufbereitung und Verarbeitung von Transportdaten. Solche IKT-gestützten Geschäftssysteme werden bei allen Verkehrsträgern (Wasser, Straße, Schiene, Luft) vorgefunden. Deutschland weist eine sehr gute Infrastruktur in diesem Bereich auf.

Mit Bezug zum Verkehrsträger Straße ist die Ausstattung der Fahrzeuge mit On-Bord-Units (OBU) als flächendeckend zu bezeichnen und verfügen regelmäßig über Telematiksysteme und -anwendungen. Die Verkehrsträger Schiene und Binnenschiff sind besonders bei der Bahn mit entsprechenden IKT-gestützten Systemen ausgestattet, jedoch vorwiegend für interne Zwecke mit proprietären Standards.

Derzeit besteht in Deutschland kein flächendeckender Datenstandard nach Struktur (Aufbau), Format, Umfang und Inhalt. Eine entsprechende Harmonisierung des elektronischen Datenaustausches zum Aufbau eines möglichst einheitlichen Datenstandards auf der Basis internationaler Normen wie UN/EDIFACT und XML (eXtensible Markup Language) unter Berücksichtigung proprietärer Anforderungen aus Wirtschaft und Verwaltung ist anzustreben.

Die größten deutschen Seehäfen Hamburg und die Bremischen Häfen (Bremerhaven, Bremen) verfügen seit den 1980-Jahren über Datenkommunikationssysteme, um die Daten zwischen den am Transport und Umschlag beteiligten Unternehmen nach festen lokalen Regeln auszutauschen. Neben der Funktion als Datenkommunikationssystem werden hierbei auch IKT Anwendungen als Application Service Provider (ASP) für Unternehmen aus verschiedenen Branchen, z.B. Spedition, Handel und Industrie, Frachtführer, angeboten, welche die zollseitige Abwicklung von Aus-/Einfuhren von Waren und die elektronische Kommunikation mit dem Zollsystem ATLAS (Automatisiertes Tarif- und Lokales Zoll-Abwicklungs-System) ermöglichen. Heute sind alle an der Zollabwicklung Beteiligten verpflichtet die Daten elektronisch beim Zoll einzureichen. Die entsprechenden Bescheide und Genehmigungen werden ebenfalls den Beteiligten elektronisch vom Zoll zur Verfügung gestellt.

In Abbildung 14 sind die teilvernetzten Insellösungen dargestellt (wie zuvor schon in Abbildung 3 gezeigt), und wie diese prinzipiell zur ContainIT IKT Plattform miteinander vernetzt werden. Die Erweiterung ist dargestellt durch rote Verbindungslinien und das zentrale rote Symbol für ContainIT.

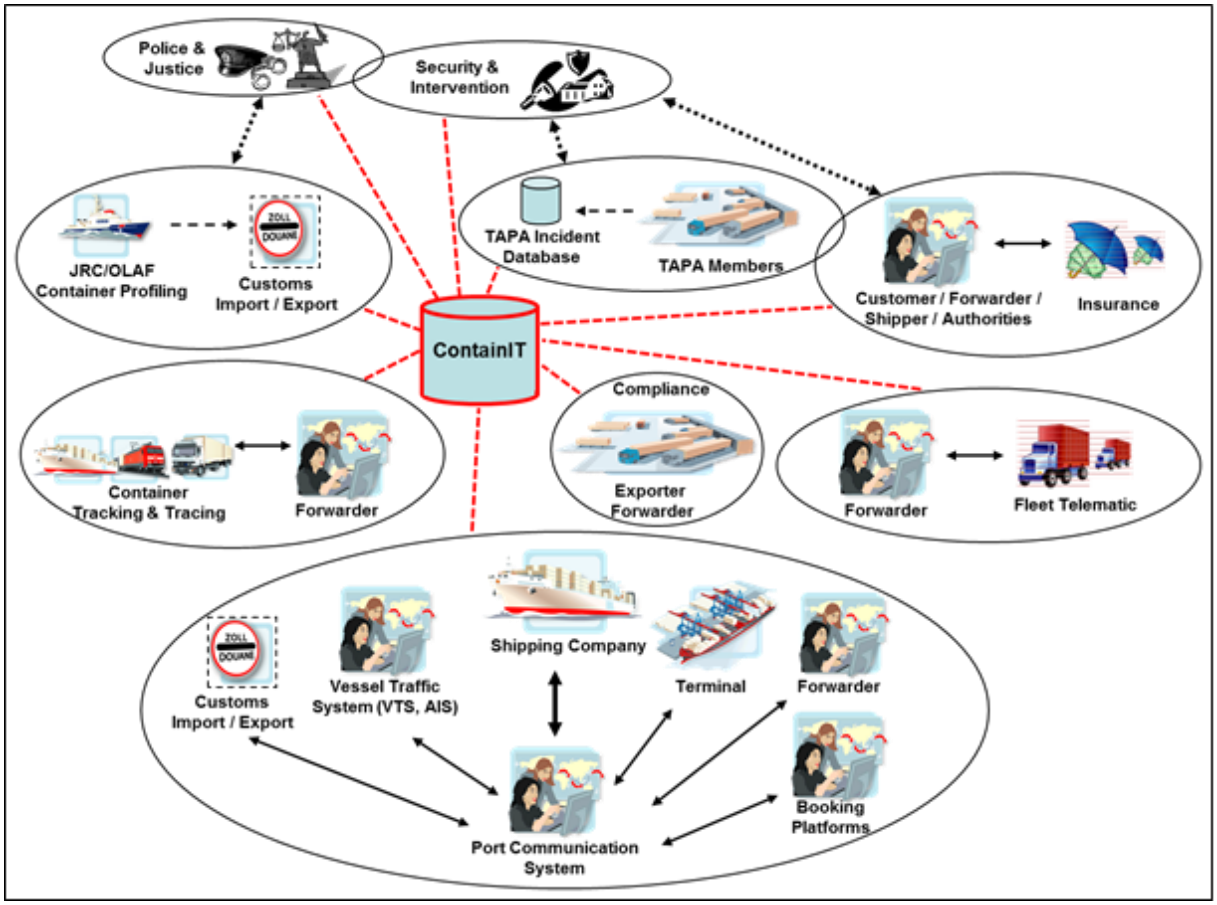


Abbildung 14: Prinzipiell zur ContainIT Plattform vernetzte IKT Insellösungen der Akteure

Bei genereller Betrachtung des Transportes und der Logistik von Containern sind eine große und variantenreiche Anzahl von Transport- und Logistikketten, Arbeitsabläufen (work flow), Transportarten und -typen, Transportmittel, Beteiligten und Branchen mit unterschiedlichen individuellen Kommunikations- und Kooperationsabsichten vorzufinden. Dieses manifestiert sich ähnlich in der Vielzahl der eingesetzten IKT Lösungen bei den verschiedenen Beteiligten in Transport und Logistik.

Alle diese Systeme sind entwickelt worden, um die Vielfalt in Transport und Logistik abzubilden. Mehrheitlich sind diese Systeme individualisiert auf Unternehmen zugeschnitten und dienen regelmäßig den Anforderungen eines Unternehmens, andere sind standardisiert für eine Gruppe von Unternehmen oder für eine gesamte Branche. In manchen dieser Systementwicklungen fehlt jedoch die Fähigkeit des automatisierten Datenaustausches nach standardisierten Datenformaten und damit die Interkonnektivität und Interoperabilität.

Daneben agieren Behörden als genehmigungspflichtige Aufsichtsinstitutionen, z.B. Zoll, Gefahrgutüberwachung, Gesundheitsamt, Pflanzenschutzamt, um den grenzüberschreitenden Containerverkehr bzw. die Aus- und Einfuhrabwicklung von Waren zu überwachen und zu kontrollieren.

Alle diese Akteure verfügen regelmäßig über eigene IKT-gestützte Anwendungen, die entsprechend für die Unternehmen maßgeschneidert programmiert wurden. ContainIT soll sicherstellen, dass mit begrenztem Aufwand und ohne große Änderungen eine Kopplung dieser proprioritären Systeme mit der ContainIT Plattform ermöglicht wird. Dazu gehört die Berücksichtigung unternehmensindividueller Verarbeitungsabläufe, Schnittstellen und Datenstrukturen.

Es ist notwendig, dass die bestehenden IKT Systeme der Akteure mit begrenztem Aufwand und ohne große Änderungen an die ContainIT Plattform angekoppelt werden können. Zu diesem Zweck werden sowohl generische als auch standardisierte Schnittstellen für Nutzer der Plattform angeboten. Die bereits heute von verschiedenen Akteuren wie z.B. den Hafenkommunikationssystemen von DAKOSY oder dbh bzw. von Reedereien oder Spediteuren angebotenen standardisierten Schnittstellen sollen hierzu weiterhin genutzt bzw. zukünftig deren Nutzung als eigenständige Dienstleistung zur Datenbereitstellung für ContainIT angeboten werden.

ContainIT sollte hierbei die bestehenden IKT Strukturen in den Unternehmen nicht wesentlich beeinflussen oder verändern. Es wird angestrebt, dass wo immer möglich, entsprechende bestehende Standards oder quasi Standards auf höchst möglichem Niveau angewendet werden. Ein Bündel von typischen standardisierten Schnittstellen soll die problemlose Verbindung zwischen den heutigen bestehenden Geschäftssystemen der Wirtschaft als auch Behörden und der ContainIT Plattform schaffen und für zukünftige Anforderungen absichern.

Die Akzeptanz des Marktes, und somit der Erfolg von einer IKT Plattform wie ContainIT, wird also weitgehend davon abhängen, ob und wie solche Marktanforderungen erkannt und umgesetzt werden. Neben den zuvor z.B. genannten standardisierten Schnittstellen ist es jedoch unabdinglich, dass ContainIT einen anerkannten „Trust Level“ für die Akteure bereitstellen kann. Die beteiligten Akteure müssen also darauf vertrauen können, dass die Daten auf der ContainIT Plattform nicht missbraucht werden oder vor Verlust oder Beschädigung gefährdet sind. Weiterhin erwarten die Akteure, dass deren Geschäftsabwicklung weder negativ beeinträchtigt noch wesentlich verändert wird. Der Datenschutz hat daher im Konzept in der Konzeption eine prioritäre Bedeutung.

Eine ContainIT Plattform wird sich zur also zur wirtschaftlichen Neutralität verpflichten müssen und eine Bevorzugung oder Benachteiligung von Unternehmen darf nicht erfolgen. Alle beteiligten Akteure, auch die im wirtschaftlichen Wettbewerb stehen, können davon ausgehen, dass sie keinen Nachteil durch unterschiedliche Behandlung durch die Plattform befürchten müssen. Die Unabhängigkeit und Souveränität der wirtschaftlich Beteiligten bleiben unangetastet.

Wenn möglich, soll die Plattform zusätzlich zu den primären Sicherheitsfunktionalitäten die Möglichkeiten eines wirtschaftlichen Mehrwertes durch die Entwicklung und Bereitstellung von Services mit Zusatznutzen für die Akteure schaffen. Dies kann die Neigung zur Teilnahme und das Interesse der potenziellen künftigen Nutzer an ContainIT steigern. Allerdings darf durch solche Zusatzfunktionen die primäre Funktionalität - die Containersicherheit – nicht ausgehöhlt oder gar ausgehebelt werden.

Letztendlich muss aber die obligatorische Teilnahme an der Sicherheitsplattform durch gesetzliche Grundlagen und Verordnungen geregelt werden, da nur so eine umfassende Erfassung aller Containertransporte und somit eine lückenlose sicherheitstechnische Bewertung aller Containertransporte gewährleistet werden kann.

Die Verbreitung von IKT Systemen bei Behörden und hoheitlichen Institutionen ist ebenso bereits weit fortgeschritten. Die Abwicklung erfolgt in manchen Bereichen bereits überwiegend papierlos und bei der Abwicklung von Ein- und Ausfuhren durch die Behörden müssen bereits heute viele Daten elektronisch zur Prüfung bzw. zur Anmeldung oder Genehmigung übermittelt werden.

Es ist, wenn immer möglich, sicherzustellen, dass alle relevanten Sicherheitsbehörden und Ämter, die zur Risikobeurteilung, Risikomanagement und Intervention mit eingebunden werden wie z.B. das Bundeskriminalamt (BKA), Landeskriminalämter (LKA), Zollkriminalamt (ZKA), Bundespolizei, etc. sowie evtl. Organisationen, die bei Vorliegen sicherheitsrelevanter Tatbestände bzw. im Schadensfall mit hinzugerufen werden wie z.B. Feuerwehr, Technisches Hilfswerk (THW), etc.

Zur Einbindung von Behörden an die ContainIT Plattform sind unter anderen folgende Punkte zu berücksichtigen:

- Politische Klärung der Zuständigkeiten seitens Behörden und Ministerien, damit z.B. hierbei anfallende Kosten durch entsprechende Haushaltsplanungen berücksichtigt werden können oder auch das jeweilige Mandat verschiedener Behörden untereinander klar geregelt ist.
- Die Einrichtung von „Zentralen Sicherheitszentren“ unter Beteiligung verschiedenster Behörden wie z.B. Zoll, Bundespolizei, Hafenbetreiber, Verbände ist aufgrund von Erfahrungen seitens der Behörden sehr zielführend, um Informationsflüsse und somit deren Effektivität zu optimieren.
- Bzgl. des Zugriffs und der Nutzung von Daten und Informationen sind ebenso klare Regelungen zu vereinbaren und strikt einzuhalten, wie z.B. Einrichtung von allgemein zugänglichen, privat-wirtschaftlichen und hoheitlichen Bereichen (bzw. auch gemischte Bereiche). D.h. die Verfahren, Struktur, Inhalt und Umfang der unmittelbaren Zugriffsmöglichkeiten zur Nutzung muss entsprechend der verschiedenen Nutzerprofile festgelegt werden.
- Eine „Erkenntnisdatenbank“ mit sicherheitsrelevanten Informationen darf nur von hoheitlichen Stellen verwendet werden.

Das Thema Sicherheit spielt in der Gesellschaft in der Wahrnehmung und Bedeutung eine zunehmend stärkere Rolle. Daher müssen grundrechtliche, ethische oder auch soziologische Aspekte umfassend berücksichtigt werden, wenn eine solche Sicherheitsplattform Akzeptanz in der Gesellschaft finden soll. Hierzu gehören Aspekte wie z.B. der Schutz des Individuums, die Wahrung der Privatsphäre oder auch datenschutzrechtliche Aspekte, die unbedingt im Gesamtkonzept einer solchen Sicherheitsplattform berücksichtigt werden müssen.

Mit Hinblick auf die Situation, Anforderungen und Bedürfnisse neben Deutschland, d.h. in Europa und anderen Ländern kann zusammengefasst werden:

In Deutschland bestehen bereits flächendeckende Infrastrukturen, um einen leistungsfähiges Netzwerk zum Datenaustausch von sicherheitsrelevanten Daten einführen zu können. In den Seehäfen bestehen darüber hinaus bereits leistungsfähige Datenkommunikationssysteme, die den geplanten Einsatz einer Sicherheitsplattform unterstützen können, um die Datenströme der Akteure an der Sicherheitsplattform zu bündeln und / oder zu verteilen. IKT gestützte Anwendungen für den Containertransport sind bei vielen Beteiligen vorhanden und beim Zoll besteht ebenfalls ein flächendeckendes verpflichtendes Zolldokumentationssystem.

In den europäischen industrialisierten Ländern finden wir ähnliche Strukturen wie in Deutschland vor, jedoch nicht immer in der flächendeckenden Verbreitung. Alle großen europäischen Seehäfen, z.B. Rotterdam, Antwerpen, Le Havre, betreiben ebenfalls entsprechende Hafenkommunikationssysteme. Behörden, hier insbesondere der Zoll, arbeiten an einem integrierten europaweiten Anwendungssystem, das bereits in Teilen eingeführt wurde. In den Unternehmen, die sich mit Containertransporten beschäftigen, sind regelmäßig IKT Infrastrukturen vorzufinden. Jedoch herrschen noch Inkompatibilitäten zwischen den Informationen und Daten der Unternehmen, bedingt durch unterschiedliche Verfahren, Dateninhalte und Sprache.

In Nordamerika ist die Situation ähnlich wie in Europa zu beurteilen. Die dortigen Seehäfen verfügen regelmäßig ebenfalls über leistungsfähige Hafenkommunikationssysteme. Da in Nordamerika der Großteil der Waren im Container befördert wird, sind entsprechende IKT-gestützte Anwendungen im Einsatz. Im Bereich der Sicherheit und des begleitenden Datenaustausches nimmt die USA eine führende Rolle ein, auch bedingt durch den Terroranschlag vom 11. September 2001 in New York und die entsprechenden Folgen, die zu vielen Initiativen im Sicherheitsbereich geführt haben: Daraus haben sich konkrete Vorhaben gebildet, die letztlich die gesamte Betrachtung und Bewertung von Sicherheit global beeinflusst haben.

Die Situation in Asien ist geprägt, dass es nur in den Ballungszentren wie z.B. Singapur, Hongkong und in den industrialisierten Staaten wie Japan, Südkorea, Taiwan und teilweise in der Volksrepublik China entsprechende IKT Strukturen gibt, wobei die größten Seehäfen ebenfalls über entsprechende Hafenkommunikationssysteme verfügen. Eine flächendeckende Infrastruktur ist regelmäßig nicht vorhanden. IKT-gestützte Anwendungen sind bei größeren Unternehmen der Transportbranche im Einsatz.

Die Situation in Afrika zeichnet sich dadurch ein, dass es nur im südlichen Afrika Ansätze für eine entsprechende IKT Infrastruktur gibt, ansonsten ist keine vorhanden, aber wohl auch nicht notwendig, weil der containergestützte Warenverkehr im Verhältnis zu anderen Relationen wesentlich weniger entwickelt ist.

In Südamerika finden sich nur in den Großstädten entsprechende IKT Infrastrukturen, wobei Chile bereits eine sehr fortschrittliche und führende Rolle für Südamerika einnimmt. Ansonsten kann von einer flächendeckenden IKT Infrastruktur keine Rede sein.

Zusammengefasst kann jedoch gesagt werden, dass beginnend z.B. mit Deutschland oder Europa ein IKT basiertes System zur Containersicherheit aufgebaut werden kann Hierbei sind bereits bestehende IKT Strukturen unbedingt und direkt in die ContainIT (oder vergleichbare) IKT Architektur zu übernehmen. Dies ist notwendig, um finanzielle und technische Aufwände auf ein notwendiges Minimum zu begrenzen, aber vor allem um die Akzeptanz und Bereitschaft zur Beteiligung an einer Plattform wie ContainIT durch die Transportbeteiligten zu maximieren.

Heutige Ansätze wie bei Dakosy oder dbh (Seehäfen von Hamburg und Bremen) basierend auf einer stabilen Datenkommunikation mit unterschiedlichen Zugangsmöglichkeiten (EDI (Electronic Data Exchange), Web, E-Mail etc.), der Bereitstellung von homogenen Schnittstellen und Datenstrukturen zum standardisierten und harmonisierten Empfang, Verarbeitung und Weitergabe der Daten sollten konsequent weiterverfolgt werden.

Alle beteiligten und angeschlossenen IKT Systeme sollten dabei autark bleiben. Einige der wenigen notwendigen Anpassungen sind die Berücksichtigung und Anwendung der Regeln, Konventionen und Prozeduren der IKT Plattform, um die Kompatibilität und die Interoperabilität innerhalb der heterogenen Anwendungslandschaft zu sichern.

IKT Gesamtarchitektur

Die Struktur, Funktionen und somit die IKT Architektur der ContainIT Plattform kann kurz wie folgt zusammengefasst werden:

Die ContainIT Plattform dient als „Datendrehscheibe“ zur Aufnahme bzw. Vorverarbeitung operativer und administrativer Nachrichten, Informationen und Daten zu einem Containertransport. Hierbei sollen die innerhalb der ContainIT Plattform aufbereiteten Daten bzgl. sicherheitsrelevanter Tatbestände untersucht und bewertet werden. Der jeweilige Sicherheitslevel des einzelnen Containertransportes wird bewertet und abgebildet und gegebenenfalls sind entsprechende Interventionen bei bzw. ab einem noch festzulegenden Sicherheitslevel durch verantwortliche Stellen anzustoßen.

Die IKT Plattform stellt sich generell in verschieden strukturierten funktionalen Ebenen dar, welche in der nachfolgenden Grafik in Abbildung 15 dargestellt sind.

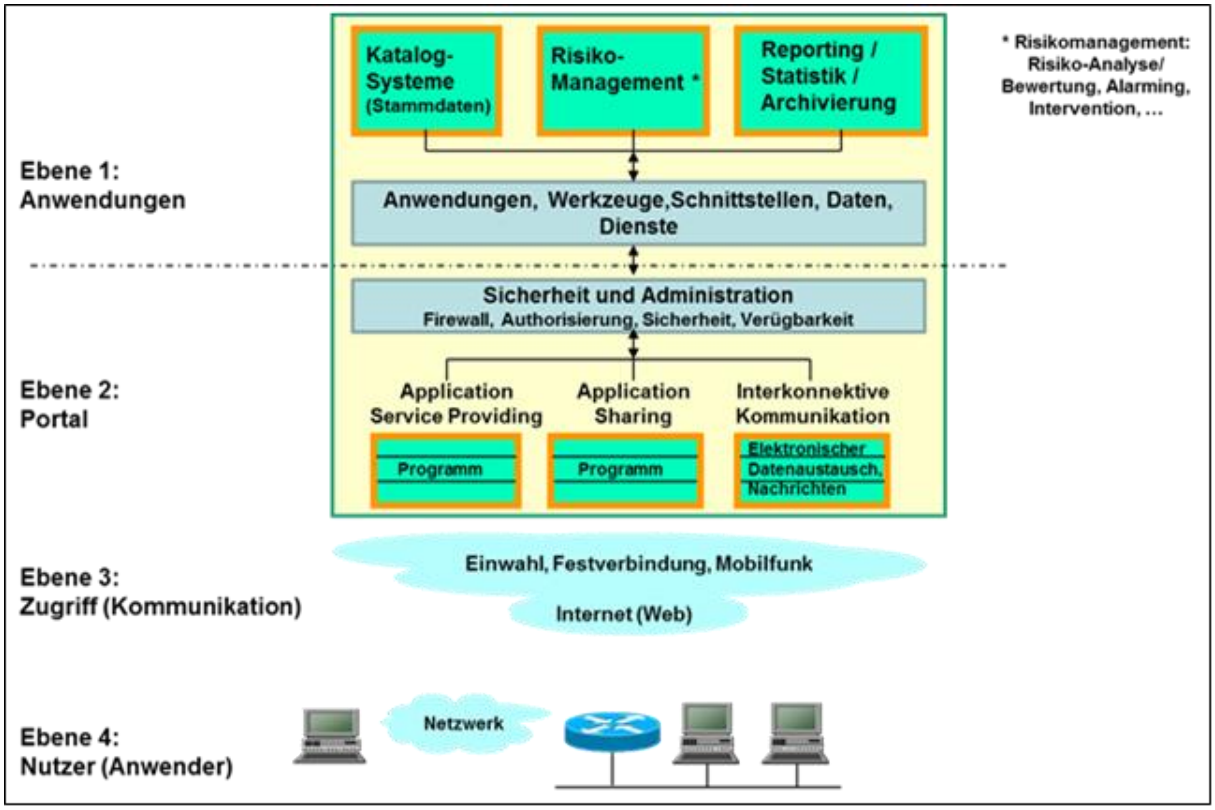


Abbildung 15: Generelle Struktur und Funktionen der ContainIT IKT Plattform

Die Struktur der geplanten IKT Plattform ContainIT ist in vier horizontale Ebenen gegliedert, wobei die unterste Ebene 4 den Nutzer bzw. Anwender repräsentiert. In diesem Sinne wird der Nutzer als ein Plattformpartner mit eigenem autonomen IKT Systemen und individueller Anwendung gesehen. Auf dieser Ebene befinden sich die originären Transportabwicklungssysteme und Datenquellen der Nutzer, aus denen die entsprechenden Daten extrahiert und der Plattform zur Verfügung gestellt werden.

Die Ebene 4 zeigt, dass der Anwender nicht generell mit eigenem System an der Plattform angeschlossen sein muss, sondern auch z.B. über eine webbasierte Anwendung bzw. im Rahmen einer ASP Lösung (Application Service Providing) auf die Plattform zugreift und die Daten intern erfasst. Diese Daten werden dann in der Plattform weiter verarbeitet und aufbereitet.

In Ebene 3 wird der Zugriff auf die IKT Plattform geregelt und die notwendige Datenkommunikation zwischen Teilnehmer bzw. Anwender und IKT Plattform beschrieben. Hierbei kann unter anderem zwischen verschiedenen Arten der Datenkommunikation unterschieden werden:

Die Ebenen 1 und 2 gehören zusammen und sind nur logisch getrennt. Auf der zweiten Ebene, die eng mit der ersten Ebene, der Anwendung verknüpft ist, werden die bereitgestellten Daten der Teilnehmer bzw. Nutzer in der IKT Plattform verarbeitet. Auf dieser Ebene sind auch die Aspekte Datensicherheit und Systemadministration angesiedelt.

In der Ebene 1 befinden sich die interne Anwendungen zur Verarbeitung und Speicherung sicherheitsrelevanter Daten, die benötigten Werkzeuge und Dienste, die die IKT Plattform steuern und die interne Datenkommunikation und -übergabe zwischen den verschiedenen Unteranwendungen in der Rechnerumgebung regeln. Unteranwendungen sind insbesondere das Katalogsystem zur Bearbeitung der Stammdaten, das Risikomanagementsystem, das die empfangenen Daten aus- und bewertet, ob und in welchem Maße Risiken bestehen und weitere Schritte, z.B. Interventionen, notwendig werden. In diesen Bereich gehören auch das Reporting, die Auswertung von Statistiken, die dann wiederum in das Risikomanagement als Erfahrungswerte aufgenommen werden und gegebenenfalls die Sicherheitsbewertungen modifizieren bzw. anpassen und die mittel- bis langfristige Archivierung der Geschäftsvorfälle und deren Daten.

Zwischen Ebene 1 und Ebene 2 finden permanente interaktive Prozesse statt, da sie einander bedingen und zusammenhängen. Hierbei umfassen die Funktionen der Plattform ContainIT drei wesentliche Aktionsbereiche:

- Empfang und die Weitergabe von Nachrichten, Informationen und Daten (Daten-kommunikation, Netzwerkunterstützung, Netzwerkprotokoll, Wiederholung von Datensitzungen, Wiederaufsetzpunkte, Logging etc.)
- Die Verarbeitung und Aufbereitung der Daten zur laufenden Bewertung der Sicherheitslage des Containertransportes erfolgt im Risikomanagement.
- Die Erstellung von generellen und spezifischen Auswertungen zur Dokumentation und Archivierung der Daten zu den bearbeiteten Containertransporten erfolgt im Bereich Reporting, Statistik, Archivierung.

Als Beispiel zu einer vorhandenen standardisierten Schnittstelle, welche auch als Basis für ContainIT weiter verwendet werden soll, kann das „German Port Order“ (GPO) aufgeführt werden. Von Dakosy und dbh, den Herstellern und Betreibern der Hafenkommunikationssysteme der Hamburger Häfen und der Bremischen Häfen, wurde in einem Gemeinschaftsprojekt das „German Port Order“ (GPO) als eine standardisierte Schnittstelle für Electronic Data Interchange (EDI) entwickelt. Ziel war die Bereitstellung einer harmonisierten Beschreibung für die Teilnehmer der Hafenkommunikationssysteme, um eine Kompatibilität zwischen den ansonsten organisatorisch und kommunikationstechnisch unterschiedlichen Systemen herzustellen. Viele Transportbeteiligte versenden bzw. empfangen Güter in den beiden größten deutschen Seehäfen. Nun kann der Teilnehmer, der Transportaufträge oder andere Nachrichten senden und / oder empfangen will, jeweils über sein lokales System das andere Hafenkommunikationssystem erreichen und Hafenaufträge versenden und empfangen. Die Datenstrukturen wurden dabei ebenfalls harmonisiert und kompatibel gestaltet. Anhand dieser Schnittstelle ist es zukünftig möglich, neue Akteure im Bereich der Containertransporte sowie im allgemeinen Kunden der entsprechenden Seehafenterminals auf einfachstem und standardisiertem Wege an die bestehenden Hafenkommunikationssysteme anzubinden. Es besteht auch die Möglichkeit, dass sich inländische Transportbeteiligte an ein Hafenkommunikationssystem anschließen können.

Die IKT Architektur der ContainIT Plattform setzt sich aus mehreren Teilarchitekturen mit teils unterschiedlichen Funktionen zusammen. Grundsätzlich gibt zur Datenaggregation einerseits eine seehafen-zentrierte (Hamburg, Bremerhaven, …) und andererseits eine inländische bzw. Binnenland Teilarchitektur zur Anbindung der am Containertransport beteiligten Akteure.

Der Unterschied zwischen den beiden Teilarchitekturen liegt in den zentralen Kommunikationsknoten, welche einmal durch die Hafenkommunikationssysteme der Seehäfen (z.B. Dakosy oder dbh) und einmal durch große Spediteure (z.B. Kühne + Nagel, DB Schenker Rail oder DHL) oder auch durch Kooperationen für Systemverkehre, d.h. Zusammenschlüsse von Spediteuren (z.B. CTL, CargoLine, GO, Confern oder DTL) gebildet werden.

Die beiden nachfolgenden Grafiken in Abbildung 16 und Abbildung 17 zeigen die seehafen-zentrierte (Hamburg, Bremerhaven, …) und andererseits die inländische bzw. Binnenland Teilarchitektur.

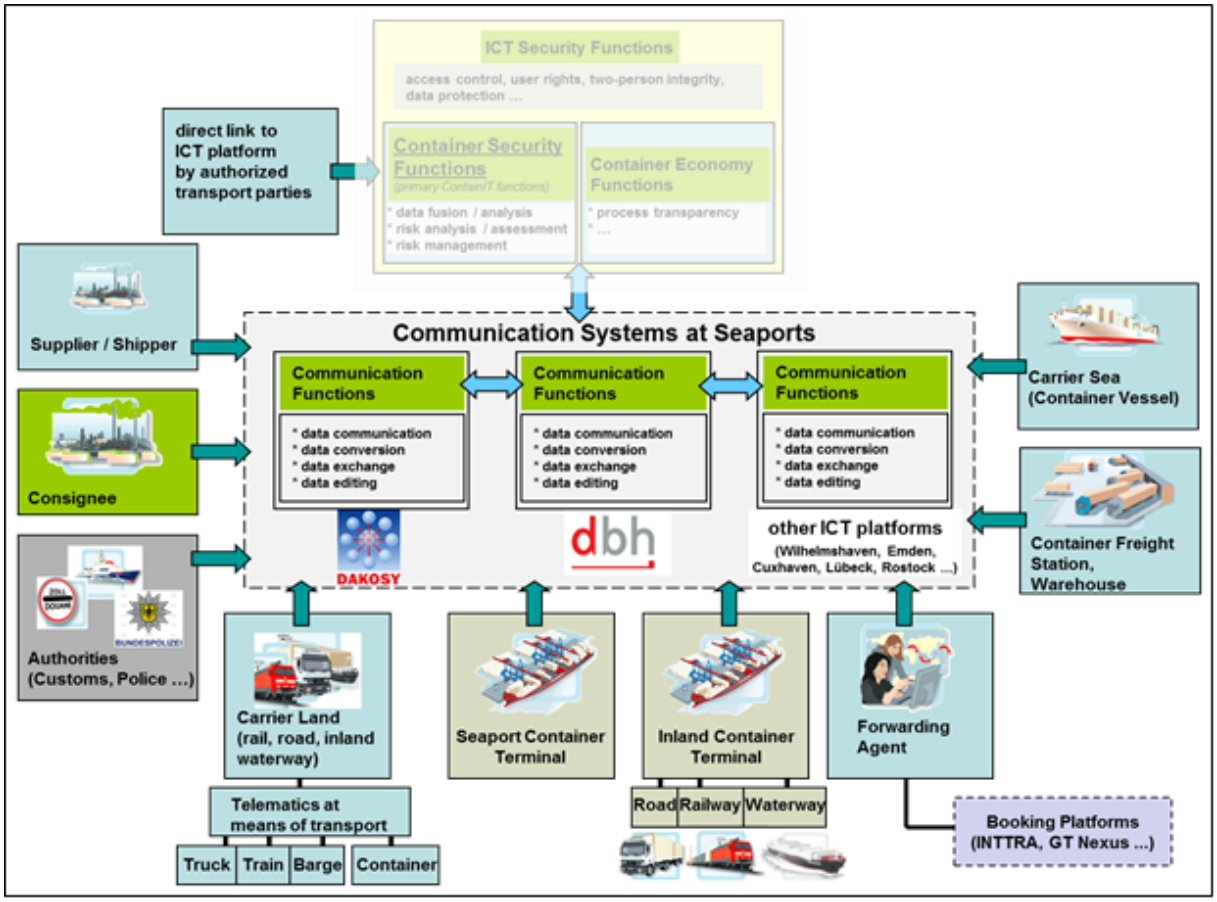


Abbildung 16: IKT Architektur für Seehafen zentrierte Containertransporte

Die vorangegangene Grafik in Abbildung 16 zeigt die generelle Struktur zur Anbindung von seehafen-zentrierten Containertransporten über die in den deutschen Seehäfen vorgefundenen Hafenkommunikationssysteme, an denen wiederum für den Containertransport relevante Branchen, Unternehmen und in Teilen auch Behörden für die Abwicklung von Containertransporten, besonders im Ex- und Import, sich am elektronischen, weitgehend papierlosen, Datenaustausch beteiligen. Diese Hafenkommunikationssysteme werden im Sinne einer Bündelungsfunktion betrachtet und verringern somit die Komplexität zu schaffender Schnittstellen zu den Akteuren. Es bedeutet, dass ein wesentlich höhere Produktivität und quantitative Abdeckung von internationalen Containertransporten bei der Verarbeitung der Daten zu erwarten ist.

Der wesentliche Teil dieser IKT Architektur in den deutschen, aber auch vielen europäischen Seehäfen, ist heute bereits real existent und im Einsatz, wie z.B. in Deutschland die Systeme DAKOSY (Datenkommunikationssystem für den Hafen Hamburg) im größten deutschen Seehafen Hamburg oder bei der dbh (Datenbank Bremische Häfen) in den Bremischen Häfen Bremen und Bremerhaven. Auf diese lokalen Strukturen kann bereits heute direkt zugegriffen werden, d.h. diese können als Kommunikationsknoten („Communication Systems at Seaports“) in die ContainIT IKT Plattform als integriert und genutzt werden.

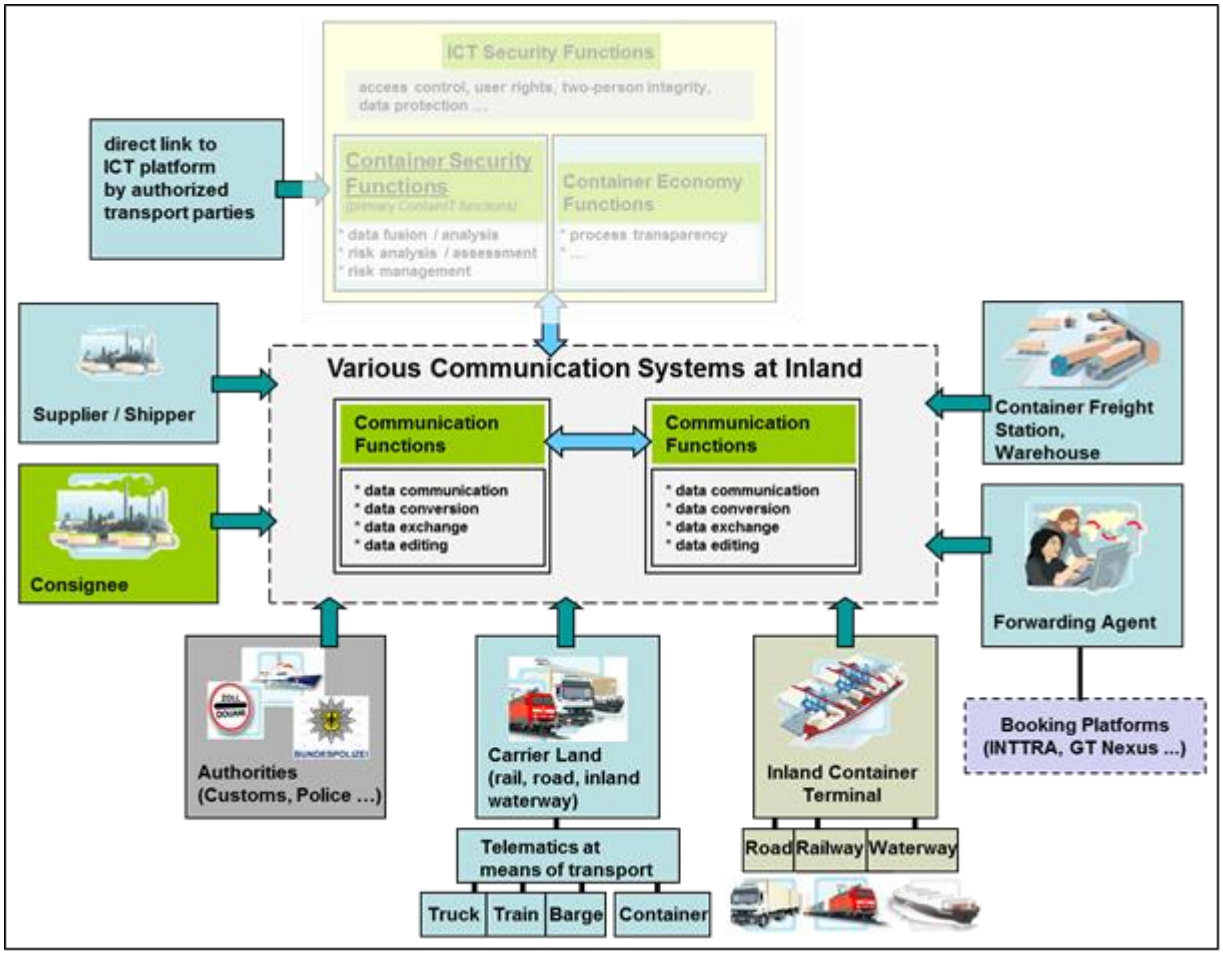


Abbildung 17: IKT Architektur für Inland Containertransporte

Die vorangegangene Grafik in Abbildung 17 zeigt die generelle Struktur und Wirkungsweise der IKT gestützten Integrationsplattform beim Inland Containertransport. In der Fläche sind, bedingt durch unterschiedliche IKT Strukturen bei den Akteuren, derzeit nur geringfügige Bündelungseffekte vorhanden. Regelmäßig kommt es jedoch bereits jetzt schon zu einer Direktkommunikation und zur Verarbeitung von Einzeltransporten bei den Akteuren. Dies hat zur Folge, dass wesentlich mehr Datenkommunikationsverbindungen aufgebaut werden bzw. werden müssen, was jedoch direkt der Sicherheit des Warenverkehrs bei Containertransporten zugutekommt.

Solche IKT Architekturen sind heute bereits bei großen Spediteuren wie z.B. Kühne + Nagel, DB Schenker Logistics, DB Schenker Rail, oder DHL direkt verfügbar. Weiter sind bei Kooperationen für Systemverkehre, d.h. bei Zusammenschlüssen von Spediteuren wie z.B. CTL, CargoLine, GO, Confern oder DTL, ebenso vergleichbare Plattformen existent und bereits im Einsatz.

Diese bereits bestehenden IKT Architekturen können prinzipiell ebenso genutzt und als Kommunikationsknoten („Communication Systems at Inland“) in die ContainIT Plattform integriert werden. Hierzu sind jedoch evtl. Anpassungen bzgl. der Datenstrukturen, Prozesse zur Datenerfassung, … erforderlich.

Die nachfolgende Grafik in Abbildung 18 zeigt die neu zu schaffende Erweiterung für die ContainIT Sicherheitsfunktionalitäten, die Zusammenarbeit mit den entsprechenden Sicherheitsorganen wie z.B. den Zoll- und Polizeibehörden sowie den verschiedenen möglichen Arten der Intervention.

Hierbei sind Aspekte wie z.B. hoheitliche Befugnisse und Aufgaben der verschiedenen Behörden und deren Zusammenarbeit mit privatwirtschaftlichen Betreibern der Plattform im Besonderen zu berücksichtigen.

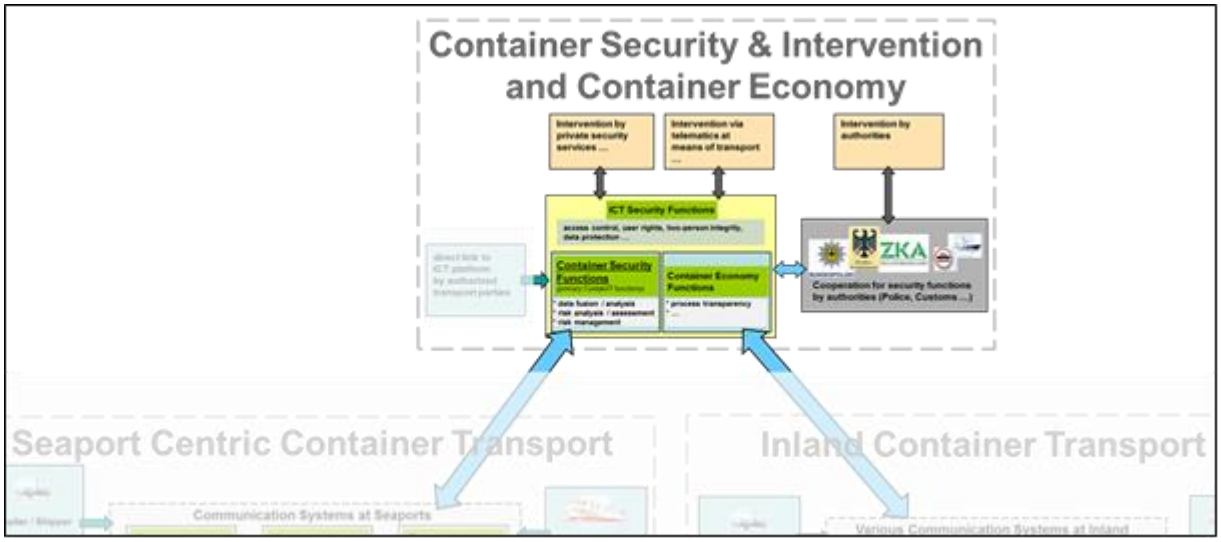


Abbildung 18: Erweiterung der IKT Architektur für Sicherheitsfunktionen, Einbindung von Sicherheitsbehörden und um Intervention zur Containersicherheit

Die Grafik dargestellt in Abbildung 19 bildet den kompletten und generellen Zusammenhang der ContainIT Plattform inkl. der sicherheitsrelevanten Organe auf nationaler Ebene ab. Es wird eine direkte Datenverbindung zwischen der Plattform ContainIT und verschiedenen nationalen Trägern zur sicherheits-orientierten Begleitung des Containers gestützten Warenverkehrs geben. Dies soll jedoch nicht nur eine Abgabe von Daten durch ContainIT sein, sondern auch Erkenntnisse und Daten von den Behörden sollen in die Plattform mit einfließen, berücksichtigt und verarbeitet werden.

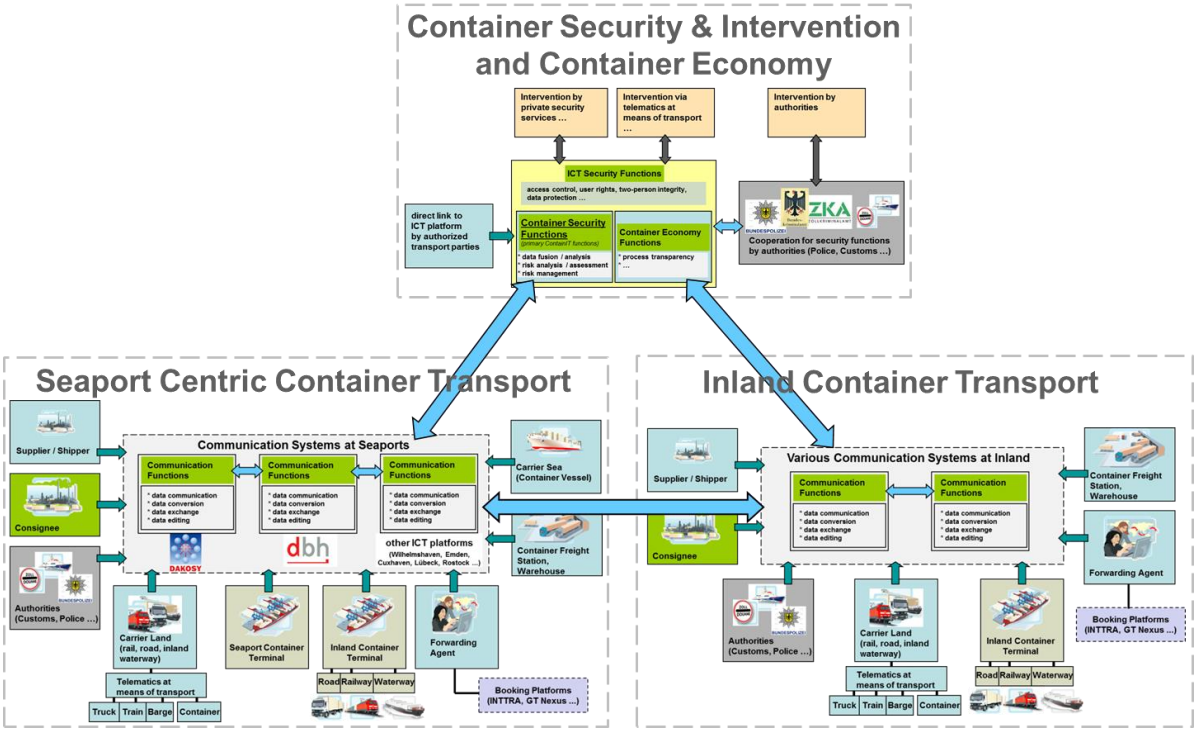


Abbildung 19: IKT Architektur der ContainIT Plattform auf nationaler Ebene

Eine evtl. national beginnende ContainIT Plattform wird und muss mittel- bzw. langfristig auch die Einbeziehung internationaler und globaler Waren- und Containertransportströme anstreben. Dies setzt jedoch voraus, dass sich in anderen Ländern entsprechende Plattformen ebenfalls etablieren und sich miteinander vernetzten. Das gleiche trifft ebenso auf die Kooperation mit den entsprechenden Sicherheitsbehörden zu.

Die nachfolgende Grafik in Abbildung 20 veranschaulicht die Struktur der geplanten IKT-gestützten Integrationsplattform zur Sicherheit des Warenverkehrs bei Containertransporten in seiner letzten Ausbaustufe. Die nationale Plattform ContainIT wird langfristig die Einbeziehung weltweiter Waren- und Containertransportströme anstreben, da der internationale Warenverkehr global ausgerichtet ist und Sicherheit nicht an nationalen Grenzen endet. Dies setzt jedoch voraus, dass sich in anderen Ländern entsprechende Plattformen und Sicherheitssysteme ebenfalls etablieren, damit eine Zusammenarbeit im Bereich der Sicherheit möglich wird.

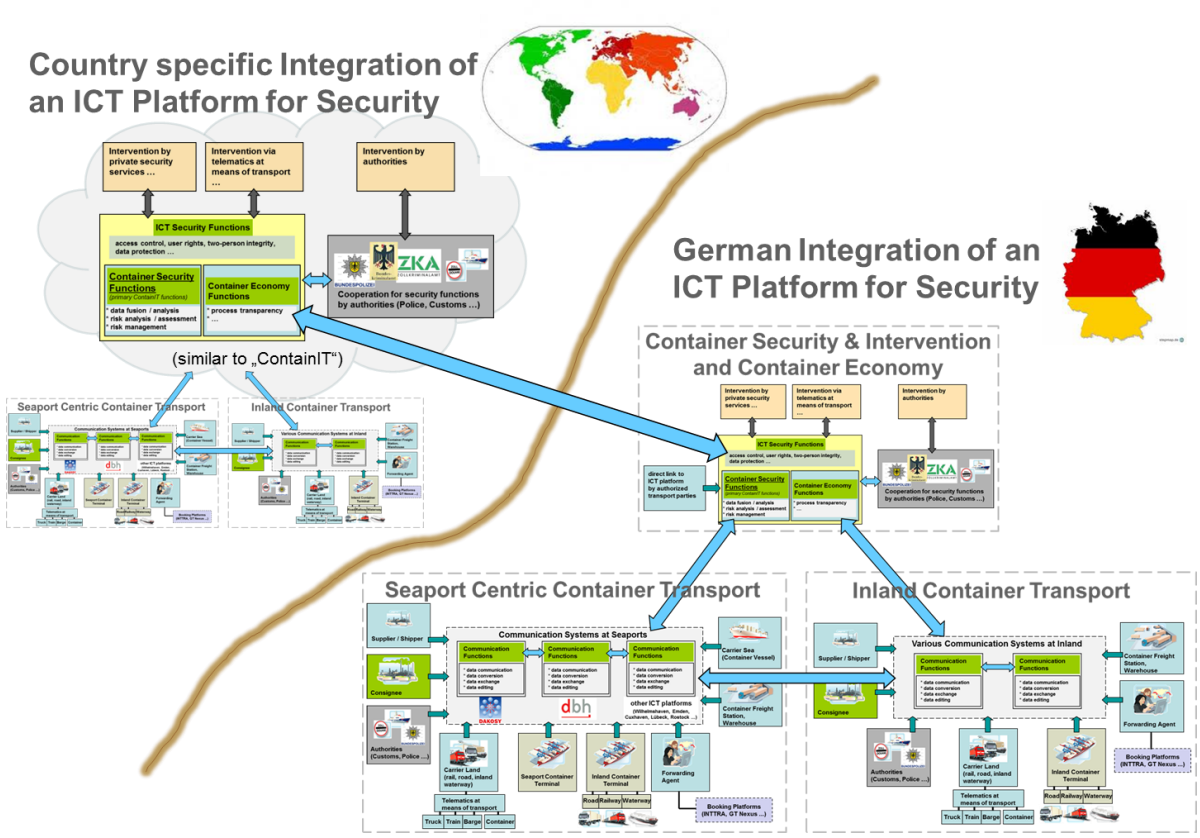


Abbildung 20: IKT Architektur der ContainIT Plattform auf internationaler Ebene

Datenaustausch und generisches Datenmodell

Nachfolgend wird die Kommunikation von Daten und Informationen zwischen den Teilnehmern der ContainIT Plattform beschrieben, insbesondere die Aggregation der Daten und Informationen bis hin zu Ihrer grundsätzlichen weitergehenden Nutzung zur Containersicherheit.

Der Datenaustausch auf der der ContainIT Plattform soll elektronisch erfolgen, d.h. weder sprachlich (Telefon, …) noch schriftlich (Brief, Liste, Fax, …). Dies setzt das Vorhandensein entsprechender elektronsicher Medien voraus.

Bei der Vernetzung zur Nutzung der Plattform spielt die Interoperabilität eine wichtige Rolle. Die außerhalb der Plattform liegenden Systeme verfügen in aller Regel über Kommunikationsverfahren, um mit Dritten zu kommunizieren. Allerdings werden dabei unterschiedliche Kommunikationsprotokolle genutzt, die nicht immer kompatibel miteinander sind. Darüber hinaus verfügen die externen Nutzer über proprietäre Geschäftssysteme, die regelmäßig nicht kompatibel sind und es werden auch unterschiedliche Daten generiert bzw. ist zu prüfen, ob die benötigten Daten auch zur Verfügung gestellt werden können.

Im ersten Schritt müssen daher die Kommunikationsverfahren vereinbart werden. Als Kommunikationsverfahren zum Austausch von Daten sind unter anderen folgenden Zugangsmöglichkeiten generell offen:

- Electronic Data Interchange (EDI, UN/EDIFACT, ...)
- Übermittlung via E-Mail Services
- Übermittlung via Internet
- Übermittlung via mobiler Systeme (On-Board Unit, Mobilfunk, SMS (Short Message Service) etc.)

Daneben kann es notwendig werden, dass auch die Plattform mit Daten versorgt wird, die via Telefon oder Fax kommend, manuell ins System erfasst werden.

Der Datenaustausch auf der ContainIT Plattform hat nach definierten Regeln zu erfolgen.

Generell empfängt die Plattform nur Daten, verarbeitet sie und ermittelt einen Sicherheitslevel aus den empfangenen Daten. Nach erfolgter Analyse und Bewertung wird der gefundene Sicherheitslevel an berechtigte Teilnehmer des Systems zurück gemeldet. Hierbei wird es sich im Wesentlichen um Behörden oder andere Institutionen handeln, die hoheitlich tätig sind und für Sicherheit zuständig sind. Grundsätzlich können Transportbeteiligte keine Daten aus der Plattform abrufen. Dies kann aus Datenschutzgründen nicht erfolgen.

Vor Beginn des physischen Transportes, vor der Containergestellung, werden in der Phase „Transportplanung“ die grundsätzlichen Daten als Plandaten vom verantwortlichen Datenversender (Versender, Spediteur,) an die Plattform ContainIT gesendet, damit ein Gesamttransport (vom ersten Beladeort bis zum letzten Entladeort), der sich in Transportabschnitte aufteilen kann, angelegt wird und eine eindeutige Kennung erhält, die Transport-ID (Identification Number).

Die Grundeinheit ist der Container, der innerhalb eines Transportes das Kernobjekt dar-stellt, da jeder Container einzeln adressierbar sein muss, damit im Falle einer Bedrohung dieser eindeutig ermittelt und identifiziert werden kann.

Bei der Erstanlage wird die Berechtigung des sendenden Transportbeteiligten gegen eine Teilnehmer- und Berechtigungsdatei geprüft, um sicherzustellen, dass die Daten formal korrekt von einem berechtigten Teilnehmer kommen. Die Berechtigungsprüfung prüft, wer welche Daten, wie und wann senden und empfangen kann und darf.

Zu diesem Zweck wird ein Berechtigungsprofil jedes Nutzers erstellt. In dieser Datei wer-den aufgeführt unter anderem:

- Name und Adresse des Transportbeteiligten
- Rolle im Rahmen der Containertransportabwicklung
- Berechtigungsklasse

Es wird jeder Datenempfang inhaltlich und zeitlich protokolliert und archiviert.

Die Transport-ID besteht aus einer Kennung des Erstsendenden und Anleger des Transportes sowie einer entsprechenden Transportreferenz, z.B. SSCC – Serial Shipping Container Code. Diese Transport-ID ist die eineindeutige Referenz über die gesamte Lebensdauer des Containertransportes.

Die Transport-ID dient zusammen mit der (bzw. mehrere) Container-ID (inkl. Zeitstempel) als Referenz zur eindeutigen Kennzeichnung eines Containertransports.

Die Zuordnung von Transport-ID und Container-ID hat zum frühest möglichen Zeitpunkt vom entsprechend verantwortlichen Transportbeteiligten zu erfolgen, z.B. von der Packstation, wenn die Ware in den Container verladen wird oder vom Frachtführer, der die Containergestellung durchführt.

Jeder Transportbeteiligte hat die Daten der für ihn verantwortlichen Transportkette bzw. Transportabschnitte in sequenzieller korrekter Abfolge nach Zeit und Tätigkeit für seinen verantwortlichen Transportabschnitt bzw. der in der Transportkette stattfindenden Aktivitäten an ContainIT in angemessener Frist bei Beginn und Ende und bei Übergabe an den folgenden Transportbeteiligten mitzuteilen.

ContainIT prüft dabei nur zusammenhängende Daten eines Transportes bzw. eines Transportabschnittes und keine Einzeldaten ohne Zusammenhang.

Eine Prüfung und Bewertung eines generellen Sicherheitslevels kann erst dann durchgeführt werden, wenn die erste Nachricht hinsichtlich des physischen Transportflusses eingetroffen ist und mit den im

System vorgehaltenen Plandaten verglichen werden kann.
Bei der Erstanlage des Transportes (Erzeugung Transport-ID) sollten alle bereits bekannten und feststehenden Transportbeteiligten, jedoch mindestens die nationalen, sowie möglichst alle anderen relevanten Informationen zum Transport übermittelt werden.

Zur Ermittlung eines belastbaren Sicherheitslevels für einen Container ist eine minimale Anzahl von notwendigen „Muss-Daten“ zu senden, da sonst keine sinnvolle Prüfung der Daten / Informationen möglich ist und eine zur Containersicherheit gültige Aussage nicht getroffen werden kann.

Weiter werden noch ergänzenden „Kann-Daten“ erhoben werden, welche die notwendigen Daten / Informationen ergänzen oder präzisieren. Beispielsweise kann so neben dem definieren eines Transportbeginns mittels Datumsangabe durch eine entsprechende Uhrzeit präzisiert werden. Ein anderes Beispiel wäre z.B. die Definition einer Transportroute für den Transportverlauf nur durch Angabe eines geografischen Korridors erfolgen oder präziser noch durch die ergänzende der Angabe von Zeitabschnitten gekoppelt mit Abschnitten des geografischen Korridors.

Die Übermittlung von „Optionalen-Daten“ bei besonderen Transporttypen, z.B. bei Gefahrgut oder Wertgut, ist notwendig und erhöht die Aussagekraft der sicherheitsrelevanten Prüfungen.

Ebenso legt ContainIT sogenannte Referenzdaten (d.h. Datenkataloge) als Datenbasis an, um sicherzustellen dass z.B. Gültigkeiten von Schreibweisen und logische Korrektheit wie z.B. Ort und zugehörige Postleitzahl gegeben sind. Diese Referenzdaten werden angelegt für unter anderem Transporttyp, Transportbeteiligte (Namen, Adressen), Orte und Lokationen, Maßeinheiten, internationale Datenstandards (Location Code, Country Code, Packaging Type Code etc.) und Kodierungen, denn nur mittels korrekter Inhalte von Daten / Informationen können automatische und widerspruchsfreie Prüfungen zur Containersicherheit durchgeführt werden.

Als Basis für alle verwendeten Daten / Informationen auf der ContainIT Plattform, wurde basierend auf den vorhandenen realen Datenstrukturen (Transportdokumente, Transportnachrichten, Compliance-Listen, Telematiksysteme für LKW und Container, etc.) eine Art Datenkatalog mit sogenannten Referenzdaten entworfen. Die Katalogdaten sind je nach Art und Herkunft der Daten / Informationen strukturiert in verschiedene Gruppen wie z.B. Transportdokumente, Listen, Transportnachrichten, Telematik Container oder Telematik LKW. Diese Gruppen sind wiederuntergliedert in Untergruppen, welche dann entsprechende Einzelelemente an Daten / Informationen beinhalten. Aufgrund eines eindeutigen, fortlaufenden und erweiterungsfähigen Nummernschemas, ist es möglich jedes Einzelelement der Daten / Informationen eindeutig zu identifizieren.

Die nachfolgenden Tabellen zeigen einen Auszug aus der Liste mit den Referenzdaten von ContainIT.

Gruppen-Nr.	Element-Nr. (mit allen einzelnen Datenelementen)	Gruppe von Daten/Informationen	Bemerkung
0		Transportplanung (Vorstufe zu den Transportdokumenten)	Container- / Transportbuchung / -auftrag
1		Transportdokumente	Bill of Lading (B/L), Frachtbriefe (LKW, Bahn, See, ...)
2		Listen	Compliance, Baykott, Terror, ...
3		Transportnachrichten	UN/EDIFACT Nachrichten zum physischen Container Handling
4		Telematik Container - generisch	allgemeingültige Beschreibung für Telematik Container
4a		Telematik Container - Astrium	dient als Input zur allgemeingültigen Beschreibung der "Telematik Container - generisch"
4b		Telematik Container - Bosch	dient als Input zur allgemeingültigen Beschreibung der "Telematik Container - generisch"
5		Telematik LKW - generisch	allgemeingültige Beschreibung für Telematik LKW
5a		Telematik LKW - FET	dient als Input zur allgemeingültigen Beschreibung der "Telematik LKW - generisch"
6		Telematik Schiff (Binnen)	ist nicht im aktuellen Projektumfang enthalten bzw. nur der definierte Testtransport wird betrachtet
7		Telematik Schiff (See)	ist nicht im aktuellen Projektumfang enthalten bzw. nur der definierte Testtransport wird betrachtet

Tabelle 7: Generelle Struktur der Referenzdaten als Datenkatalog

Gruppen-Nr.	Element-Nr. (mit allen einzelnen Datenelementen)	Gruppe von Daten/Informationen	Daten/Informationen	einzelnes Datenelement	Bemerkung
0		Transportplanung (Vorstufe zu den Transportdokumenten)			Container- / Transportbuchung / -auftrag
1		Transportdokumente			Bill of Lading (B/L), Frachtbriefe (LKW, Bahn, See, ...)
2		Listen			Compliance, Baykott, Terror, ...
3		Transportnachrichten			UN/EDIFACT Nachrichten zum physischen Container Handling
	3.1.1		COSTOR; Auftrag zum Be-/Entladen von Containern	Container ID(s)	
				Reedereicode	die beteiligte Schiffahrtslinie
	3.1.3			Frachtführer	Transportdurchführender
	3.1.4			Spediteur	beteiligter Spediteur
	3.1.5			Kühlaggregatnummer	bei Kühlcontainer
	3.1.6			Temperatur	eingestellte Temperatur bei Abgang / Ankunft
	3.1.7			Gefahrgut ID	
	3.1.8			Gefahrgut ID	Import / Export Kennzeichen
	3.1.9			kennzeichen Leased Container	eigener oder gemieteter Container
	3.1.10			Import / Export	Import / Export Kennzeichen
	3.1.11			Zustand Container	Kennzeichen, ob Beschädigung vorliegt
	3.1.12			Beförderungstyp	LCL / FCL / MT
	3.1.13			Bruttogewicht	
	3.1.14			Nettogewicht	
	3.1.15			Tara	
	3.1.16			Siegeltyp	
	3.1.17			Siegel ID	
	3.1.18			Kilometerstand	bei Ankunft / Abfahrt (LKW)
	3.1.19			Buchungsnummer	
	3.1.20			Freistellungsnummer	
	3.1.21			Warenart	
	3.1.22			HS Code	
	3.2		COARRI; Container Lösch-/Ladebericht	Bewegungsart	Nachrichtentyp
	3.3		CODECO; Container Terminal Eingangs-/Ausgangsmeldung	Bewegungsdatum	tatsächliches Datum der Aktivität (evtl.)

Tabelle 8: Beispielhafte detaillierte Struktur der Referenzdaten der Transportnachrichten

Gruppen-Nr.	Element-Nr. (mit allen einzelnen Datenelementen)	Gruppe von Daten/Informationen	Daten/Informationen	einzelnes Datenelement	Bemerkung
0		Transportplanung (Vorstufe zu den Transportdokumenten)			Container- / Transportbuchung / -auftrag
1		Transportdokumente			Bill of Lading (B/L), Frachtbriefe (LKW, Bahn, See, ...)
2		Listen			Compliance, Baykott, Terror, ...
3		Transportnachrichten			UN/EDIFACT Nachrichten zum physischen Container Handling
4		Telematik Container - generisch			allgemeingültige Beschreibung für Telematik Container
	4.1		Container ID		
	4.2.1		Türstatus	Status Sensor Türstatus	wurde geöffnet/verschlossen sowie autorisiert/unautorisiert
	4.2.2			geografische Breite	Breitengrad
	4.2.3			geografische Länge	Längengrad
	4.2.4			Datum	
	4.2.5			Uhrzeit	
	4.3.1		Innenraumstatus	Status Sensor(en) Innenraumstatus	Licht, Gas, Bewegung detektiert, etc.
	4.3.2			geografische Breite	Breitengrad
	4.3.3			geografische Länge	Längengrad
	4.3.4			Datum	
	4.3.5			Uhrzeit	
	4.4.1		Container eingestappelt	Status ob eingestapelt oder nicht	eingestapelt/ausgestapelt
	4.4.2			geografische Breite	Breitengrad
	4.4.3			geografische Länge	Längengrad
	4.4.4			Datum	
	4.4.5			Uhrzeit	

Tabelle 9: Beispielhafte detaillierte Struktur der Referenzdaten der Telematikeinheit eines Containers

Für die ContainIT Sicherheitsfunktionen zur Containersicherheit werden aus der Liste der Referenzdaten bestimmte Daten und Informationen benötigt. Hierbei wird zwischen drei Klassifikationen unterschieden:

- M = Muss-Daten, d.h. unbedingt notwendige Datenelemente
- K = Kann-Daten, d.h. ergänzende Datenelemente
- O = Optionale-Daten, d.h. Datenelemente für einen bestimmten Transporttyp, z.B. Gefahrgut

D.h. im Einzelnen werden Datenelemente zum jeweiligen Transportabschnitt benötigt welche absolut notwendig (M), ergänzend (K) oder optional (O) für eine Risikobewertung eines Containertransports sind.

Die ContainIT Plattform empfängt Daten der Containertransportkette im Warenverkehr von den Beteiligten in den Tätigkeitsfeldern Transport, Umschlag und Administration. Nach dem Empfang, Analyse und Prüfung von Berechtigungen werden diese Daten auch gegen die hinterlegten Katalogdaten (Stammdaten) geprüft, um offensichtliche Fehler herausfiltern zu können und diese zu berichtigen. Dabei kann keine inhaltliche Prüfung erfolgen, ob die gesendeten Daten inhaltlich korrekt, richtig und vollständig sind. Es finden nur formale Plausibilitätsprüfungen statt, z.B. korrekte Schreibweisen von Orten, gültige Formate bei Datum und numerischen Daten und auf die Einhaltung von Kodierungen.

Für eine aussagefähige Bewertung werden Datenelemente von den am Transport beteiligten Akteuren in jedem Transportabschnitt

- von der Gestellung des Containers bei der Beladestelle
- über die Beladung der Ware beim Lieferanten / Hersteller
- über den Transport(e) des Containers im Inland bzw. Hinterland
- über den Umschlag im Ladehafen
- über den Transport über See
- über den Umschlag im Löschhafen
- über die Entladung der Ware am Bestimmungsort
- bis zur Rücklieferung des Containers an das Depot

bereitgestellt.

Die Auflistung der Transportabschnitte zeigt beispielhaft einen Gesamttransport im Export mit Start- und Zielort im jeweiligen Hinterland mit vielen einzelnen Transportabschnitten auf. In jedem dieser Transportabschnitte fallen Daten an, die mit denen des vorherigen bzw. des folgenden Transportabschnittes korrespondieren müssen, ansonsten kann eine Unschärfe, Störung oder gar ein ungerechtfertigter Eingriff in den Containertransport nur schwer vermutet bzw. festgestellt werden.

Nach erfolgter formaler Prüfung werden diese Daten aufbereitet und analysiert und bewertet. Dies geschieht in der Art, dass Sicherheitsfunktionen gebildet wurden, welche sich in vier Bereiche Transportdokumente, Compliance, Containerhandling und Containerstatus aufteilen. Der Ausgang bzw. das Ergebnis der Datenprüfung mit Bezug zu den jeweiligen Sicherheitsfunktionen fließt in eine Risikoanalyse und -bewertung ein, um eine entsprechende Aussage über den Sicherheitsstatus des Containers treffen zu können.

Insgesamt gibt es in ContainIT vier Bereiche von Sicherheitsfunktionen zur Containersicherheit, welche sich wie folgt aufgliedern:

- Transportdokumente
- Compliance
- Containerhandling
- Containerstatus

Beispielhaft wird in der nachfolgenden Tabelle aufgezeigt, welche Datenelemente aus der Liste der Referenzdaten u.a. typischerweise für den Sicherheitsfunktionsbereich der Transportdokumente benötigt werden. Sicherheitsüberprüfungen aus dem Bereich der Transportdokumente sind z.B.:

- Prüfung von Plausibilität und Vollständigkeit von Transportdokumenten bzw. -daten sowie elektronische Transportnachrichten (z.B. UN/EDIFACT Containernachrichten), gesplittet nach Verkehrsträger (Schiene, Straße, See) und Transportabschnitt
- Konsistenzprüfung von Transportdokumenten / -daten, gesplittet nach Verkehrsträger Schiene, Straße, See) und Transportbeteiligten / Kommunikationspartnern und Transportabschnitt

Informationsgruppe	Datenelement-Nr.	Datenelement
Container	1.6.x	Container-ID, Transport-ID, Container-Typ
Transportbeteiligte	1.1x, 1.2x, etc.	Versender, Empfänger, Meldeadresse, Ankunftsort, Abgangsort
Transportmittel	1.10.x	Typ, Kennung
Daten / Zeiten	1.12.x	Ankunftsdatum/-zeit, Abfahrtdatum/-zeit, Ausstellungsdatum, Unterschrift
Transportnachricht	3.x	Nachrichtentyp, Nachrichtenkennung, Bewegungsart
Transportgut (Ware)	3.x.21, 3.x.22, 3.x.12 / 3x1.13,	Menge, Warenbeschreibung, Verpackung, Gewichte
Siegel	3.x.16, 3.x.17	Siegel-ID, Siegel-Typ

Tabelle 10: Daten zum Sicherheitsfunktionsbereich der Transportdokumente

Nachfolgend noch eine Zusammenfassung zur Datenspeicherung und zum Datenschutz:

Innerhalb der ContainIT Plattform besteht die Notwendigkeit aus den unter anderem nachfolgend aufgeführten Gründen der Bedarf für eine zwischenzeitliche / kurzfristige bzw. längerfristige Speicherung der erfassten Daten / Informationen der Akteure sowie der daraus gewonnenen und abgeleiteten Informationen:

- Generell die zwischenzeitliche / kurzfristige Speicherung der erfassten Daten / Informationen der Akteure für den Lebenszyklus eines Containertransport zu deren Auswertung
- Individuell die längerfristige Speicherung der erfassten Daten / Informationen der Akteure sowie der daraus gewonnenen und abgeleiteten Informationen wenn ein Containertransport auffällig wurde, z.B. zur späteren Beweisführung für Sicherheitsbehörden
- Längerfristige Speicherung der Grundinformationen eines Containertransports (z.B. Transport-ID und Container-ID und Zeitstempel vom Anlegen des ersten Datums zum Containertransport) für z.B. Statistische Auswertungen
- Zwischenzeitliche / kurzfristige der Speicherung der erfassten Daten / Informationen der Akteure sowie der daraus gewonnenen und abgeleiteten Informationen für erweiterte Funktionalität für Betrachtung und Vergleich mit mehreren vergleichbaren z.B. zeitlich parallelen Containertransporten, Containertransporten der Vergangenheit, Containertransporte gleicher Akteure …

Für unauffällige Containertransporte, d.h. wenn die Risikobeurteilung definierte Schwellwerte für den Risikolevel/Risikoindex nicht überschritten hat (z.B. eine Meldestufe zur Information von Behörden), könnten über einen definierten Zeitraum (z.B. 2 Jahre) folgende Daten auf der ContainIT Plattform gespeichert:

- Transport-ID und Container-ID und Zeitstempel vom Anlegen des ersten Datums zum Containertransport werden organisatorisch in dem Bereich der ContainIT IKT Plattform gespeichert, wo auch die Daten/Informationen zur Containersicherheit ausgewertet werden
- Referenzen zu den beteiligten Akteuren (Spediteur, Frachtführer, …), da diese selbst aufgrund gesetzlicher Vorgaben diese Daten/Informationen über einen definierten Zeitraum vorzuhalten haben

Für auffällige Containertransporte, d.h. wenn die Risikobeurteilung definierte Schwellwerte für den Risikolevel/Risikoindex überschritten hat (z.B. eine Meldestufe zur Information von Behörden), könnten über einen definierten Zeitraum (z.B. 10 Jahre) folgende Daten/Informationen auf der ContainIT Plattform gespeichert:

- Transport-ID und Container-ID und Zeitstempel vom Anlegen des ersten Datums zum Containertransport werden organisatorisch in dem Bereich der ContainIT IKT Plattform gespeichert, wo auch die Daten/Informationen zur Containersicherheit ausgewertet werden
- Alle zugehörigen Daten/Informationen die zur Auswertung des erreichten Risikolevel/Risikoindex geführt haben werden organisatorisch in dem Bereich der ContainIT IKT Plattform gespeichert, wo auch die Daten/Informationen zur Containersicherheit ausgewertet werden

- Referenzen zu den beteiligten Akteuren (Spediteur, Frachtführer, …), da diese selbst aufgrund gesetzlicher Vorgaben diese Daten/Informationen über einen definierten Zeitraum vorzuhalten haben

Beim Zugriff auf und der Speicherung von Daten/Informationen muss aus Sicht des Datenschutzes zumindest folgendes als Minimalanforderung sichergestellt sein:

- Es muss angestrebt sein, dass weitestgehend nur funktionale Daten/Informationen zum Einsatz kommen, d.h. Daten die keinen direkten Bezug zu einzelnen Personen als solches haben wie z.B. Containerinformationen, Ladungsinformationen oder allgemeine Informationen zu den Transportbeteiligten
- Kommen personenbezogene Daten/Informationen zum Einsatz, so muss hierbei genau ersichtlich sein, in welchen Zusammenhang diese Daten/Informationen er-hoben und gespeichert werden, dass es sich z.B. um personenbezogene Daten/Informationen zur Rolle eines LKW Fahrers handelt und nicht um weitere Daten/Informationen zu dieser Person. Die personenbezogene Daten/Informationen dürfen dann auch in keinem anderen Zusammenhang verwendet werden
- Es muss einen genau definierten Verteilerschlüssel für alle erhobenen Daten/Informationen geben um eine unkontrollierte Verbreitung der Daten/Informationen zu unterbinden
- Die Eigentumsrechte von Daten/Informationen müssen soweit gewährleistet sein, dass vertrauliche Daten/Informationen von z.B. einem Akteur nicht ohne Einwilligung von diesem an andere Akteure weitergeben werden. Zur Risikobeurteilung für den Risikolevel/Risikoindex müssen jedoch alle Daten/Informationen zur Verfügung stehen und ebenso vertraulich behandelt werden
- Für den Zugriff auf die erhobenen und gespeicherten Daten/Informationen muss es ebenso eine Unterscheidung zwischen einem hoheitlichen, gemischten sowie privatwirtschaftlichem Zugriff bzw. Nutzung der Daten/Informationen geben

2.1.2 Risiko-Profiling

In den Unterarbeitspaketen AP25 und AP26 fokussiert sich der Arbeitsschwerpunkt seitens EADS auf die folgenden beiden Themen:

- Definition von Konzepten bzw. Methoden zur Optimierung der physischen Sicherheit basierend auf der Analyse und Bewertung von Bedrohungen und Risiken.
- Analyse und Definition von Konzepten und Methoden für ein integriertes Risikomanagement, d.h. z.B. Profiling von Containertransporten.

Bedrohung und Überwachungserfordernisse

Das relevante Gefahrenpotential ist grob durch folgende Aufzählung strukturiert:

- Gelegenheitskriminalität
  (Diebstahl, Einbruch, Beschädigung, Vandalismus)
- Schmuggel
  (Zollvergehen, Steuerhinterziehung, Falschdeklaration, Plagiate)
- Schwerkriminalität
  (Schmuggel in großem Umfang, Drogenhandel, Waffenhandel, Piraterie)
- Terrorismus
  (Anschläge, Unterstützung zu Anschlägen, Anschläge auf die Warenkette, Sabotage, organisierte Piraterie)
- Nukleare Schwerkriminalität
  (Schmuggel mit Nukleartechnik, Uran,...)
- Nuklearer Terrorismus
  (Nukleare Anschläge, Unterstützung)

Gelegenheitskriminalität und Piraterie führt zu versicherbaren oder bezahlbaren Schäden für Händler und Frachtführer, damit in erster Linie zu einem ökonomischen Problem.

Schwerkriminalität ist überwiegend ein unmittelbares Problem für den jeweiligen Staat, nur ein mittelbares Problem für den Handel und das Frachtgeschäft.

Insbesondere in den USA wird (nuklearer) Terrorismus wird als abstrakte Gefahr gesehen.

Container sind ideale Behälter zum Transport von machbaren

- Bomben mit hoher Sprengkraft
- „schmutzigen“ Bomben (Uran, Kobalt, etc.)
- einfachen Uranbomben (Little-boy- oder Kanonendesign)

Zur 100%-igen Gefahrenabwendung gibt es Konzepte zu Scanning-Techniken (Röntgen- und Gammastrahlen, Neutronenstrahlen), deren Anwendung in Ausfuhrhäfen von Seiten der US-Behörden politisch gefordert wird. Aus wirtschaftlichen Gründen ist dieser Aufwand kaum zu vertreten, weshalb wirtschaftlichere Alternativen diskutiert werden. Grundsätzlich ist daher die permanente sensorische Containerüberwachung ein Ansatz, dessen Wirksamkeit gegen alle o.g. Angriffe Schutz bieten kann.

Überwachung durch Statusinformationen

Dabei geht es um Container-Statusinformationen wie

- Türzustand (geschlossen, geöffnet)
- Siegelzustand (unberührt, gebrochen)
- Position

ergänzt durch Informationen aus den Frachtpapieren, um die Rahmenbedingungen verdächtiger Aktionen in die Gefahren- oder Risikobewertung einzubeziehen, also Informationen über

- Sender
- Verschiedene Frachtführer
- Personal
- Empfänger

aber auch über

- Waren
- Material

Die Fusion der bisher ganz getrennt behandelten Daten erlaubt es dann, Entscheidungen in Verdachtsfällen bei Unregelmäßigkeiten zu untermauern. Direkte Unregelmäßigkeiten können isoliert schon heute durch

- Türsensorik
- Türsiegelüberwachung

ebenso durch prinzipiell durch

- Vergleich von SOLL- und IST-Routen/Positionen
- Vergleich von SOLL- und IST-Zeiten

festgestellt werden. Im Falle sehr seltener krimineller Ereignisse ist allerdings mit einer hohen Fehlalarmrate zu rechnen, da es immer plausible Unregelmäßigkeiten gibt, die nicht mit kriminellen Handlungen einhergehen.

Autorisierung

Um Fehlalarme zu vermeiden, sind Autorisierungen von Unregelmäßigkeiten einzuführen, um Planungsfehler oder Abweichungspraxis zu tolerieren. Gerade die Verwendung möglicher SOLL-Routen ist sonst schwierig, weil es noch keine Tradition gibt, SOLL-Routen scharf einzuhalten. Übliche Abweichungen müssen in der Praxis daher als „erlaubt“ autorisiert werden.

Historie

Da Gewohnheiten in der Historie durch Wiederholungen gekennzeichnet sind, ist in Zweifelsfällen die Historie eine Unterstützung bei Entscheidungen, da sich die Praxisrandbedingungen oft nur langsam ändern. Daher ist die Speicherung von historischen Daten und deren Wiederverwendung in einem aktuellen Fall eine Bewertungsunterstützung.

Anforderungen an die Datenverarbeitung

Autorisierung und Historie haben also eine unmittelbare Auswirkung auf die Algorithmen Entwicklung für die Gefahrklassifikation in AP26. Dabei erfordert die Verwendung der Historie die Integration einer Datenbank. Neben zahlreichen denkbaren abstrakten Fällen ist beispielsweise die Erfassung von Waren bzw. Materialien, deren Mengen und der Berufszweig des jeweiligen Empfängers. Der Terroranschlag durch A. Breivik im Juli 2011 in Oslo mit 950 Kilogramm ANFO (Ammoniumnitrat und Dieselöl)[23] zeigt, wie man spezielle Produkte für die Landwirtschaft zweckentfremden kann, in diesem Fall für eine Autobombe. Im September 2011 wurde durch die Überprüfung einer Lieferung ähnlicher Chemieprodukte für die Landwirtschaft ein Terroranschlag in Berlin verhindert. Das war bei einer Einzellieferung möglich. Bei einer gestückelten Lieferung mit Einzellieferungen in kleinen Mengen hätte diese Kontrolle kein positives Ergebnis gehabt. Mit einer Erfassung der Historie in unterschwelligen Verdachtsfällen wäre aber auch unter Verwendung der Historie eine Gefahrenabwehr möglich gewesen.

Echtzeitrandbedingungen

Da es sich bei der wirksamen Containerüberwachung um eine Echtzeitaufgabenstellung handelt, sind erhebliche technische Randbedingungen einzuhalten. Das betrifft die Ebenen

- Abtasten der Sensorwerte mit entsprechend hoher Rate
- Zeitstempelung
- Angepasste Übertragungsfrequenz für die Datenkommunikation
- Eigenüberwachung der Sensoren
- Eigenüberwachung der Kommunikation
- Eigenüberwachung des IT-Systems

Dabei ist zu berücksichtigen, dass beispielsweise beim größten anzunehmenden Anschlag mit einer Atombombe (s.o.) mit den heutigen Beladungstechniken lediglich wenige Minuten erforderlich sind, um eine Palette mit einer derartigen Waffe unter Einsatz eines geeigneten Gabelstaplers in einen Container einzuladen. Systeme mit Abtastlücken der Sensordaten oder mit größeren Kommunikationsverzögerungen werden diesen Anforderungen nicht gerecht. Die Kommunikationsverzögerungen können dann zu einem realen Problem führen, wenn zwischen dem Messzeitpunkt einer verdächtigen Unregelmäßigkeit und dem Gefahreneintritt weniger Zeit verstreicht als zur Verhinderung des Gefahreneintritts erforderlich ist. Beispielsweise ist eine Systemverzögerung im Stundenbereich dann nicht mehr tolerierbar, wenn die Restfahrzeit zum Hafen, in dem der Terrorangriff geplant ist, kürzer ist.

Dokumentenüberprüfung

Ein seriöses Problem stellen aber auch die Erstbeladung und autorisierte Umladungen dar, da es selbst mit Kameraüberwachung bei täuschender Verpackung zu einer Ladung mit hohem Gefährdungspotential kommen kann, die im weiteren Transport dann ohne jegliche Unregelmäßigkeiten zum Ziel gebracht werden kann. Diese Situation erfordert dann die begleitende Überprüfung der Frachtdokumente mit Profiling-Techniken.

[23] Quelle: http://de.wikipedia.org/wiki/Ammoniumnitrat

Konzept der Gefahrenklassifikation

Die Gefahrenklassifikation muss vom Konzept her so aufgebaut sein, dass zusätzliche Überwachungsinformationen, auch basierend auf technische Neuerungen, ohne grundsätzliche Veränderungen integrierbar sind. Das betrifft Dokumenteninformationen und Sensordaten gleichermaßen. Bisher standen Türöffnungs- und Lichtsensorik im Vordergrund, aber Gassensorik oder Beschleunigungssensorik zur Stoßerfassung (in Untersuchung beim Verbundpartner EADS Astrium) könnten ebenso in Zukunft eingesetzt werden. Um diese Fragestellung zu studieren, wurden zwei unterschiedliche Vorgehensweisen praktiziert:

- isolierte Überwachungstechniken wurden in einer Bestandsaufnahme aufgelistet (Excel-Liste der „Sicherheitsfunktionen“) und untersucht (bottom-up-Verfahren)
- algorithmisch erforderliche Überwachungsinformationen wurden identifiziert (top-down-Verfahren)

Als ein allgemeines Prinzip im zweiten Verfahren kann die bereits erwähnte Autorisierung gesehen werden, die beispielsweise bei Einführung von Beschleunigungssensoren zu fordern wäre. Um den Sinn dieser Forderung zu überprüfen, kann man Mikroszenarien untersuchen, in denen beispielsweise die folgenden vier Zustände erfasst werden:

- (kein Stoß, keine Autorisierung) → kein Alarmfall
- (Stoß, keine Autorisierung) → Alarmfall (Unfall, Angriff)
- (kein Stoß, Autorisierung) → kein Alarmfall
- (Stoß, Autorisierung) → kein Alarmfall (erlaubte Umladung)

Der vierte Fall würde ohne Autorisierung zu einem (positiven!) Fehlalarm führen. Für den Fall, dass man im zweiten Zustand Unfall und Angriff algorithmisch unterscheiden möchte, wäre der Einsatz eines zusätzlichen Sensors erforderlich. Aus der Automobiltechnik bietet sich ein Drehratensensor an, der für das Elektronisches-Stabilitäts-Programm (ESP) zur Fahrsicherheit als preisgünstiges Massenprodukt eingesetzt wird. Die Überschreitung von Drehrateschwellen, für die ein Sensor dieser anspruchslosen Genauigkeitsklasse ausreicht, dürfte bei reinen Umladevorgängen eher selten sein. Miniszenarien für einen Drehratensensor zeigen sofort, dass er allerdings allein keine Hilfe ist, um einen Alarmfall für einen Angriff auszulösen. Für die zwei genannten Sensoren gibt also formal 2 x 2 x 2 x 2 = 16 Miniszenarien, wobei der Alarmfall für einen Angriff für den Zustand

- (Stoß, keine Autorisierung, keine Drehrate, keine Autorisierung)

ausgelöst werden müsste. Der Zustand

- (Stoß, keine Autorisierung, keine Drehrate, Autorisierung)

ist unlogisch und weist auf eine explizite falsche Autorisierung für Drehratenüberschreitungen hin, also einen Anfangsverdacht für Manipulationen, die als Initialisierungsfehler/Informatikfehler oder als Kommunikationsfehler erscheinen.

Es lassen sich ganz allgemein zahlreiche „unlogische Zustände“ wie beispielsweise bei „Türöffnungen ohne Siegelbruch“ – explizit falsche Zustandserfassung/Messung - finden, die indirekt auf Manipulationen hinweisen, die direkt aber nicht in Erscheinung treten. Daher ist der Ansatz der algorithmischen Zustandsvollständigkeit, der einerseits alle realistischen Zustände umfasst, aber formal auch solche einbezieht, die als unrealistische Zustände Unregelmäßigkeiten – in der Zustandserfassung/Messung oder Autorisierung – verraten, von allgemeiner Bedeutung.

Daraus ergeben sich auch Anforderungen an die Eingabedaten für eine Gefahrenklassifikation, die an Beispielszenarien in im Rahmen der Projektdemonstration in Unterarbeitspaket AP35 konkret vorgestellt werden.

Zustandsüberwachung mit Zeit- und Positionsangabe

Allgemein ist es zur Lagebeurteilung erforderlich

- ungewöhnliche Ereignisse durch einen Flagzustand an den Gefahrenklassifikator zu melden, dazu aber eine Zeit- und Positionsangabe zu liefern.
- auch die aktuelle Container-Position mit Zeitangabe zu liefern, wenn die klassifizierte Gefahr gemeldet wird.

Diese Position- und Zeitangaben unterscheiden sich, da gerade bei mehreren kritischen Flagwerten die korrespondierenden Ereignisse deutlich vor der Meldung eingetreten sein können, also auch vorher auf der Fahrtroute.

Sensorische und visuelle Zustandsüberwachung

Die Festlegung eines Flagzustandes geschieht nicht ausschließlich durch einen Sensor, sondern u.U. auch durch eine visuelle Überwachungsmaßnahme wie beim Siegelbruch. Da ein Siegelbruch somit nicht direkt überwacht wird, sondern indirekt, kann nur durch Fehlen des unbeschädigten Originalsiegels dessen Bruch festgestellt werden. Technisch ist dann aber beispielsweise nicht die Verbalmeldung „ Siegel mit falscher Siegelnummer festgestellt“ abzusetzen, sondern – ohne weitere Erklärung - FLAG_TÜRSIEGEL_OFFEN = WAHR, da es nur darum geht, die entdeckte faktische Abweichung vom Normalzustand FLAG_TÜRSIEGEL_OFFEN = FALSCH festzustellen. Das ist dann auch direkt in die Eingabedatei für die Gefahrenklassifikation eintragbar. Formal bedeutet das, dass bei einer visuellen Zustandsüberwachung formal wie bei einer sensorischen Überwachung vorgegangen wird. Das Konzept sollte für alle visuellen Überwachungen eingehalten werden. Wird ein Sensor bestücktes elektronisches Siegel zu Grunde gelegt, dann beziehen sich die Zeitangabe und die Positionsangabe auf das physikalische Ereignis, während bei der visuellen Überprüfung sich diese Angaben auf das meist deutlich spätere Überprüfungsereignis beziehen. Noch später findet dann die Datenkommunikation statt.

Verhaltensweise bei Zustandsmeldungen

Eine nichtzulässige Art der Datenaufbereitung für die Gefahrenklassifikation besteht darin, beispielsweise aus Flagzuständen zu schließen, „welchen richtigen Zustand logischer Weise ein anderes Flag anzeigen müsste“. Zum Beispiel ist bei einer Türöffnung physikalisch ein Siegelbruch erforderlich. Ist aber visuell erkennbar das Originalsiegel im Normalzustand, dann muss FLAG_TÜRSIEGEL_OFFEN =FALSCH gesetzt bleiben. Eine gutgemeinte logische Korrektur zu FLAG_TÜRSIEGEL_OFFEN =WAHR ist verboten, da das Datenverarbeitungsmodell sich auf die „sensorische und visuelle Erkennung von Zuständen“ bezieht, nicht aber auf die Realität.

Die Verwendung von Zustandsflags ist damit für die sensorische und die visuelle Überwachung in ein einheitliches Schema gebracht worden. Es sind so alle Zeit- und Positionsangaben echtzeitkonform definiert.

Datenverarbeitungskonzept der Gefahrenklassifikation

Im Rahmen dieses Unterarbeitspakets wurde die erforderliche Gefahrenklassifikation auch von der algorithmischen Seite her untersucht, um u.a. die Wohldefiniertheit und Vollständigkeit des Konzeptes überprüfen zu können. Basis dieses Konzepts ist das Datenflussdiagramm in Abbildung 21.

Dabei sind die Dokumenteninformationen ein Auszug aus den Frachtpapieren, um die Fracht zu identifizieren. Weiterhin erlauben sie Überprüfungen der beteiligten Firmen, Personen, Produkte und Materialien.

Die Überwachungsdaten sind Sensordaten, aber auch Meldungen von visuellen Überwachungen, beispielsweise Siegelprüfungen.

Die Ausgabedaten liefern die Information, um interne Interventionen wie Nachüberprüfungen auszulösen oder externe Meldungen an Behörden abzusetzen.

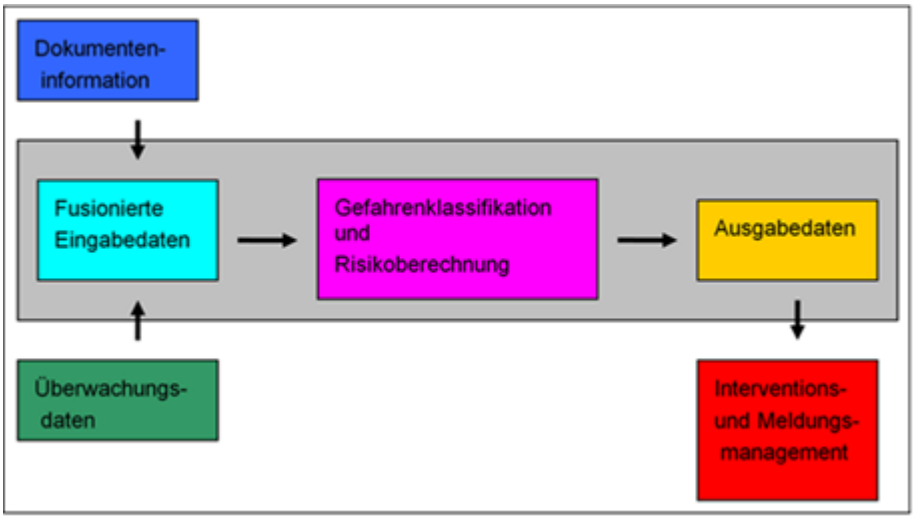


Abbildung 21: Datenflussdiagramm zur Gefahrenklassifikation mit fusionierten Eingabedaten

Die Arbeiten fokussieren sich im Wesentlichen auf die grau hinterlegten Elemente im Datenflussdiagramm der Abbildung 21.

Die fusionierten Eingabedaten lassen sich in drei Klassen aufteilen:

- Textdaten (aus Frachtpapieren)
- Kontinuierliche Messdaten (wie Positionsdaten)
- Logische Zustandsdaten (wie Türzustands-Flag)

Es hat sich herausgestellt, dass beispielsweise die Textdaten und kontinuierlichen Messdaten zwei unterschiedliche Rollen spielen:

- Sie dienen der Identifikation und Lokalisierung für interne und externe Interventionen
- Sie dienen der Gefahrenklassifikation

Im ersten Fall werden sie also durchgeschleift und den Ausgabedaten zugeschlagen. Im zweiten Fall spielen nur Bereichsüberschreitungen eine Rolle wie SOLL-IST-Abweichungen von Positionen über bestimmte Schwellwerte. In diesem Fall ist auch den kontinuierlichen Daten für die Gefahrenklassifikation eine (oder mehrere!) logische Variable, die wir als Flag bezeichnen, zuzuordnen, die die Schwellenüberschreitung angibt. – Auch die Textdatenüberprüfung durch die Profiling-Technik führt zu Treffer-Flags, also logische Variable, die angeben, ob die Profiling-SW eine verdächtige Information festgestellt hat. Das detaillierte Datenflussdiagramm in Abbildung 22 fasst dies zusammen.

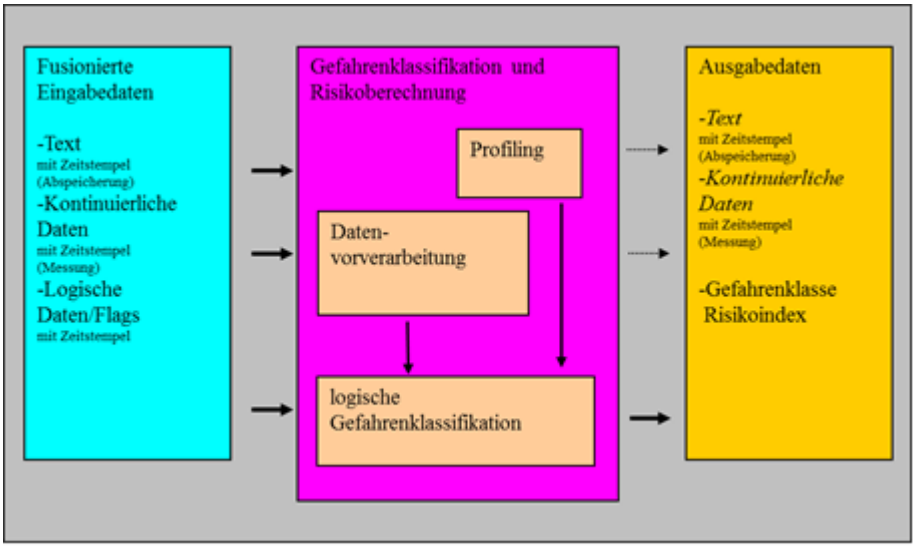


Abbildung 22: Datenflussdiagramm zur Gefahrenklassifikation in höherer Detaillierung

Die Datenvorverarbeitung ist elementar. Sie erfordert die einheitliche Festlegung der dimensionierten Koordinatensysteme für die kontinuierlichen Messgrößen und die entsprechenden Werte für die Schwellen.

Algorithmus zur Gefahrenklassifikation

Der Algorithmus für die logische Klassifikation erfordert die Definition und die Parametrierung logischer Funktionen. Die Parametrierung erfordert für diese Funktionen zunächst eine vollständige Wertezuordnungstabelle, die hier für die spezifische Anwendung aufzustellen ist. Da analytische Methoden für logische Funktionen wie Interpolationstechniken nicht existieren, ist zunächst die vollständige Tabelle erforderlich. Erst mit den daraus errechneten Parameterwerten entsteht dann eine in der Regel kompaktere Darstellung. Aus den zahlreichen Darstellungen logischer Funktionen bieten sich insbesondere bei Funktionen von mehreren unabhängigen Variablen übersichtliche algebraische Darstellungen an. Anknüpfend an bekannten Methoden aus der Analysis bietet sich die Fourier-Darstellung

$$\mathrm{funBool}(\mathbf{Flag},A) = \sum_{k1,k2,\ldots,kN} A_{k1,k2,\ldots,kN}\ \phi_{k1}(\mathrm{Flag}_{i1}))*\phi_{k2,}(\mathrm{Flag}_{i2})*\ldots*\phi_{kN}(\mathrm{Flag}_{iN})$$

an, die auch im einfachsten Zahlenkörper K2 ={0,1} (0 entspricht FALSCH, 1 entspricht WAHR) mit der periodische Addition „+“ (hier 1+1=0!) und der üblichen Multiplikation funktioniert. Als (einstellige!) Basisfunktionen dienen

- die Identität ($x = \phi_0(x)$, x aus K_2 ={0,1})
- die Negation ($x+1 = \phi_1(x)$, x aus K_2 ={0,1})

also die einzigen nicht-konstanten einstelligen logischen Funktionen neben den beiden konstanten logischen Funktionen ($0=f_0(x)$, $1=f_1(x)$ f.a.x aus K_2 ={0,1}). Die Fourier-Koeffizienten $A_{k1,k2,\ldots,kN}$ sind auch aus K_2 ={0,1} und formal wie üblich bestimmbar.

Von logischen Vektorfunktionen mit Werten im Vektorraum K_2^{dim} sind so die Komponentenfunktionen darstellbar. Damit sind aber auch nicht-logische Funktionen mit diskretem Wertebereich darstellbar, da man beispielsweise eine Wertebereich {0, 1, 2, 3, 4} binär als {000, 001, 010, 011, 100} darstellen kann und die Werteberechnung auf die Bit-Wertberechnung zurückführen kann. Es steht einem dann frei, eine nötige Umskalierung etwa auf {0, 25, 50, 75, 100} für die Ergebnisdarstellung zu verwenden.

Die vorgeschlagene Fourier-Darstellung hat den entscheidenden Vorteil, dass man in der Zahl der Flags, N, frei ist. Hier werden durch „*“ und „+“ die bekannten 2-stelligen logischen Funktionen/Operatoren „AND“ und „XOR“ verwendet, also nicht Neues erfunden.

Technisch lässt sich also die SW in zwei Anteile zerlegen:

- Berechnung der Fourier-Koeffizienten aus der Wertezuordnungstabelle
- Anwendung der Klassifikation mit den berechneten Fourier-Koeffizienten

Die erste Berechnung ist die Parametrierung, die einmal durchzuführen ist. Bei konstanten Systemparametern kann dann die Klassifikation beliebig oft durchgeführt werden. Je nach Implementierungssprache oder Compiler ist eine Codeoptimierung erforderlich, in der die zahlreichen Multiplikationen mit den Fourier-Koeffizienten (= 0 oder =1) nicht mehr explizit auftreten. Reduktionspotential ergibt sich zusätzlich auch bei Summen von Fourier-Koeffizienten vom Wert=1 wegen 1+1=0. Die so generierbaren Funktionsdarstellungen führen dann zu sehr schnellem Code.

Diese vorgestellte Vorgehensweise ist nicht neu und wird im Chip-Design und der Programmierung von Field Programmable Gate Arrays (FPGA) genutzt, um (automatisch(!) z.B. mit VHDL (Very high speed integrated circuit Hardware Description Language) als Designsprache platzsparend Funktionen (parallel!) zu integrieren, die dann maximale Ausführungsgeschwindigkeiten aufweisen, die mit Standard-Hardware (HW) nicht erreichbar sind.

Parametrierung

Bekanntlich werden Parameter von Klassifikatoren durch sog. Trainingsrechnungen berechnet, die experimentelle Beispielsammlungen verwenden. In der Sicherheitstechnik sind – zum Glück – keine hinreichend umfassende Beispielsammlungen einsetzbar, weil gerade Terroranschläge außergewöhnlich selten sind. Daher ist es unumgänglich, die Wertezuordnungstabelle manuell zu erstellen.

Eingabe- und Ausgabekonventionen

Zur der Darstellung der notwendigen Ein- und Ausgabedaten für das Profiling wurden entsprechende generische Formate definiert. Für schon sehr einfache Betrachtungen hat sich gezeigt, dass eine Autorisierung und auch eine Historie der Daten eine sehr wichtige Rolle spielen. Die systematische Verwendung von Autorisierungs-Flags und den Einsatz von historischen Flags ist somit zwingend notwendig. Das erhöht zwar die Gesamtanzahl der Flags, was allerdings algorithmisch durch den gewählten und oben erläuterten Ansatz unproblematisch ist. Die in **Fehler! Verweisquelle konnte nicht gefunden werden.** (siehe unten) eingetragene Datenbank wird in diesem Rahmen in ihrer allgemeinen Funktion untersucht, die sich dann nicht allein auf die Historie eines einzigen Transports bezieht.

Das in Abbildung 22 gezeigte detaillierte Datenflussdiagramm legt nahe, ein Software/Hardware-(SW/HW) Schnittstellenkonzept so zu definieren, das eine konfliktfreie asynchrone Kooperation ermöglicht. Konkret wurde ein Konzept in den Vorarbeiten zum Demonstrator in Unterarbeitspaket AP35 umgesetzt und getestet, das naturgemäß ohne zu komplexe Standardisierungen praktisch im jeder Umgebung (Implementierungssprache, Betriebssystem, Netzwerk) einsetzbar ist. Die Verwendung der „lesbaren“ Text-Dateien für eine Echtzeitanwendung – im Rahmen des Entwicklungsprozesses - ist dabei nicht alternativlos, da Festplattenzugriffe bei Comuptern nicht gerade schnell sind, ein Problem, das allerdings durch die aufkommenden Flashspeicher – getrieben durch den Videomarkt – eher geringer werden dürfte. Für Testsysteme, die auch eine größere Anzahl von Transporten simultan überwachen, sollte dieser Ansatz zunächst ausreichen.

Struktur der Eingabedatei für die Gefahrenklassifikation

Mit dem Projektpartner SAPPER zusammen wurde die Struktur für die Eingabedatendatei ausgearbeitet. Die Struktur der Daten anhand von Flags ist wie folgt

- Identifikation

- Profiling
- Überwachung

Dieses Musterbeispiel ist für die Projektdemonstration in AP35 auf die Adressen von Sender, Frachtführer und Empfänger beschränkt. Hier können in der gleichen Art weitere Frachtführer ergänzt werden. Ebenso kann auch Personal, beispielsweise LKW-Fahrer, hier eingesetzt werden. Dazu korrespondierend sind die Profilingflags dann zu ergänzen.

Bei den Überwachungssensoren wurde eine einheitliche Datenstruktur definiert, die durch das Beispiel des Kommunikationsflags

```
FLAG_KOMMUNIKATION
FALSE
TIME_FLAG_KOMMUNIKATION
10.01.2012 17:16:20
FLAG_KOMMUNIKATION_AUT
FALSE
TIME_FLAG_KOMMUNIKATION_AUT
10.01.2012 17:16:20
FLAG_KOMMUNIKATION_HIST
FALSE
TIME_FLAG_KOMMUNIKATION_HIST
10.01.2012 17:16:20
FLAG_KOMMUNIKATION_AUT_HIST
FALSE
TIME_FLAG_KOMMUNIKATION_AUT_HIST
10.01.2012 17:16:20
```

gegeben ist. Es werden also immer 4 Flags definiert. Neben dem primären Flag gibt es ein Autorisierungsflag. Zu diesem Paar gibt es dann noch ein Paar historischer Flags, die aus einer Datenbank eingelesen werden können. Das Datenalter ist jeweils angegeben, das nicht mit der Savetime der Datei zu verwechseln ist.

Beim Einsatz weiterer Sensoren wie z.B. Beschleunigungssensoren/Stoßsensoren sind die entsprechenden Flags zu ergänzen.

Für weitere denkbare Daten wie z.B. Statusmeldungen und spätere Interventionen ist die zum Zeitpunkt der Meldung entsprechend zugehörige Container-Position erforderlich.

Weiter denkbar sind neben der aktuellsten Containerposition auch noch weitere frühere Positionswerte des Containers, welche den historischen Zusammenhang des Setztens anderer Flags (z.B. Überwachung oder Identifikation) von FALSCH (normal) auf WAHR (Ereignis) aufzeigen.

Dann würde einerseits die aktuelle Position unter der neuen Rubrik

Positionsüberwachung

```
POSITION_NORD
NNN
POSITION_EAST
EEE
TIME_POSITION
10.01.2012 17:17:20
```

und die Ergänzung

```
FLAG_KOMMUNIKATION
FALSE
TIME_FLAG_KOMMUNIKATION
10.01.2012 17:16:20
```



```
POSITION_NORD_FLAG_KOMMUNIKATION
NNN
POSITION_EAST_FLAG_KOMMUNIKATION
EEE
```

für jedes Überwachungsflag erforderlich sein, wobei die Zeit sich dann auch auf diese Positionsmessung beziehen sollte. Auch den historischen Flags sollte dann die (historische!) Position zugeordnet sein. Bei den Autorisierungsflags spielt die Position natürlich auch eine relevante Rolle, insbesondere dann, wenn Autorisierungen bei Routenabweichungen, Türöffnungen, Siegelbruch oder Verladung in Abhängigkeit eines Zeit- und Positionsintervalls gegeben werden.

Die nachfolgenden drei Tabellen (Tabelle 11, Tabelle 12 und Tabelle 13) zeigen wie die generischen Eingabedaten strukturiert sind. Diese Struktur wurde auch später zur Projektdemonstration in Unterarbeitspaket AP35 verwendet.

```
Eingabe_Datei_1
SAVE_TIME
10.01.2012 17:11:31
CLID
85299965832541
SOURCEID
800015760012
NAME_1
Peter Burger OHG
STREEET_1
Sylvesteralle 47
CITY_1
Berlin
ZIP_1
10845
COUNTRY_1
Deutschland
NAME_2
Hermann Lichtorgel GmbH
STREEET_2
An der Nahe 47
CITY1
Hannover
ZIP_2
50001
COUNTRY_2
Deutschland
NAME_3
ASS Transporte
STREEET_3
Kochhannstrasse 28
CITY_3
Berlin
ZIP_3
10249
COUNTRY_3
Deutschland
```

Tabelle 11: Struktur einer Eingabedatendatei - Identifikationsdaten

```
FLAG_TREFFER_1
```



```
FALSE
TIME_FLAG_TREFFER_1
10.01.2012 17:16:20
FLAG_TREFFER_1_AUT
FALSE
TIME_FLAG_TREFFER_1_AUT
10.01.2012 17:16:20
FLAG_TREFFER_1_HIST
FALSE
TIME_FLAG_TREFFER_1_HIST
10.01.2012 17:16:20
FLAG_TREFFER_1_AUTH_HIST
FALSE
TIME_FLAG_TREFFER_1_AUTH_HIST
10.01.2012 17:16:20
FLAG_TREFFER_2
FALSE
TIME_FLAG_TREFFER_2
10.01.2012 17:16:20
FLAG_TREFFER_2_AUT
FALSE
TIME_FLAG_TREFFER_2_AUT
10.01.2012 17:16:20
FLAG_TREFFER_2_HIST
FALSE
TIME_FLAG_TREFFER_2_HIST
10.01.2012 17:16:20
FLAG_TREFFER_2_AUTH_HIST
FALSE
TIME_FLAG_TREFFER_2_AUTH_HIST
10.01.2012 17:16:20
FLAG_TREFFER_3
FALSE
TIME_FLAG_TREFFER_3
10.01.2012 17:16:20
FLAG_TREFFER_3_AUT
FALSE
TIME_FLAG_TREFFER_3_AUT
10.01.2012 17:16:20
FLAG_TREFFER_3_HIST
FALSE
TIME_FLAG_TREFFER_3_HIST
10.01.2012 17:16:20
FLAG_TREFFER_3_AUTH_HIST
FALSE
TIME_FLAG_TREFFER_3_AUTH_HIST
10.01.2012 17:16:20
```

Tabelle 12: Struktur einer Eingabedatendatei - Profiling-Flags

```
FLAG_KOMMUNIKATION
FALSE
TIME_FLAG_KOMMUNIKATION
10.01.2012 17:16:20
FLAG_KOMMUNIKATION_AUT
FALSE
```



```
TIME_FLAG_KOMMUNIKATION_AUT
10.01.2012 17:16:20
FLAG_KOMMUNIKATION_HIST
FALSE
TIME_FLAG_KOMMUNIKATION_HIST
10.01.2012 17:16:20
FLAG_KOMMUNIKATION_AUT_HIST
FALSE
TIME_FLAG_KOMMUNIKATION_AUT_HIST
10.01.2012 17:16:20
FLAG_TÜR_OFFEN
FALSE
TIME_FLAG_TÜR_OFFEN
10.01.2012 17:16:20
FLAG_TÜR_OFFEN_AUT
FALSE
TIME_FLAG_TÜR_OFFEN_AUT
10.01.2012 17:16:20
FLAG_TÜR_OFFEN_HIST
FALSE
TIME_FLAG_TÜR_OFFEN_HIST
10.01.2012 17:16:20
FLAG_TÜR_OFFEN_AUT_HIST
FALSE
TIME_FLAG_TÜR_OFFEN_AUT_HIST
10.01.2012 17:16:20
FLAG_TÜRSIEGEL_OFFEN
FALSE
TIME_FLAG_TÜRSIEGEL_OFFEN
10.01.2012 17:16:20
FLAG_TÜRSIEGEL_OFFEN_AUT
FALSE
TIME_FLAG_TÜRSIEGEL_OFFEN_AUT
10.01.2012 17:16:20
FLAG_TÜRSIEGEL_OFFEN_HIST
FALSE
TIME_FLAG_TÜRSIEGEL_OFFEN_HIST
10.01.2012 17:16:20
FLAG_TÜRSIEGEL_OFFEN_AUT_HIST
FALSE
TIME_FLAG_TÜRSIEGEL_OFFEN_AUT_HIST
10.01.2012 17:16:20
FLAG_POSITION_1
FALSE
TIME_FLAG_POSITION_1
10.01.2012 17:16:20
FLAG_POSITION_1_AUT
FALSE
TIME_FLAG_POSITION_1_AUT
10.01.2012 17:16:20
FLAG_POSITION_1_HIST
FALSE
TIME_FLAG_POSITION_1_HIST
10.01.2012 17:16:20
FLAG_POSITION_1_AUT_HIST
FALSE
TIME_FLAG_POSITION_1_AUT_HIST
```



```
10.01.2012 17:16:20
FLAG_POSITION_2
FALSE
TIME_FLAG_POSITION_2
10.01.2012 17:16:20
FLAG_POSITION_2_AUT
FALSE
TIME_FLAG_POSITION_2_AUT
10.01.2012 17:16:20
FLAG_POSITION_2_HIST
FALSE
TIME_FLAG_POSITION_2_HIST
10.01.2012 17:16:20
FLAG_POSITION_2_AUT_HIST
FALSE
TIME_FLAG_POSITION_2_AUT_HIST
10.01.2012 17:16:20
FLAG_POSITION_3
FALSE
TIME_FLAG_POSITION_3
10.01.2012 17:16:20
FLAG_POSITION_3_AUT
FALSE
TIME_FLAG_POSITION_3_AUT
10.01.2012 17:16:20
FLAG_POSITION_3_HIST
FALSE
TIME_FLAG_POSITION_3_HIST
10.01.2012 17:16:20
FLAG_POSITION_3_AUT_HIST
FALSE
TIME_FLAG_POSITION_3_AUT_HIST
10.01.2012 17:16:20
FLAG_POSITION_1
FALSE
TIME_FLAG_POSITION_1
10.01.2012 17:16:20
FLAG_POSITION_1_AUT
FALSE
TIME_FLAG_POSITION_1_AUT
10.01.2012 17:16:20
FLAG_POSITION_1_HIST
FALSE
TIME_FLAG_POSITION_1_HIST
10.01.2012 17:16:20
FLAG_POSITION_1_AUT_HIST
FALSE
TIME_FLAG_POSITION_1_AUT_HIST
10.01.2012 17:16:20
FLAG_POSITION_2
FALSE
TIME_FLAG_POSITION_2
10.01.2012 17:16:20
FLAG_POSITION_2_AUT
FALSE
TIME_FLAG_POSITION_2_AUT
10.01.2012 17:16:20
```



```
FLAG_POSITION_2_HIST
FALSE
TIME_FLAG_POSITION_2_HIST
10.01.2012 17:16:20
FLAG_POSITION_2_AUT_HIST
FALSE
TIME_FLAG_POSITION_2_AUT_HIST
10.01.2012 17:16:20
FLAG_POSITION_3
FALSE
TIME_FLAG_POSITION_3
10.01.2012 17:16:20
FLAG_POSITION_3_AUT
FALSE
TIME_FLAG_POSITION_3_AUT
10.01.2012 17:16:20
FLAG_POSITION_3_HIST
FALSE
TIME_FLAG_POSITION_3_HIST
10.01.2012 17:16:20
FLAG_POSITION_3_AUT_HIST
FALSE
TIME_FLAG_POSITION_3_AUT_HIST
10.01.2012 17:16:20
FLAG_INFORMATIK
FALSE
TIME_FLAG_INFORMATIK
10.01.2012 17:16:20
FLAG_INFORMATIK_AUT
FALSE
TIME_FLAG_INFORMATIK_AUT
10.01.2012 17:16:20
EOF
```

Tabelle 13: Struktur einer Eingabedatendatei - Überwachungsflags

Struktur der Ausgabedatei der Gefahrenklassifikation

Die vorgeschlagene Ausgabedatei hat die Struktur:

- Durchgeschleifte Daten
  - Identifikationsdaten (siehe Eingabedatei)
  - Profiling_Flags (Wert, Datum, Position)
  - aktuelle Positionsdaten
  - Überwachungs_Flags (Wert, Datum, Position)
- Berechnete Ergebnisse
  - Risikoindex aus z.B. {0.00, 0.25, 0.50, 0.75, 1.00}
  - Standardmeldungsnummer (Zugeordnete Meldung müsste vorgefertigte Erklärung enthalten.)
  - (später neue historische Flags als Ausgabe an Datenbank)

Die vorgeschlagene generische Vorgehensweise erlaubt darüber hinaus bei Bedarf spezielle Ergänzungen.

Datenschutz

Aufgrund der gesetzlichen Rahmenbedingungen ist gerade Speicherung, Verwertung, Weitergabe und vor allem der Schutz von Daten in einer solchen Datenbank bzw. IKT System nicht nur aus technischer Sicht zu betrachten.

Eine solch „kleine Lösung“ mit reduzierten und abstrahierten Datensätzen, wie sie hier diskutiert wurde, bei der es allein um die historische Daten während einer Fracht geht, dürfte von den gesetzlichen Einschränkungen dabei kaum betroffen sein.

Jedoch sind zum Datenschutz dennoch Kriterien wie nachfolgend aufgeführt jederzeit kritisch zu hinterfragen und auf deren korrekte Umsetzng zu prüfen:

- Keine neue „Super-Datenbank“ erstellen, sondern nur die Verlinkung zwischen den bereits existenten Datenbanken der Transportbeteiligten
- Im Normalfall ausschließlich kurzfristige Datenspeicherung für den Lebenszyklus eines Containertransports
- Im Sonderfall die längerfristige Datenspeicherung bei Auffälligkeit eines Containertransports, z.B. zur Intervention oder späterer Beweisführung
- Weitergabe von Daten erfolgt nur im Sonderfall bei Auffälligkeit eines Containertransports und nur an Sicherheitsbehörden mit einem definierten und nachvollziehbaren Verteilerschlüssel und Auftrag bzw. Mandat
- Eigentumsrechte und Vertraulichkeit von Daten müssen gewährleistet werden
- So weit als möglich erfolgt eine Reduktion auf funktionale Daten, ohne Bezug auf personenbezogene Daten
- Beim Umgang mit personenbezogene Daten muss jederzeit die Transparenz bzgl. Erfassung, Speicherung, Verwendung und Weitergabe der Daten bestehen

Umsetzung des Risiko-Profiling zur Projektdemonstration

Die Projektdemonstration in Unterarbeitspaket AP35 erfolgte mit einem reduzierten und daher im Rahmen des Projekts einfach, sicher und zuverlässig handzuhabenden IKT System, um die Wirksamkeit der Datenfusion und des Risiko-Profiling zur Containersicherheit anschaulich zu zeigen. Im wesentlichen wurden hierzu die Zahl der Eingabevariablen und deren möglichen Zustandswerte entsprechend beschränkt. Grundsätzlich bleibt – wenn auch unter vereinfachten Bedingungen – der vorgeschlage Ansatz des Risiko-Profiling erhalten und wird entsprechend umgesetzt.

2.1.3 Projektdemonstration

Um das Gesamtkonzept zur Containersicherheit durch vernetzte IKT-Systeme von ContainIT im Rahmen der Projektdemonstration im Unterarbeitspaket AP35 darzustellen, wurde ein entsprechendes Demonstrationsszenario entworfen.

Das Demonstrationsszenario wurde an das im Projekt umfassend untersuchte Mustertransportszenario sowie den damit zusammenhängenden Musterangriffsszenarien angelehnt. Die Teilszenarien der Demonstration wurden in der Form geplant, damit das Prinzip des IKT-basierten Multi-Layer-Konzepts zur Containersicherheit von ContainIT anhand eines typischen Containertransports verständlich dargestellt werden kann. Hierbei soll verdeutlicht werden, dass durch die Zusammenführung verschiedenartiger Informationen zu einem deutlichen Mehrwert an Informationsgehalt gegenüber den einzelnen betrachteten Informationen führt.

Final ergab sich eine Demonstration mit dem Vergleich der einerseits aktuellen Situation zur Containersicherheit eines Containertransports unter Nutzung der unvernetzten IKT Insellösungen der beteiligten Akteure inklisive deren Ergänzung um moderne Telematiksysteme (z.B. LKW Telematik oder Containerüberwachung) und andererseits zum im Projekt ContainIT untersuchten Zusammenschluss aller IKT-Insellösungen inklusive der Nutzung von heute verfügbaren Telematiksystemen Telematiksysteme (z.B. LKW Telematik oder Containerüberwachung) als auch mit der Leistungsfähigkeit der gesamtheitlichen Datenanalyse zum Risiko-Profiling, d.h. letztendlich dem Konzept zur Containersicherheit von ContainIT.

Das Gesamtkonzept und Organisation der Projektdemonstration, die IKT-Neztwerkinfrastruktur zur Projektdemonstration als auch die Softwareimplenentierung des Risiko-Profiling zur Projektdemonstration wurden hierbei von EADS durchgeführt.

Da nicht alle Projektergebnisse wie z.B. IKT Architektur, IKT Sicherheit oder Wirtschaftlichkeitsbetrachtungen mit der dem Demosntrationsszenario abgebildet werden können, ist deren Vorstellung mittels verschiedener PowerPoint Präsentationen erfolgt.

Das finale ContainIT Demonstrationsszenario ist nachfolgend in der Abbildung 23 dargestellt.

Abbildung 23: Demonstrationsszenarios als sequentieller Ablauf

Die Abbildung 24 zeigt anschaulich, wie die zur Demonstration notwendige Datenkommunikation unter Nutzung realer sich teils im operativen Betrieb befindlichen IKT Systemen die verschiedenen ContainIT Projektpartner während der Projektdemonstration interagieren.

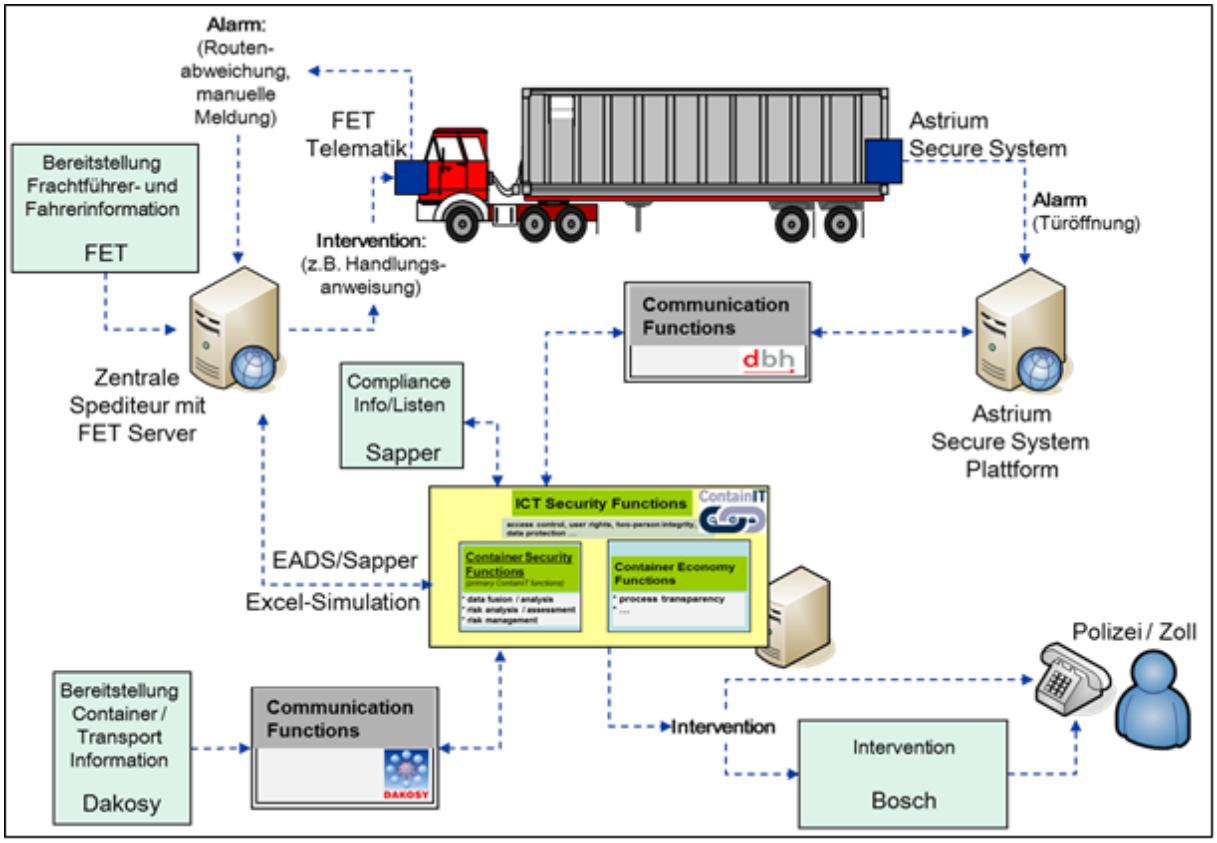


Abbildung 24: Reale Interaktionen der Projektpartner beim Demonstrationsszenario

Die in Abbildung 24 dargestellte Demonstration des ContainIT Containersicherheitkonzepts wurde aufgrund der Komplexität und der begrenzten Möglichkeiten in der technischen Umsetzung vereinfacht.

Das zentrale Element der Projektdemonstration ist dabei die Datenfusion als auch das Risiko-Profiling. Die hierzu erstellte Softwareimplementierung, welche in Abbildung 24 als „Excel-Simulation“ benannt ist, erfolgte auf Basis von Microsoft Excel mit Visual Basic Application (VBA).

Hierzu wurde ein Konzept für eine portable Lösung entwickelt, die ohne zusätzliche Lizenzen und Kosten auf normalen Computern/Notebooks mit „Standardausstattung“ in einem einfachen Computernetzwerk einsetzbar ist.

Als Eingangsdaten wurden die Informationen zu den einzelnen Zeitphasen die Ereignisse des Containertransports entsprechend des Demonstrationsszenarios eingespielt. Die Ausgangsdaten wurden entsprechend als Informationen zum Risikomanagement, wie z.B. zur Intervention, bereitgestellt. Hierbei wurden die zuvor in Kapitel 2.1.2 vorgestellten Methoden zum Risiko-Profiling, der Datenstruktur zur Beschreibung der aktuellen Zustände der einzelnen Eingangsgrößen, etc. verwendet. Dieses Konzept ist direkt aus dem in Unterarbeitspaket AP26 vorgestellten Ansatz abgeleitet und ist daher methodisch dazu konform.

Abbildung 25 zeigt das Programmfenster der Excel-Simulation zur Datenfusion und zum Risiko-Profiling mit allen zur Projektdemonstration verwendeten Daten, wie z.B. die der beteiligten Aktuere zur Compliance-Prüfung sowie die Eingabe- und Ausgabedaten in Form von Flags und deren zugehörigem Zeitstempel sowie der teilweise notwendigen Positionsdaten.

Im grafischen Element links oben in Abbildung 25 sind die 4 Risikoklassen mit deren Risikostufen als Ergebnis des Risiko-Profiling dargestellt. Direkt darunter sind als eine Art „Klaviatur“ die Wahr/Falsch-Werte aller Flags der einzelnen Eingabewerte dargestellt. Die Balken für Falsch sind dabei nach unten hin und die Werte für Wahr nach oben hin ausgerichtet.

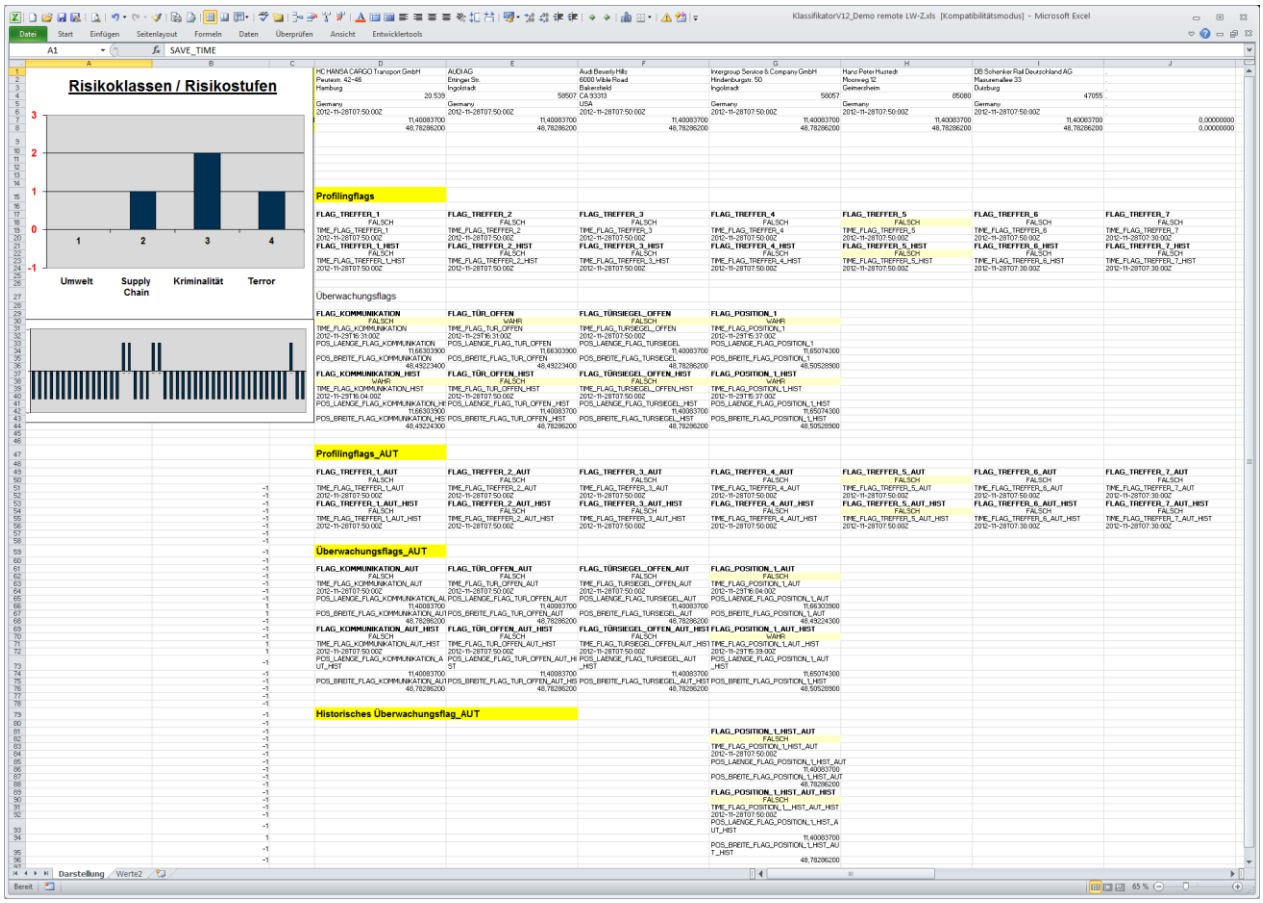


Abbildung 25: Excel-Simulation zur Datenfusion und zum Risiko-Profiling

In Abbildung 26 ist ein Ausschnitt aus des finalen VBA-Quellcode zur Excel-Simulation dargestellt.

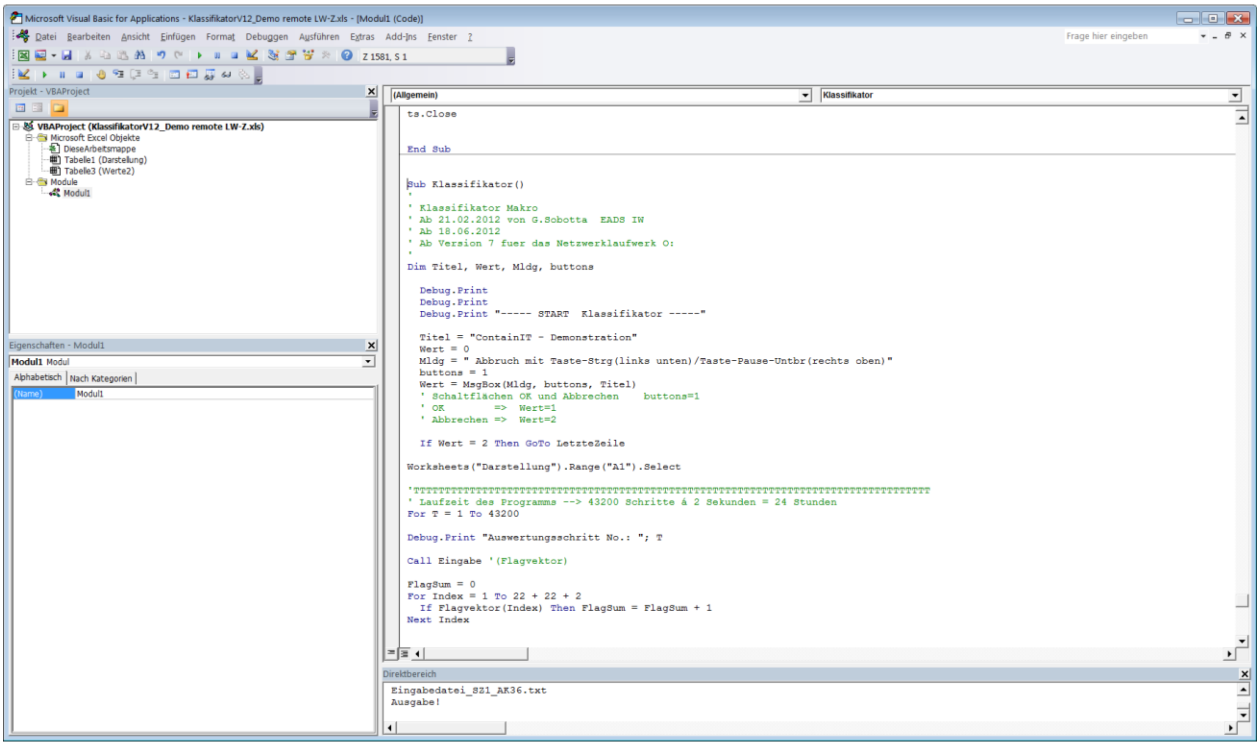


Abbildung 26: Ausschnitt aus VBA-Quellcode zur Excel-Simulation

In Abbildung 27 ist die Funktionalität der Datenfusion als auch des Risiko-Profiling der Excel-Simulation für die Projektdemontration dargestellt.

Die Information der Eingabedaten als auch die Ausgabedaten der Datenbank sind jeweils in Form von Text-Dateien dargestellt, welche auf für die IKT Systeme der Projektpartner zugänglichen Netzwerk-Festplatten lokalisiert wurde. Konflikte durch gleichzeitige Lese- und Schreibzugriffe wurden per Software abgefangen, damit ohne besondere Berücksichtigung der Datenentstehung und -speicherung durch z.B. die Telematiksysteme diese parallel dazu für das Risiko-Profiling weiter zu verarbeiten. Diese Forderung war u.a. dadurch gegeben, dass auch manuelle Einträge in die Text-Dateien beispielsweise für Profiling-Ergebnisse möglich sein sollten, ohne dafür zusätzliche komplexe Interfaces zur real operativen Software des Verbundpartners SAPPER einsetzen zu müssen.

Für die Ausgabedaten wurde an diesem Konzept gleichermaßen festgehalten. Durch diese Vorgehensweise wird es ermöglicht, simultan mehrere gleiche Ein- und Ausgabedateien parallel zu verwenden, um damit unnötige Wartezeiten durch Kommunikationskonflikte zwischen den einzelnen IKT-Systemen zu verhindern. Für die Klassifikation wird nach jedem Zugriff eine Aktualisierung der Daten nach deren Datenalter vorgenommen, bevor der Klassifikationsalgorithmus eingesetzt wird. Die in Abbildung 27 gezeigte Datenbank hat für die Projektdemonstration diese Aufgabe.

Im Rahmen eines Containertransports müssen auffällige dynamische Daten wie Sensordaten dann gespeichert werden, wenn sie „verdächtige Werte“ aufweisen, die aber noch nicht zu einem Alarmfall führen können, aber für spätere Entscheidungen relevant sind. Diese Rolle übernimmt ebenfalls die Datenbank.

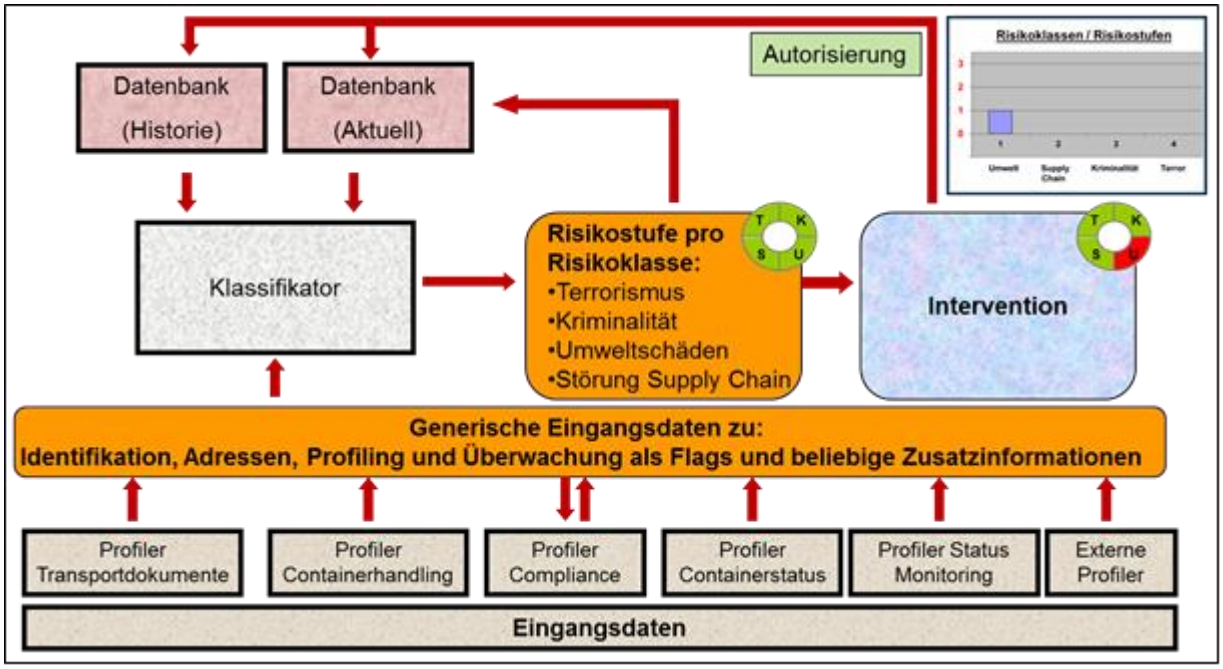


Abbildung 27: Konzept der Excel-Simulation zur Gefahrenklassifikation für die Projektdemonstration

In Abbildung 28 ist beispielhaft eine real umgesetzte Datenkommunikation unter Nutzung operativer IKT Systeme von EADS Astrium und dbh während der Projektdemonstration zur Excel-Simulation von EADS IW aufgegezeigt. Die verschlüsselten Datenlinks von erfolgen dabei über eine Iridium Satellitenkommunikation sowie über das Internet.

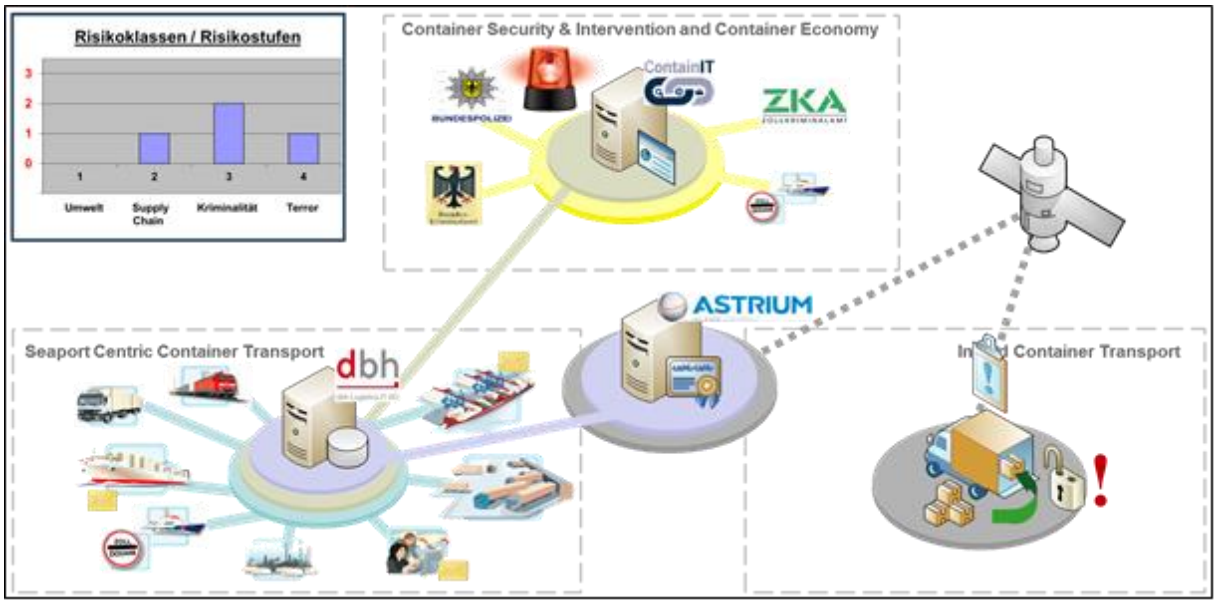


Abbildung 28: Reale Datenkommunikation während der Demonstration

Ergänzend zur Livepräsentation der Projektdemonstration wurde anhand einer PowerPoint Präsentation, wie hier stellvertretend in Abbildung 29 für Schritt 7.4 der „Finalen Intervention“ des Demonstrationsszenarios von Abbildung 23 dargestellt, nochmals der permanent Unterschied zwischen der heutigen realen Welt der Containertransporte und der ContainIT Lösung sowie deren Benefit aufgezeigt.

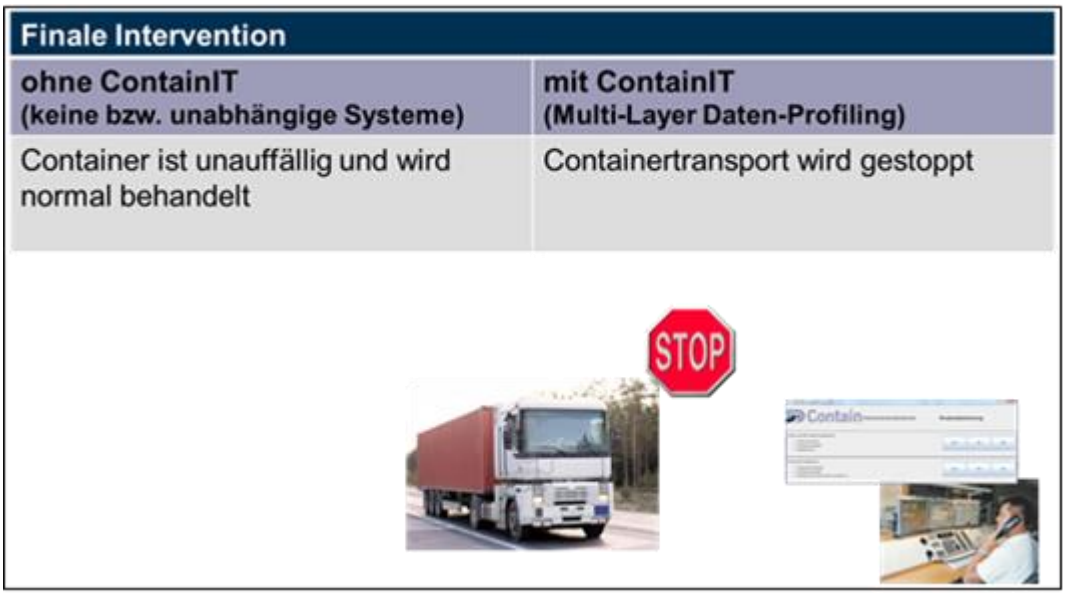


Abbildung 29: Slideshow zur unterstützenden Erklärung während der Demonstration

2.2 Positionen des zahlenmäßigen Nachweises

Die während der Durchführung des Projekts entstandenen Kosten erstrecken sich zum Großteil für eigene Personalmittel seitens EADS IW. Ein kleinerer Anteil der Kosten betrug die Unterbeauftragung der Unternehmensberatung Meyer aus Hamburg, für deren fachliche Unterstützung im Bereich der Containerlogistik, elektronischer Geschäftsverkehr sowie Standardisierung in logistischen und sicherheitsrelevanten Geschäftsprozessen.

Die seitens EADS IW für das Projekt vorkalkulierten Kosten wurden eingahalten.

2.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Wie bereits zuvor in den Kapiteln 1.1 und 1.2 dargestellt, bestand aufgrund der Komplexität der Projektthematik die direkte Notwendigkeit, dass nicht einzelne Akteure sondern nur eine Gruppe ausgewählter Akteurer von Containertransporten zusammen an einer Lösung zur verbesserten Sicherung von Transportketten erfolgreich arbeiten können - was sich im Nachhinein bestätigt hat. Darauf basierend hat es sich als ebenso richtig erwiesen, wie letztendlich das gesamte Projektkonsortium in Anzahl und Art der Partner zusammengesetzt war.

Die verkürzte Projektlaufzeit mit Hinblick auf die damlige politische Situation bzgl. der dynamischen Entwicklungen seitens der Gesetzeslage zur Containersicherheit in verschiedenen relevanten Ländern, wie z.B. in den USA, war ebenfalls sinnvoll und hilfreich.

Die seitens EADS IW als auch der anderen Projektpartner geleistete Arbeit wie auch die gesamten Projektergebnisse wurden nach der Abschlusspräsentation und der dabei gezeigten Live-Projektdemonstration des IKT-basierten Gesamtkonzepts zur Containersicherheit von ContainIT seitens den Gästen von Behörden, der Industrie als auch von den BMBF-Partnerprojekten zur Containersicherheit einhellig bestätigt.

Die seitens EADS IW als auch der anderen Projektpartner im Rahmen des Projekts ContainIT entstandenen Konzepte, Methoden und Technologien können somit die Realisierung von einzelnen Teilaspekten der Projektidee von ContainIT als auch die Übertragung bzw. die Weiterführung des Gesamtkonzepts in anderen Projekten ermöglichen.

Die im Gesamtvorhaben des Projektverbunds von ContainIT als auch die im Teilvorhaben von EADS IW zu anfangs definierten Projektziele wurden innerhalb der Projektlaufzeit erreicht.

2.4 Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse

Die im Gesamtverbundvorhaben ContainIT generell gewonnenen Erkenntnisse zum Themenkomplex der Containertransporte und zur Containersicherheit als auch die Projektergebnisse aus dem Teilvorhaben ContainIT EADS werden von EADS IW allen Geschäftsbereichen der EADS zugänglich und nutzbar gemacht werden. Hierbei kann einerseits eine direkte Nutzung der Erkenntnisse und Ergebnisse aus dem Projekt durch Unterstützung der EADS Geschäftsbereiche auf dem Themengebiet der Containersicherheit und Containertransporte erfolgen. Indirekt werden andererseits ebenso alle Erkenntnisse und Ergebnisse aus dem Projekt in neue Forschungsaktivitäten seitens EADS IW mit einfließen und somit für die Geschäftsbereiche der EADS nutzbar gemacht werden.

In Bezug auf die wirtschaftliche Verwertbarkeit der Projektergebnisse stehen dabei der im Gesamtverbundvorhaben ContainIT beteiligte EADS Geschäftsbereich Astrium im Vordergrund, welcher durch EADS IW in seinen Aktivitäten im Bereich der Containertelematiksysteme mit dem Produkt SecureSystem bei dessen technologische Weiterentwicklung sowie dessen positiver Marktentwicklung unterstützt werden kann. Dabei spielen z.B. die generellen Erkenntnisse zur Landschaft der beteiligten Akteure, deren unterschiedlichen Rollen und Interessen bei Containertransporten (teils auch variierend von Containertransport zu Containertransport) eine wesentliche Erkenntnis. Noch relevanter sind technische Aspekte der nutzbaren Projektergebnisse wie z.B. Anforderungen und Ausprägungen zur IKT-Infrastruktur, IKT-Sicherheit, Systemfunktionalitäten oder Datenmanagement (Erfassung, Aufbereitung, Verwertung, Sicherheit).

Weiter wird seitens EADS IW angestrebt, dass z.B. die aktuellen und zukünftigen Aktivitäten für Dienstleistungen und technische Lösungen im Bereich der Logistik und Sicherheit in verschiedenen anderen EADS Geschäftsbereichen, entsprechend unterstützt werden können. Hierbei sind Projektergebnisse wie z.B. zur Systemstatusbeschreibung mittels Flag-Zuständen, der Datenfusion als auch der Bewertung eines Systemstatus in Form eines Risiko-Profiling von großem Interesse.

Daneben spielt die wissenschaftlich/technologische Verwertung der Projektergebnisse ebenfalls eine große Rolle. So beinhaltet diese z.B. das Vorantreiben der Aktivitäten auf Veranstaltungen und Initiativen wie im März 2003 bei einem mehrtägigen Workshop der EU Kommission beim JRC in Ispra/Italien. Die EU Kommission hatte zu einem Workshop für „Supply Chain Security Technology“ eingeladen. Ziel des Workshops war bzw. ist hierbei eine multinationale Kooperation zwischen der EU und den USA auf dem Gebiet der Containersicherheit. Es wird angestrebt im Rahmen laufender Aktivitäten im 7. Rahmenprogramm der EU bzw. auf neu zu schaffender Basis ein Pilot Projekt zur „Supply Chain Security“ zu etablieren. Im Fokus stehen dabei die Stimulation von neuen Innovationen durch die Entwicklung neuer Standards, Methoden und Tools, deren gemeinsame Nutzung sowie des Transfers von Knowhow zwischen den beteiligten Staaten als auch innerhalb der Community. Hierbei hat EADS IW die Interessen Astrium bzw. EADS als auch des gesamten Projektkonsortiums von ContainIT vertreten.

2.5 Während der Projektdurchführung bekannt gewordener Fortschritt auf dem Arbeitsgebiet

Zusammen mit ContainIT wurden in Deutschland drei weitere Projekte mit der Thematik Containersicherheit zur Absicherung der Warenketten gestartet. Zu einen war die Laufzeit dieser Projekte länger als für ContainIT veranschlagt, so dass Projektergebnisse teils erst später verfügbar waren. Relevanter ist jedoch, dass die jeweilige Projektidee als auch die damit verbundenen spezifischen Arbeitsschwerpunkte der Projekte sehr unterschiedlich gestaltet waren. Es konnte somit bzgl. der Projektinhalte von EADS IW keine thematische Überschneidung als auch kein entsprechender Fortschitt mit zugehörigen Ergebnissen bekannt werden. Mit dem Projekt ECSIT bestand während der kompletten Projektlaufzeit der direkte Kontakt, da zwei Projektpartner von ContainIT dort ebenfalls Projektpartner waren. Zu anderen Projekten hatten einzelne Projektpartner von ContainIT einen etwas loseren Kontakt. Ein formloser Austausch zum Status bzw. zur Entwicklung des jeweiligen Projekts war somit gegeben.

Seitens der EU gab bzw. gibt es ebenso einige beachtenswerte Projektaktivitäten zum Themenkomplex der Container Sicherheit als auch generell zur Absicherung von Warenketten. Wie auf nationaler Basis war auch hier die thematische Spreizung der Projekte sehr groß, als auch deren Zeitfenster waren dem von CotnainIT nachgelagert, so dass diese Projekte derzeit noch andauern.

Zu nennen sei hier vor allem das EU-Projekt Contain. In Contain werden im Wesentlichen Informationen von Container Monitoring Devices, wie z.B. Position, Zeit oder Containerstatus (Tür, Temperatur, etc.), in einem Netzwerk dem sogenannten EU Containers Surveillance Framework zusammengebracht und zusammen mit weiteren zusätzlichen Informationen zum Containertransport bewertert, was zu einer entsprechenden Risikoeinstufung führt. Der umfassende Ansatz von ContainIT zur Vernetzung aller IKT-Systeme und zur Nutzung aller vorhandener Informationen wie z.B. die von Fracht- und Transportpapieren kommt dabei jedoch nicht zum tragen. Der technische Fokus liegt deutlich mehr ausgerichtet auf die Container Monitoring Devices und deren technologischen Möglichkeiten sowie zur Integration und Demonstration der genutzten Technologien in einem realen Containertransportszenario. Zum Projekt Contain wie auch zu anderen FP7-Projekten der EU besteht seit dem Workshop der EU Kommission für „Supply Chain Security Technology“ beim JRC in Ispra/Italien im März 2013 ein direkter Kontakt als auch das Interesse zu einer Kooperation in einem zukünftigen Projekt. Während ausführlichen Gesprächen auf dem Workshop hat sich gezeigt, dass sich beide Projekte ContainIT und Contain inhaltlich als auch seitens der Projektpartner sehr gut ergänzen würden und eine gemeinsame Projektkooperation sich wohl als sinnvoll und zielführend erweisen würde.

2.6 Erfolgte oder geplante Veröffentlichungen des Ergebnisse

Klassische Veröffentlichungen in Form von Konferenzbeiträgen oder Journalbeiträgen gabe es seitens EADS IW keine.

Das Projekt ContainIT wurde im April 2012 in Berlin auf dem BMBF Innovationsforum für Zivile Sicherheit zusammen mit dem Projektpartner TH-Wildau mit einem gemeinsamen Poster im Namen aller Projektpartner während einer Postersession vorgestellt.

Im Rahmen der Projektabschlussveranstaltung im Dezember 2012 bei EADS IW in Ottobrunn bei München wurden zusammen mit allen Projektpartnern die Projektergebnisse vorgestellt, in Form von mehreren Präsentationen, Postern und einer Live-Projektdemonstration wie zuvor bereits in Kapitel 2.1.3 dargestellt. Zu Gast waren dabei z.B. Vertreter des Projektträgers VDI-TZ, BMBF-Partnerprojekte zur Containersicherheit, Vertreter von Behörden wie z.B. der WCO der UN, BAFA, TAPA EMEA oder BITKOM und vom Intitut ISPC des JRC der Europäischen Kommission.

Berichtsblatt

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

3. Titel

ContainIT EADS - Entwurf einer vernetzten standardisierten IKT Architektur sowie Entwurf von Konzepten / Methoden zur Optimierung der physischen Sicherheit und des integrierten Risikomanagements

4. Autor(en) [Name(n), Vorname(n)] Neubauer, Frank	5. Abschlussdatum des Vorhabens 31.12.2012
	6. Veröffentlichungsdatum
	7. Form der Publikation
8. Durchführende Institution(en) (Name, Adresse) EADS Deutschland GmbH EADS Innovation Works Germany 81663 München	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N11006
	11. Seitenzahl 65
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben -
	14. Tabellen 13
	15. Abbildungen 29

16. Zusätzliche Angaben

-

17. Vorgelegt bei (Titel, Ort, Datum)

-

18. Kurzfassung

Innerhalb des Gesamtvorhabens “ContainIT” war das übergeordnete Ziel die Steigerung der Containersicherheit durch vernetzte IT-Systeme. Im Teilvorhaben “ContainIT EADS” war zur Erreichung dessen der Fokus der Arbeiten von EADS Innovation Works auf den Entwurf einer vernetzten standardisierten IKT Architektur sowie der Entwurf von Konzepten und Methoden zur Optimierung der physischen Sicherheit und des integrierten Risikomanagements ausgerichtet. Hierzu wurde ein Konzept für eine vernetzende IKT Architektur sowie für ein generisches Datenmodell zum übergreifenden Datenaustausch entworfen. Weiter wurden ein Konzept und Methoden zur sicherheitsbezogenen Gesamtsystembeschreibung mittels Flag-Zuständen zur Datenfusion und ein darauf aufbauendes Risiko-Profiling entworfen. Im Rahmen der Projektdemonstration erfolgte eine funktionale Implementierung der vernetzenden IKT Architektur als auch Risiko-Profiling basierend auf Flag-Zuständen.

19. Schlagwörter

Container, Sicherheit, Container-Security, Informations- und Kommunikations-Technologie (IKT), Risiko-Profiling, Risiko-Management, Multi-Layer-Ansatz, tri-modale Logistik, Telematik

20. Verlag -	21. Preis -

Document Control Sheet

1. ISBN or ISSN -	2. type of document (e.g. report, publication) final report
3. title ContainIT EADS – design of an cross-linked standardised ICT architecture as well as the design of concepts / methods for optimisation of the physical security and an integrated risk management	
4. author(s) (family name, first name(s)) Neubauer, Frank	5. end of project 31.12.2012
	6. publication date
	7. form of publication
8. performing organization(s) (name, address) EADS Deutschland GmbH EADS Innovation Works Germany 81663 München	9. originator's report no.
	10. reference no. 13N11006
	11. no. of pages 65
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references -
	14. no. of tables 13
	15. no. of figures 29
16. supplementary notes -	
17. presented at (title, place, date) -	
18. abstract Within the project "ContainIT" the overall goal was to increase container security through networked IT systems. In the project "ContainIT EADS" the work of EADS Innovation Works was focused on the design of a cross-linked standardised ICT architecture and the design of concepts and methods for optimizing the physical security and integrated risk management to achieve the overall goal of the project. For this purpose, a concept for a cross-linking ICT architecture as well as a generic data model has been designed for general data exchange. Next a concept and methods for safety-related overall system description using flag states for data fusion and a following risk profiling were designed. As part of the demonstration of the project, a functional implementation of the cross-linking ICT architecture and risk profiling based on flag states were built.	
19. keywords container, security, information- and communication-technology (ICT), risk-profiling, risk-management, multi-layer approach, tri-modal logistics, telematics	
20. publisher -	21. price -