Schlussbericht

Containersicherheit durch vernetzte IT-Systeme (ContainIT):

Kosten-/Nutzen-Modelle sowie Buchungsplattform-Konzept zur Sicherung der Warenketten

FKZ:	13N11008
Laufzeit des Vorhabens:	01.08.2010 – 31.12.2012
Berichtszeitraum:	01.08.2010 – 31.12.2012

Inhaltsverzeichnis

I. Kurzdarstellung

1. Aufgabenstellung

Das Forschungsprojekt ContainIT beabsichtigte eine Verbesserung der Sicherheit internationaler Container Supply Chains.

Ein wesentliches Ziel des Projektes war dabei der Entwurf eines Informations- und Kommunikationstechnologie (IKT)-basierten Multi-Layer-Ansatzes (physische Handhabung des Containers, Umgang mit den containerbegleitenden Dokumenten und IKT-basierter Datenaustausch entlang der Transportkette) für die sichere Logistik von Containertransporten – von der Gestellung und Beladung bis zur Entladung und Ablieferung des leeren Containers in das Depot.

Die zentrale Idee des Projektes bestand in der innovativen Vernetzung der heute schon im Einsatz oder in der Entwicklung befindlichen einzelnen IKT-Systeme sowie der intelligenten Verdichtung aller Einzelinformationen zu einem konsolidierten Lagebild. Dieses ermöglicht es, Prozessausnahmen (Störungen) echtzeitnah zu identifizieren und in ihrer Ausprägung im Rahmen einer Risikoquantifizierung zu bewerten.

Inhaltlich wurden im Rahmen des Projektes drei wesentliche Themenfelder bzw. Arbeitspakete (AP) bearbeitet.

- **AP1:** Analyse bestehender **IKT-Architekturen** im Transportumfeld und Erarbeitung einer idealtypischen Soll-Architektur unter Einbeziehung der ContainIT-Plattform
- **AP2: Risikoanalyse und -management** im Status Quo sowie hinsichtlich der zentralen zu schaffenden ContainIT-Plattform
- **AP3: Wirtschaftlichkeitsbetrachtung** der Plattform und Erarbeitung möglicher Geschäftsmodelle (GM)

Als wesentliche Aufgabe gestaltete sich für Bosch im Rahmen von ContainIT die Durchführung der Wirtschaftlichkeitsanalyse der Plattform im dritten und letzten Arbeitspaket des Forschungsprojektes. Dies beinhaltete neben der Durchführung einer Kosten-Nutzen-Analyse auch die Ausarbeitung von Geschäftsmodellen zum Betrieb der Plattform. Darüber hinaus war Bosch an einer Reihe von weiteren Arbeitspaketen sowohl zu Fragen der IKT-Architektur als auch zu Risikoanalysen und -management beteiligt.

2. Voraussetzungen

Das Konsortium des ContainIT-Projektes bestand aus den in unten stehender Abbildung dargestellten elf Unternehmen bzw. Forschungseinrichtungen. Diese Zusammensetzung garantierte eine optimale Abdeckung und Aufteilung von Projektinhalten und -zielen.

Abbildung 1: Konsortialpartner von ContainIT

Die Laufzeit von ContainIT war ursprünglich von August 2010 bis Ende Juli 2012 vorgesehen und wurde Anfang 2012 kostenneutral bis Ende Dezember 2012 verlängert.

Wesentliche Beweggründe für die Initiierung von ContainIT waren die zunehmende Bedeutung des Containers im stetig wachsenden internationalen Warenverkehr und die damit einher gehende Relevanz der Sicherung des Transportes vor immanenten Gefahren wie etwa Terrorismus. Nicht zuletzt die Verabschiedung des HR1-Gesetzes durch die USA zum Scanning jedes Containers mit Ziel USA am Abgangshafen (100%-Scanning-Initiative) – ursprünglich vorgesehen ab dem 01.07.2012 – und die damit verbundenen Zeitverluste und Kosten forcierten die Suche nach Alternativen zur Sicherung von Containertransporten.

Vor diesem Hintergrund sei auch auf unterschiedliche Forschungsprojekte mit Förderung durch die EU verwiesen, die – wie ContainIT – die Sicherung von internationalen Gütertransporten verfolgen. Hier sind beispielhaft INTEGRITY, SMART-CM oder CASSANDRA zu nennen. Auch auf Bundesebene bestehen inhaltliche Überschneidungen, etwa zu den Forschungsprojekten ECSIT und SefLog, beide ebenfalls Bestandteil des Bundesministerium für Bildung und Forschung (BMBF)-Forschungsprogramms „Forschung für die zivile Sicherheit“, insb. Sicherung der Warenketten. Nachfolgend wird eine kurze Übersicht der genannten Forschungsprojekte gegeben. Hinsichtlich weiterer Informationen siehe auch Abschnitt I.4.

Das EU Forschungsprojekt INTEGRITY – „Intermodal Global Door-to-Door Container Supply Chain Visibility“ (Laufzeit 2008-2011) – verfolgte das Ziel, die Transparenz globaler Containertransporte vom Versender bis zum Empfänger zu verbessern. Kern des Projektes war dabei die Entwicklung der IT-Plattform „SICIS – Shared Intermodal Container Information System“, welche Unternehmen und Behörden die Möglichkeit bietet, jederzeit auf Planungsdaten und Statusinformationen der Containertransporte zuzugreifen. Zudem ist die SICIS eine offene, weltweit nutzbare Plattform, zu der alle Akteure der Warenkette Zugang haben.

Das EU Projekt SMART-CM (Laufzeit 2008-2011) wiederum zielte auf eine Sicherung von Container Supply Chains insb. durch den Einsatz von Container Security Devices (CSDs) ab. Dabei soll auf die durch den Einsatz von unterschiedlichen Telematiksystemen resultierenden Informationen über eine zentrale Plattform zugegriffen werden können.

Ferner baut das EU Forschungsprojekt CASSANDRA auf vorherigen EU-Forschungsprojekten wie INTEGRITY und SMART-CM auf. Gestartet in 2011, hat das Projekt eine Laufzeit bis 2014 und zielt ebenfalls auf eine effektivere und effizientere

Containersicherheit ab. Dabei werden Daten aggregiert und auf dieser Basis Risiken für Privatwirtschaft und Behörden bewertet. Somit liegen signifikante Parallelen zum ContainIT-Projekt vor, allerdings mit einem europaweiten und nicht nationalen Ansatz.

Das BMBF-Forschungsprojekt ECSIT („Erhöhung der Containersicherheit durch berührungslose Inspektion im Hafen-Terminal“) mit einer Laufzeit von 2010 bis 2013 zielt ebenfalls auf die Verbesserung der Sicherheit bei Containertransporten ab. Es untersucht insb. den Einsatz neuartiger Inspektionstechnologien im Hafenumfeld und quantifiziert u.a. die finanziellen Auswirkungen einer eventuellen Umsetzung der 100%-Scanning-Initiative der USA.

Auch das BMBF-Forschungsprojekt SefLog beabsichtigt die Verbesserung der Sicherheit im Umfeld der Transportlogistik. Dabei werden im Rahmen des Projektes Transportprozesse im Detail gezielt auf Sicherheitsrisiken untersucht und die Wahrscheinlichkeit und Attraktivität für kriminelle Handlungen analysiert. In weiteren Projektschritten werden entlang der Liefer- bzw. Prozesskette gezielt die Aufdeckung, die Möglichkeiten der Abwendung und die Maßnahmen zum Umgang mit entstandenen Sicherheitsrisiken untersucht.

Das Alleinstellungsmerkmal von ContainIT gegenüber den anderen genannten Forschungsprojekten ist ein zentrales Risikoprofiling eines jeden transportierten und auf der Plattform aufgeschalteten Containers, verbunden mit der Möglichkeit zur Intervention bei einer identifizierten Gefahr. Ferner ist hier auch der geographische Fokus auf Deutschland zu nennen. Bei der ContainIT-Plattform wird dem jeweiligen Container auf Basis aggregierter entlang der Container Supply Chain bei Transportbeteiligten verfügbaren Informationen ein Risikostatus zugewiesen. So identifiziert die Plattform frühzeitig gefährliche Container und ermöglicht die zeitnahe Einleitung von Interventionsmaßnahmen.

3. Planung und Ablauf des Vorhabens

Bereits in der Vorbereitung des Forschungsprojektes fand ein intensiver Ideenaustausch zwischen einzelnen Projektpartnern statt.

In unten stehender Abbildung ist ein Projektplan mit Zeitindikation zur Abarbeitung der einzelnen Arbeitspakete dargestellt. Ferner sind hier auch verschiedene Meilensteine des Projektes genannt.

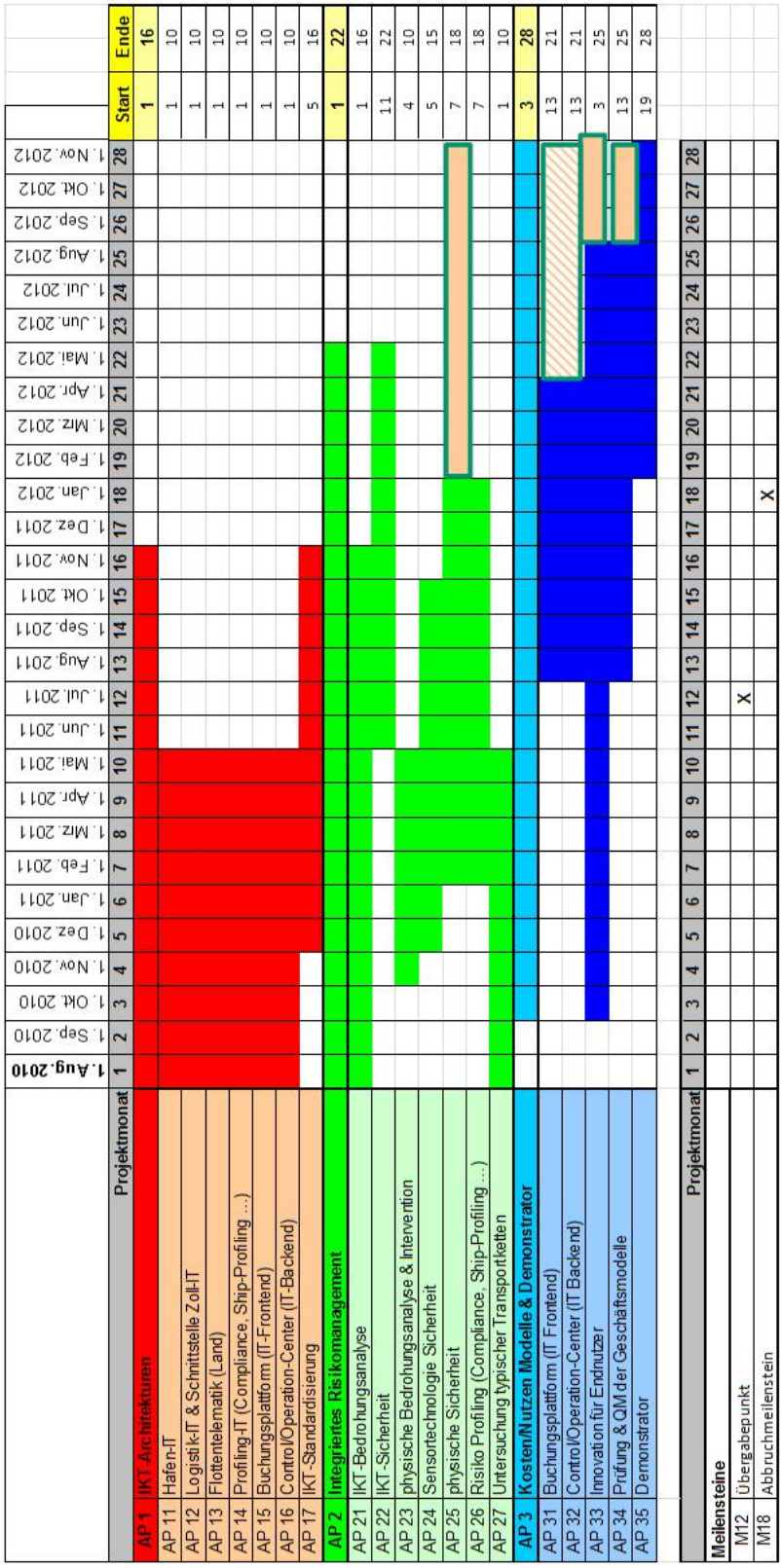

Abbildung 2: Projektplan ContainIT

4. Wissenschaftlicher und technischer Stand

Heutige Überwachungskonzepte im Bereich des Containertransports bilden überwiegend Insellösungen für Teilbereiche der Logistikkette ab. Dies führt zu einem lückenhaften und unzureichenden Informationsfluss innerhalb des Containertransportes. Folglich sind eine umfassende Risikobetrachtung sowie die daraus resultierende angemessene Intervention in Gefahrensituationen nicht oder nur bedingt möglich.

Auf europäischer Ebene stellte bspw. das bereits zuvor genannte, vom ISL koordinierte und EU-geförderte Projekt „INTEGRITY -Intermodal Global Door-to-Door Container Supply Chain Visibility“ erste Ansätze dar, die das Ziel verfolgen, die Transparenz globaler Containertransporte vom Versender bis zum Empfänger zu verbessern. Mittels der unter I.2. angesprochenen „SICIS-Plattform“ können Unternehmen und Behörden jederzeit auf Planungsdaten und Statusinformationen der Containertransporte zugreifen. Auch die anderen unter I.2 genannten Forschungsprojekte, welche sich zum Teil noch in der Ausarbeitung befinden, zeigen die gestiegene Relevanz der Containersicherheit auf und verdeutlichen diesbzgl. die exponierte Forschungsaktivität.

Vor dem Hintergrund von ContainIT ist auch auf die heute existierenden unterschiedlichen Systeme zur Containerüberwachung, die über eigenständige Buchungsplattformen verfügen, hinzuweisen. Diese Systeme sind jedoch auf Teilaspekte bzw. Teilprozesse beschränkt oder auf einzelne Anwendergruppen zugeschnitten, wodurch eine ganzheitliche Überwachung des Containers entlang seines Transportweges verhindert wird.
Auch wenn vereinzelt Ansätze und Pilotprojekte bestehen, die die Konsolidierung und Bereitstellung von Logistikdaten untersucht haben bzw. untersuchen, wurde dabei jedoch bisher kein ganzheitlicher Ansatz gewählt, der eine übergreifende Buchungsplattform beinhaltet und eine kommerzielle Anwendung erreicht hat.

Basierend auf der Tatsache, dass in Deutschland derzeit nur Systeme vorhanden sind, welche sich auf bestimme Teilaspekte bzw. Teilprozesse konzentrieren, wurde durch ContainIT diesbzgl. ein ganzheitlicher Ansatz verfolgt, welcher geographisch einen Fokus auf Deutschland legt.

Vor diesem Hintergrund wurde durch ContainIT die technische und wirtschaftliche Machbarkeit einer ganzheitlichen Containerüberwachung – vom Urversender bis Endempfänger – untersucht. ContainIT soll dabei verfügbare Informationen aus IKT-Systemen von Beteiligten entlang der Containertransportkette aggregieren und darauf aufbauend ein Risikoprofiling je Container durchführen. Ferner bietet ContainIT Beteiligten über eine Buchungsplattform nach individuellen Zugriffs- und Editierungsrechten Zugang zu diesen Informationen.

Insbesondere das dynamische Risikoprofiling der ContainIT-Plattform, gepaart mit der Möglichkeit der Einleitung von entsprechenden Interventionsmaßnahmen und dem geographischen Fokus auf Deutschland sind hier als Alleinstellungsmerkmale von ContainIT anzusehen.

Nachfolgend ist eine Auswahl wesentlicher Literatur dargestellt, welche für die Ausarbeitung des ContainIT-Projektes herangezogen wurden:

Bonte, D. / Carlaw, S. (2011): ABI-Research Report: Cargo Container Security and Tracking

Bieger, T. / zu Knyphausen-Aufseß, D. / Krys, C. (2011): Innovative Geschäftsmodelle, Berlin, Heidelberg.

Brugger, R. (2009): Der IT Business Case, 2. Auflage, Berlin, Heidelberg.

European Commission (2010): Commision Staff Working Document: Secure trade and 100% scanning of containers, http://ec.europa.eu/taxation_customs/resources/documents/common/whats_new/sec_2010_131_en.pdf, Abruf: 21.11.2012.

Eurostat (2012): Datenbank, http://epp.eurostat.ec.europa.eu/portal/page/portal/statistics/search_database, Abruf: 15.11.2012.

INTEGRITY / SMART-CM (2008): Global Container Supply Chain Compendium, http://www.integrity-supplychain.eu/, Abruf: 15.11.2012.

Martonosi, S.E. / Ortiz, D.S. / Willis, H.H. (2005): "Evaluating the viability of 100 per cent container inspection at America's ports", in: Richardson, H.W. / Gordon, P. / Moore, J.E. (eds.): The economic impacts of terrorist attacks, Cheltenham/Northampton, S. 218-241.

Porter, M. E. (1980): Competitive Strategy: Techniques for analyzing industries and competitors, New York.

5. Zusammenarbeit mit anderen Stellen

Während des Forschungsprojektes erfolgte eine Zusammenarbeit im Rahmen einer externen Kooperation mit folgenden assoziierten Projektpartnern:

- **Transported Asset Protection Association (TAPA)**, welche sich als Organisation mit der Sicherheit der gesamten Lieferkette befasst und in der die Bosch Sicherheitssysteme Mitglied sind. Dabei wurde mit der TAPA innerhalb von ContainIT im Rahmen von Experteninterviews die Ausgestaltung und Validierung von unterschiedlichen potenziellen Angriffsszenarien (z.B. hinsichtlich Diebstahl, Terrorismus) für einen beförderten Container vorgenommen (vgl. hierzu auch II.1).
- **„Joint Research Centre of the European Commission“ (JRC)** mit dem Institut für Schutz & Sicherheit der Bürger (IPSC), welches Bürger vor ökonomischen und technologischen Risiken schützt. Die Zusammenarbeit mit JRC im Rahmen von ContainIT wurde von Projektpartnern koordiniert; die Einbindung von Bosch war nur informativer Natur.
- **European Anti-Fraud Office of the European Commission (OLAF)**, welches die finanziellen Interessen der EU schützt und die erforderlichen Legislativmaßnahmen zur Verschärfung einschlägiger Vorschriften vor dem Hintergrund der Betrugsbekämpfung leitet. Die Zusammenarbeit mit OLAF im Rahmen von ContainIT wurde von Projektpartnern koordiniert; die Einbindung von Bosch war nur informativer Natur.

Ferner fand innerhalb der Ausarbeitung der einzelnen Arbeitspakete eine Zusammenarbeit mit zahlreichen Unternehmen und Behörden im Logistikumfeld statt. Diese wurden im Rahmen von Experteninterviews und Workshops hinsichtlich relevanter Fragestellungen konsultiert (siehe unten stehende Abbildung).

Behörde/Firma	Nutzergruppe	Astrium	Bosch	Daxosy	DFN	EADS	FT	Fraunhofer	SAP	SAGEM	THW ibau	TUHH	Datum
Polizei Bremen	Polizei	■	■										26.01.11
Gesamtverband der Deutschen Versicherungswirtschaft e.V.	Versicherung	■	■			■							02.02.11
Transfracht	Frachtführer Bahn		■										02.03.11
Hellmann	Spediteur/Frachtführer	■	■					■			■		14.03.11
CTS	Terminal (Inland)		■								■		22.03.11
Contargo	Leercontainer, Terminal (Inland), Frachtführer LKW/Binnenschiff		■								■		19.04.11
Eurogate	Terminal (Seehafen)	■	■								■	■	17.05.11
Wasserschutzpolizei Hamburg	Polizei		■	■							■	■	18.05.11
boxXpress	Frachtführer Bahn		■								■	■	18.05.11
Hapag Lloyd	Reederei	■	■								■	■	19.05.11
Zollamt Hamburg-Waltershof	Behörde	■	■	■								■	24.05.11
DB Schenker Rail	Frachtführer Bahn		■										26.05.11
Landeskriminalamt NRW	Polizei		■										05.09.11
Zoll Hamburg	Behörde	■	■										24.04.12
DB Schenker Rail	Frachtführer Bahn	■	■										24.04.12
Duisport	Hafen / Terminalbetreiber		■								■		13.06.12
Contargo	Leercontainer, Terminal (Inland), Frachtführer LKW/Binnenschiff		■										22.06.12
Hapag Lloyd	Reederei	■	■								■		27.06.12

■ = Lead / Orga
■ = Teilnahme

Abbildung 3: Experteninterviews im Rahmen von ContainIT

In diesem Zusammenhang ist auch ein Workshop mit Teilnehmern aus dem behördlichen Umfeld zu nennen, welchen die Projektpartner EADS, Astrium und Bosch im Januar 2012 veranstalteten. Hier lieferten Vertreter von Bundespolizei, Wasserschutzpolizei, Zollfahndungsamt sowie des Bundesministeriums für Verkehr, Bau und Stadtentwicklung wertvollen Input.

Zudem erfolgte ein Informationsaustausch des ContainIT-Projektkonsortiums mit weiteren Forschungsprojekten.

Hier ist auf Bundesebene das ebenfalls durch das BMBF geförderte Projekt ECSIT zu nennen. Dieses erforscht vor dem Hintergrund der 100%-Scanning-Initiative der USA, inwieweit neuartige Inspektionstechnologien zu einer Erhöhung der Sicherheit von Containern führen können und inwieweit sich diese in ein ganzheitliches Konzept einbinden lassen. Im Rahmen der Durchführung der Wirtschaftlichkeitsbetrachtung von ContainIT lieferte ECSIT wertvollen Input für die Projektarbeit (vgl. II.1).

Auf EU-Ebene erfolgte zudem ein Austausch mit dem Projekt „SMART-CM“, welches – vor dem Hintergrund des Einsatzes von Container Security Devices (CSD) – eine höhere Effizienz, Sicherheit, Transparenz und Wettbewerbsfähigkeit internationaler Containertransporte zum Ziel hat. Dieser Termin schaffte ein exponiertes Verständnis der verschiedenen existenten Forschungsprojekte im Containersicherheitsumfeld auf EU-Ebene und half dem ContainIT Projektkonsortium, das Alleinstellungsmerkmal von ContainIT im Folgenden weiter herauszuarbeiten. Ferner diente der Austausch auch als

wertvoller Input für die Ausarbeitung der in II.1. aufgezählten Sicherheits- und Wirtschaftsfunktion der Plattform.

II. Eingehende Darstellung

1. Verwendung Zuwendung und Ergebnis

AP 1: IKT-Architektur:

Im Rahmen der Bearbeitung von AP1 wurden mit ausgewählten Experten verschiedener potenzieller Nutzergruppen der ContainIT-Plattform Interviews durchgeführt. Die Erkenntnisse und Ergebnisse aus diesen Interviews haben neben AP1 auch Relevanz für die Ausarbeitung von AP2 und AP3.

Die wesentlichen Ergebnisse der Experteninterviews sind:

- Die genauere Erfassung des Status Quo von IKT-Struktur und Datenaustausch
- Ein besseres Verständnis von Anforderungen an ein ContainIT-Frontend und die IKT-Architektur
- Identifikation erster wirtschaftlicher Funktionen der ContainIT-Plattform / erster Abgleich mit potentiellen Systemusern (auch zur Identifikation von Innovationen)

Ferner erfolgten im Rahmen von AP1 eine Beschreibung der Bosch Container Security Box (CSB) und die Untersuchung dessen Funktionalität. Die CSB stellt ein Container Security Device (CSD) dar und ermöglicht die Überwachung von Containern mit Hilfe von Telematik. Dabei werden mittels Kontakt- und Infrarotsensoren sowohl die unauthorisierte Öffnung der Container-Türen als auch Bewegungen im Container-Innenraum detektiert.
Die Ortung des überwachten Containers findet satellitengestützt mittels GPS statt, die Emission eines Notrufs sowie der Positionsdaten an die Bosch-Leitstelle wird durch den Mobilfunkstandard GSM erzielt. Nach Eingang des Notrufs wird der Alarm zunächst seitens der Leitstelle verifiziert (z.B. durch Anruf beim LKW-Fahrer). Im tatsächlichen Angriffsfall findet im Anschluss anhand zuvor mit dem Kunden definierten Maßnahmenplänen eine Intervention, z.B. durch die Polizei, statt. In der unten stehenden Grafik ist die Containerüberwachung mittels der CSB dargestellt.

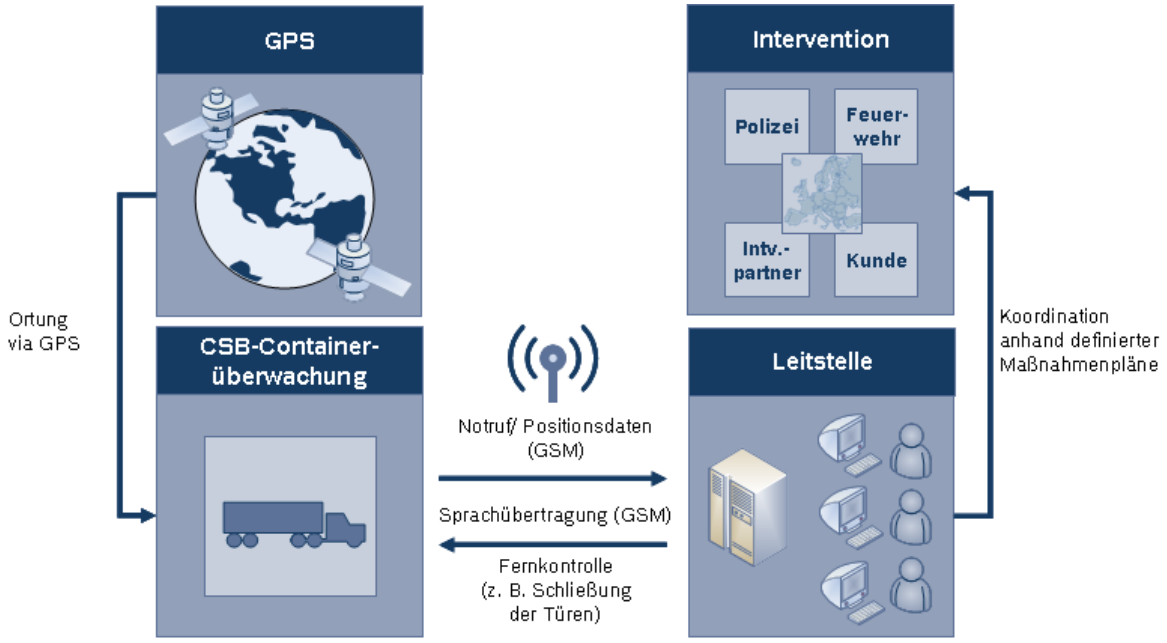

Abbildung 4: Containerüberwachung mit Hilfe der CSB

Im weiteren Verlauf des Arbeitspakets wurde zunächst durch das Konsortium die Gesamtarchitektur von ContainIT erarbeitet. Bosch war dabei verantwortlich für die Konzeption des Frontends der Plattform.

Eine grundlegende Frage in der Ausarbeitung der IKT-Architektur stellte die Anbindung verschiedener existenter Systeme im Transportumfeld an die ContainIT-Plattform dar. Grundsätzlich wäre hier eine Vielzahl von Schnittstellen erforderlich, um die unterschiedlichen Systeme anzubinden. Um dies zu umgehen und eine hohe Komplexität der Systemanbindung zu vermeiden, wurde entschieden, die IKT-Architektur der Plattform auf existenten Hafenkommunikationssystemen wie von Dakosy oder dbh zu basieren. Diese aggregieren schon heute Daten aus verschiedenen Systemen im Transportumfeld. Neben einer Anbindung dieser zentralen „Datenhandler“ ist der Anschluss externer Systeme direkt an ContainIT über Standardschnittstellen ebenfalls möglich. In unten stehender Abbildung ist die entwickelte IKT-Architektur von ContainIT dargestellt.

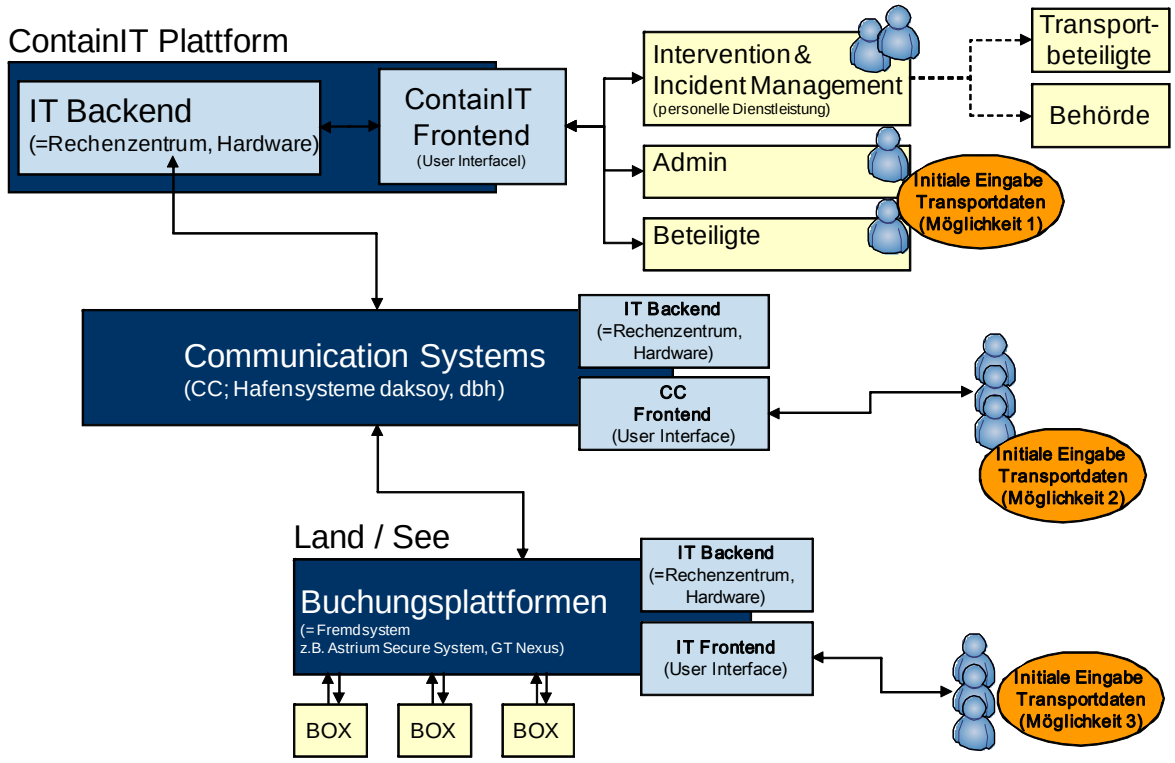

Abbildung 5: Gesamtarchitektur ContainIT

Wie in der Abbildung veranschaulicht, lassen sich grundsätzlich zwei Arten von Frontends der ContainIT Plattform unterscheiden. Einerseits ist dies das „eigene“ Frontend der ContainIT Plattform („ContainIT Frontend“) und andererseits sind es Frontends, welche auf bestehenden Kommunikationsplattformen – beispielsweise dakosy oder dbh im Hafenumfeld – existieren.
Als Ergebnis einer tiefer gehenden Analyse der bestehenden Strukturen wurde ausgearbeitet, dass einzig über das Frontend der ContainIT-Plattform eine Datenausgabe erfolgen muss. Diese für die Projektziele wichtige Ausarbeitung liegt nicht zuletzt darin begründet, dass auf diese Weise die Sicherheit der Ausgabedaten der Plattform gewährleistet werden kann.
Zudem erfolgte eine Identifikation von Gefährdungspotentialen beim Containertransport. Dieser Arbeitsschritt wurde begleitet von einer Identifikation und Definition potenzieller Nutzer der ContainIT-Plattform und fand Eingang in die funktionale Beschreibung des ContainIT-Frontends.
Als Konsequenz der Ermittlung von Nutzergruppen fand eine detaillierte Darstellung von Ist-Strukturen und -Prozessen diverser Beteiligter entlang der Containertransportkette – sowohl in Bezug auf den physischen Transport als auch die vorhandenen IKT-Systeme – statt. Hierbei gestalteten sich die zuvor beschriebenen Experteninterviews als besonders hilfreich. Im Rahmen dieser Experteninterviews konnten auch verschiedene Anforderungen potenzieller Nutzer an die ContainIT-Plattform, sowohl für das Front- als auch für das Backend, erarbeitet werden.
Bei der Ausarbeitung des Frontends der ContainIT-Plattform wurde im weiteren Verlauf von AP1 durch Bosch der logische Aufbau von ContainIT näher betrachtet (siehe unten stehende Abbildung). So konnten insb. Sicherheits- und Wirtschaftsfunktionen der Plattform

identifiziert werden. Hier lieferte neben den diversen durchgeführten Experteninterviews auch der Informationsaustausch mit dem EU-Projekt SMART-CM wertvollen Input.

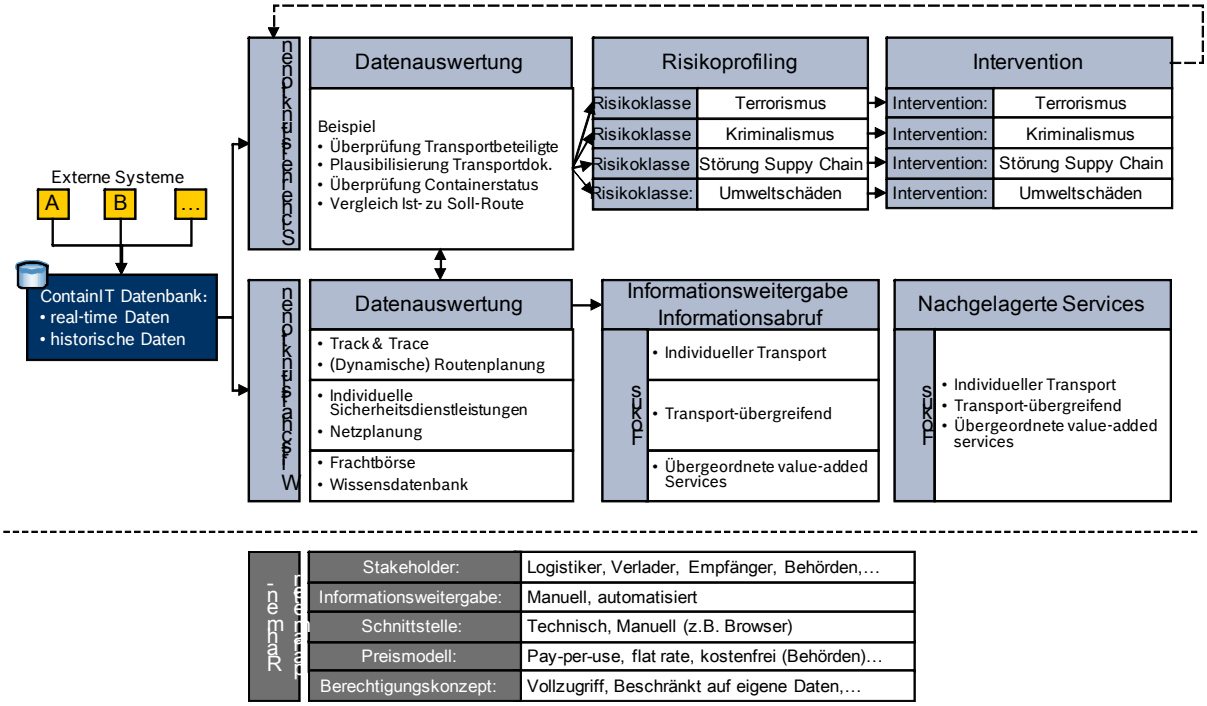

Abbildung 6: Logischer Aufbau ContainIT-Plattform

Die o.g. Sicherheitsfunktionen zielen auf eine Verbesserung der Sicherheit eines Containertransportes ab und lassen sich in die drei wesentlichen Schritte Datenauswertung, Risikoprofiling und Intervention unterteilen. Während bei der Datenauswertung bspw. die Überprüfung von Transportbeteiligten oder des Containerstatus stattfindet, erfolgt beim Risikoprofiling eine Kategorisierung in eine Risikoklasse, welche je nach Risikoursprung – Terrorismus, Kriminalismus, Supply Chain Störung oder Umweltschaden – in der Ausprägung differiert. Diese Differenzierung wird vorgenommen, damit innerhalb der Intervention zielgerichtet Maßnahmen eingeleitet werden können, denn die Maßnahmen, die bei möglichen Umweltschäden – z.B. einem Unfall mit Gefahrgütern – einzuleiten sind, sind andere, als z.B. bei einem Frachtdiebstahl auf einem Parkplatz.
Die wirtschaftlichen Funktionen hingegen stellen aus betriebswirtschaftlicher Sicht einen Mehrwert für Transportbeteiligte dar. Sie sind in die drei Schritte Datenauswertung (z.B. bei Tracking & Tracing), Informationsweitergabe/-abruf (z.B. in Bezug auf einen individuellen oder mehrere Transporte) und nachgelagerte Services (ebenfalls bspw. auf den einzelnen Transport oder eine Mehrzahl) zu unterteilen.
Als wirtschaftliche Funktion für Nutzer der Plattform ist bspw. die Überwachung eines Containers im Sinne von Tracking und Tracing zu nennen. Hier ist zwischen einer Echtzeitüberwachung (telematikunterstützt mit CSD) und einer diskreten Überwachung (ohne CSD) an ausgewählten Punkten entlang der Transportroute (z.B. durch Statusinformationen bei sämtlichen Containerumschlägen) zu unterscheiden.
Eine weitere wirtschaftliche Funktion stellt die Buchung von Interventionsleistungen im Falle einer Gefährdung des Containers, bspw. bei Türöffnung, dar. Hier werden im

Alarmfall entlang zuvor definierter Maßnahmenpläne bspw. Behörden oder Sicherheitsdienste informiert und etwa ein möglicher Diebstahl von Waren verhindert. Auch die Weitergabe von Risikoprofilen – etwa bzgl. diebstahlgefährdeter Routen oder Regionen – oder die Identifikation von Plagiaten anhand von Widersprüchen in Transportdokumenten sowie bisherigem Transportverlauf stellen weitere zentrale wirtschaftliche Funktionen der ContainIT-Plattform dar.
Mögliche weitere wirtschaftliche Funktionen der Plattform sind ein sicherer Informations- & Dokumentenaustausch über die Plattform, statische wie dynamische Planung von Transportrouten unter Berücksichtigung von aktuellen oder historischen Gefährdungslagen oder Stauinformationen sowie eine Wissensdatenbank, etwa mit Lagekarten oder transportmittelspezifischen Fahrplänen.
Eine Übersicht der verschiedenen wirtschaftlichen Funktionen der Plattform ist in unten stehender Abbildung dargestellt.

Abbildung 7: Wirtschaftliche Funktionen der ContainIT-Plattform

Ferner wurde in AP1 auch ein Berechtigungskonzept für die Nutzung der Plattform durch verschiedene Nutzergruppen – insbesondere hinsichtlich individuellen Lese- und Schreibrechten – sowie ein mögliches User Interface derselben entworfen. Zugleich erfolgte der Entwurf eines Sicherheitskonzeptes der Plattform, insb. hinsichtlich Benutzer-Authentifizierungsverfahren, verschlüsselter Datenkommunikation sowie Dokumentation und Protokollierung aller relevanten Vorgänge im Frontendsystem.

AP 2: Risikomanagement

Nachdem in AP1 bereits Anforderungen und Bedürfnisse potenzieller Nutzer einer ContainIT-Plattform eruiert werden konnten, wurde im weiteren Projektverlauf deutlich, dass insb. das behördliche Umfeld noch stärker eingebunden werden muss. Aufgrund der

Bedeutung von ContainIT für die nationale Sicherheit wurden die beiden Ziele verfolgt, das behördliche Verständnis für den Nutzen der IKT-Plattform zu verbessern sowie spezifische behördliche Anforderungen weiter zu ermitteln. Insb. in Bezug auf eine tatsächliche Umsetzung der konzipierten Plattform gestalten sich diese Ziele als erfolgsrelevant.
Die Bedeutung eines Austauschs zwischen Forschungsprojekt und Behördenumfeld hatte sich bereits in der Problematik der Datenbeschaffung zur Speisung der Plattform gezeigt, für die ein gesetzlicher Rahmen erforderlich scheint. Zusätzlich verdeutlichte sich im Rahmen der Forschungsarbeit, dass eine Plausibilisierung der ausgearbeiteten Schwachstellen entlang der trimodalen Logistikkette (Straße, Schiene, Wasser) und der darauf aufbauenden möglichen Angriffsszenarien wichtig ist.

Aus diesem Grund veranstalteten die Projektpartner EADS, Astrium und Bosch im Januar 2012 den bereits unter I.5. angesprochenen Workshop mit Teilnehmern aus dem behördlichen Umfeld. Hier lieferten Vertreter von Bundespolizei, Wasserschutzpolizei, Zollfahndungsamt und dem Bundesministerium für Verkehr, Bau und Stadtentwicklung wertvollen Input.

Folgende wesentliche Erkenntnisse resultierten aus dem Workshop:

1. Aus operativer, behördlicher Sicht gab es ein positives Feedback zu ContainIT. Hervorgehoben wurde ein besseres Lagebild durch die Vernetzung von vorhandenen Informationen. Ferner gestaltet sich das automatisierte Risikoprofiling für den Zoll sehr interessant, da heute der Prozess der Importkontrolle manuell geprägt ist.

2. Zur Realisierung von ContainIT ist eine politische Begleitung notwendig, die zum einen die Zuständigkeit auf ministerieller Seite regelt und zum anderen mittelfristig notwendige rechtliche Rahmenbedingungen für die Realisierung schafft.

Somit ist ein rechtlicher Rahmen für die wirtschaftliche Einführung der ContainIT-Plattform von grundlegender Bedeutung. Dies ist u.a. auf die geringe Bereitschaft von Transportbeteiligten zurückzuführen, relevante Daten und Informationen für eine Verbesserung der Prozesstransparenz preiszugeben. Vor diesem Hintergrund ist zu erwähnen, dass der betriebswirtschaftliche Erfolg vieler Marktteilnehmer auf der Intransparenz der Organisation des Transportes, insb. hinsichtlich Versendern, Empfängern, Logistikdienstleistern und/oder eingesetzten Sub-Dienstleistern, basiert.

Aufbauend auf den Experteninterviews mit Bedarfsträgern und direkten Beteiligten eines Containertransportes (siehe Abschnitt I.5) sowie den projektinternen Arbeiten wurde eine Methodik entwickelt, mit der differenzierte und umfassende Bewertungen des Risikos möglicher Angriffe auf die Container-Transportkette – bestehend aus Wahrscheinlichkeit und Auswirkung des Angriffs – vorgenommen werden können. Die Ausarbeitung der Methodik fand dabei federführend durch SAP und Bosch statt. Auf die Methodik wird im weiteren Verlauf dieses Abschnitts näher eingegangen.

Um potenzielle Angriffe auf Containertransporte bewerten zu können, fand im weiteren Verlauf des Arbeitspaketes auf Basis einer exemplarisch definierten Transportkette – welche die Transportmittel LKW, Bahn und Schiff beinhaltet – eine Ausarbeitung verschiedener Angriffsszenarien statt. Hier erfolgte auch wesentlicher Input durch die TAPA im Rahmen eines Experteninterviews, welcher sich in der Ausarbeitung und Validierung der Szenarien manifestierte.

Letztere basieren auf dem Transport eines Containers mit Fahrzeugteilen vom Werk eines Automobilherstellers in Ingolstadt bis zum Hafen Bremerhaven. Dabei erfolgt der Vorlauf Hinterland per LKW, der Hauptlauf per Bahn sowie die Hafenumfuhr von Hamburg nach Bremerhaven (aufgrund einer Dispositionsänderung durch den Hersteller mit verbundener Modifikation der Containerdestination und analoger Anpassung des Ladehafens) per LKW. Dieser grundlegende exemplarische Transportprozess ist nochmals in unten stehender Abbildung dargestellt.

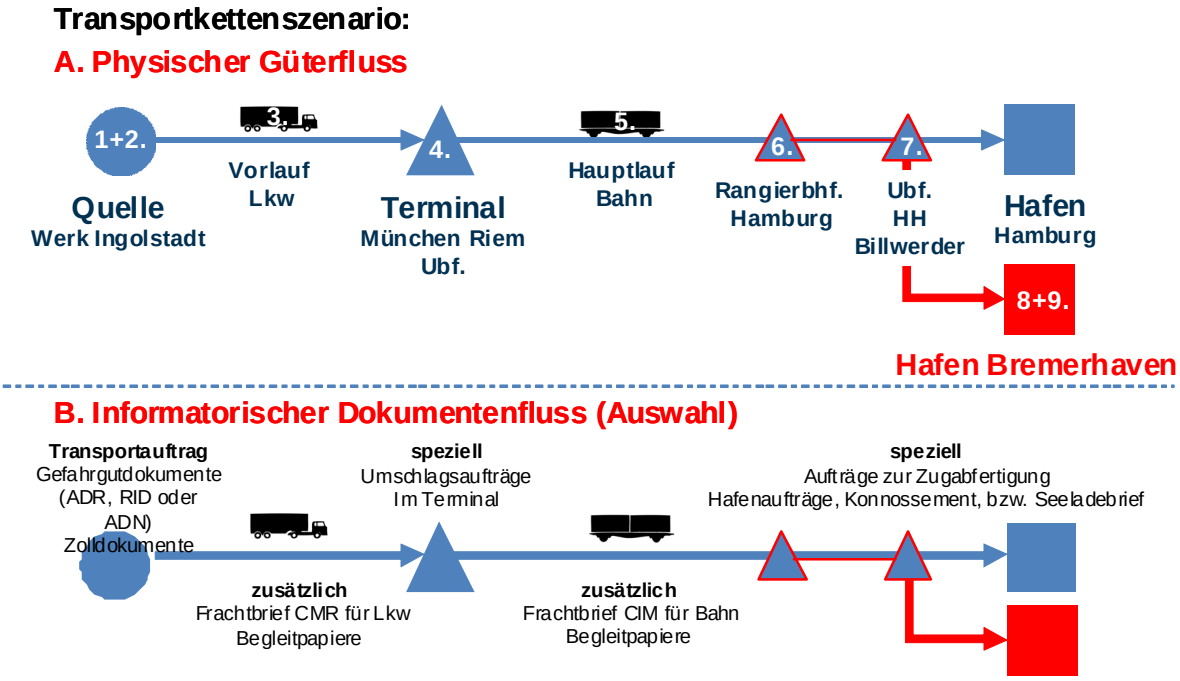

Abbildung 8: Exemplarisches Transportszenario

Mit Hilfe der Prozessmodellierungssoftware BizAgi wurde das oben beschriebene Transportszenario detailliert auf Prozessschrittbasis und gemäß der „Business Process Modelling Notation“ (BPMN) abgebildet. Dabei fand sowohl eine Berücksichtigung des physischen Transports des Containers als auch des begleitenden Dokumenten- und Informationsflusses statt. Unten stehende Abbildung stellt einen Ausschnitt des Gesamtmodells dar.

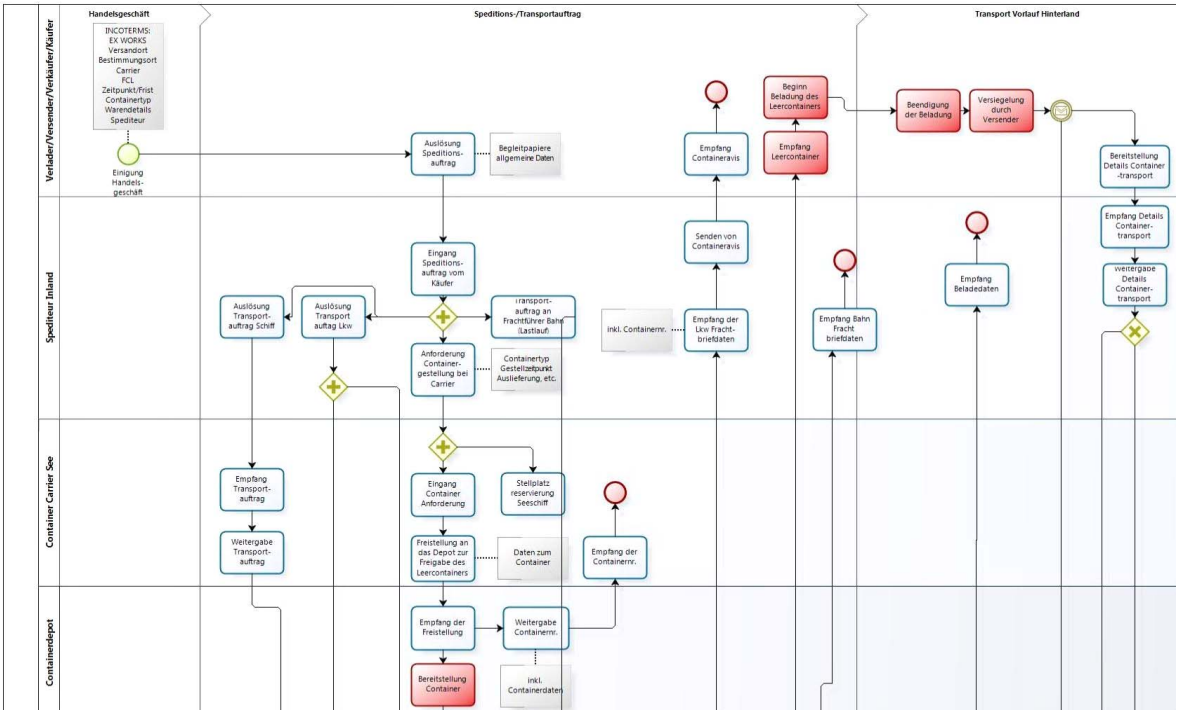

Abbildung 9: Ausschnitt des modellierten Transportszenarios gemäß BPMN

Die auf dem Transportszenario basierenden Angriffsszenarien wurden im Anschluss hinsichtlich des jeweiligen Risikos, bestehend aus Wahrscheinlichkeit und Auswirkung des Angriffs, bewertet.

Die Quantifizierung der Wahrscheinlichkeit eines Angriffs erfolgte dabei auf Basis einer Matrix, welche in Bezug auf den Angreifer dessen individuellen Fähigkeiten sowie dessen Bedarf an Unterstützung durch Dritte auf einer Ordinalskala von 1 (geringe Ausprägung) bis 4 (starke Ausprägung) je Angriffsszenario bewertet. Gleiches galt auch hinsichtlich der Umstände des Angriffs, z.B. in Bezug auf Zugangskontrollen des Angriffsziels oder die Auffälligkeit der Handlung zur Vorbereitung/Durchführung des Angriffs.
Zur Quantifizierung der Auswirkung eines Angriffs wurden in der Matrix ebenfalls auf einer Skala von 1 (geringe Ausprägung) bis 4 (starke Ausprägung) physische (z.B. Personen- und Umweltschäden) wie informatorische Schäden (z.B. hinsichtlich Vertraulichkeit und Integrität von Daten) bewertet. Ferner wurden allgemeine Auswirkungen eingeschätzt (z.B. finanzielle Schäden, Auswirkungen auf die Supply Chain, Imageschäden oder das Ausmaß der Rechtsverletzung). Die zugrunde gelegte Systematik ist in unten stehender Abbildung nochmals dargestellt.

		Bewertung Wahrscheinlichkeit (W)									x	Bewertung Auswirkung (A)									=	Risiko
		Angreifer			Umstände							Allgemein				Physisch		Informatorisch				
	Einschätzung	Organisation	Fähigkeit	Kooperation	Zugangskontrolle	Widerstand	Handlung	Überprüfung	Zugehörigkeit	Wahr-schein-		Finanziell	Suppy Chain	Imageschaden	Rechtsverletzung	Peronenschäden	Umwelt	Vertraulichkeit	Verfügbarkeit	Integrität	Aus-wirkung	W x A =
Szenario / Gewichtung		0,2	0,2	0,05	0,2	0,2	0,05	0,05	0,05	lichkeit		0,2	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	1	**Risiko**
U1: IT Angriff	G																					
U2a: Bombe LKW-Fahrer	E																					
	O																					
U2b: Bombe Ubf Riem	E																					
	O																					
U3: Nachsiegelung	E																					
	O																					
U4: IT Angriff Status	G																					

Abbildung 10: Matrix zur Bewertung des Risikos je Angriffsszenario

Die Angriffsszenarien unterschieden sich bspw. hinsichtlich der Motivation des Angreifers zwischen terroristischen (z.B. Bombenexplosion) und wirtschaftlichen (z.B. Diebstahl von Ware) Interessen.
Die Bewertung der Angriffsszenarien inklusive der jeweiligen Bildung einer Risikopunktzahl verfolgte verschiedene Ziele. Neben der Identifikation von Schwachstellen in exemplarischen Container-Supply Chains wurde in der Bewertung auch zwischen einer „Logistik-Welt“ ohne und mit einer Contain-IT-Plattform unterschieden. Auf diese Weise sollte der Mehrwert der Plattform, insb. für die Sicherheit im Containertransport, untersucht werden. **So konnte im Rahmen der Bewertung gezeigt werden, dass ContainIT das Risiko der betrachteten Angriffsszenarien merklich senkt**. Die Reduktion des Risikos beruht vor allem auf der Aggregation von Daten aus verschiedenen Quellen und der dynamisch – während des Transports fortlaufenden – Risikobewertung sowie dem damit verbundenen frühzeitigen erkennen von möglichen Gefährdungen.
Abschließend ist jedoch darauf hinzuweisen, dass ContainIT nicht alle denkbar möglichen Angriffsarten erkennen kann. Insbesondere Angriffe, die keine „Spuren“ in IT-Systemen hinterlassen, sind über ContainIT gar nicht oder nur indirekt zu identifizieren.

AP 3: Wirtschaftlichkeitsbetrachtung

Fokaler Bestandteil von AP 3 war die Erstellung einer Kosten-Nutzen-Analyse (KNA) der Plattform sowie die Erarbeitung von Geschäftsmodellen zu dessen Betrieb. Dabei ist grundsätzlich zu erwähnen, dass KNA und Geschäftsmodelle in einer gegenseitigen Abhängigkeit zueinander stehen.

Wesentliche Annahmen der Durchführung der KNA waren u.a.,

- dass die ContainIT Plattform für den behördlichen und kommerziellen Markt als Gesamtsystem entwickelt wird,
- dass auf Seiten der Behörden die Bereitschaft besteht, Risiko-Profiling durch einen ContainIT Betreiber durchführen zu lassen,
- sowie dass auf Seiten der Behörden eine Zahlungsbereitschaft für die Nutzung der Angebote besteht (hier ist insbesondere das Risiko-Profiling zu nennen).

Um die Auswirkungen der verschiedenen Geschäftsmodelle auf die Kosten-Nutzen-Analyse der Plattform abbilden zu können, erfolgte in einem ersten Schritt die Ausarbeitung zwei zentraler Geschäftsmodelle. Dabei wurde auf Basis existenter Techniken von Porter sowie dem wertbasierten Geschäftsmodellansatz ein Fragenkatalog erarbeitet und in Bezug auf ContainIT beantwortet. Inhalt war eine detaillierte Analyse von Wertschöpfung und Geschäftsumfeld der Plattform.
Auf Basis der beiden erarbeiteten Geschäftsmodelle wurde im Anschluss eine Kosten-Nutzen-Matrix erstellt, welche auf Annahmen und Erfordernisse beider Geschäftsmodelle eingeht. Mittels eines interaktiven Auswahlfeldes innerhalb der Kalkulation konnte das jeweilige Geschäftsmodell selektiert und somit die korrespondierende Wirtschaftlichkeitsbetrachtung aufgerufen und der Kapitalwert der Investition berechnet werden.
Hier fand auch die Ausarbeitung unterschiedlicher Szenarien statt, die eine optimistische, pessimistische oder neutrale Entwicklung der Rahmenbedingungen der Plattform-Implementierung widerspiegeln. Gleichzeitig erfolgte auch hinsichtlich der Schaffung eines gesetzlichen Rahmens zur obligatorischen Aufschaltung von Containertransporten auf die Plattform eine Berücksichtigung verschiedener Entwicklungen.
Ferner wurde im Anschluss an Geschäftsmodellerarbeitung und Kosten-Nutzen-Betrachtung eine Sensitivitätsanalyse durchgeführt, bei der wesentliche Parameter der Kalkulation modifiziert und resultierende Effekte betrachtet wurden. Auch Einflüsse auf die Kalkulation, wie eine volumenabhängige Preisbildung, wurden exemplarisch untersucht.

Einen wesentlichen Einfluss auf die Erstellung von Geschäftsmodellen und Kosten-Nutzen-Analyse hatten zudem die durchgeführten Experteninterviews, welche u.a. Aufschluss über mögliche Innovationen der Plattform und dessen potenzielle kundenseitige Nachfrage sowie Bepreisung lieferten.

In nachfolgendem Schaubild ist die Vorgehensweise im Rahmen der Ausarbeitung von Geschäftsmodellen und Kosten-Nutzen-Analyse nochmals dargestellt.

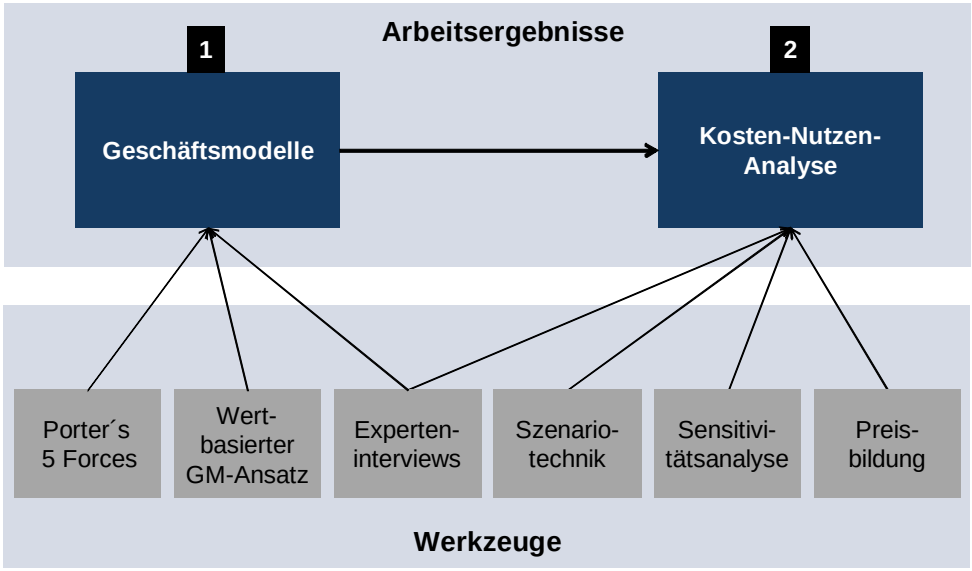

Abbildung 11: Vorgehensweise Geschäftsmodelle und Kosten-Nutzen-Analyse

Die beiden erarbeiteten Geschäftsmodelle unterscheiden sich durch eine diskrete Überwachung des Containers an ausgewählten Punkten, wie z.B. Containerumschlägen an Terminals, Bahnhöfen etc., verglichen mit einer kontinuierlichen Überwachung mittels eines CSD, wie z.B. oben beschriebener CSB.

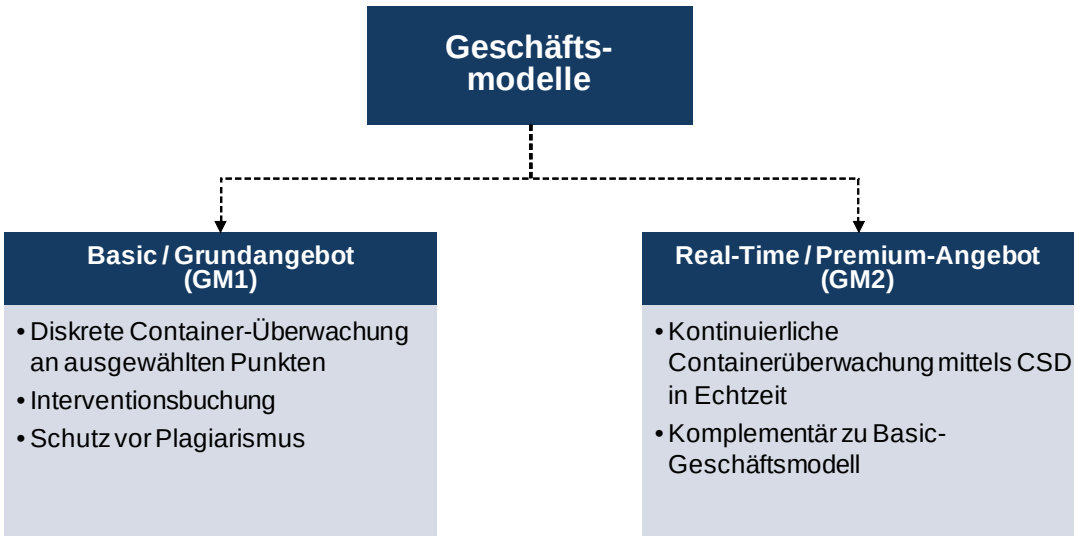

Abbildung 12: Geschäftsmodelle zum Betrieb von ContainIT

Die Geschäftsmodelle stellen die Basis für die Quantifizierung der Wirtschaftlichkeit der Plattform im Rahmen der Kosten-Nutzen-Analyse dar.
Innerhalb der Kosten-Nutzen-Analyse wurden unterschiedliche Parameter berücksichtigt, wie etwa Einmalkosten und laufende Kosten oder Umsatz mit Behörden und mit der Privatwirtschaft. Die wesentlichen Parameter sind in unten stehender Abbildung verdeutlicht.

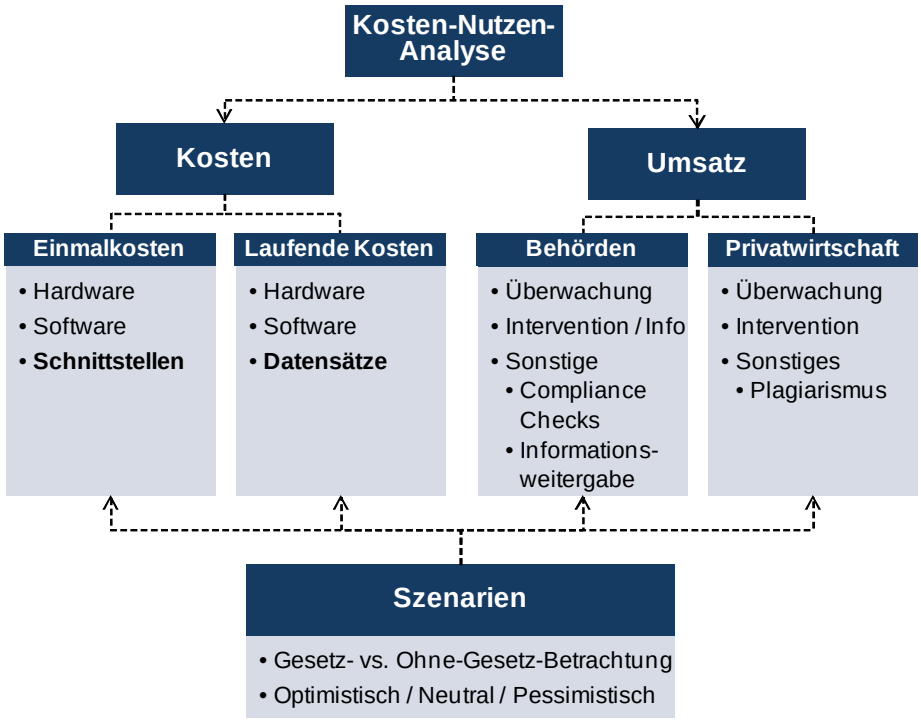

Abbildung 13: Betrachtete Parameter im Rahmen der Kosten-Nutzen-Analyse

Aufgrund der zweidimensionalen Szenarienbildung bzgl. Gesetzesinitiative (ja/nein) und Entwicklungsverlauf der Modellannahmen (optimistisch, neutral und pessimistisch) entsteht ein weites Feld möglicher Ergebnisse zur Wirtschaftlichkeit der ContainIT-Plattform. Dieses reicht, wie in unten stehender Abbildung auszugsweise dargestellt, von einem diskontierten Barwert über einen Investitionszeitraum von 10 Jahren (Beginn im Jahr 2013) in Höhe von knapp -39 Mio. EUR (ohne Gesetz, pessimistischer Entwicklungsverlauf) bis hin zu etwa 380 Mio. EUR (mit Gesetz, optimistischer Entwicklungsverlauf). Der Barwert pro Container reicht hier von -7,15 EUR pro Container im ersten bis 3,67 EUR pro Container im zweiten Fall.

Ergebnisse		
Umsatz: • Gesamt: 56 – 435 Mio. € • Pro Jahr: 5,6 – 43,5 Mio. €	**Kosten:** • Gesamt: 51 – 104 Mio. € • Pro Jahr: 5,1 – 10,4 Mio. €	**Kapitalwert:** • Gesamt: -39 – 380 Mio. € • Pro Jahr: -3,9 – 38 Mio. €

Abbildung 14: Ergebnisse Wirtschaftlichkeitsanalyse ContainIT-Plattform

Grafisch aufbereitet ergibt sich je Szenario folgende Entwicklung des Barwerts der Plattform im Zeitverlauf.

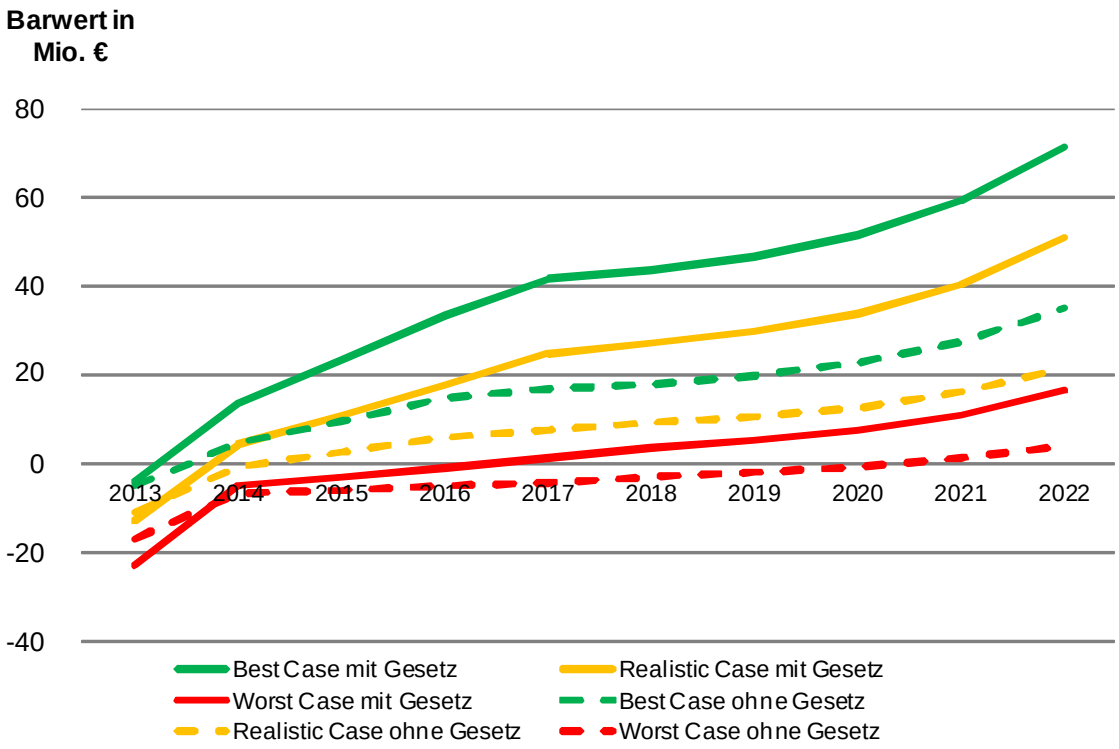

Abbildung 15: Barwert ContainIT-Plattform je Szenario im Verlauf von 10 Jahren

Grundlegend ist anzumerken, dass die dargestellten Ergebnisse sehr stark von der hinterlegten Entwicklung des zukünftigen Marktes für CSD-basierte Containerüberwachung abhängen. Dieser wird in verschiedenen Studien sehr unterschiedlich bewertet. Zudem ist darauf hinzuweisen, dass zum Abschluss des Projektes bekannt wurde, dass die Weltzollorganisation plant, ihren Mitgliedern – also den nationalen Zollbehörden – dem Anschein nach ein Risiko-Profiling System kostenfrei zur Verfügung zu stellen. Es ist davon auszugehen, dass dieses Vorgehen die Zahlungsbereitschaft der Behörden für ContainIT herabsetzten würde und insofern einen negativen Effekt auf die verschiedenen betrachteten Szenarien hätte. Insgesamt ist auch eine geringe Bereitschaft der Behörden festzustellen, Risiko-Profiling für behördliche Zwecke durch einen nicht-hoheitlichen Anbieter durchführen zu lassen. Diesbezüglich erscheint zudem die gleichzeitige Erbringung privatwirtschaftlicher Dienstleistungen sowie die Übernahme hoheitlicher Aufgaben wie Risikoprofiling – ausgehend von derselben Datenbasis und demselben Akteur – als fraglich.

Mit Blick auf die durch die USA initiierte 100%-Scanning-Initiative, welche eine Durchleuchtung sämtlicher Container mit Ziel USA am Abgangshafen vorsieht, wurde im Rahmen des Projektes eine Quantifizierung der damit potenziell verbundenen Kosten vorgenommen. Diese wurden in einem weiteren Schritt mit den Kosten von Einrichtung und Betrieb der ContainIT-Plattform verglichen.

Die Ermittlung der 100%-Scanning-Kosten erfolgte auf zwei Wegen. Zum einen wurde ein Experteninterview mit einem Hersteller von Scanning-Geräten als Grundlage für die Kalkulation genommen. Zum anderen basierte die Quantifizierung auf einer bereits existierenden Studie der RAND-Corporation. Im Rahmen der Ausarbeitung beider Ansätze

fand auch ein inhaltlicher Austausch mit dem unter I.5. genannten Forschungsprojekt ECSIT statt. Dieser diente einer Validierung erster erarbeiteter Ergebnisse und zeigte vor diesem Hintergrund Parallelen sowie Unterschiede im konzeptuellen Aufbau der Kalkulation auf.

Beide im Rahmen von ContainIT erarbeiteten Ansätze betrachteten nur die Containerverkehre von Deutschland in die USA. Ferner wurden Kosten für die Anschaffung der Anlagen und deren Betrieb sowie für erforderliche Infrastrukturanpassungen berücksichtigt. Kosten bei Logistikdienstleistern oder der verladenden Industrie, etwa durch längere Transportzeiten, fanden hingegen keine Berücksichtigung.
Des Weiteren erfolgte eine Szenario-Betrachtung, bei der zwischen optimistischen und pessimistischen Rahmenbedingungen in beiden Ansätzen differenziert wurde. Unterschiede zwischen den Szenarien liegen dabei in differierenden Anschaffungs-, Betriebs- und Infrastrukturkosten mit jeweils günstiger bzw. teurer Ausprägung.
Unten stehende Abbildung stellt beide Ansätze gegenüber und zeigt die jeweiligen Ergebnisse, welche sich aus Kosten von etwa 26 € bis 86 € pro Scan bzw. 8 bis 34 Mio. € insgesamt pro Jahr zusammensetzen.

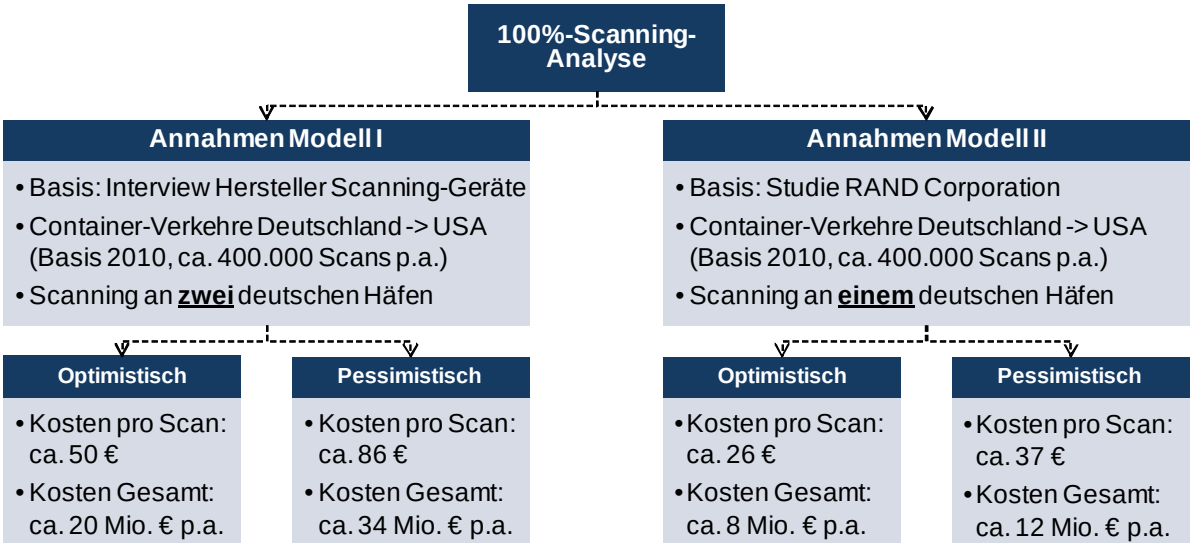

Abbildung 16: Quantifizierung der Kosten durch 100%-Scanning-Initiative

Im Vergleich mit den durch eine Implementierung der ContainIT-Plattform resultierenden Kosten in Höhe von zwischen 5 und 10 Mio. € pro Jahr gestaltet sich das 100%-Scanning folglich deutlich kostspieliger.
Gleichzeitig werden bei ContainIT deutlich mehr Container in das Risikoprofiling einbezogen. Somit hat die ContainIT-Plattform gegenüber dem Scanning-Ansatz deutliche Vorteile hinsichtlich Effektivität und Effizienz, was auch in unten stehender Abbildung nochmals verdeutlicht wird.

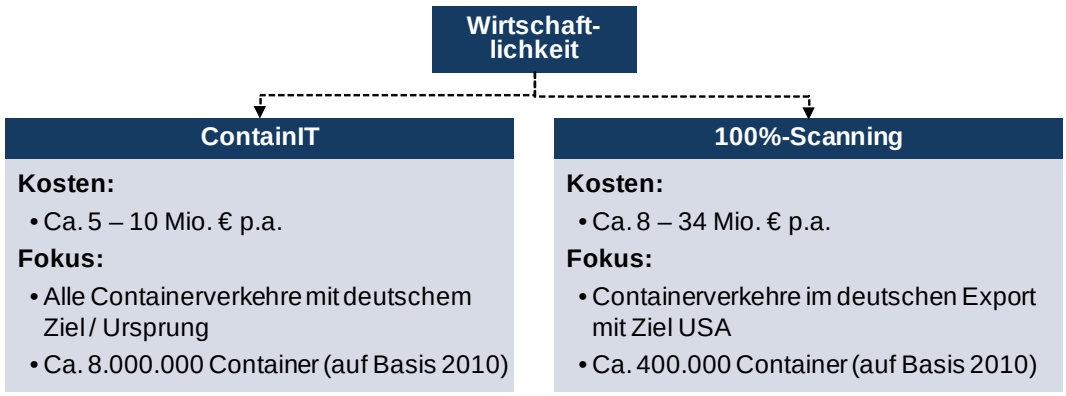

Abbildung 17: Vergleich ContainIT-Plattform und 100%-Scanning

Die Ergebnisse der Wirtschaftlichkeitsbetrachtung zeigen auf, dass grundsätzlich ein wirtschaftlicher Betrieb der ContainIT-Plattform möglich ist, der Erfolg derselben allerdings wesentlich von einer Gesetzesinitiative zur Überwachung von Containertransporten abhängt. Ferner haben auch wirtschaftliche Rahmenbedingungen, wie die Entwicklung des Containertransportmarktes sowie die Marktdurchdringung von CSDs erheblichen Einfluss auf den Erfolg der Plattform.
Die grundsätzliche Funktionalität der Plattform sowie die wesentlichen Ergebnisse der Projektarbeiten konnte mit Hilfe einer technischen Demonstration im Dezember 2012 beim Projektpartner EADS gezeigt werden. Hierfür erfolgte eine Vernetzung verschiedener existierender IT-Systeme der Projektpartner und die Zusammenführung transportrelevanter Daten aus diesen Systemen. Letztere Daten wurden ferner für ein dynamisches Risikoprofiling mit daraus resultierender sich anschließender Intervention genutzt. Die Demonstration baute dabei auf einem exemplarischen Angriffsszenario eines beförderten Containers auf, der auf seinem Weg von Ingolstadt nach Bremerhaven mit einer unkonventionellen Spreng- und Brandvorrichtung (USBV) versehen wird. Hier fand exemplarisch die Erläuterung und Demonstration der auf ContainIT resultierenden Prozesse hinsichtlich Risikoprofiling und Intervention statt. So konnte beispielhaft gezeigt werden, welcher Sicherheitszuwachs mit der Implementierung von ContainIT einher geht.

2. Zahlenmäßiger Nachweis

Die bewilligten Fördermittel wurden seitens Bosch entsprechend der Projektbedürfnisse eingesetzt. Hier sind insb. folgende wesentlichen Ausgabenblöcke zu nennen:

- Personalkosten zur Projektausarbeitung stellen den größten Teil der Aufwände dar. In Summe wurden ca. 26 Personenmonate auf das Projekt verwendet.
- Reisekosten zu
    - Projekttreffen
    - Experteninterviews
    - Workshops
- IT (insb. Laptops) zur Durchführung der Projektarbeit
- Sekundärliteratur

Abschließend bleibt festzuhalten, dass das Bosch zur Verfügung gestellte Budget nicht vollständig ausgeschöpft wurde.

3. Notwendigkeit und Angemessenheit der Arbeit

Die Abarbeitung des Forschungsprojektes erfolgte entlang der im Rahmen der Verbundbeschreibung formulierten Planung. Dabei wurden sämtliche formulierte Aufgaben mit den zur Verfügung stehenden Ressourcen erfolgreich bearbeitet.

Der zuvor erwähnte Projektverzug, welcher in einer kostenneutralen Verlängerung von ContainIT resultierte, ist im Wesentlichen auf die Vielzahl von durchgeführten Experteninterviews zurückzuführen. Diese lieferten jedoch im Rahmen der Ausarbeitung von AP1, aber auch hinsichtlich der weiteren Projektinhalte, einen signifikanten Mehrwert in Bezug auf die Projektergebnisse.

4. Nutzen und Verwertbarkeit der Ergebnisse

Wirtschaftliche Verwertbarkeit:

Das Ziel von ContainIT war es, nach Abschluss des Projektes die Forschungsergebnisse in ein ganzheitliches Produkt-, Plattform- und Dienstleistungskonzept zur umfassenden Containersicherheit einfließen zu lassen. Hierbei ist zwischen Angeboten für den behördlichen Markt (insb. Risiko-Profiling) sowie für den kommerziellen Markt zu unterscheiden (beispielsweise Track & Trace oder Schutz vor Plagiarismus).

Eine wirtschaftliche Verwertbarkeit von ContainIT basierte im Wesentlichen auf der Implementierung des o.g. Produkt-, Plattform- und Dienstleistungskonzeptes als Gesamtsystem. Insgesamt sind die Realisierungschancen von ContainIT als Gesamtsystem als niedrig einzustufen. Wesentliche Gründe hierfür sind:

- Im behördlichen Markt ist auf internationaler Ebene momentan von Seiten der Weltzollorganisation ein Risiko-Profiling-System in der Entwicklung, dass den nationalen Zollorganisationen voraussichtlich kostenfrei zur Verfügung gestellt werden soll. Zudem ist beim deutschen Zoll eine ähnlich gelagerte Risiko-Profiling-Lösung in der Entwicklung.
- Die Ergebnisse des Forschungsprojektes zeigen auch, dass ein ContainIT-Gesamtsystem nur unter gewissen Rahmenbedingungen zur wirtschaftlichen Markteinführung gebracht werden kann. Hier ist insbesondere ein gesetzlicher Rahmen zur Etablierung einer zentralen IT-Plattform zur Gefahrenabwehr im Containertransport zu nennen.
- Diese Erkenntnis steht auch in Verbindung mit dem Umstand, dass auf Seiten der Transportbeteiligten eine geringe Bereitschaft besteht, (Transport-)Daten zur Verfügung zu stellen. Hierfür konnten verschieden Gründe identifiziert werden: Datenschutzbedenken, die Befürchtung etwaige Wettbewerbsnachteile zu erleiden sowie der Umstand, dass die Geschäftsmodelle einzelner Transportbeteiligter auch auf der momentan vorherrschenden Intransparenz innerhalb der Supply-Chains beruhen.
- Grundsätzlich ist zudem eine geringe Zahlungsbereitschaft auf Seiten der Transportbeteiligten für die untersuchten Leistungsmerkmale festzustellen.

Wesentliche Teile der potenziell durch Bosch angebotenen Dienstleistungen für den kommerziellen Markt basieren ebenfalls auf einer Realisierung des Gesamtsystems ContainIT. Diese zielen bspw. auf Track & Trace-Dienstleistungen für Transportbeteiligte oder auf die Erbringung von Support-Funktionen für die ContainIT-Plattform ab. Hinsichtlich letzterer wären der Betrieb einer Technischen Hotline, die Verwaltung von Nutzerprofilen oder die Übernahme von Abrechnungs-Dienstleistungen denkbar.

Mit Blick auf die laufenden „Mobile Security“ Aktivitäten von Bosch im Logistikbereich ist festzustellen, dass heute fast ausschließlich High-Value-Container überwacht werden. Low-Value- oder Gefahrguttransporte werden praktisch nicht überwacht - dies ist in erster Linie auf die mit einer Überwachung (Monitoring) verbundenen Kosten und die geringe Zahlungsbereitschaft der entsprechenden Beteiligten zurückzuführen. Die im Projekt geprüfte Überwachung von Low-Value- und Gefahrguttransporten über die Plattform zeigt wenig wirtschaftliches Potential. So haben die im Rahmen des Forschungsprojektes durchgeführten Experteninterviews eine hohe Preissensibilität hinsichtlich zusätzlicher Dienstleistungen im Bereich der Containersicherheit und Prozesstransparenz ergeben. Dies lässt – für den Fall der Markteinführung der ContainIT-Plattform – die Überwachung von Low-Value-Containern als unwahrscheinlich erscheinen.

Einen positiven Effekt auf die Realisierungschancen von ContainIT könnte die Einführung des 100%-Scannings durch die USA darstellen. Hier könnte ContainIT als komplementärer Dienst einen zentralen Bestandteil eines möglichen Green-Lane-Verfahrens darstellen. Ziel wäre dabei, laut ContainIT-Plattform unbedenkliche Container ohne Scan auf das Schiff zu verladen, während nicht auf der Plattform registrierte sowie bedenkliche Container weiterhin gescannt werden müssten. So könnte neben der allgemein höheren Sicherheit der Containertransporte auch eine Reduktion des Scanningaufwands an Terminals erzielt werden.

Neben den wirtschaftlichen Angeboten, die auf einer Realisierung von ContainIT als Gesamtsystem beruhen, ist festzustellen, dass Teile des Leistungsspektrums auch ohne ein ContainIT-Gesamtsystem realisiert werden können. Für Bosch sind hierbei insbesondere die Aktivitäten zur Transportsicherung interessant: Resultierend aus der Zusammenarbeit in ContainIT befindet sich gegenwärtig zwischen Astrium und Bosch eine bilaterale Vertriebskooperation zur Sicherung von Transporten in der Abstimmung und Ausarbeitung. Diese soll bis Ende 2013 vereinbart sein und ab dem 1. Quartal 2014 den Vertrieb von Container Security Devices (Astrium) mit der Aufschaltung des überwachten Transports auf eine Sicherheitsleitstelle (Bosch), mit der Möglichkeit zur Intervention im Alarmfall, kombinieren.

Ferner sind für Bosch durch die Projektarbeit wertvolle Vertriebskontakte zu Logistikbeteiligten entstanden, die an einer Sicherung ihrer Warenverkehre mittels CSD und einer Buchung von Interventionsleistungen Interesse zeigen. Mit diesen Kontakten laufen weiterhin Gespräche. Mögliche Geschäftsvereinbarungen würden hier die Marktposition von Bosch im Bereich der Überwachung mobiler Objekte festigen und somit zu einer Sicherung bestehender Arbeitsplätze in der deutsch-geprägten Bosch-Leitstellenstruktur führen.

Somit versucht Bosch sowohl durch die Vertriebskooperation mit Astrium als auch durch die entstandenen Vertriebskontakte Marktanteile im wachsenden Markt der Transportüberwachung durch Telematiksysteme zu gewinnen. Dieser wird laut der Studie „Cargo Container Security and Tracking“ von ABI Research (2011) mit einer

durchschnittlichen jährlichen Wachstumsrate von knapp 70% von weltweit ca. 4 Mio. USD Umsatz durch den Endgeräteverkauf in 2008 auf mehr als 170 Mio. USD in 2016 ansteigen.

Abschließend ist zu erwähnen, dass Bosch im Rahmen von ContainIT wertvolles Know-How hinsichtlich der Ausarbeitung und Anwendung eines Kosten-Nutzen-Modells auf eine IKT-Architektur aufbauen konnte. Dieses wird bereits bei der Bewertung von anderen IKT-Systemen und deren Geschäftsmodellen intern angewendet.

Darüber hinaus hat sich gezeigt, dass auch für Projektpartner Einzelkomponenten des ContainIT-Gesamtsystems wirtschaftliches Potential bergen (beispielsweise im Bereich der Compliance Prüfungen).

Wissenschaftliche / technologische Verwertbarkeit:

Einzelne Erkenntnisse aus der Bearbeitung von ContainIT finden Eingang in eine Dissertation, welche von Herrn Prof. Dr. Eric Sucky am Lehrstuhl für Produktion und Logistik an der Universität Bamberg betreut wird und bis 2014 abgeschlossen sein soll.

Mittels des bereits im vorangegangen Abschnitt beschriebenen Know-How-Aufbaus durch ContainIT – etwa hinsichtlich der Wirtschaftlichkeitsbetrachtung von IKT-Systemen – konnte die Bosch Sicherheitssysteme GmbH bestehende methodische und inhaltliche Kompetenzen weiter ausbauen. Diese können und konnten bereits sowohl innerhalb der Organisation bei differierenden Themen gewinnbringend eingesetzt werden als auch Bosch für mögliche zukünftige Forschungsprojekte zusätzlich qualifizieren.

Auch an dieser Stelle sei nochmals darauf verwiesen, dass das angesprochene Know-How und die erarbeiteten Ergebnisse hinsichtlich des oben angesprochenen ganzheitlichen Produkt-, Plattform- und Dienstleistungskonzeptes insb. im Falle einer gesetzlichen Regelung in zusätzlichen Anwendungspotenzialen resultieren.

Wirtschaftliche und wissenschaftliche Verwertbarkeit:

Bei ContainIT handelte es sich um ein rein deutsches Projekt, das von der Bundesregierung gefördert wurde, an welchem ausschließlich deutsche Firmen an der Ausarbeitung beteiligt waren und innerhalb welchem weitestgehend deutsche Experten involviert waren. Im Gegensatz dazu beschäftigt sich ContainIT thematisch betrachtet mit der sehr internationalen Fragestellung der Containersicherheit, insbesondere vor dem Hintergrund grenzüberschreitender Themen wie Logistikprozessen sowie wirtschaftlich und terroristisch motivierter Kriminalität. Folglich scheint es erstrebenswert, die Ergebnisse des Projektes ContainIT in einen internationalen Kontext zu überführen. Auch mit Blick auf eine mögliche zukünftige Umsetzung einer zentralen IKT-Plattform im Logistikumfeld ist eine Implementierung im internationalen Rahmen anzustreben.

Nicht zuletzt wegen des 100%-Scanning-Ansatzes und der Bedeutung der USA als deutschem und auch europäischem Handelspartner liegt hier eine Einbindung der USA nahe.

In diesem Zusammenhang wurde bereits während der Projektlaufzeit von ContainIT eine Deutsch-Amerikanische Kooperation angestrebt, mit dem Ziel der Klärung von Fragen der Containersicherheit im bilateralen Handel. Diese Kooperation sollte auf Initiative des BMBF mit dem US-amerikanischen „Department of Homeland Security“ (DHS) vereinbart werden. Neben vielen Konsortialpartnern von ContainIT beteiligten sich auch die Bosch Sicherheitssysteme an diesem Vorhaben und überreichten im Dezember 2010 unter Führung der EADS ein entsprechendes Whitepaper an BMBF und DHS. Bis Dezember

2012 ist diese Deutsch-Amerikanische Kooperation jedoch nicht zustande gekommen. Sollte die Kooperation und ein sich anschließendes Forschungsprojekt im deutsch-amerikanischen Umfeld wider Erwarten doch noch beschlossen werden, könnten relevante Ergebnisse aus ContainIT für die Ausarbeitung des Projektes herangezogen werden.

Auch hier sei auf die Nutzung und den weiteren Ausbau von Know-How aus ContainIT bei einem möglichen Folgeprojekt im Deutsch-Amerikanischen-Umfeld sowie bei weiteren zukünftigen Forschungsprojekten hingewiesen.

5. Fortschritte

Wie bereits zuvor unter I.2 dargestellt, behandeln neben Forschungsprojekten auf Bundesebene auch Projekte auf EU-Ebene die Verbesserung der Sicherheit bei Containertransporten schwerpunktmäßig. Somit handelt es sich hier um ein Forschungsfeld mit hoher Aktivität und Dynamik, welches durch die mediale Präsenz der verschiedenen Forschungsansätze zunehmend Aufmerksamkeit bei Beteiligten entlang Containertransportketten schafft. Gleichzeitig werden diverse Akteure der Branche in Bezug auf Transportsicherheit sensibilisiert. Die hohe Dynamik des Forschungsgebietes zeigt sich auch in den sich stetig ändernden politischen Rahmenbedingungen.

So wurde die Implementierung des 100%-Scanning-Ansatzes (Stand Dezember 2012), welcher zum 01.07.2012 starten sollte, auf unbestimmte Zeit verschoben. Medienberichten zufolge ist auch eine Abkehr vom Ansatz seitens der USA zukünftig nicht auszuschließen. Diese Entwicklung verringert folglich die politischen Anreize in Deutschland oder der EU zur Forcierung der Einführung von Alternativtechnologien.

In diesem Zusammenhang sind hier auch sich verändernde technische Rahmenbedingungen zu nennen, welche sich – resultierend aus technologischem Fortschritt – in höheren Durchsatzraten (Anzahl Scans pro Stunde) oder etwa günstigeren Anschaffungskosten manifestieren können.

6. Veröffentlichungen

Eine Vorstellung des Projektes ContainIT fand seitens Bosch bei folgenden Veranstaltungen und Einrichtungen statt:

- Logistikkonferenz „Logistikmanagement 2011“ in Bamberg (29.09.2011):
  Vortrag: „Supply Chain Risk Management: Forschungsaktivitäten der Bosch Sicherheitssysteme GmbH“, Referent: Ingo Boost
- “ITS-World Congress 2011” in Orlando (16.-20.10.2011):
  Vortrag: “Safety and Security: Activities of Bosch Sicherheitssysteme GmbH”, Referent: Matthias Trautner
- “ITS-World Congress 2012” in Wien (22.-26.10.2012):
  Messegrafik: “ContainIT: Container security through connected & intelligent IT systems”
- Handelshochschule Leipzig (07.06.2011 und 18.10.2011):
  Vortrag: “Security Services and Research Projects“, Referent: Andreas Döring

- BMBF-Innovationsforum „Zivile Sicherheit“ in Berlin (17.-19.04.2012):
  Poster: „ContainIT – Containersicherheit durch vernetzte IT-Systeme“
- „Forschungssymposium der Polizei“ in Münster (19./20.06.2012):
  Poster: „ContainIT – Containersicherheit durch vernetzte IT-Systeme“

Berichtsblatt

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

3. Titel
Containersicherheit durch vernetzte IT-Systeme (ContainIT):
Kosten-/Nutzen-Modelle sowie Buchungsplattform-Konzept zur Sicherung der Warenketten

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens Dezember 2012
Döring, Andreas Offermann, Tobias	6. Veröffentlichungsdatum
	7. Form der Publikation

8. Durchführende Institution(en) (Name, Adresse)	9. Ber. Nr. Durchführende Institution
Bosch Sicherheitssysteme GmbH	10. Förderkennzeichen 13N11008
	11. Seitenzahl 28

12. Fördernde Institution (Name, Adresse)	13. Literaturangaben 8
Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	14. Tabellen 0
	15. Abbildungen 17

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)

18. Kurzfassung

1. Derzeitiger Stand von Wissenschaft und Technik: Heutige Überwachungskonzepte im Bereich des Containertransports bilden überwiegend Insellösungen für Teilbereiche der Logistikkette ab. Dies führt zu einem lückenhaften und unzureichenden Informationsfluss innerhalb des Containertransportes. Folglich sind eine umfassende Risikobetrachtung sowie die daraus resultierende angemessene Intervention in Gefahrensituationen heute nicht oder nur bedingt möglich.

2. Begründung/Zielsetzung der Untersuchung: Das Forschungsprojekt ContainIT zielte auf eine Verbesserung der Sicherheit und Transparenz internationaler Containertransporte ab. Hierzu sollte ein Informations- und Kommunikationstechnologie (IKT)-basierter Multi-Layer-Ansatz (physische Handhabung des Containers, Umgang mit den containerbegleitenden Dokumenten und IKT-basierter Datenaustausch entlang der Transportkette) entworfen werden, welcher auf einer zentralen IT-Plattform basiert.

3. Methode: Um die potenzielle Wirtschaftlichkeit einer derartigen Plattform zu bestimmen, erfolgte durch Bosch neben der Durchführung einer Kosten-Nutzen-Analyse auch die Ausarbeitung von Geschäftsmodellen zum Betrieb der Plattform.

4. Ergebnis: Die ContainIT-Plattform kann nur unter gewissen Bedingungen zur wirtschaftlichen Markteinführung gebracht werden. Hier ist insbesondere eine mögliche Gesetzesinitiative zur Etablierung einer zentralen IT-Plattform zur Gefahrenabwehr im Containertransport zu nennen.

5. Schlussfolgerung/Anwendungsmöglichkeiten: Die Markteinführung einer zentralen IT-Plattform im Logistikumfeld hängt insb. von gesetzlichen Rahmenbedingungen ab. Im Falle der Plattform-Implementierung ist ferner aufgrund der Internationalität von Warenströmen ein internationaler Ansatz anzustreben, vermeidet dieser doch nationale Insellösungen.

19. Schlagwörter
Container, Sicherheit, Logistik, Supply Chain, Plattform, Risiko, Profiling, Überwachung, IT-Systeme

20. Verlag	21. Preis

Document Control Sheet

1. ISBN or ISSN Planned	2. type of document (e.g. report, publication) Report
3. title Containersicherheit durch vernetzte IT-Systeme (ContainIT): Kosten-/Nutzen-Modelle sowie Buchungsplattform-Konzept zur Sicherung der Warenketten Container security through networked IT systems (ContainIT): Cost-benefit models and booking platform concept to secure supply chains	
4. author(s) (family name, first name(s)) Döring, Andreas Offermann, Tobias	5. end of project December 2012
	6. publication date
	7. form of publication
8. performing organization(s) (name, address) Bosch Sicherheitssysteme GmbH	9. originator's report no.
	10. reference no. 13N11008
	11. no. of pages 28
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 8
	14. no. of tables 0
	15. no. of figures 17
16. supplementary notes	
17. presented at (title, place, date)	

18. abstract

1. Current status of science and technology: Current monitoring concepts in the area of container transports mainly consist of isolated solutions, focusing only on a small fragment of the entire logistics chain. This leads to a fragmented and insufficient flow of information regarding the container transport. Furthermore, today a holistic risk assessment approach resulting in adequate intervention measures – in case of occurring threats – does not exist.

2. Goals of research: The research project ContainIT strived to improve security and transparency in international container transports. In order to achieve this, the project team developed an information and communication technology (ICT) based multi-layer approach (handling of the container and transport documents as well as ICT-based data exchange along the transport chain), which is based on a central IT platform.

3. Content of research: In order to assess the economic viability of the platform, Bosch exercised a cost-benefit analysis and developed several business models to run the platform.

4. Results: The economic viability of the ContainIT platform depends heavily on its regulatory framework. Only in case of a possible legislative initiative to monitor container transports out of security and safety reasons will the platform be run profitably.

5. Application and outlook: A successful launch of a central IT platform in the logistics arena depends heavily on its regulatory framework. In case of a positive decision to introduce the platform on the market, the initiators will have to bear in mind the international character of container transports, choosing an international approach while avoiding national isolated solutions.

19. keywords
Container, Security, Logistics, Supply Chain, Platform, Risk, Profiling, Monitoring, IT system

20. publisher	21. price