InPoSec Abschlussbericht Westfälische Wilhelms-Universität Münster (WWU)

ABSCHLUSSBERICHT AN DEN PROJEKTTRÄGER VDI TECHNOLOGIEZENTRUM, DÜSSELDORF

Zuwendungsempfänger	Westfälische Wilhelms-Universität Münster (WWU)
Förderkennzeichen	13N12298
Vorhabenbezeichnung	Sichere Lieferketten im Postverkehr
Laufzeit des Vorhabens	01.06.2012 – 31.05.2015
Berichtszeitraum	01.06.2012 – 31.05.2015

Inhalt

1 Kurze Darstellung

1.1 Aufgabenstellung

In den letzten Jahren ist es wiederholt zu versuchten Briefbombenanschlägen gekommen. Dies hat noch einmal die Verletzlichkeit der postalischen Infrastruktur deutlich gemacht. Aufgrund der Bedeutung von postalischen Dienstleistungen, insbesondere für die Bürger Deutschlands und Frankreichs, ist eine verbesserte Risikobewertung und Sicherheitsprüfung im grenzüberschreitenden Brief- und Paketverkehr dringend erforderlich.

Die Maßnahmen zur Bedrohungsabwehr lassen sich in die Identifikation gefährlicher Stoffe und den Schutz der Lieferkette unterteilen. Für beide Fälle waren bisher keine geeigneten Prozesse und IT-Systeme definiert, die helfen könnten, Angriffe auf die Schwachstellen abzuwehren. Das Ziel dieses Teilprojekts von InPoSec war es, zu untersuchen, wie Prozesse und IT-Systeme der Postsysteme gestaltet werden sollten, um die Sicherheit zu erhöhen und dadurch Bürger besser vor Bedrohungen zu schützen.

Das Projekt fokussiert sich auf die Warenströme, die von außerhalb der EU nach Deutschland oder Frankreich laufen. Aufgrund des Schengen-Abkommens und der Zollunion dürfen keine Kontrollen im Bereich des Binnenmarktes, also beispielsweise zwischen diesen beiden Ländern, stattfinden. Dennoch profitieren die beiden Nationen in besonderem Maße von der erzielten Projektlösung zur Steigerung der Sicherheit im postalischen Umfeld. Einerseits wird Vertrauen in die Sicherheitskontrollen des jeweils anderen Landes aufgebaut, sodass die Gefahr einer Beschränkung der Freiheit des Binnenmarktes unwahrscheinlich wird, was zum Vorteil für Bürger und Unternehmen beider Länder ist. Darüber hinaus wurde ein Standard für Informationen, Prozesse und deren Management nach deutsch-französischen Vorstellungen geschaffen, der mit hoher Wahrscheinlichkeit maßgeblich für die übrigen Staaten der Europäischen Union sein wird. Dieser Standard umfasst die Teilbereiche des sicheren Prozessdesigns für eine sicherheitsbezogene Bewertung der postalischen Prozesse, eine integrierte Informationsbewertung auf Grundlage neugestalteter informatorischer Prozesse und des Sicherheitsmanagementkonzepts, welches die erzielten Ergebnisse aller Partner in einen gemeinsamen Leitfaden für die Sicherheit in der postalischen Lieferketten abbildet.

Ein wichtiger Faktor während des gesamten Projektverlaufs war die Evaluation und Berücksichtigung rechtlicher Rahmenbedingungen. Im Zuge des InPoSec-Projekts stellen sich zwei zentrale Fragen, die ihren Ursprung im Zollrecht und im Datenschutzrecht haben.

1. Unter welchen Voraussetzungen ist die Kontrolle des Inhalts von Postsendungen nach dem Zollrecht zulässig?
2. Ob und wie können die in diesem Zusammenhang stehenden Informationen zwischen den Postgesellschaften und den Zollbehörden in Übereinstimmung mit den postrechtlichen und datenschutzrechtlichen Bestimmungen erhoben, verarbeitet und weitergegeben werden?

Für die rechtliche Begleitung der Entwicklung der Prozess- und IT-Architektur war die Beantwortung dieser Rechtsfragen elementar.

1.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Die Westfälische Wilhelms-Universität kann auf Erfahrungen aus zahlreichen nationalen, wie auch internationalen Projekten bauen. Das Institut für Wirtschaftsinformatik pflegt zudem als Hauptsitz des European Research Center for Information Systems (ERCIS) enge Kontakte zu wissenschaftlichen Einrichtungen weltweit. Das Institut für Steuerrecht bietet mit der Abteilung für Zölle und Verbrauchsteuern zudem starke Kompetenzen in diesem Bereich.

Der Lehrstuhl für Wirtschaftsinformatik und Logistik der WWU Münster wird von Prof. Dr.-Ing. Bernd Hellingrath, zuvor Hauptabteilungsleiter für Unternehmensmodellierung am Fraunhofer-Institut für Materialfluss und Logistik und Professor für die Planung und Modellierung von Produktions- und Logistiknetzwerken an der Universität Paderborn, geleitet. Prof. Hellingrath war bereits an verschiedenen deutschen und europäischen Forschungsprojekten beteiligt, bspw. SFB 559 „Modellierung großer Netze in der Logistik“, EU FP6 ILIPT „Intelligent Logistics for Innovative Product Technologies“ und „BMWi InTerTrans „Integrierte Terminierung und Transportplanung“ und besitzt eine umfangreiche Publikationsliste im Supply Chain Management.

Prof. Dr. Wolffgang ist seit 1995 Leiter der Abteilung Zölle und Verbrauchsteuern im Institut für Steuerrecht der Universität Münster. Zahlreiche eigene Publikationen und betreute Dissertationen sind in dem Institut entstanden, die jeweils den Forschungsschwerpunkt im Zollrecht haben.

1.3 Planung und Ablauf des Vorhabens

Das Gesamtvorhaben in InPoSec wurde in neun Arbeitspakete aufgeteilt, denen jeweils ein Projektpartner als Hauptverantwortlicher zugeordnet ist. Abbildung 1 zeigt eine schematische Übersicht aller Arbeitspakete in einer farblichen Trennung für die jeweiligen Partner. Die WWU hast sich folglich auf folgende Arbeitspakete fokussiert:

- *AP 2: Analyse sicherheitsrelevanter Schwachstellen gegenwärtiger postalischer Lieferketten*
  Hierbei wurden die aktuellen Prozesse bei der Deutschen Post und Groupe La Poste erhoben und mittels eigens entwickelter Evaluationskriterien auf sicherheitsrelevante Schwachstellen analysiert. Hierzu wurde unter anderem die Modellierungs- und Evaluationsplattform Pivot implementiert und weitere Evaluationsmethoden, wie eine Simulationsstudie, für spätere Arbeitspakete entworfen.
- *AP 3: Entwurf informatorischer Prozesse*
  Basierend auf der erhobenen Ist-Situation und den Ergebnissen der Evaluation hinsichtlich sicherheitsrelevanter Schwachstellen wurden in diesem Arbeitspaket die informatorischen Prozesse neugestaltet. Hierzu wurden sowohl informatorische als auch technische Anforderungen berücksichtigt, um einer integrierten Informationsbewertung gerecht zu werden.
- *AP 6: Rechtliche Aspekte*
  Die Evaluation und Berücksichtigung der rechtlichen Rahmenbedingungen war in wichtiger Faktor um das Projektziel zu erreichen. Daher wurden in diesem Arbeitspaket die

relevanten Bestimmungen aus deutschem, französischem und europäischem Recht betrachtet und mit den Projektergebnissen im Rahmen eines Privacy-by-Design Ansatzes abgeglichen.

Darüber hinaus war die WWU ebenfalls an anderen Arbeitspaketen beteiligt.

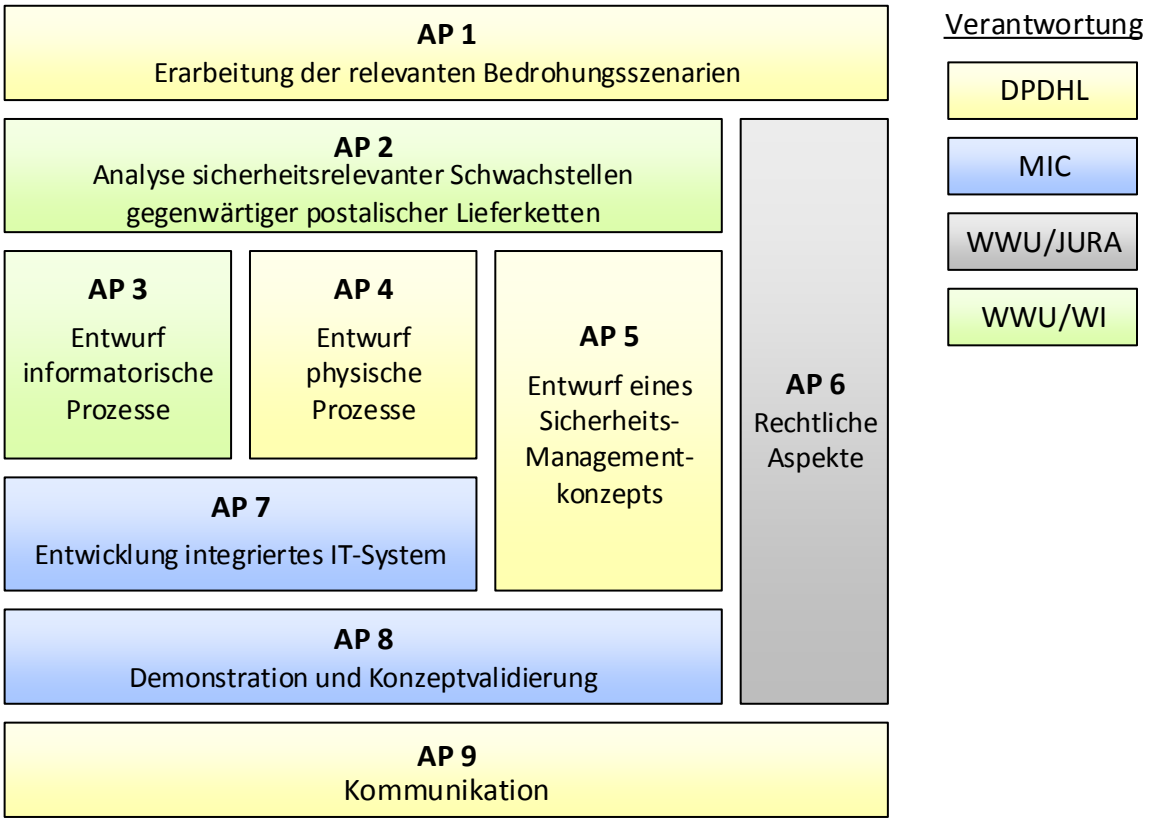


Abbildung 1: Übersicht Arbeitspakete

Eine detaillierte Aufstellung und zeitliche Einordnung aller Arbeitspakete und der jeweiligen Unterarbeitspakete kann der Abbildung 2 entnommen werden. Hierbei wurden alle Arbeiten, an denen die WWU nicht beteiligt war, ausgegraut. Die WWU war über den Projektverlauf hinweg an fast allen Arbeiten hauptverantwortlich oder begleitend beteiligt und hat dabei aus logistischer und rechtlicher Sicht den Stand der Forschung vertreten und neue Entwicklungen zum Projekt beigetragen.

Fast alle Arbeiten an den einzelnen Unterarbeitspaketen konnten entsprechend des Zeitplans abgeschlossen werden. Vereinzelt traten Verzögerungen auf, die jedoch keine Auswirkungen auf den Gesamtverlauf des Projekts hatten oder sich negativ auf das Projektergebnis ausgewirkt haben. Zum Projektende konnten alle Arbeiten entsprechend des Vorhabens vollständig erfüllt werden.

Arbeitspakete (AP)		Aufwand der Partner Personal-monate (PM)			Zeit- und Ablaufplan
Nr.	Beschreibung	WWU	WWU/JURA	WWU/WI	laufender Projektmonat (LM)
1	Erarbeitung der relevanten Bedrohungsszenarien	0	0	0	
2	**Analyse sicherheitsrelevanter Schwachstellen gegenwärtiger postalischer Lieferketten**	37	3	34	
2.1	Aufnahme der existierenden sicherheitsrelevanten Prozesse in postalischen Lieferketten	8		8	
2.2	Entwicklung einer Plattform zur Prozessmodellierung und -evaluation	16		16	
2.3	Modellierung der aufgenommenen Prozesse in der Plattform	4		4	
2.4	Evaluation der gegenwärtigen Prozesse hinsichtlich Schwachstellen und Risiken	3		3	
2.5	Ableitung der Anforderungen an Sicherheitsmanagement, Prozesse und Inspektionsverfahren	6	3	3	
3	**Entwurf der informatorischen Prozesse**	11	0	11	
3.1	Gestaltung der informatorischen Prozesse	3		3	
3.2	Modellierung und Evaluation der informatorischen Prozesse in Plattform	4		4	
3.3	Verfeinerung der informatorischen Prozesse	2		2	
3.4	Ableitung von Anforderungen an integrierendes IT-System	2		2	
4	**Entwurf der physischen Prozesse**	14	1	13	
4.1	Abstimmung von Anforderungen und Fähigkeiten physischer Inspektionsverfahren	2		2	
4.2	Gestaltung der physischen Prozesse	4	1	3	
4.3	Modellierung und Evaluation der physischen Prozesse in Plattform	3		3	
4.4	Verfeinerung der physischen Prozesse	3		3	
4.5	Ableitung von Anforderungen an integrierendes IT-System	2		2	
5	**Entwurf eines Sicherheitsmanagementkonzepts**	14	1	13	
5.1	Evaluation existierender Sicherheitsmanagementkonzepte	6		6	
5.2	Prüfung bestehender Unternehmensrichtlinien zur Sicherheit in der postalischen Lieferkette	2		2	
5.3	Entwicklung von Prozeduren zur kontinuierlichen Risikoidentifikation	2		2	
5.4	Abstimmung des Sicherheitsmanagements mit neu entwickelten Prozessen	2	1	1	
5.5	Ableitung von Anforderungen an den operativen Betrieb	1		1	
5.6	Definition von Prozeduren zur Überwachung und kontinuierlichen Verbesserung	1		1	
6	**Rechtliche Rahmenbedingungen**	33	33	0	
6.1	Beschreibung existierender Zollanmeldeprozesse	5	5		
6.2	Identifikation veränderter Anforderungen an den Zoll	4	4		
6.3	Rechtliche Anforderungen zur physischen Inspektion von Postsendungen	7	7		
6.4	Rechtliche Anforderungen zum Austausch von Informationen	8	8		
6.5	Prüfung der Vereinbarkeit des Gesamtkonzepts mit den rechtlichen Rahmenbedingungen	9	9		
7	**Entwurf eines integrierten IT-Systems**	2	0	2	
7.1	Anpassung von Methoden zur Bewertung der Integrierten Informationen (Risikobewertung)				
7.2	Abstimmung fachlicher und softwaretechnischer Anforderungen	1		1	
7.3	Entwurf Softwarearchitektur				
7.4	Entwurf Kommunikationsschnittstellen und -standards	1		1	
7.5	Implementierung des Softwaredemonstrators				
8	**Demonstration / Konzeptvalidierung**	3	0	3	
8.1	Integration der technischen Konzepte und des Sicherheitsmanagements	2		2	
8.2	Demonstration und Validierung des Gesamtkonzepts	1		1	
9	**Kommunikation**	4	1	3	
9.1	Website				
9.2	Workshop	2	1	1	
9.3	Wissenschaftliche Veröffentlichungen und Konferenzen	2		2	
9.4	Ansprache der Wirtschaft				
9.5	Endnutzer-Integration				

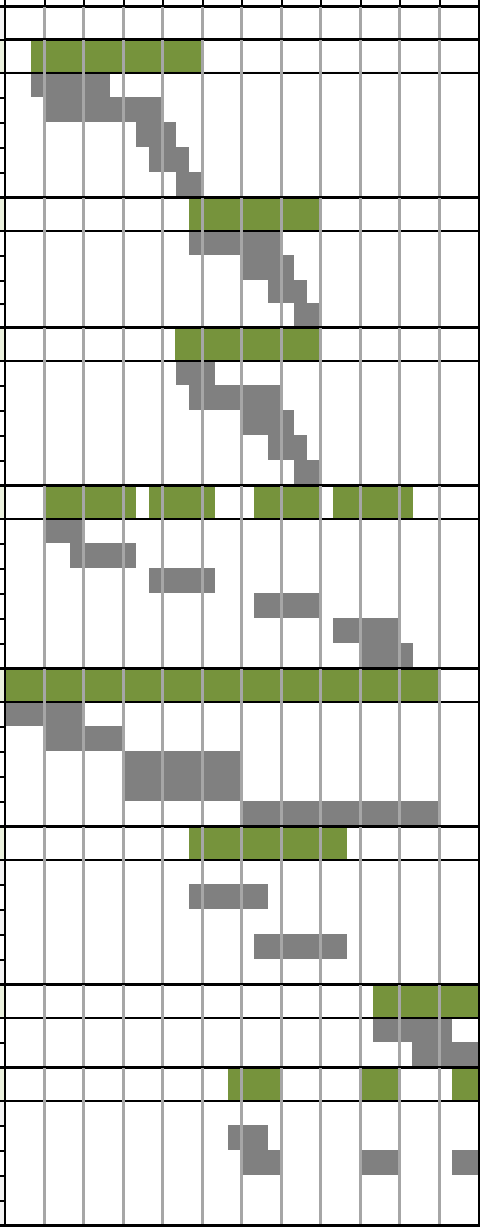


Abbildung 2: Projektplan Gantt-Diagramm

1.4 Anknüpfung an den wissenschaftlichen und technischen Stand

Der Gesamtansatz zur Steigerung der Sicherheit postalischer Lieferketten basiert auf der verbesserten Verfügbarkeit von Informationen über Sendungen, deren integrierter Bewertung und einer entsprechenden physischen Behandlung in Abhängigkeit vom Bewertungsergebnis. Hierzu wurden insbesondere im Rahmen der Prozessanalyse sowie der Prozessneugestaltung Ergänzungen zum wissenschaftlichen und technischen Stand entwickelt. Insbesondere waren Ansätze der Prozessmodellierung und Prozessevaluation zu betrachten. Weiterhin wurde ein konzeptioneller Beitrag für eine effektive Umsetzung des Gesamtkonzepts als Sicherheitsmanagementkonzept geleistet.

Vor dem Projekt gab es keine umfassende Prozessmodellierung und Analyse der Prozesse bei Postunternehmen. Ebenfalls existierte keine domänenspezifische Modellierungssprache für die Dokumentation und Evaluation von Sicherheit in physischen Prozessen wie die der postalischen Lieferkette. Hier konnte auf die im Rahmen der Geschäftsprozessmodellierung umfangreichen Arbeiten der letzten Jahrzehnte zurückgegriffen werden. In diesem Kontext sind insbesondere die Ereignisgesteuerte Prozesskette (EPK)[1], sowie die in jüngerer Zeit sich durchsetzende Business Process Model and Notation (BPMN)[2] zu nennen. Entsprechend fehlte es auch an geeigneten Evaluationstechniken, um die domänenspezifischen Anforderungen an die Sicherheit bewerten zu können. Hier bietet sich insbesondere die Simulation der dem Gesamtkonzept zugrundeliegenden Prozesse an. Methoden und Werkzeuge zur Simulation von Prozessen und Systemen existieren in der Forschung ebenfalls. Die zugrundeliegenden Simulationssprachen weisen hinsichtlich Abstraktionsgrad und Modellierungsumfang deutliche Unterschiede zu den oben angeführten Modellierungssprachen auf, sodass die Anforderungen zur Prozessvisualisierung und qualitativen Prozessanalysen von Simulationssprachen allein nicht erfüllt werden konnten.

Sicherheitsmanagement ist kein gänzlich neues Thema innerhalb des Supply Chain Managements, allerdings zielen die meisten Bestimmungen und Vorhaben auf den kommerziellen Bereich ab. Zu nennen sind insbesondere C-TPAT (Customs-Trade Partnership Against Terrorism)[3], das Konzept des AEO (Authorized Economic Operator)[4] und die Zertifizierung der TAPA (Technology Asset Protection Association)[5]. Für den Postbereich existierte bisher keine maßgeschneiderte Lösung, die auf die speziellen Bedürfnisse und rechtlichen Rahmenbedingungen eingeht. Das entwickelte Sicherheitsmanagementkonzept überträgt daher existierende Konzepte auf den Kontext postalischer Lieferketten und verknüpft diese im Sinne eines Rahmenkonzepts mit den entwickelten Prozess- und IT-Lösungen.

Die für das Projekt relevanten Rechtsfragen berühren nicht nur verschiedene überschneidende Rechtsgebiete (z.B. Zollrecht, Postrecht, Datenschutzrecht), sondern beziehen sich auch auf Vorschriften des Unionsrechts, des deutschen und französischen Rechts. Eine zentrale Bedeutung hat der Zollkodex zusammen mit seinen Durchführungsvorschriften als das größte harmonisierte Gesetzeswerk innerhalb der Europäischen Union. Daneben finden nationale Rechtsvorschriften wie das deutsche Zollverwaltungsgesetz, der französische Code des douanes und entsprechende Postgesetze Anwendung. Außerdem müssen europarechtliche und nationale Datenschutzbestimmungen Beachtung finden. Nationale Unterschiede in der Gesetzgebung müssen unter Berücksichtigung der entsprechenden europarechtlichen Bestimmungen eine gesetzeskonforme Auslegung erfahren, um ein Nebeneinander und Ineinandergreifen der Bestimmungen zu gewährleisten. Diese Besonderheiten mussten bei der Entwicklung der Prozess- und IT-Architektur berücksichtigt und abgebildet werden.

[1] Vgl. bspw. Nüttgens und Rump, 2002.
[2] Vgl. bspw. White, 2004.
[3] Vgl. United States Customs and Border Protection, 2007.
[4] Vgl. Europäische Kommission, 2006.
[5] Vgl. Transported Asset Protection Association, 2012.

1.5 Zusammenarbeit mit anderen Stellen

Für die Zusammenarbeit mit anderen Stellen im Projekt ist vor allem Siemens als Mitglied des Advisory Board zu nennen, welches besonders in der Anfangsphase des Projekts und der Entwicklung der neugestalteten Prozesse stark eingebunden wurde. Siemens nahm an mehreren telefonischen Absprachen teil und wurde durch Ingolf Rauh auf dem Konsortiumstreffen am 13. und 14. Juni 2013 vertreten. Auf Grund interner Umstrukturierungen sah Siemens sich 2014 gezwungen die Mitarbeit im Advisory Board zu beenden. Beidseitig wurde die Zusammenarbeit als sehr positiv angesehen.

Über die Deutschen Post AG bestand ebenfalls Kontakt zur PostEurop Customs Working Group. Hier wurde am 22.10.2013 das EU-Projekt SAFEPOST und InPoSec erstmalig vorgestellt und es wurde erkannt, dass ein großes Potential für einen Austausch besteht.

Mit dem EU-Projekt SAFEPOST hat über das Projekt hinweg ein regelmäßiger Austausch stattgefunden, da beide Projekte eine ähnliche Zielsetzung anstreben. Das InPoSec Konsortium war auf mehreren Treffen vertreten, um die aktuellen Fortschritte beider Projekte zu diskutieren.

- EU Projekt SAFEPOST, 27-29.11.2013, Vilnius, Litauen
- EU Projekt SAFEPOST, 10-11.06.2015, Saragossa, USA

Auf verschiedenen Veranstaltungen und Projekttreffen konnte ein Austausch mit der britischen Border Force stattfinden. Herr Trevor Francis zeigte sich fortwährend interessiert an den aktuellen Arbeiten und beteiligte sich regelmäßig an Diskussionen über Ergebnisse und Ziele von InPoSec, als auch über aktuelle Problemstellungen der Border Force. Bei folgenden Veranstaltungen haben Absprachen stattgefunden:

- EU Projekt ITOM 19-20.1.2015, Rotterdam, Niederlande
- EU Projekt DOGGIES, 27.05.2015, Münster, Deutschland
- Zudem auf mehreren SAFEPOST Projekt Treffen

Mit dem Deutschen Zoll hat ein Treffen am 05.11.2013 bei der Bundesfinanzdirektion Nord in Hamburg stattgefunden. Hier wurde das Projekt vorgestellt und seitens der BFD wurde ein Fragenkatalog zur aktuellen Risikoprüfung durch den Zoll beantwortet.

2 Eingehende Darstellung

2.1 Verwendung der Zuwendungen im Einzelnen und erzielte Resultate

2.1.1 AP 2 Analyse sicherheitsrelevanter Schwachstellen gegenwärtiger postalischer Lieferketten

Kernpunkt des AP 2 ist die Aufnahme und Evaluation der sicherheitsrelevanten Schwachstellen gegenwärtiger postalischer Lieferketten. Dazu wurde zunächst die aktuelle Situation der im Projekt fokussierten Teile der postalischen Lieferkette für ein einheitliches Verständnis der Bedrohungsszenarien erfasst und in konsistenter Form für sämtliche Partner als Kommunikations- und Analysebasis bereitgestellt. Darauf aufbauend wurden Schwachstellen bewertet und Anforderungen an die neu zu gestaltende postalische Lieferkette abgeleitet.

2.1.1.1 UAP 2.1 Aufnahme der existierenden sicherheitsrelevanten Prozesse in postalischen Lieferketten

Das UAP 2.1 befasste sich mit der Aufnahme der Ist-Prozesse unter Verwendung eines systematischen Vorgehens zur Erfassung aller sicherheitsrelevanten Aspekte des betrachteten Ausschnitts der postalischen Lieferkette.

Erhebung und Dokumentation der Ist-Modelle

Vor der konkreten Erhebung der Prozesse für dieses Projekt wurden zunächst allgemeine Methoden und Konventionen für die sicherheitsbezogene Modellierung von generellen Lieferketten erarbeitet. Die Modellierung der Sicherheitsanforderungen und -ziele, der Architektur und der Prozesse findet auf drei miteinander verknüpften Ebenen statt. Dieser Ansatz ist in der Secure Logistics Processes (SLP) Methodology beschrieben, welche im Rahmen der wissenschaftlichen Veröffentlichungen publiziert wurde (Böhle et al., 2013). Auf oberster Ebene befindet sich das Zielmodell, welches die Anforderungen und Ziele für eine sichere Lieferkette aus Sicht der Interessensvertreter (z. B. Unternehmen, Gesellschaft etc.) darstellt und in Relation setzt. Diese werden im Architekturmodell auf der nächsten Ebene aufgegriffen, welches die Interessenvertreter in ihren Rollen mit den Prozessen und IT-Systemen in Verbindung bringt und so eine Gesamtdarstellung der Domäne zeigt. Schließlich werden alle relevanten Prozesse durch detaillierte Geschäftsprozessmodelle dargestellt, die die gesamten Aktivitäten zur Erreichung der betriebswirtschaftlichen und sicherheitsrelevanten Ziele abbilden. Eine Übersicht der Ebenen kann aus Abbildung 3 entnommen werden.

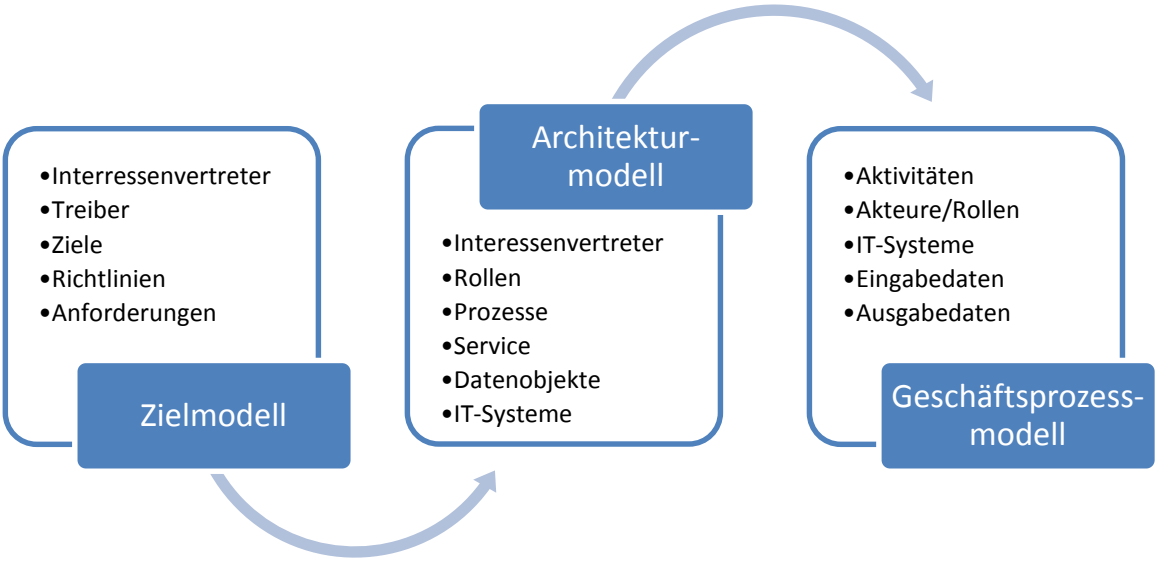


Abbildung 3: Modellierungsebenen

Im Folgenden wird das Erstellen der Modelle für den Ist-Zustand der postalischen Lieferkette im InPoSec-Projekt dargestellt. Das Ergebnis der Zielmodellierung ist in Abbildung 4 dargestellt. Aktuell werden nur die Anforderungen an eine Risikoidentifikation und Qualitätskontrolle durch die Sicherheitsabteilung der Deutschen Post erfüllt. Diese Anforderungen sind jedoch nicht in den operativen Prozessen beschrieben. Daher besteht noch keine Verbindung vom Zielmodell zu den Prozessmodellen.

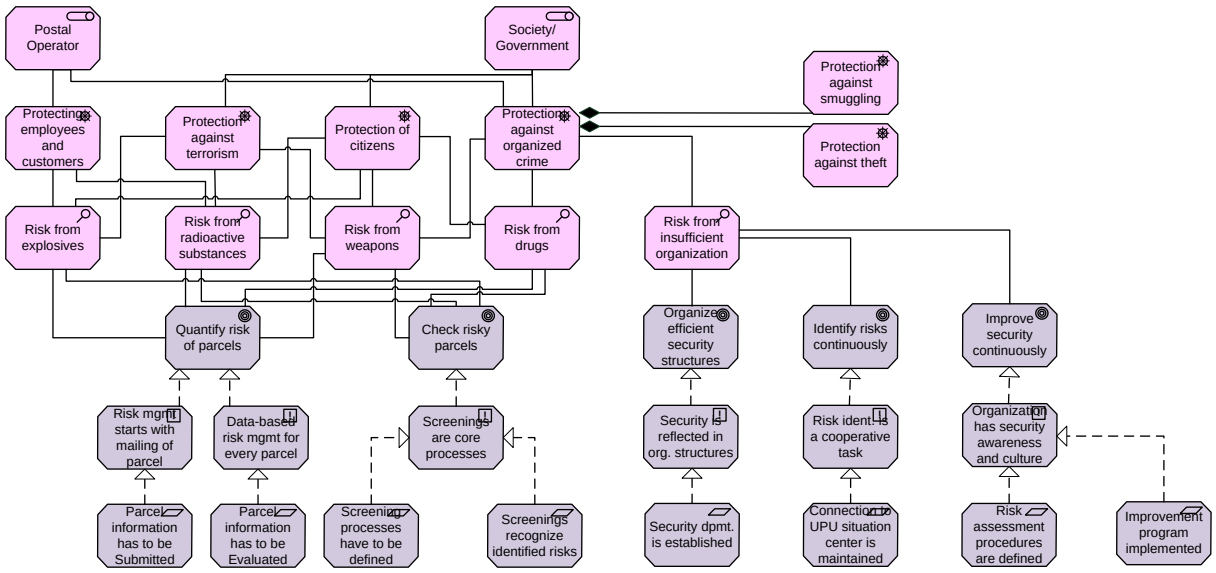


Abbildung 4: Ziele und Anforderungen für sichere postalische Prozesse

Die Erhebung und Dokumentation der jeweiligen Ist-Modelle der verschiedenen postalischen Lieferketten und Paketzentren in Deutschland und Frankreich wurden basierend auf den Prozessaufnahme-Workshops in Speyer (10.12.2012) und Frankfurt (28.03.2013) sowie weiteren Telefonkonferenzen unter den Projektpartnern und Experten der Deutschen Post durchgeführt. Ebenso wurden die Prozesse des französischen Projektpartners La Poste bei einem Workshop in Chilly-Mazarin (Paris) erhoben (07.02.2013). Wie in den vorangegangenen Phasen identifiziert, sind der nationale Importprozess und die darin enthaltene Zollkontrolle die priorisierten Problembereiche. Diese wurden entsprechend der zuvor beschriebenen Modellebenen zunächst in einem Architekturmodell der gesamten postalischen Lieferkette dokumentiert. Das Architekturmodell zeigt die abstrahierte Gesamtdarstellung der an der Lieferkette beteiligten Akteure, der Prozesse und IT-Systeme, beginnend mit der Aufnahme von Sendungen durch die sendende Postgesellschaft im Ausland bis zur Auslieferung im Inland. Die im Architekturmodell beschriebenen Prozesse der priorisierten Problembereiche sind in den Geschäftsprozessmodellen detaillierter auf Aktivitätsebene abgebildet.

Die Ist-Prozesse wurden zunächst in textueller Form dokumentiert und anschließend in den Architektur- sowie den Prozessmodellen abgebildet. In den erhobenen aktuellen Prozessen sind keine Sicherheitsaspekte enthalten, die in den Modellen berücksichtigt werden können. Die sicherheitsrelevanten Ziele und Anforderungen im Zielmodell werden daher nicht durch die Prozesse erfüllt. Im Rahmen der AP 3 und AP 4 werden diese Anforderungen in der Prozessneugestaltung berücksichtigt.

Modellkonsolidierung

Im Rahmen der Modellkonsolidierung wurden die erhobenen Prozesse aus den Workshops in den Paketzentren der Deutschen Post in Speyer (10.12.2012), Frankfurt (28.03.2013) und von La Poste in Chilly-Mazarin (Paris, 07.02.2013) verglichen. Hierzu wurde ein adäquater Detaillierungsgrad auf den jeweiligen Ebenen gewählt und die gemeinsamen Prozessbausteine und Bezeichnungen vereinheitlicht. Die Resultate wurden auf den Konsortiumstreffen (14.06.2013

und 04.12.2013) unter den Projektpartnern diskutiert und als vollständig und korrekt angenommen. Die nationalen Importprozesse der Deutschen Post und La Poste basieren auf den gleichen Bausteinen und weichen nur geringfügig durch vereinzelte individuelle Prozesse voneinander ab, sodass eine Konsolidierung der Bausteine und Bezeichnungen auf Architekturebene möglich war. Die Prozessdokumentation, sowie Ziel-, Architektur- und Prozessmodelle können dem Ergebnisdokument zu UAP 2.1 entnommen werden.

2.1.1.2 UAP 2.2 Entwicklung einer Plattform zur Prozessmodellierung und -evaluation

Zur Unterstützung der Modellierung und Evaluation von sicherheitsrelevanten Aspekten in den erfassten Prozessmodellen beschäftigte sich das UAP 2.2 mit der Entwicklung einer informationssystemgestützten Plattform zur Prozessmodellierung und -evaluation. Hierzu gehören die Definition bzw. die Anpassung eines übergeordneten Ordnungsrahmens, einer Modellierungssprache sowie eines graphischen Modellierungseditors. Weiterhin wurden Methoden und Tools zur Evaluation der Prozessmodelle hinsichtlich einer Bewertung der Sicherheitsaspekte bereitgestellt. Ziel des UAP war es eine allgemein verwendbare Plattform zu entwickeln, die für Projekte zur Verbesserung der Sicherheit logistischer Systeme eingesetzt werden kann.

Ordnungsrahmen für die postalische Lieferkette

Ein Ordnungsrahmen dient als abstrahierte Grundlage für die Entwicklung spezieller Prozesse, wie z.B. für unternehmensinterne Abläufe (Becker et al. 2008). Die Verwendung eines Ordnungsrahmens fördert die Vergleichbarkeit zwischen z.B. Unternehmen und beinhaltet zudem Best Practices, wodurch der Aufwand der Prozessentwicklung reduziert wird. Zur Erfassung eines solchen Ordnungsrahmens für die postalische Lieferkette wurde eine Literaturrecherche durchgeführt, in der vier Hauptprozesse identifiziert wurden (vgl. van der Lijn et al. 2005, Walsh 2006):

1. Vereinnahmung (engl. Clearance): Aufnahme von Sendungen an z.B. Paketstationen. (Dieke, Junk, & Zauner, 2010, p. 8; Hempsch, 2010, p. 23; van der Lijn et al., 2005, p. 42)
2. Sortierung im Absenderland (engl. Inward Sorting): Sortierung der abgehenden Sendungen nach Zielort (bei internationalen Sendungen das Empfängerland). (Hempsch, 2010, p. 21)
3. Transport (engl. Transport): Transport der Sendungen mittels Luft-, See-, Straßen- oder Zugtransport.
4. Sortierung im Empfängerland (engl. Outward Sorting): Sortierung der eingehenden Sendungen nach Zielort (Empfänger oder regionales Verteilzentrum). (Hempsch, 2010, p. 21)
5. Zustellung (engl. Delivery): Zustellung und Übergabe der Sendung an den Empfänger. (Dieke et al., 2010, p. 3)

Eine Darstellung des Ordnungsrahmens ist in Abbildung 5 gegeben. Die fünf postalischen Hauptprozesse lassen sich aus Sicht einer generischen Transportkette auch in einen Vorlauf (Pre Run), Hauptlauf (Main Run), Nachhalf (After Run) und Zustellung (Delivery Run) unterteilen.

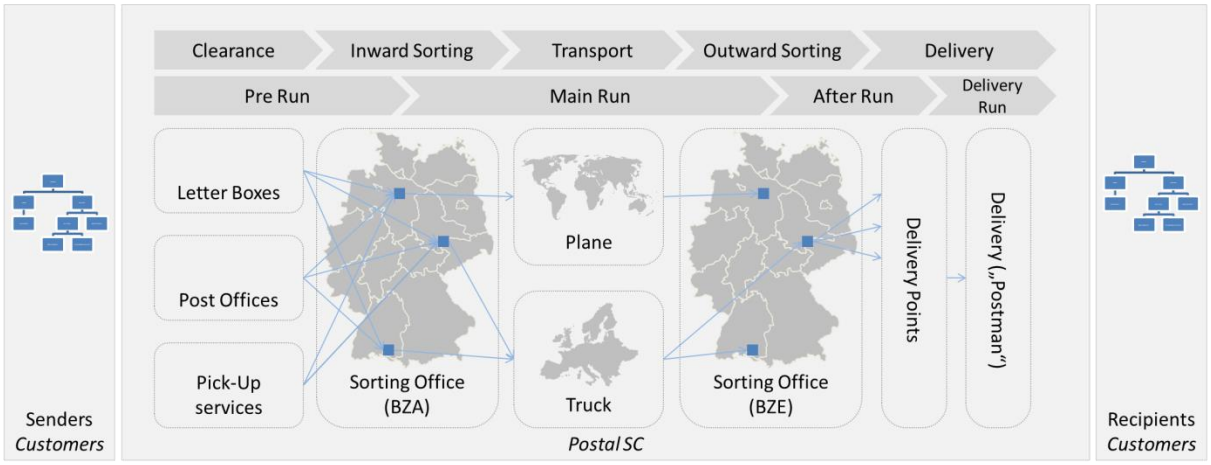


Abbildung 5: Ordnungsrahmen der postalischen Lieferkette

Modellierungskonventionen

Aufgrund der Verwendung von standardisierten Modellierungssprachen im Projekt wurden keine weiteren Modellierungskonventionen benötigt, mit Ausnahme einer Übereinstimmung zwischen den verwendeten Modelltypen, z.B. Architektur- und Prozessmodelle. Hierfür wurde eine Liste von erweiterten Modellierungskonventionen erstellt, die auf den Spezifikationen der verwendeten Modelltypen aufbaut und eine einheitliche Verknüpfung zwischen Modellebenen und zu realen postalischen Prozessen sicherstellt.

Erweiterte Modellierungssprache

Die Dokumentation und Evaluation von sicherheitsrelevanten Aspekten in Prozessmodellen erfordert die Verwendung einer Modellierungssprache mit Sicherheitsnotationen. Eine Literaturrecherche zeigte viele verzweigte und eigenständige Ansätze, standardisierte Modellierungssprachen zu erweitern (Jakoubi et al., 2009). Keine der Lösungen erfüllt die Anforderungen physischer Prozesse in der postalischen Lieferkette. Ebenso Verfahren zur Analyse der Sicherheit in Geschäftsprozessen, wie das MoSSBP Framework (Hermann, Hermann, 2006) oder HAZOP (Srivatanakul, Clark, Polack, 2004), verfehlen eine Berücksichtigung dieser Anforderungen. Daraus resultierte die Notwendigkeit, eine eigene Erweiterung zu erstellen. Diese ist Teil der Secure Logistics Processes (SLP) Methodology, welche im Rahmen des Projekts entwickelt wurde (Böhle et al., 2013, pp. 177-179). Die Erweiterung baut auf der Spezifikation der Business Process Modelling and Notation auf (Object Management Group, 2010).

Modellierungseditor

Die „Pivot" genannte Plattform unterstützt die Rollen des Projektmanagers, Prozessdesigners und Sicherheitsexperten in einer gemeinsamen Umgebung. Die Plattform setzt sich zusammen aus einer zentralen Serveranwendung zur Datenhaltung und zur Unterstützung der Kooperation zwischen den Nutzern, sowie einer Clientanwendung, die die Modellierungsumgebung und Analysefunktionen bereitstellt. Beide Bausteine stehen in enger Verbindung, können jedoch auch eingeschränkt einzeln genutzt werden.

Der Projekt-Server basiert auf einer Microsoft SharePoint-Umgebung, die um zusätzliche Funktionen ergänzt wurde. Diese dienen zum einen der *Projekterstellung* und der fortlaufenden

Entwicklung und Analyse von Prozessmodellen. Abbildung 6 zeigt das Hauptfenster der Projekt-Konfiguration, das durch weitere Optionsfenster Anpassungen am Projekt ermöglicht. Für jedes Projekt lassen sich Projektphasen anlegen, die für das Projektmanagement mit Zeithorizonten versehen werden. Jeder Phase können Meilensteine und Aufgaben hierarchisch zugewiesen werden. Später werden diese Informationen neben der reinen Aufgabenverwaltung zur Strukturierung der Projektumgebung genutzt. Dokumente und Modelle sind somit ihren übergeordneten Aufgaben zugewiesen, welche wiederum in den Projektphasen angesiedelt sind. Dies ermöglicht eine einheitliche Struktur und Wiederverwendung von Projektdefinitionen und Wissensbibliotheken über mehrere unabhängige Projekte.

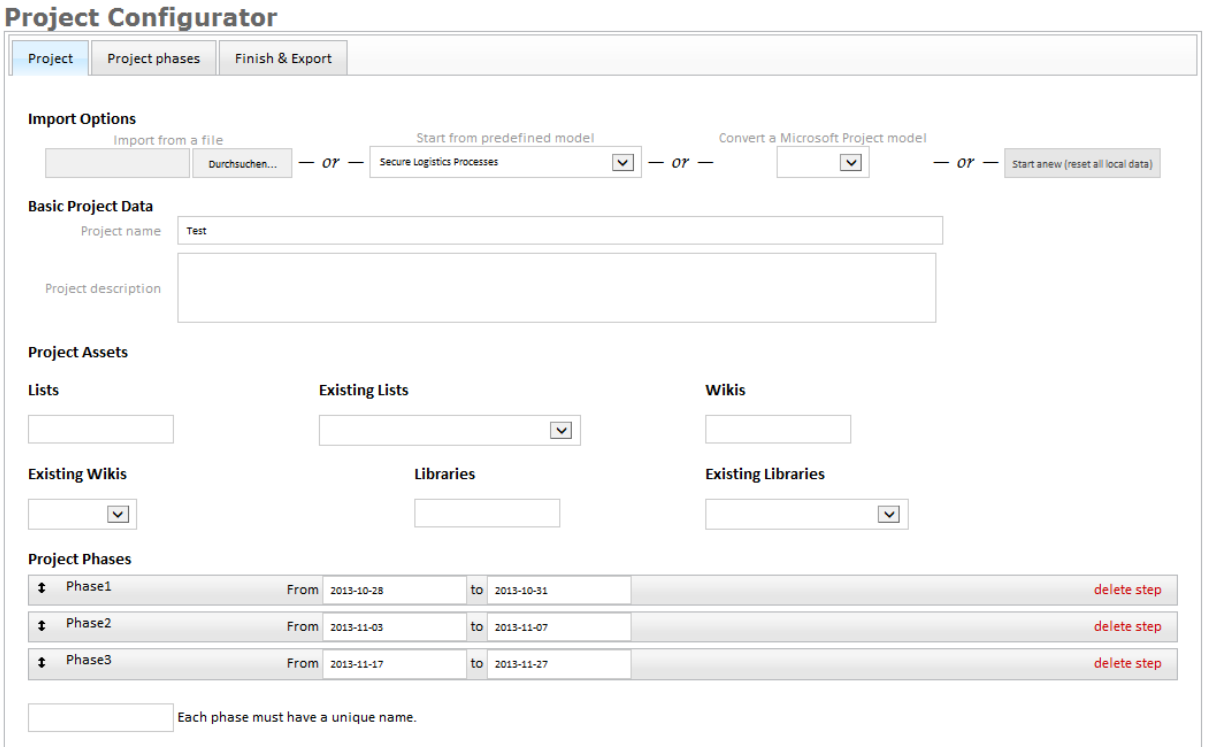


Abbildung 6: Projekt-Konfigurator

Die Client-Anwendung ist eine Erweiterung von Microsoft Visio und bietet eine enge Integration mit dem SharePoint-basierten Server und anderen Office-Anwendungen. Für die Modellierung und Analyse von Prozessmodellen wurden zwei Kernelemente der Plattformerweiterung entwickelt: die *Analyseschnittstelle* und das *ModelRepository*. Mittels der Analyseschnittstelle können spezielle Analysefunktionen für die Evaluation und Bearbeitung der Prozesse verwendet werden. Dadurch ist es möglich, den Funktionsumfang der Analysebibliothek stetig zu erweitern und an neue Anforderungen anzupassen. Zum Beispiel können Aufgaben in Form einer ToDo-Liste durch eine Analyse automatisch erstellt und zur weiteren Bearbeitung auf den Server hochgeladen werden. Das Modell Repository bietet als weitere Komponente eine zentrale Definition von Instanzen der Modellelemente. Jedes Modell und dessen Elemente werden in diesem Repository hinterlegt und sind für alle anderen Modelle verwendbar. Die damit abgebildeten logischen Verknüpfungen zwischen den Modellen erlauben es, komplexe Analysen zu erstellen.

Methoden zur Prozessevaluation

Für die Evaluation von Prozessen innerhalb der Pivot Plattform wird die zuvor beschriebene Analyseschnittstelle verwendet. Mittels dieser Schnittstelle bietet der lokale Client eine Plugin-Architektur in der beliebige weitere Analysen durch den Anwender hinzugefügt werden können. Die Analysen können die erweiterte Modellierungssprache nutzen, um die sicherheitsrelevanten Aspekte in den Prozessmodellen zu evaluieren. Im Rahmen des Projekts wurden zudem verschiedene Analysen entwickelt.

Unter Verwendung des ModelRepositories kann eine Compliance Prüfung zwischen dem Zielmodell und den Prozessmodellen durchgeführt werden. Dabei werden alle Anforderungen im Zielmodell automatisch auf ihre Umsetzung durch die Prozessmodelle geprüft. Die Umsetzung wiederum wird durch eine Verknüpfung von Anforderungen zu den erfüllenden Prozessen dokumentiert.

Für eine quantitative Analyse der Prozesse wurde eine semi-automatische Transformation vom Prozessmodell in ein AnyLogic Simulationsmodell entwickelt. Dazu wird jedem Element aus dem Modell ein entsprechendes Element aus der Simulationsumgebung zugeordnet. Dabei werden die Anforderungen aus den physischen Prozessen berücksichtigt, z.B. dass eine Sendung stets nur einen Prozess zur gleichen Zeit durchlaufen kann.

Basierend auf der Unterscheidung zwischen sicheren, unbekannten und unsicheren Prozesspfaden aus der Modellerweiterung, wurde eine Sichere-Pfad-Analyse entwickelt. Diese analysiert zusammenführende Prozesswege verschiedener Sicherheitsstufen auf eventuelle Konflikte. So ist z.. B. ist eine Vermischung von sicheren und unbekannten Sendungen zu vermeiden, ausgenommen es erfolgt eine weitere Prüfung, die zu einer endgültigen Aufteilung der Sendungen führt.

Als weiteres Beispiel können aus den Prozessmodellen automatisiert Berichte generiert werden, die in einem Dokument den Prozess und den Ablauf beschreiben und alle Informationen aus dem Modell zusammenfassen. Diese Berichte können für das Projektmanagement und die Dokumentation der Prozesse verwendet werden.

2.1.1.3 UAP 2.3 Modellierung der aufgenommenen Prozesse in der Plattform

Zur Verwendung der entwickelten Modellierungs- und Evaluationsmethoden wurde das InPoSec Projekt in der eigenen Pivot Plattform erstellt. Dies beinhaltet nicht nur die erhobenen Prozesse, sondern auch eine Übersicht aller Arbeitspakete und Meilensteine. Hierzu wurde der Projektplan im Projekt-Konfigurator der Pivot Plattform abgebildet. Die Arbeitspakete wurden als Projektphasen eingetragen, um deren Ergebnisse zum Erfüllungsdatum zu prüfen.

Hauptbestandteil sind jedoch die formalen Prozessmodelle, die entsprechend der textuellen Dokumentation aus UAP 2.1 im Visio Client modelliert und auf den SharePoint Server hinterlegt wurden. Die von der Plattform bereitgestellten Analysefunktionen konnten nur eingeschränkt auf die Prozessmodelle der Ist-Situation angewendet werden, da diese noch keine sicherheitsrelevanten Aspekte enthalten, welche erst im Rahmen von AP 3 hinzugefügt wurden.

2.1.1.4 UAP 2.4 Evaluation der gegenwärtigen Prozesse hinsichtlich Schwachstellen und Risiken

Gegenstand des UAP 2.4 war die Evaluation bestehender Prozesse hinsichtlich der Schwachstellen und Risiken unter Verwendung von qualitativen und quantitativen Methoden. Dazu wurde ein qualitatives Evaluationsframework für Sicherheitsaspekte in Lieferketten entwickelt und auf die im InPoSec-Projekt erhobenen Prozesse angewendet. Zudem wurde eine Simulationsstudie zur quantitativen Evaluation möglicher Inspektionsverfahren im Importprozess durchgeführt.

Prozessbewertung (Ist-Situation)

Das Evaluationsframework klassifiziert mögliche Schwachstellen in Prozessen in den Perspektiven *Mensch*, *Zeit*, *Struktur*, *Screening*, und *Information* sowie den Dimensionen *statisch* und *dynamisch*. Jede Kategorie enthält Kriterien nach denen die Prozesse bewertet werden. Eine vollständige Auflistung aller Kriterien ist in Tabelle 1 gegeben. Eine Beschreibung der Perspektiven und Dimensionen kann zusammen mit einer Auswertung für alle aufgenommenen Prozesse dem Ergebnisbericht zu UAP 2.4 entnommen werden.

	Mensch	Zeit	Struktur	Screening	Information
Statisch	• Subjektivität • Expertise • Rückverfolgbarkeit	• Zeitbestimmungen	• Risiko Events • Alternative Prozesspfade • Sequenz • Komplexität • Aufteilung • Einhaltung Sicherheitsmanagement • Referenzprozess	• Technologien • R. A. Methoden	• Inf. Verfügbarkeit • IT Support • Medienbrüche
Dynamisch		• Schicht • Zeit-bis-Kontrolle • Belastung	• Abweichungen	• Detektionsrate • Inspektionsrate	• Datenqualität

Tabelle 1: Prozessevaluations-Framework

Simulationsmodell

Die Simulationsstudie für die quantitative Analyse wurde basierend auf den aktuellen Prozessen unter Berücksichtigung möglicher zukünftiger Scanning-Technologien durchgeführt. Die Modellentwicklung basiert auf den Vorgaben der VDI-Richtlinie 3633 und stützt sich zudem auf die Ergebnisse des AP 1 zur Erfassung der relevanten Prozesse und AP 2 zur Erhebung des aktuellen Prozessdesigns. Die Simulation unterstützt Analysen und Vergleiche verschiedener Scanning-Technologien in variierender Anordnung und untersucht dabei quantitative Faktoren wie Zeit, Anzahl vermuteter Bedrohungen, Anzahl entdeckter Bedrohungen und weitere. Details können dem Ergebnisbericht zu UAP 2.4 und der wissenschaftlichen Veröffentlichung (Hellingrath et al., 2013) entnommen werden.

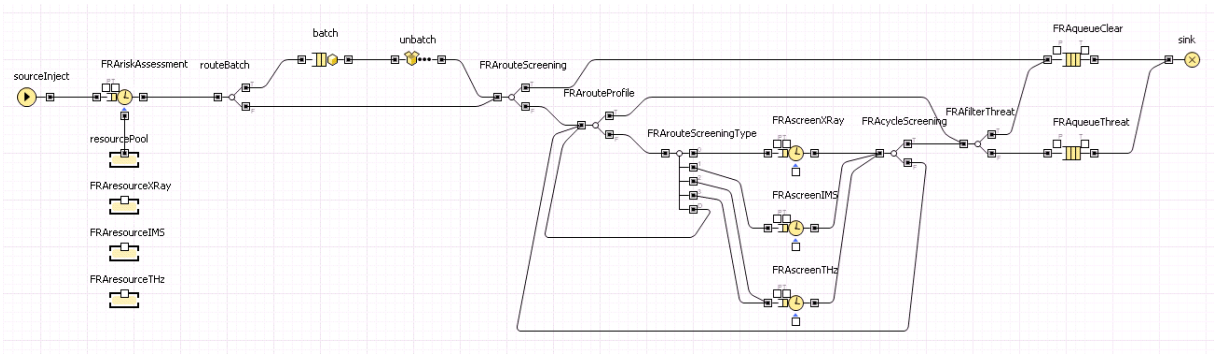


Abbildung 7: Simulationsmodell

2.1.1.5 UAP 2.5 Ableitung der Anforderungen an Sicherheitsmanagement, Prozesse und Inspektionsverfahren

Basierend auf den Ergebnissen aus UAP 2.4 wurde in diesem UAP ein Katalog abgeleitet, der die Anforderungen an das Sicherheitsmanagement (AP 5), die informatorischen (AP 3) und physischen (AP 4) Prozesse enthält. Diese Anforderungen werden bei der Neugestaltung der Prozesse und in der Entwicklung des Sicherheitsmanagements berücksichtigt und in der nachfolgenden Überarbeitung zur Evaluation verwendet. Der Katalog wurde mit dem Konsortium auf dem deutschen Konsortiumstreffen am 20. und 21. Januar 2014 besprochen und finalisiert. Dabei wurde er auf Unklarheiten hin überprüft und vervollständigt. Die Anforderungen wurden als Grundlage für die Prozessneugestaltung vereinbart. Die vollständige Liste der Anforderungen ist dem Ergebnisbericht von UAP 2.5 zu entnehmen.

2.1.2 AP 3 Entwurf der informatorischen Prozesse

AP 3 beschäftigte sich mit der Neugestaltung der informatorischen Prozesse basierend auf den in AP 2 definierten Anforderungen. Dazu wurden die Daten und Schnittstellen definiert und in Relation zu den zugrunde liegenden physischen Prozessen gesetzt.

2.1.2.1 UAP 3.1 Gestaltung der informatorischen Prozesse

Das UAP 3.1 befasste sich mit der Neugestaltung der informatorischen Prozesse, basierend auf den Erhebungen zum postalischen Netzwerk in AP 1 und der Evaluation der aktuellen Prozesse in AP 2. Die Neugestaltung der informatorischen Prozesse stand in engem Zusammenhang mit den physischen Prozessen in UAP 4.2, weshalb beide UAP gemeinsam und parallel bearbeitet wurden.

Beschreibung von Schnittstellen zwischen Post, Behörden (DE, FR) und dem geplanten InPoSec-System

Basierend auf den Erkenntnissen der Analyse der Ist-Prozesse, der Analyse rechtlicher Rahmenbedingungen und den erwarteten zukünftigen Änderungen im Zollkodex wurden mögliche Gestaltungsszenarien für die Neugestaltung der Prozesse entwickelt. Diese wurden auf dem Konsortiumstreffen am 20. und 21. Januar 2014 in Münster den Projektpartnern vorgestellt. Durch die Fokussierung auf ein Szenario und der finalen Gestaltung der informatorischen Prozesse, wurde die Grundlage für die Arbeiten in den weiteren UAP geschaffen. Durch die starke Abhängigkeit der informatorischen und physischen Prozesse zueinander, legt die Gestaltung in

diesem UAP auch die Rahmenbedingungen für das UAP 4.2 fest. Das grundlegende Szenario für die weiteren Arbeiten ist in Abbildung 8 zu sehen. Die Ausgestaltung in den informatorischen und physischen Prozessen wurde auf einem Workshop zum AP 3 und 4 am 23. April 2014 in Bonn unter den Partnern besprochen. Die finale Präsentation der Ergebnisse fand auf dem Konsortiumstreffen am 10. und 11. Juli 2014 in Bonn statt.

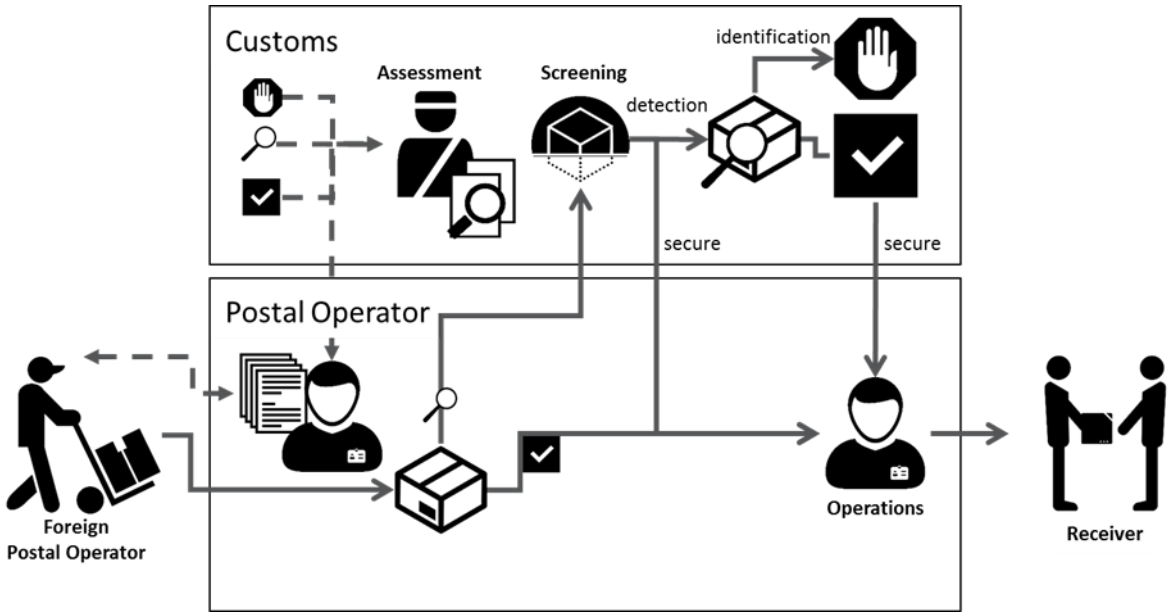


Abbildung 8: Schematische Darstellung der neugestaltenden Prozesse

Wie in der Abbildung dargestellt, werden zunächst die digitalen Vorabinformationen zu einer Sendung von der sendenden Postgesellschaft im Nicht-EU-Ausland an die empfangende Postgesellschaft übermittelt. Diese leitet die Daten für eine Risikoanalyse an die nationale Zollbehörde weiter. Die Entscheidung durch den Zoll, ob eine Sendung abgelehnt oder nach Ankunft inspiziert werden muss, wird über die empfangende an die sendende Postgesellschaft zurück übermittelt. Sobald eine Sendung eintrifft, wird diese entsprechend der zuvor getroffenen Entscheidung entweder an den Zoll geleitet oder durchläuft den regulären Importprozess und unterliegt eventuell einer Zollanmeldung. Dieses „Zwei-Ströme"-Konzept sorgt dafür, dass risikohafte Pakete getrennt vom regulären Paketstrom bearbeitet werden und somit knappe Ressourcen im Importprozess effizient eingesetzt werden können. Zudem erhöht eine klare physische Trennung die Sicherheit (siehe UAP 4.2). Potentiell gefährliche Sendungen werden vom Zoll mittels verschiedener Technologien untersucht, um Gefahrstoffe zu identifizieren und zu beschlagnahmen. Sichere Pakete gelangen zurück in den regulären Import und werden von der Postgesellschaft weiter bearbeitet. Schließlich werden diese Sendungen an den Empfänger ausgeliefert.

Prozessbeschreibungen der neu gestalteten informatorischen Prozesse

Der entwickelte Prozessablauf aus dem gewählten Szenario wurde anschließend in eine formale Prozessbeschreibung transferiert. Hierzu wurden die Schnittstellen zwischen den Systemen der Post und den Behörden in Deutschland und Frankreich zusammen mit der MIC in AP 7 ausgearbeitet. Die Modelle wurden anschließend in UAP 3.2 in der Prozessplattform angefertigt. Um nach der Neugestaltung der Prozesse sicher zu stellen, das alle relevanten Elemente aus der Ist-

Erhebung übernommen wurden und alle vollzogenen Änderungen entsprechend richtig durchgeführt wurden, wurde eine Gap Analyse durchgeführt. Dabei wurden alle Elemente aus der Ist-Ergebung den Elementen aus der Soll-Modellierung gegenüber gestellt. Dadurch wird zu jedem Element festgehalten, ob es übernommen, verändert oder entfernt wurde. Es konnte daher sichergestellt werden, dass die Soll-Modellierung ausschließlich beabsichtige Änderungen enthält. Zudem kann die Gap Analyse zur Dokumentation der Neugestaltung verwendet werden.

2.1.2.2 UAP 3.2 Modellierung und Evaluation der informatorischen Prozesse in Plattform

Für die Abstimmung der Gestaltungsszenarien zwischen den Partnern wurden alle Alternativen als Architekturmodell mit der in UAP 2.1 entwickelten Modellierungsmethode auf der Plattform modelliert. Dabei diente die Plattform als zentrales Mittel zur Kollaboration zwischen den Partnern und der Durchführung der Privacy-by-Design-Prozesse im Rahmen von AP 6. Das Ziel- und Anforderungsmodell gibt die übergeordneten Ziele vor, die durch eine Reihe von Anforderungen in den Architektur- und Geschäftsprozessmodellen erfüllt werden müssen. Das Architekturmodel fasst alle relevanten Akteure, Prozesse, IT-Systeme und Technologien im Importprozess zusammen und zeigt somit eine Gesamtübersicht des Systems. Die Geschäftsprozessmodelle dokumentieren detailliert alle Aktivitäten, die im Import durchgeführt werden. Abbildung 9 und Abbildung 10 zeigen die ungestalteten Architekturmodelle für den Import der deutschen und französischen Post.

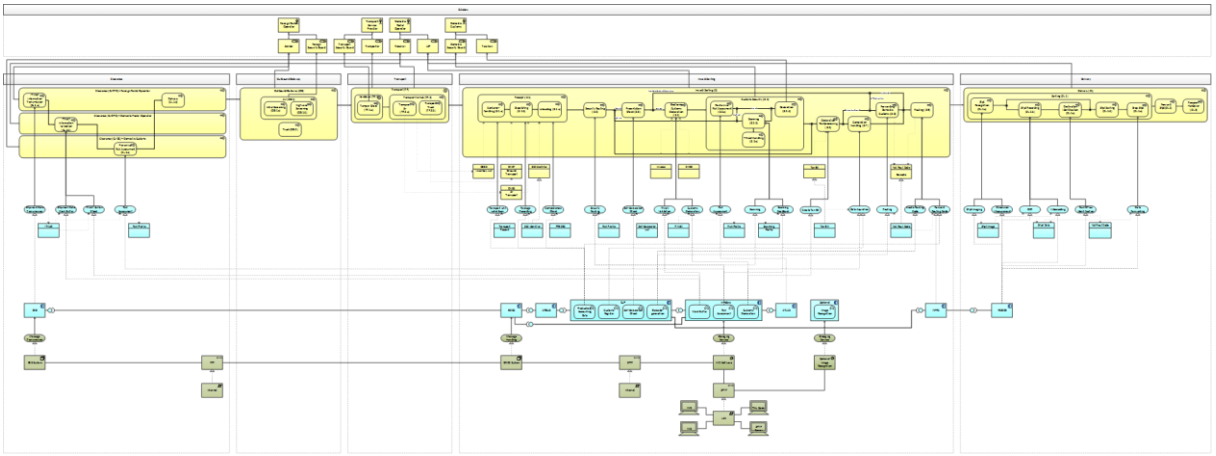


Abbildung 9: To-Be ArchiMate Architecture Model of Import Process at Deutsche Post AG

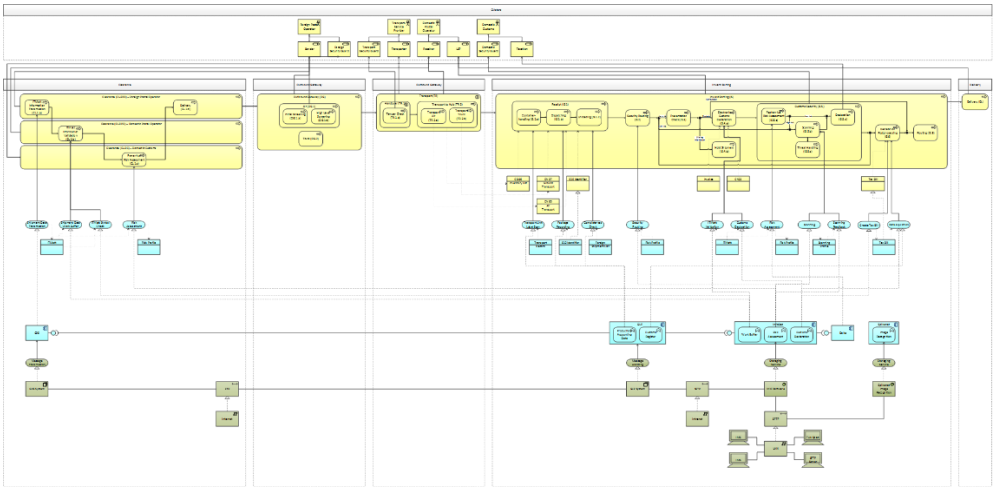


Abbildung 10: To-Be ArchiMate Architecture Model of Import Process at La Poste

In AP 2 wurde bereits das Ziel- und Anforderungsmodell gezeigt, welches die übergeordneten sicherheitsrelevanten Ziele in Anforderung an die neugestalteten Prozesse transferiert. Dieses Modell wurde nun in AP 3 genutzt, um die Erfüllung der Anforderungen zu überprüfen. Dazu wurde mittels der Plattform eine logische Verknüpfung zwischen Anforderungen und den Prozessen hergestellt. Als Ergebnis der Analyse konnte festgehalten werden, dass alle Anforderungen, die sich auf die Prozesse beziehen, vollständig umgesetzt wurden.

Für die Evaluation der resultierenden Prozesse wurden die Analysefunktionen der Plattform verwendet. Beispielhaft wurden mittels der in diesem UAP entwickelten Secure Path Analysis die verschiedenen Ströme von sicheren und risikohaften Paketen, die nach dem Zwei-Ströme-Konzept getrennt verlaufen müssen, im postalischen Prozess ausgewertet und auf eventuelle Schwachstellen geprüft. Die Analyse zeigte, dass die in AP 6 ermittelten Einschränkungen zur Erhebung von Daten durch die Universalpostdienstleister für eine Risikoanalyse in den Prozessen korrekt abgebildet wurden.

2.1.2.3 UAP 3.3 Verfeinerung der informatorischen Prozesse

Im Rahmen des UAP wurden die vorher modellierten Architekturmodelle schrittweise zu Prozessmodellen verfeinert und dabei um weitere Teilschritte und Datenobjekte erweitert.

1. Hierzu wurden zunächst alle möglichen Prozesspfade aus dem Architekturmodell ermittelt, da jedes Paket basierend auf der Risikoeinschätzung und Zollabwicklung verschieden behandelt werden kann.
2. Aus diesen Prozesspfaden wurden im nächsten Schritt alle Verbindungspunkte zwischen den Prozessschritten abgeleitet. Diese stimmen mit den Pfaden des Architekturmodells überein, insofern hier alle Pfade korrekt abgebildet wurden. Gegebenenfalls ist das Architekturmodell anzugleichen, um mit den Pfaden in den Prozessmodellen übereinzustimmen.
3. Als dritter Schritt wurden alle Elemente des Architekturmodells aus der Soll-Modellierung mit den bestehenden Prozessmodellen aus der Ist-Erhebung verbunden, um alle verbliebenen Elemente zu übernehmen. Dies resultiert darin, dass alle Schritte des neugestalteten Architekturmodells mit einem oder mehreren Prozessschritten verbunden

sind. Prozessschritte, die sich nicht in der neugestalteten Architektur wiederfinden, werden nicht übernommen.

4. Der letzte Schritt in der Verfeinerung ist die Anpassung der Prozessmodelle selbst. Hierbei werden die alten Prozesse entweder geteilt, vereinigt oder es werden neue Prozesse erstellt, wobei die Referenzen auf Vorgänger und Nachfolge entsprechend der möglichen Prozesspfade aktualisiert werden und die Prozessschritte entsprechend der neuen Architektur und der Evaluation aus AP 2 neugestaltet werden.

Wie in der Ist-Erhebung ist jedem Prozessschritt im Architekturmodell der Soll-Modellierung einem Prozessmodell zugeordnet. Die verfeinerten Prozessmodelle wurden wie in AP 2 mit dem entwickelten Evaluations Framework bewertet, um weitere sicherheitsrelevante Schwachstellen auszuschließen.

2.1.2.4 UAP 3.4 Ableitung von Anforderungen an integrierendes IT-System

Die neugestalteten Prozesse geben vor, welche Anpassungen im Rahmen des Imports vorzunehmen sind. Dies beinhaltet auch die Verwendung von Datenobjekten und IT-Systemen woraus wiederum Anforderungen an das integrierte IT-System in AP 7 resultieren. Dieses UAP hat sich mit der Ableitung solcher Anforderungen aus den Prozessbeschreibungen beschäftigt.

Um strukturiert eine vollständige Liste der Anforderungen zu erheben, wurden zunächst alle Prozessschritte identifiziert, aus denen unmittelbar Anforderungen abgeleitet werden können. Diese wurden mittels der folgenden Kriterien erfasst:

- Prozesse, mit einer direkten Verbindung zu IT-Systemen, da hier Daten ausgelesen oder erfasst werden.
- Prozesse, die Datenobjekte verwenden, hierzu jedoch nicht direkt auf ein IT-System zugreifen.
- Prozesse, die von Aktivitäten der zuvor ausgewählten Prozesse abhängig sind.

Alle erfassten Prozesse wurden auf Aktivitäten untersucht, die vom IT-System erfordern Daten zu übermitteln oder zu manipulieren, um den Prozess zu ermöglichen. Da aus den abgeleiteten Anforderungen weitere sekundäre Anforderungen entstehen können, wurde dieses Vorgehen wiederholt, bis sich keine weiteren Anforderungen mehr ergeben haben. Zusammengenommen wurden alle Anforderungen in einer Tabelle erfasst, die die Anforderung selbst, den relevanten Prozess und die mit der MIC geplanten Umsetzung im IT-System beschreibt. Die vollständige Liste an Anforderungen wurde zur Entwicklung des IT-Systems in AP 7 an die MIC übergeben und kann im Ergebnisbericht zu UAP 3.4 eingesehen werden.

2.1.3 AP 4 Entwurf der physischen Prozesse

Ziel des AP 4 war die Neugestaltung der physischen Prozesse zur Erfüllung der in AP 2 abgeleiteten Anforderungen. Die Neugestaltung betrifft den physischen Fluss von Postsendungen und hängt stark mit den Entwicklungsergebnissen zur integrierten Informationsbewertung, zur physischen Inspektion und zum Sicherheitsmanagement zusammen.

2.1.3.1 UAP 4.1 Abstimmung von Anforderungen und Fähigkeiten physischer Inspektionsverfahren

Ziel des UAP 4.1 war es, die in AP 2 erarbeiteten Anforderungen zunächst mit den Fähigkeiten der physischen Untersuchungstechnologien abzugleichen. Dabei wurden die verschiedenen Detektionsmöglichkeiten daraufhin analysiert, inwiefern sie sich auf die Anforderungen des postalischen Verkehrs übertragen lassen. Es wurde geprüft, welche Technologien sich nutzen lassen, um relevante Stoffe zu erkennen und potentiell risikobehaftete Sendungen schneller und sicherer erfassen und bewerten zu können. Die konkreten Fähigkeiten der Untersuchungstechnologien ergaben sich im Laufe des Projekts aus den erreichten Forschungsergebnissen der französischen und deutschen Partner. Ergebnis des UAP ist ein überarbeiteter, angepasster und mit Inspektionstechnologie abgestimmter Anforderungskatalog an physische Prozesse.

Die Arbeiten in diesem UAP wurden maßgeblich durch die Deutsche Post AG vollzogen und durch die WWU fortwährend begleitet. Aus dem UAP 2.4 wurden die Anforderungen aus den übergeordneten Zielen für den operativen Betrieb überprüft, wobei besonders die Untersuchungstechnologien von besonderer Relevanz für dieses UAP sind. In Absprache mit der Deutschen Post wurden für diese Anforderungen Implikationen an den operativen Betrieb ermittelt und anschließend mit den Technologien abgeglichen. Für das Ion-Mobility-Spektrometer (IMS) und der Terahertztechnologie zur Bildgebung und zur chemischen Analyse konnte so festgehalten werden, dass die Anforderungen erfüllt wurden und für die Neugestaltung der physischen Prozesse berücksichtigt werden. Eine genaue Darstellung der Anforderungen kann dem Abschlussbericht und dem Ergebnisbericht zu UAP 4.1 entnommen werden.

2.1.3.2 UAP 4.2 Gestaltung der physischen Prozesse

Wie in AP 3 geschildert basiert die Neugestaltung der informatorischen und physischen Prozesse auf dem gleichen Szenario, welches aus den verschiedenen Alternativen entwickelt wurde. Während das AP 3 die Änderungen in den informatorischen Prozessen behandelt hat, sind für das AP 4 nun die physischen Implikationen relevant. Dies betrifft den physischen Fluss der Sendungen im Import und dabei die Aufteilung von Sendungen je nach Risikobewertung und Zollverfahren.

Als erster Schritt wurde aus dem Architekturmodell aus UAP 3.2 ein Sankey-Diagramm hergeleitet. Darin wird von allen rein informatorischen Elementen abstrahiert und nur physische Bewegungen erfasst. Zusätzlich wurden in Absprache mit der Deutschen Post und basierend auf den Daten, die für die Entwicklung der Simulationsstudie in AP 2 genutzt wurden, eine Abschätzung der mengenmäßigen Aufteilung ermittelt, die ebenfalls im Sankey-Diagramm abgebildet wurde. Für eine erste Anordnung der Stationen in einer realen postalischen Umgebung, wurde ein Grundriss des Postzentrums in Speyer angefertigt. Dieser zeigt den Bereich, in dem Sendungen angenommen und falls notwendig dem Zoll vorgelegt wurden. Das Sankey-Diagramm wurde mit diesem Grundriss verbunden und ist in Abbildung 11 zu sehen. Die Dicke der Linien gibt den prozentualen Mengenanteil des Teilstroms an der Gesamtmenge von Sendungen wieder. Auf dem ersten Blick lässt sich erkennen, dass ein Großteil von Sendungen ohne weitere Bearbeitung nach der Annahme weitergeleitet werden kann. Für einen Bruchteil ist eine Kontrolle durch die Untersuchungstechnologien oder eine Zollanmeldung erforderlich.

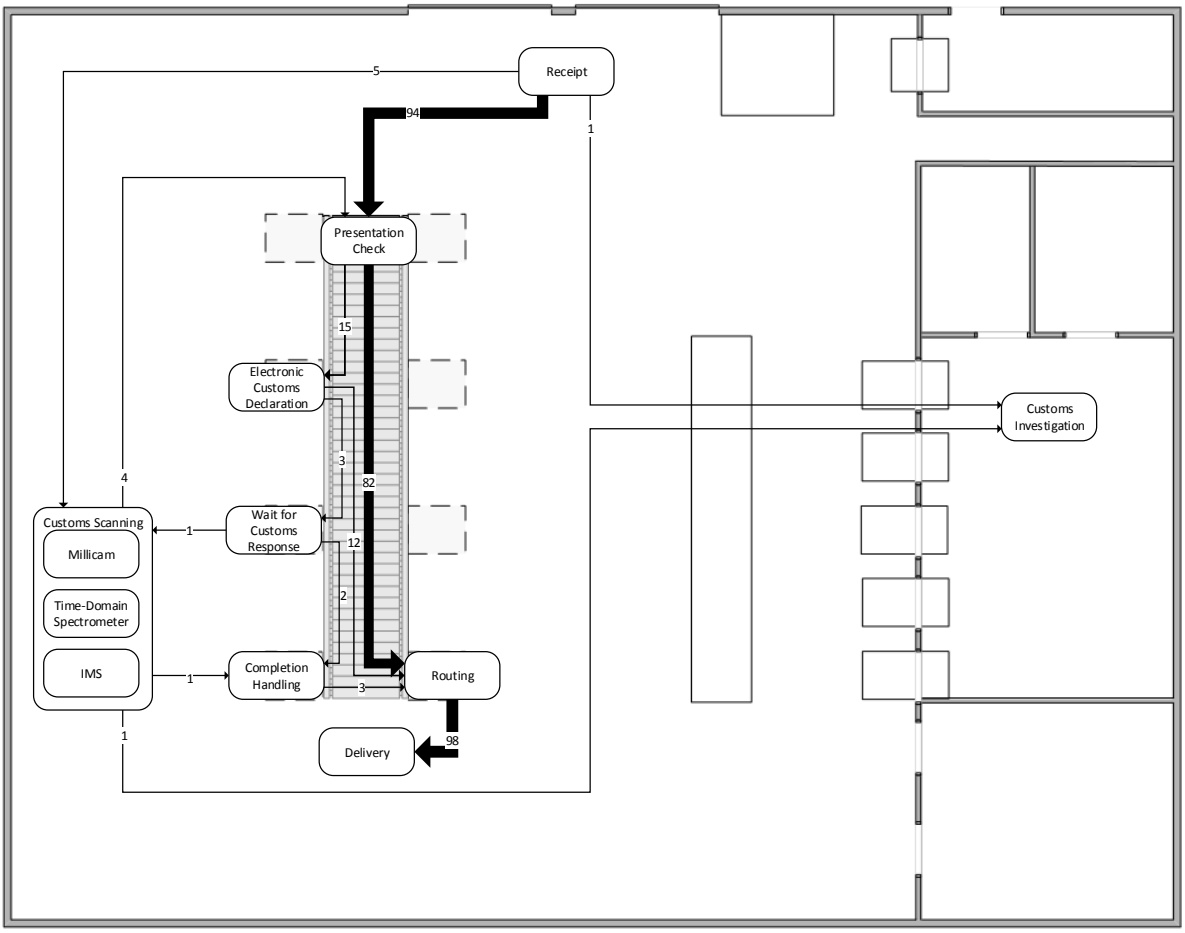


Abbildung 11: Sankey-Diagram auf Grundriss Speyer

2.1.3.3 UAP 4.3 Modellierung und Evaluation der physischen Prozesse in Plattform

Für die Modellierung und Evaluation der physischen Prozesse wurden die Abläufe aus dem Sankey-Diagramm aus UAP 4.2 in ein Warteschlangenmodell überführt. Das Warteschlangenmodell gestattet weitere Analysen zur Auslastung des Importprozesses, die ebenfalls zur Vorbereitung der Simulationsstudie verwendet wurden. Ein lineares Gleichungssystem beschreibt die Verteilung des Materialstroms in der Warteschlange und ermittelt dadurch die mittlere Auslastung der einzelnen Stationen, auf die sich der Paketstrom verteilt. Die stationäre Aufteilung kann der Tabelle 2 und Abbildung 12 entnommen werden, dabei sind die Stationen wie folgt benannt: Paketannahme (RECEIPT), Gestellungsprüfung (PC), Elektronische Zollanmeldung (ECD), Wartestation für Antwort des Zolls (WAIT), Abschlussbearbeitung (COMPL), Detektionstechnologien (SCAN), Leitkodierung (ROUT).

Service	Proportion
RECEIPT	30,81%
ROUT	30,19%
PC	30,18%
ECD	4,53%
SCAN	1,84%
COMPL	0,92%
WAIT	0,91%
THREAT	0,62%

Tabelle 2: Paketstrom Aufteilung

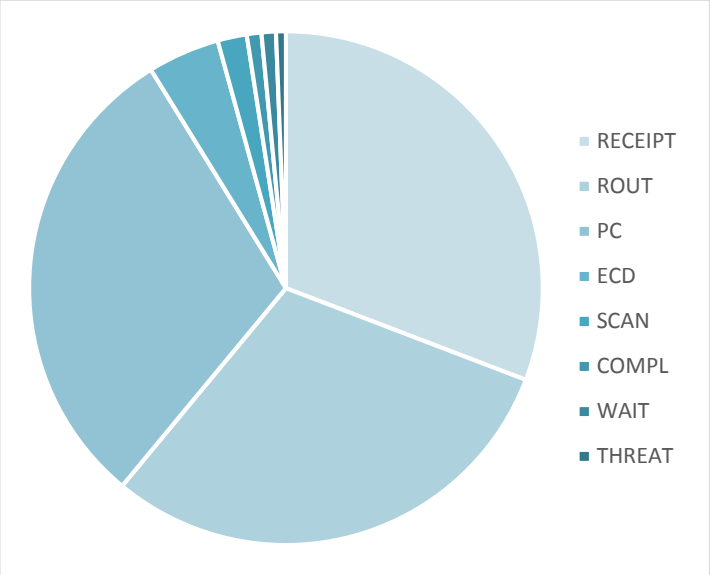


Abbildung 12: Paketstrom Aufteilung Diagramm

Unter Annahme der zugrunde liegenden Verteilungswahrscheinlichkeiten, die mit Experten der Deutschen Post abgestimmt wurden, ergibt sich, dass etwa zwei Drittel aller Pakete nach der Annahme im Paketzentrum direkt zur Auslieferung weitergeleitet werden können. Lediglich ein Drittel erfordert zusätzliche Maßnahmen, wie einer Zollanmeldung oder Sicherheitsprüfungen durch den Zoll. Auch der physische Ablauf wurde mittels des Frameworks aus AP 2 evaluiert und auf eventuelle sicherheitsrelevante Schwachstellen geprüft. Hierdurch konnte sichergestellt werden, dass informatorische und physische Prozesse den gleichen übergeordneten Sicherheitsbedingungen entsprechen.

2.1.3.4 UAP 4.4 Verfeinerung der physischen Prozesse

Das UAP 4.4 baut auf den Ergebnissen aus UAP 4.2 und 4.3 auf und hatte vorrangig zum Ziel, die neugestalteten physischen Prozesse im Simulationsmodell zu modellieren. Das Simulationsmodell aus AP 2 enthielt eine vorgezogene Neugestaltung der Prozesse auf Basis der bis dahin erzielten Ergebnisse, konnte jedoch noch nicht auf die Ergebnisse der AP 3 und 4 zurückgreifen. Hierzu wurden zunächst die Untersuchungstechnologien entsprechend der neuen Prozesse in die Simulation eingefügt. Da die ursprüngliche Simulation eine flexible Parametrisierung und Sequenzierung erlaubte, konnten nötige Anpassungen direkt vorgenommen werden, ohne umfangreiche Änderungen am zugrundeliegenden Modell vornehmen zu müssen. Hinzu kam die elektronische Zollanmeldung, die im Simulationsmodell nicht aktiv durchgeführt wird, jedoch durch eine erwartete Verzögerung betroffener Pakete simuliert wird. Zur Validierung wurden alle möglichen Wege und proportionalen Aufteilungen im Importprozess aus den Modellen der vorangehenden UAP mit dem Simulationsmodell verglichen. Als Datenbasis dienten anonyme historische Daten der Deutschen Post aus dem Jahr 2012, die auch schon für die Entwicklung des Sankey-Diagramms (UAP 4.2) und des Warteschlangenmodells (UAP 4.3) verwendet wurden. Das Simulationsmodell erfasst eine Reihe von Attributen, die den aktuellen Simulationslauf und den Ablauf jedes Pakets dokumentieren, um hierauf weitere Analysen durchführen zu können. Abbildung 14 zeigt eine 3D-Darstellung der Paketannahme und der

Aufteilung des Paketstroms in sichere und risikohafte Pakete. Letztere werden zur Inspektion unter Verwendung der Untersuchungstechnologien an den Zoll geleitet.

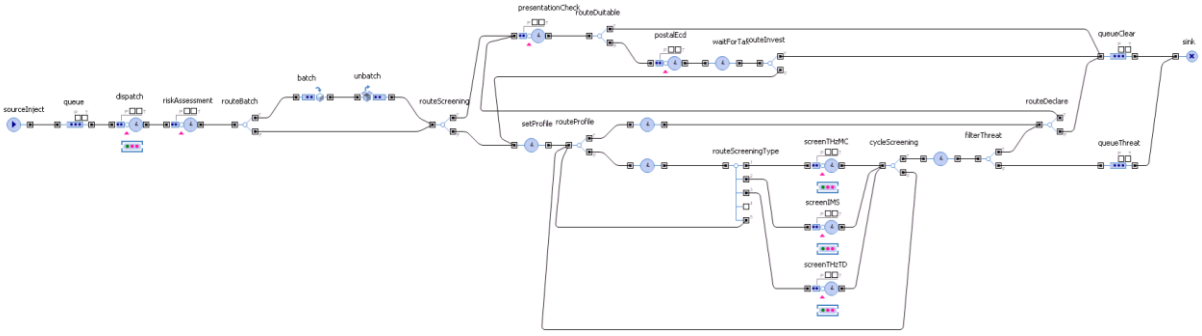


Abbildung 13: AnyLogic Simulationsmodell

Abbildung 14: Simulationsmodell 3D Ansicht

2.1.3.5 UAP 4.5 Ableitung von Anforderungen an ein integrierendes IT-System

Zur Erhebung der Anforderungen an das integrierende IT-System wurde das gleiche Vorgehen wie in UAP 3.4 verwendet. Im Unterschied zu den Anforderungen aus den informatorischen Prozessen wurde hier auf die physischen Prozesse geachtet. Ausgehend von den Schnittstellen zwischen physischen Prozessen und den IT-Systemen und ihrer abhängigen Prozesse wurden Anforderungen erfasst. Die Anforderungen wurden auf ihre Erfüllung durch das Konzept für das IT-System geprüft, oder in dieses aufgenommen. Kernaspekte neben weiteren Anforderungen sind die Unterstützung der physischen Trennung von sicheren und risikoreichen Paketen und die Möglichkeiten zur Automatisierung der Abläufe. Die Deutsche Post AG war zur Berücksichtigung ihrer IT-Systeme beratend beteiligt. Eine vollständige Beschreibung der Ergebnisse und des Vorgehens zur Erhebung ist dem Ergebnisbericht zu UAP 4.5 zu entnehmen.

2.1.4 AP 5 Entwurf eines Sicherheitsmanagementkonzepts

AP 5 befasste sich mit der Abstimmung der neugestalteten Prozesse mit dem Sicherheitsmanagementkonzept, der Ableitung von Anforderungen an den operativen Betrieb und der kontinuierlichen Verbesserung des Gesamtkonzepts.

2.1.4.1 UAP 5.1 Evaluation existierender Sicherheitsmanagementkonzepte

Im Rahmen des UAP 5.1 wurden zunächst relevante Sicherheitsinitiativen identifiziert, die aus Sicht des Projekts für die Anwendung in postalischen Lieferketten eingesetzt werden können. Hierzu wurde eine Literaturrecherche genutzt, die in einem weiteren Schritt durch eine Recherche bei Organisationen im Bereich von Lieferketten, Transportsicherheit und speziell postalischen Lieferketten ergänzt wurde. Insgesamt konnte eine Liste von 23 Standards ermittelt werden. Diese wurden zunächst mittels eines Referenzmodells analysiert und kategorisiert, um einen Katalog existierender Sicherheitsmanagementkonzepte zu entwickeln, der in einem weiteren Schritt evaluiert wurde. Das Referenzmodell in Abbildung 15 teilt die Initiativen in drei Gruppen ein: *öffentlich*, *privat-öffentlich* und *privat*. Zusätzlich erfolgt eine Evaluation hinsichtlich sechs Dimensionen: *adressierte Sicherheitsmaßnahmen*, *Effizienzeinfluss*, *adressierte Gefahren*, *beteiligte Akteure*, *Typ* und *geografische Reichweite*. Eine vollständige Beschreibung der Gruppen und Dimensionen kann dem Ergebnisbericht zu UAP 5.1 entnommen werden. Der resultierende Katalog in Tabelle 3 listet alle Standards mit ihrer Einordnung in den Ordnungsrahmen. Für die Evaluation wurden anhand von wissenschaftlicher Literatur, postspezifischer Dokumentationen und strukturierten Interviews für den postalischen Sektor spezifische Kriterien ermittelt. Mithilfe der 10 identifizierten Kriterien wurden die Standards auf ihre Anwendbarkeit im postalischen Sektor evaluiert und die Ergebnisse in Tabelle 4 zusammengefasst.

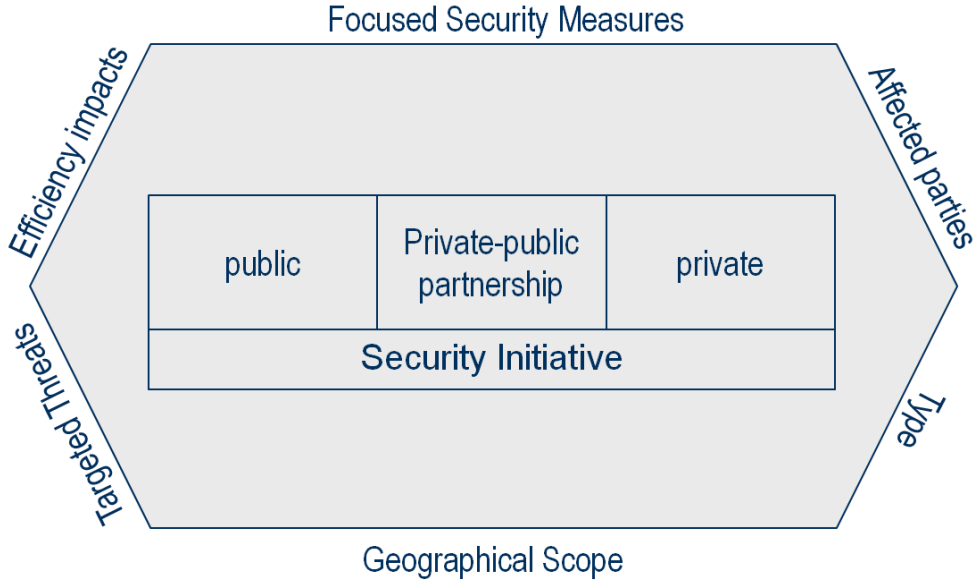


Abbildung 15: Evaluationsframework für Sicherheitsinitiativen in Supply Chains

	Public Initiatives				Public-Private Initiatives													Private Initiative					
	CSI	ACI	ISF	TWIC	ISPS	CCSP	Frontline	C-TPAT	EU AEO	SES	STP	Golden List	PIP	FAST	Stairway + StairSec	ISA	CSA	TAPA	BASC	ISO 28000	SSTL	OSC	WCO SAFE
Type	SAFE Impl.							SAFE Impl.															
regulation	x	x	x	x	x																		x
voluntary certification program						x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Focused Security Measures																							
prevention																							
facility protection					x	x		x	x	x	x	x	x		x			x	x				x
cargo protection	x				x	x		x	x	x	x	x	x	x				x	x			x	x
personnel security				x	x	x		x	x	x	x	x	x	x	x	x	x	x	x				x
data/IS protection						x		x	x	x	x	x	x		x			x	x				x
detection																							
(early) physical inspection	x				x	x																	x
inspection technology (e.g. X-Rays)	x					x																x	x
monitoring of cargo integrity					x													x					x, x
information exchange (risk ass.)	x	x	x		x		x														x	x	x
information systems (risk ass.)	x	x	x																		x	x	x
customs-customs cooperation	x																				x		x
recovery					x			x			x									x			x, x
Affected Parties																							
manufacturers						x		x	x			x							x	x			x
importers		x	x				x	x	x		x	x	x	x	x	x	x		x	x	x	x	x
exporters									x	x	x	x	x		x				x	x	x	x	x
carriers and consolidators			x		x	x	x	x	x			x	x	x	x	x	x	x	x	x		x	x
infrastructure operators	x			x	x	x	x	x							x				x				x
customs	x	x	x				x	x	x	x	x	x	x	x	x	x	x		x		x	x	x, x
Geographical Scope																							
national / local				x																x			
regional / cross-border	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x				x	x	
global								o	o	o	o	o	o					x	x			x	x, x
Efficiency Impacts																							
positive						x	o	x	x	x	x	x	x	x	x	x	x						x
negative	x	o	o																				x
Targeted Threats																							
theft				x							x							x		x			x
terrorism	x	x	x	x	x	x	x	x	x				x	x	x	x	x		x	x	x	x	x, x
damage or sabotage		x		x	x	x												x		x			x, x
introduction of unauthorized contraband	x	x	x	x		x	x	x	x	x	x		x	x	x	x	x		x		x		x, x
human trafficking	x			x			x						x	x	x	x	x		x				x, x
Modes of Transportation																							
land transport		x						x	x	x	x	x	x	x	x	x	x	x	x	x			x, x
sea transport	x	x	x	x	x		x	x	x	x	x	x	x		x	x			x	x	x	x	x, x
air transport		x				x	x	x	x	x	x	x	x		x	x		o	x	x			x, x

Tabelle 3: Katalog existierender Sicherheitsstandards für die postalische Lieferkette

Initiative	Core idea	Applicability in postal context[6]	Reasons for non-applicability
ISO 28000	Establishment of a SCS management system	Applicable	n/a
BASC	Securing the SC by implementing security standard	Not evaluated (generic goal)	n/a
C-TPAT	AEO – higher security motivated by incentives (customs – postal operator)	Not applicable (in theory), potentially applicable (in practice)	Non-applicability of typical security measures, limited information availability
	AEO – higher security motivated by incentives *transferred* (postal operator – customers)	Not applicable	Universal service requirements (QoS), acceptance requirement, postal secrecy law, non-applicability of typical security measures
WCO SAFE	AEO, Advance Cargo Information, Pre-screening of Cargo	Cf. C-TPAT, 24-hour rule and CSI results	n/a
24-hour rule	Advance Cargo Information – advance submission of manifests	Not applicable	Limited information availability, universal service requirements, postal secrecy law
TAPA	Certification of suppliers (outsourced operations)	Applicable	n/a
CSI	Pre-screening of high risk cargo which is identified based on Advance Cargo Information	Not applicable	Cf. 24-hour rule
FAST	Driver (security) certification motivated by incentives	Not evaluated (idea not transferable to postal context)	n/a
ISPS	Establishment of a comprehensive security standard for the maritime sector, involving all stakeholders	Applicable	n/a
TWIC	Issue of tamper-resistant biometric identification cards with background screening	Partially applicable (only for non-public premises)	Non-applicability of typical security measures, acceptance requirement, universal service requirements

Tabelle 4: Evaluation der Sicherheitsstandards

2.1.4.2 UAP 5.2 Prüfung bestehender Unternehmensrichtlinien zur Sicherheit in der postalischen Lieferkette

Zur Prüfung der bestehenden Unternehmensrichtlinien wurde die Deutsche Post AG seitens der WWU mit theoretischen Untersuchungen zum Sicherheitsmanagement unterstützt, speziell bezüglich ISO 28000. Dieser Standard wird ebenfalls von der Deutschen Post in der Konzernsicherheit eingesetzt. Dabei hat die WWU den Stand der Forschung zur Umsetzung der ISO 28000 mit der praktischen Anwendung durch die Konzernsicherheit der Deutschen Post abgeglichen. Dies wurde während eines Treffens in Bonn am 30.07.2013 bei der Deutschen Post und in weiteren Telefonkonferenzen zwischen den Beteiligten abgestimmt. Die WWU hat insbesondere die Koordination mit den übrigen Arbeiten in AP 5 übernommen, um die inhaltliche

[6] Applicability denotes whether a concept can theoretically be applied in a postal context. It does not give an indication on the suitability of a concept for the postal context. Therefore, a concept may be applicable but still should not be implemented as it does not provide benefits to a postal operator.

Kohärenz sicherzustellen. Die Ergebnisse zu UAP 5.2 können dem Erlebnisbericht des UAP entnommen werden.

2.1.4.3 UAP 5.3 Entwicklung von Prozeduren zur kontinuierlichen Risikoidentifikation

Zusammen mit der Deutschen Post AG wurde eine Prozedur zur kontinuierlichen Risikoidentifikation und Integration neuer Risiken in das Sicherheitsmanagementkonzept entwickelt. Die Prozedur basiert auf den Modellierungsmethoden, die durch die WWU in AP 2 entwickelt wurden und verwendet diese für die Analyse neuer Risiken. Basierend auf der ISO 28000, welches als Grundlage des Sicherheitsmanagement der DPAG und der Arbeiten in AP 5 dient, hat sich die Entwicklung zunächst auf eine Auswahl geeigneter Quellen und die Erfassung von sicherheitsrelevanten Informationen für die postalische Lieferkette konzentriert, aus denen neue Risiken identifiziert werden können. Um neue Risiken zu identifizieren wurden verschiedene Methoden ausgewählt und hinsichtlich ihrer Anwendbarkeit im postalischen Umfeld bewertet. Die ISO 31000 zur Risikoidentifikation wurde hierzu als erster Anhaltspunkt für geeignete Identifikationsmethoden herangezogen. Eine Übersicht von Methoden aus der referenzierten ISO/IEC 31010 kann der Tabelle 5 entnommen werden.

Technique	Description	Level of applicability
Check-lists	A simple form of risk identification. A technique which provides a listing of typical uncertainties which need to be considered. Users refer to a previously developed list, codes or standards	++
Preliminary hazard analysis	A simple inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility or system	++
Structured Interview and brainstorming	A means of collecting a broad set of ideas and evaluation, ranking them by a team. Brainstorming may be stimulated by prompts or by one-on-one and one-on-many interview techniques	++
Delphi techniques	A means of combining expert opinions that may support the source and influence identification, probability and consequence estimation and risk evaluation. It is a collaborative technique for building consensus among experts. Involving independent analysis and voting by experts	++
SWIFT Structured “what-if”	A system for prompting a team to identify risks. Normally used within a facilitated workshop. Normally linked to a risk analysis and evaluation technique	++
Human reliability analysis (HRA)	Human reliability assessment (HRA) deals with the impact of humans on system performance and can be used to evaluate human error influences on the system	++
Scenario Analysis	Possible future scenarios are identified through imagination or extrapolation from the present and different risks considered assuming each of these scenarios might occur. This can be done formally or informally qualitatively or quantitatively	++
Fault tree analysis	A technique which starts with the undesired event (top event) and determines all the ways in which it could occur. These are displayed graphically in a logical tree diagram. Once the fault tree has been developed, consideration should be given to ways of reducing or eliminating potential causes / sources	+
HAZOP Hazard and operability studies	A general process of risk identification to define possible deviations from the expected or intended performance. It uses a guideword based system. The criticalities of the deviations are assessed	++

Explanation: + applicable ++ strongly applicable

Tabelle 5: Methoden zur Risikoidentifikation. Tabelle entnommen aus ISO/IEC 31010, Annex A

Es existieren darüber hinaus viele weitere Methoden, die zur Risikoidentifikation genutzt werden können. Weitere Beispiele können der Tabelle 6 entnommen werden.

Surveys	- List of questions is developed beforehand - Information gained may not be accurate due to careless responses - Subjective answers and leading questions may affect the value of results
Expert Consultation	- Interviewing an individual who is experienced with similar situations - Apply their knowledge and experience on current situation
Documented Knowledge/ Historical Information	- Collection of information that is available on a subject based on past events - Historical Information is widely accepted as a fact - Applicability of information to current situation needs to be checked
Working Groups	- Risk identification group forms separate working groups - Allows a more detailed examination of one particular topic - Helpful in identification of risks that may not be obvious
Experiential Knowledge	- Collection of information that originates from personal experience - Applicability of information to current situation needs to be checked
Lessons Learned	- Experiential knowledge organized into information that may be relevant to different organizational areas - Enables identification of risks in municipality - Applicability of information to current situation needs to be checked
Analysis of Past Accidents	- Analysis of previous accidents and incidents in order to determine at which point something went wrong - Analysis of why the accident occurred - Pointer to risk areas in future situations
Risk Trigger Questions	- List of situations or events that have led to risk identification within the organization - Trigger questions can be grouped by areas such as performance, cost, schedule, etc.
Risk Lists	- Existing risk lists created in similar municipalities or situations - Applicability of risk lists to current situation needs to be checked

Tabelle 6: Methoden zur Risikoidentifikation[7]

Die WWU beschäftigte sich mit der Integration zukünftig identifizierter Risiken in das Sicherheitskonzept, welche im Folgenden kurz beschrieben wird. Die Prozedur sieht vor, dass unter Anwendung des in AP 5 entwickelten Sicherheitskonzepts neu identifizierte Risiken in das in UAP 2.1 vorgestellte Zielmodell aufzunehmen sind. Entweder bestehen bereits sicherheitsrelevante Anforderungen, die ebenfalls durch die neuen Risiken gestellt werden – in diesem Fall bedarf das Zielmodell keiner Anpassung – oder neue Anforderungen sind hinzuzufügen. Sofern die bestehende postalische Lieferkette diese Anforderungen nicht erfüllt, sind diese durch neue Prozesse oder Organisationselemente zu realisieren. Diese Entscheidung im Rahmen der Anwendung des Sicherheitsmanagement-konzepts wird durch die in diesem UAP entwickelte Prozedur unterstützt. Eine Beschreibung der kontinuierlichen Risikoidentifikation kann dem Ergebnisbericht entnommen werden.

[7] Sources for techniques and respective descriptions: Pritchard (2015, p. 65ff); Schneck (2010, p. 121-129); Clearrisk (2015); Clarizen (2013)

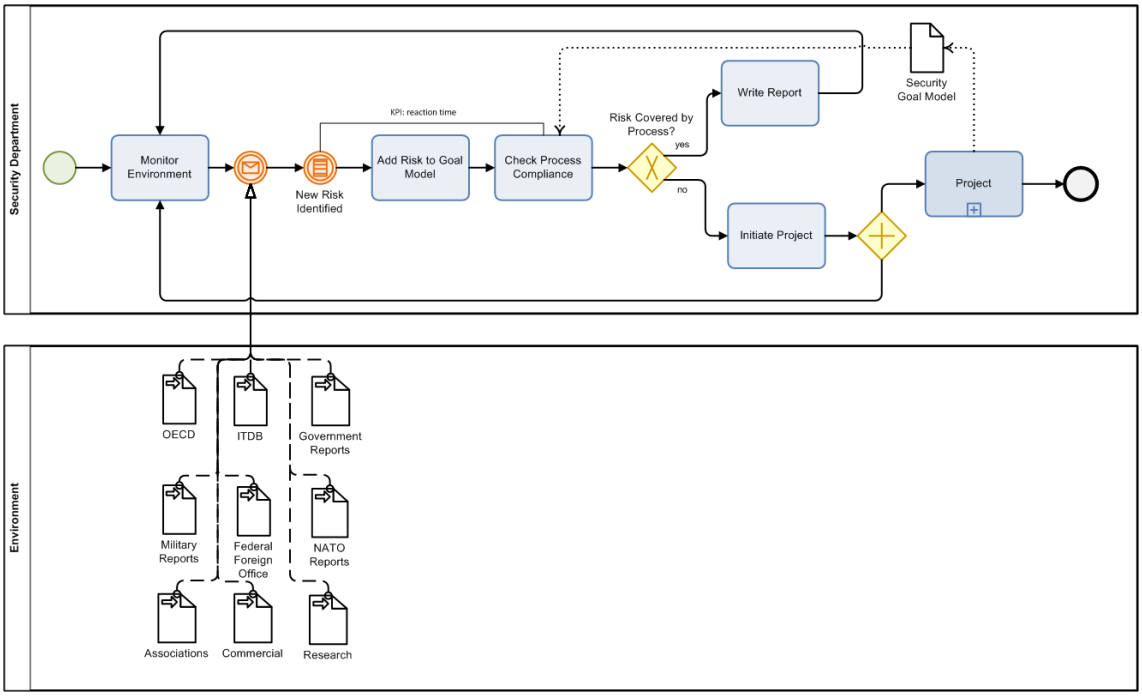


Abbildung 16: Prozess zur kontinuierlichen Verbesserung

2.1.4.4 UAP 5.4 Abstimmung des Sicherheitsmanagements mit neu entwickelten Prozessen

Auf Grund dessen, dass die Erstellung des Sicherheitsmanagementkonzepts anfänglich nicht als Teil des Vorhabens berücksichtigt wurde, haben sich die Projektpartner dazu entschieden, dieses in die Arbeiten zu AP 5 nachträglich aufzunehmen. Daher konnte die Abstimmung mit den neu entwickelten Prozessen bereits bei der Erstellung berücksichtigt werden. Alle relevanten Aspekte aus den Prozessen wurden in das Konzept mit aufgenommen. Einflüsse aus anderen Bereichen, die sich auf das Sicherheitsmanagementkonzept ausgewirkt haben, konnten rückwirkend mit den Prozessen abgestimmt werden, um deren Konformität zu garantieren. Durch den kontinuierlichen Abgleich waren keine weiteren Anpassungen mehr notwendig, weshalb das UAP 5.4 mit Fertigstellung des Sicherheitsmanagementkonzepts abgeschlossen wurde. Als Ergebnis wurde zum einen das Sicherheitsmanagementkonzept selbst und eine Liste zur Übertragung der hierin vorgegebenen Anforderungen an die Prozesse erstellt, welche in Tabelle 7 zu sehen ist. Das Sicherheitsmanagementkonzept kann der Anlage zu UAP 5.4 entnommen werden.

Index	To-be requirements	Fulfillment of requirements in to-be process architecture?	Reference	Comments
	Statutory requirements			
01	In compliance with all existing and legally valid national and international statutory requirements that affect the postal network (cf. 6)	✓	cf. chapter 2.2.1 in G-WP 3.2 (“Findings from Privacy-by-Design Review Process”)	The process architecture itself complies with legislation. For further details on legal bearings see G-WP 5.
	Risk Identification			
02	Generate a comprehensive list of risks (all risks) (cf. 7)	✓	cf. chapter 3 in G-WP 5.3 (”Risk Identification”):	Risk sources are continuously monitored and new risks are added to the monitoring list.
03	Observe entire environment of postal service to identify risks (cf. 7)	✓	cf. chapter 3 in G-WP 5.3 (”Risk Identification”) and chapter 3.1 in G-WP 5.3 (”Data Sources”)	A wide range of different providers of information on current or emerging risks is considered.
04	Make vulnerability of the postal supply chain measurable for risk analysis purposes (cf. 7)	✓	cf. chapter 4.2 in G-WP 5.6 (“Key Performance Indicators Catalogue”)	Provision of cost-, incident-, material flow-, IT-, technology-, and employee-related indicators to measure important security performance characteristics
05	System requirements derived from the goals and requirements model (cf. 7.1)	✓	cf. chapter 3.1 in G-WP 3.3 (“(A_CL.1) – Clearance”)	Parcel information is sent to the receiving postal company
			cf. chapter 3.1 in G-WP 3.3 (“(A_CL.1) – Clearance”)	Parcel information is evaluated with respect to security: The received information is validated and then forwarded to domestic customs
			cf. chapter 3.6 in G-WP 3.3 (“(D_IS.5) – Customs Screening”)	Scanning procedures are defined
			cf. chapter 4 in G-WP 5.3 (”Risk Analysis”)	Scanning procedures are adjusted to recognize identified risks
				A security dep. is already established in the participating organizations
				A connection to the UPU Situation Center is beyond the scope of the project
			cf. chapter 3.1 in G-WP 3.3 (“(A_CL.1) – Clearance”) and chapter 3.6 in G-WP 3.3 (“(D_IS.5) – Customs Screening”)	Pre-arrival and post-arrival risk assessment procedures are defined
			cf. chapter 3 in G-WP 5.6 (“3 Continuous Improvement”)	A continuous improvement process is developed according to the Plan-Do-Check-Act cycle (PDCA cycle)
06	Identify goods that are clearly of a dangerous nature (cf. 7.2)	✓	cf. chapter 3.1 in G-WP 3.3 (“(A_CL.1) – Clearance”) and chapter 3.6 in G-WP 3.3 (“(D_IS.5) – Customs Screening”)	Pre-arrival and post-arrival risk assessment procedures are defined
Index	**To-be requirements**	**Fulfillment of requirements**	**Reference**	**Comments**

		in to-be process architecture?		
	Processes and IT systems			
07	Create an architectural model in which the actors, processes, data objects, and IT systems involved are connected with one another (cf. 8)	✓	cf. G-WP 3.2	cf. to-be Archimate model
08	Individual processes are to be refined in detailed process models (cf. 8)	✓	cf. G-WP 3.3	BPMN process models refine the process models are used for refinement
	Risk assessment			
09	Implement a two stream concept that realizes a fast and a slow track (cf. 9.1)	✓	cf. chapter 3 in G-WP 4.2 (”Physical Process Design”)	Physical parcel streams are clearly separated
10	Perform a pre-arrival risk analysis (cf. 9.2)	✓	cf. e.g. chapter 2.3.2.1 in G-WP 3.2 (”Clearance”)	Domestic customs conducts pre-arrival risk assessment
11	Use fuzzy logic for risk assessment (cf. 9.3)	✓	cf. G-WP 7.1	
	Scanning technologies			
12	Use technologies that can identify the content of a parcel without the parcel having to be opened (cf. 10)	✓	cf. chapter 4.6 (“(D_IS.5) – Customs Screening”)	Use of THz, IMS, (X-Ray)
	Layout planning			
13	Create a layout plan that ensures the separation of potential / actual risks (cf. 11)	✓	cf. e.g. chapter 3.2 in G-WP 4.2 (“Material Flow Routing”)	
	Continuous improvement			
14	Constant threat monitoring (cf. 13.1)	✓	cf. chapter 3.1 in G-WP 5.3 (“Data Sources”)	Provision of data sources from supranational, governmental, military, commercial, and academic organizations
15	Establish Security Performance measurement (cf. 13.2)	✓	cf. chapter 4 in G-WP 5.6 (“Security measurement”)	Presentation of the ‘Security Performance Scorecard’, a six-perspective framework which structures the security performance indicators given in the KPI catalogue in chapter 4.2 in G-WP 5.6
16	Regularly check whether security measures are state of the art (cf. 13.3)	✓	cf. chapter 3 in G-WP 5.6 (“Continuous Improvement”)	Continuous improvement of the security management concept

Tabelle 7: Übertragung der Anforderungen aus Sicherheitsmanagementkonzept zu Prozessen

2.1.4.5 UAP 5.5 Ableitung von Anforderungen an den operativen Betrieb

Die Ableitung von Anforderungen an den operativen Betrieb wurde von der Deutschen Post durchgeführt. Hierbei war die WWU beratend tätig und hat anhand der neugestalteten Prozesse die hieraus resultierenden Anforderungen ermittelt. Als Beispiel wurden aus dem Sankey-Diagramm und der Layoutplanung aus AP 4 Anforderungen an den Platzbedarf abgeleitet. Während der Entwicklung des Sicherheitsmanagementkonzepts wurde auf eventuelle Auswirkungen auf den operativen Betrieb geachtet und mit der Deutschen Post abgestimmt.

2.1.4.6 UAP 5.6 Definition von Prozeduren zur Überwachung und kontinuierlichen Verbesserung

Bei der Entwicklung der Prozeduren zur Überwachung und kontinuierlichen Verbesserung wurde im Projekt ein grundlegendes Problem in der Bewertung von Sicherheit, speziell in einer postalischen Lieferkette, erkannt. Da die Sicherheit auf allen Gliedern in der Lieferkette basiert, ist diese durch die hohe Anzahl von Akteuren und der Komplexität nicht in einen Wert abzubilden. Spezifische Gefahren können nicht vorhergesehen werden, solange diese nicht bereits in der Vergangenheit auftraten und erkannt wurden. Zudem ist die Gesamtmenge an Gefahren für die postalische Lieferkette unbekannt, da Angreifer stets mit neuen Variationen die Sicherheit gefährden können. Ebenso kann die Effektivität von Sicherheitsmaßnahmen erst dann bestimmt werden, wenn diese in der realen Umgebung eingesetzt und getestet werden.

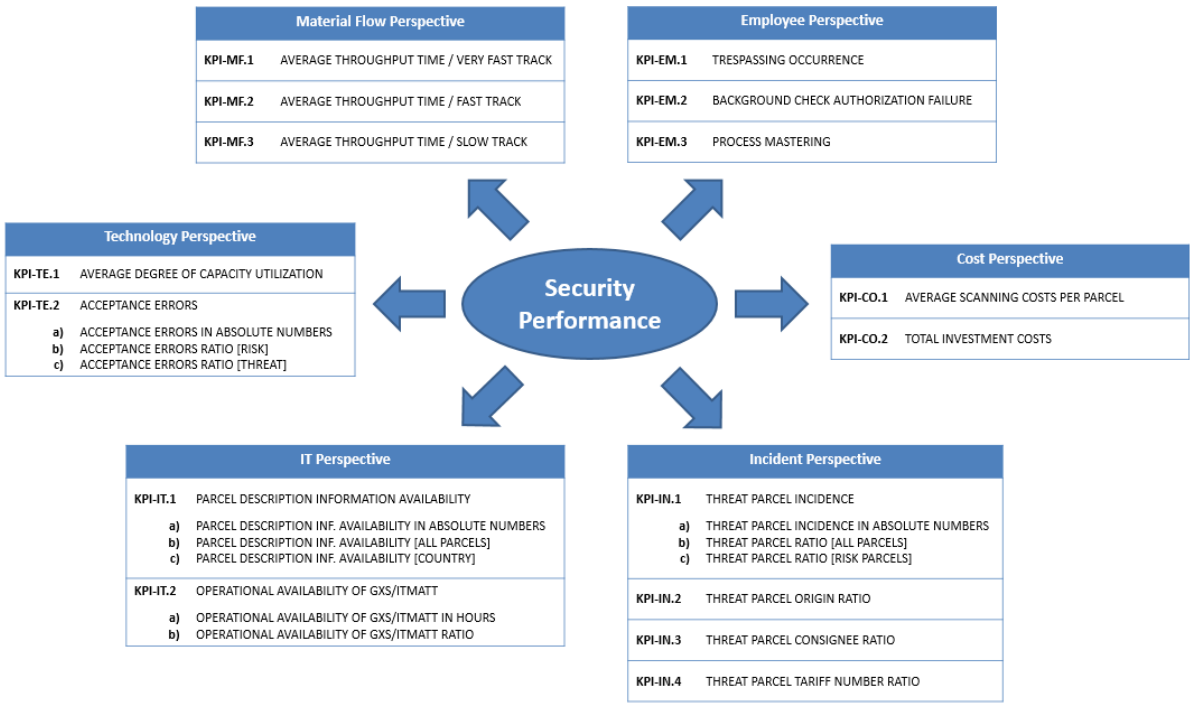


Abbildung 17: Security Performance Scorecard

Um diesem Problem entgegenzutreten, wurden im Projekt zwei Aspekte entwickelt. Das Sicherheitsmanagementkonzept aus UAP 5.4 beinhaltet einen Plan-Do-Check-Act Zyklus, in dem die aktuelle Sicherheitslage geprüft, entsprechende Sicherheitsmaßnahmen geplant und umgesetzt, die Effektivität überprüft und auf Veränderungen durch neue Anpassungen reagiert wird.

Dieser Zyklus wird kontinuierliche wiederholt, um neue Gefahren in das Konzept zu integrieren. Des Weiteren wurde ein Katalog von sicherheitsbezogenen Kennzahlen entwickelt, der die Sicherheit in der Lieferkette aus verschiedenen Perspektiven betrachtet, um so eine möglichst realitätsnahe Bewertung zu ermöglichen. Dieser Katalog beinhaltet kostenbezogene Faktoren, vergangene Vorkommnisse, Materialflussbewertungen, IT-System Evaluationen, Technologiestatistiken und Faktoren zu den Mitarbeitern. Abbildung 17 zeigt eine Übersicht dieser Perspektiven und der beinhalteten Faktoren. Eine genaue Beschreibung jedes Faktors kann dem Ergebnisbericht zu UAP 5.6 entnommen werden.

2.1.5 AP 6 Rechtliche Rahmenbedingungen

Mit dem AP 6 wurde sichergestellt, dass ein System zur Erhöhung der Sicherheit der postalischen Lieferketten entwickelt wird, das die geltenden rechtlichen Rahmenbedingungen des Zoll-, Post- und des Europarechts beachtet. Mit Blick auf den Privacy-by-Design-Ansatz wurden die rechtlichen Rahmenbedingungen (deutsches, französisches und EU-Recht) untersucht, um diese bereits bei der Entwicklung der Prozess- und IT-Architektur entsprechend berücksichtigen zu können.

2.1.5.1 UAP 6.1 Beschreibung existierender Zollanmeldeprozeduren

Gemäß den postrechtlichen Vorschriften werden unter „Postverkehr“ allein die Dienst- und Beförderungsleistungen verstanden, welche durch einen „Universaldienstleister“, der Mitglied im Weltpostverein ist, erbracht werden. In Deutschland und Frankreich erfüllt die Deutsche Post AG bzw. die französische La Poste die Voraussetzungen eines „Universaldienstleisters“. Der Begriff des „Postverkehrs“ ist auch im Sinne des europäischen Zollrechts eng auszulegen. Damit sind zollrechtlichen Bestimmungen (einschließlich Verfahrenserleichterungen), die den Postverkehr betreffen, allein auf die Universaldienstleister und nicht auf sämtliche am Markt tätigen Postdienstleister anwendbar.

2.1.5.2 UAP 6.2 Identifikation veränderter Anforderungen an den Zoll

Die Aufgaben des Zolls sind innerhalb des letzten Jahrzehnts gestiegen und vielfältiger geworden. Einerseits besteht die Notwendigkeit einer schnelleren Zollabfertigung, um im Zuge wachsender Globalisierung den wirtschaftlichen Erfordernissen gerecht zu werden. Andererseits muss an den EU-Außengrenzen ein Anstieg der Wirtschaftskriminalität, des organisierten Verbrechens und terroristischer Aktivitäten beobachtet werden. Damit wächst zugleich die Bedeutung des Zolls im Bereich „Sicherheit“ („Wächter an den Pforten der Gemeinschaft“; laut EU-Kommission). Die Risikoanalyse ist für den Zoll ein wirksames Instrument zur Identifikation von Risiken durch eine EDV-gestützte Auswertung von Datensätzen. Hierdurch kann das Risiko von einzelnen Waren bereits vor oder bei Verbringen in das Zollgebiet der EU bewertet werden, um dann darauf entsprechend reagieren zu können. Vereinheitlichte Standards und Kriterien sollen zudem ein gleichmäßiges Kontrollniveau im gesamten Zollgebiet sicherstellen.

Zollrechtliche Bestimmungen sehen für den Postverkehr verschiedene Verfahrensvereinfachungen vor. Nachteil dieser Verfahrensvereinfachungen ist jedoch, dass im Ergebnis für die Risikoanalyse weniger Daten zur Verfügung stehen. Eine effektive Risikoanalyse benötigt allerdings möglichst viele Daten. Wenn der Risikoanalyse mehr Daten zugeführt werden sollen und damit mehr Daten anfallen, dann müssen unter Beachtung des Datenschutzes die Systeme,

Verfahren, technischen Prozesse und Programme zur Risikoanalyse entsprechend ausgestaltet werden.

2.1.5.3 UAP 6.3 Rechtliche Anforderungen zur physischen Inspektion von Postsendungen

Die schriftliche Kommunikation (d.h. der Austausch von Informationen zwischen natürlichen oder juristischen Personen) ist sowohl in Deutschland als auch in Frankreich umfassend geschützt. Soweit das Schutzniveau der Charta der Grundrechte der EU über dem Schutzniveau des deutschen Grundgesetzes liegt, muss das Schutzniveau der Charta der Grundrechte der EU bei der Anwendung europäischer Zollrechtsbestimmungen Berücksichtigung finden.

§§ 5 und 10 ZollVG sowie Art. 66 Codes des Douanes ermächtigen die deutschen bzw. französischen Zollbehörden zum Öffnen und Kontrollieren von postalischen Sendungen. Weder die Deutsche Post AG noch La Poste haben zollrechtliche Kontrollbefugnisse. Das gilt auch für den Einsatz non-intrusiver Methoden, die Aufschluss über den Inhalt der Sendung geben. Den Universaldienstleistern ist es somit nicht gestattet, den Inhalt einer Postsendung zu kontrollieren, ohne dabei die Postsendung zu öffnen (z.B. durch den Einsatz von Röntgentechnik oder jedweder anderen Technik, die Aufschluss darüber gibt, was sich in der Sendung befindet). Dieses Privileg haben nur die Zollbehörden.

2.1.5.4 UAP 6.4 Rechtliche Anforderungen zum Austausch von Informationen zwischen Postdienstleistern und Zollbehörden

Der Umgang mit Daten wird sowohl in Deutschland als auch in Frankreich annähernd gleich und damit umfassend geschützt. Für den Postverkehr manifestiert sich dies im Postgeheimnis; geschützt jeweils durch das französische und das deutsche Postrecht. Gemäß § 41 Abs. 2 PostG ist dem Universaldienstleister das Erheben, Verarbeiten und Nutzen von Daten nur zur betrieblichen Abwicklung von geschäftsmäßigen Postdiensten erlaubt. Das Erheben, Verarbeiten und Nutzen von Daten, die sich auf den Inhalt der Postsendung beziehen, ist demzufolge grundsätzlich verboten. Eine Ausnahme besteht allerdings, wenn bestimmte Daten aufgrund einer gesetzlichen Bestimmung z.B. für die Zollabwicklung benötigt werden und der Universaldienstleister diese Daten zu diesem Zweck verwertet (vgl. Zollinhaltserklärung CN 22 bzw. CN 23).

2.1.5.5 UAP 6.5 Prüfung der Vereinbarkeit des Gesamtkonzepts mit den rechtlichen Rahmenbedingungen

Mit Abschluss der Arbeitspakete 6.1 bis 6.4 folgte im Dezember 2013 die rechtliche Begleitung der technischen und organisatorischen Entwicklungsstufen der Prozess- und IT-Architektur. Die Aufgaben, die hierbei anfielen, waren ebenso vielfältig wie herausfordernd. WWU Jura nahm beispielsweise regelmäßig an der wöchentlichen Telefonkonferenz der übrigen Projektteilnehmer teil, um offene Rechtsfragen entweder noch während der Besprechung oder später im Nachgang nach entsprechender Prüfung zu klären. Daneben wurden umfassende Projektarbeiten wie der Demonstrator und das Sicherheitsmanagementkonzept auf rechtliche Mängel untersucht. Zusätzlich mussten die rechtlichen Rahmenbedingungen in entsprechender Form an Projektexterne kommuniziert werden, um in der Öffentlichkeit mögliche Missverständnisse über das Projekt aufzuklären und Angst vor einem vermeintlich unberechtigten Eingriff in einen

solch sensiblen Bereich wie den Datenschutz zu nehmen. Hierzu dienten beispielsweise die Teilnahme an einer Podiumsdiskussion der Petersberg-Konferenz im Juni 2014 und die Einrichtung einer FAQ-Seite auf der Homepage von InPoSec. Mit dieser FAQ-Seite wurden der Öffentlichkeit die drängendsten Rechtsfragen zu dem Projekt in einem ersten Schritt beantwortet.

Außerdem wurden mit Blick auf die Entwicklung der Prozess- und IT-Architektur nochmals die Grundsätze des Privacy-by-Design herausgearbeitet: Datenvermeidung, Kontrollierbarkeit und Vertraulichkeit der Daten (durch eng umgrenzte Zugriffsrechte), Beachtung der Datenqualität (Verwendung der „richtigen" Daten für den rechtlich zulässigen Zweck) und die Möglichkeit der Trennung von Daten.

Zusammenfassend konnte folgendes Ergebnis festgestellt werden:

Ausschließlich den Zollbehörden ist das Erheben, Verarbeiten und Nutzen von Daten vorbehalten, um mit diesen eine Risikoanalyse zur Gefahrenabwehr vorzunehmen. Die Universaldienstleister sind hierzu nicht ermächtigt. Damit darf auch keine Datenübermittlung von dem Universaldienstleister an die Zollbehörden stattfinden, die eine Risikoanalyse bezwecken soll. Eine Datenübermittlung ist indes zulässig im Wege der regulären Zollabwicklung (z.B. Zollanmeldung), wenn bestimmte Daten aufgrund einer gesetzlichen Bestimmung z.B. für die Zollabwicklung benötigt werden und der Universaldienstleister diese Daten zu diesem Zweck übermittelt (vgl. Summarische Eingangsanmeldung). Eine Datenübermittlung von dem Universaldienstleister an die Zollbehörden kann danach nur im Wege der regulären Zollabwicklung erfolgen (z.B. Zollanmeldung). Eine Verwertung dieser Daten zum Zwecke der Risikoanalyse muss von den Zollbehörden in eigener Zuständigkeit und ohne eine Beteiligung der Universaldienstleister vorgenommen werden.

2.1.6 AP 7 Entwurf eines integrierten IT-Systems

2.1.6.1 UAP 7.2 Abstimmung fachlicher und softwaretechnischer Anforderungen

Die geplante Neugestaltung der informatorischen und physischen Prozesse wurde auf dem Konsortiumstreffen am 20. und 21. Januar 2014 diskutiert. Dabei wurden auch die Anforderungen hinsichtlich der Softwareintegration diskutiert. Die vorgestellten Entwürfe durch den Projektpartner MIC wurden seitens der WWU mit den aktuellen und geplanten Prozessen abgeglichen und in die Prozessmodelle für die neugestalteten Prozesse (AP 3 und 4) aufgenommen. Die Ergebnisse aus dem UAP 7.2 sind dem Ergebnisbericht zu entnehmen.

2.1.6.2 UAP 7.4 Entwurf Kommunikationsschnittstellen und -standards

Die WWU hat für den Entwurf der Kommunikationsschnittstellen und -standards den Stand der Forschung erhoben und diese mit den Konzepten der MIC verglichen. Dabei hat die WWU die Vor- und Nachteile verschiedener Alternativen diskutiert und insbesondere die Vorzüge einer serviceorientierten Architektur herausgestellt. Die entworfenen Schnittstellen wurden mit den neugestalteten Prozessen aus AP 3 abgestimmt und in das Gesamtkonzept aufgenommen. Die Ergebnisse aus dem UAP 7.4 sind dem Ergebnisbericht zu entnehmen.

2.1.7 AP 8 Demonstration und Konzeptvalidierung

2.1.7.1 UAP 8.1 Integration der technischen Konzepte und des Sicherheits-managements

Zur Integration der technischen Konzepte und des Sicherheitsmanagements hat die WWU als Experte für die neugestalteten informatorischen und physischen Prozesse und der Schnittstellen zu den IT-Systemen mitgewirkt. Bei der Planung der Integration und Konzeptionierung des Demonstrators wurde das in den vorherigen Arbeitspaketen entwickelte Simulationsmodell verwendet. Hierdurch konnten verschiedene Möglichkeiten der Anordnung und sequenziellen Folge von Prozessen und Detektionsgeräten erprobt und evaluiert werden. Als Resultat wurde gemeinsam im Konsortium ein Integrationskonzept für den Demonstrator entwickelt.

Der Projektplan sah ursprünglich eine Integration des Konzepts in den operativen Betrieb der Deutschen Post vor. Dies ist jedoch aus verschiedenen Gründen nicht umsetzbar. Es ist organisatorisch nicht möglich, den Demonstrator, d.h. Technologien und veränderte Prozessabläufe, in seiner frühen Entwicklungsphase in den operativen Betrieb zu integrieren, ohne dabei den fehlerfreien Betrieb der Deutschen Post zu gefährden. Aus logistischer Sicht sind ohne eine dauerhafte Umstrukturierung der Paketzentren keine ausreichenden Flächen vorhanden und zum Zeitpunkt der Demonstration sind nicht alle Untersuchungstechnologien dauerhaft verfügbar. Des Weiteren ist es rechtlich nicht gestattet, reale Pakete und personenbezogene Daten im Rahmen eines Demonstrators zu verwenden. Die WWU hat daher zusammen mit den Partnern im Konsortium eine mögliche Lösung zur Integration aller Komponenten in einer Testumgebung unter Verwendung von Testdaten entworfen. Hierzu fanden regelmäßige Absprachen in den wöchentlichen Telefonkonferenzen und ein Workshop am 27. und 28. Oktober 2014 in Münster statt. Für die Konzeptionierung des Demonstrators wurden Ablauf und Aufbau im Konsortium gemeinsam entwickelt.

Die Demonstration am 17. März 2015 am Hauptsitz der französischen Post in Paris wurde vom deutschen Konsortium unterstützt. Da die französischen Partner den Fokus auf Technologien gelegt haben, wurde das im deutschen Konsortium entwickelte IMS zur Verfügung gestellt. Von Seiten der WWU hat Herr Carsten Böhle an einem 30-minütigen Vortrag zum deutschen Projekt mitgewirkt. Abbildung 18 zeigt einige Bilder des Demonstrator-Events in Frankreich.

Auf dem Demonstrator Event am 6. Mai 2015 in Troisdorf wurde neben Vorträgen zum Projekt und einer freien Beschau des Testaufbaus eine Live-Demonstration des Imports inklusive der Untersuchungstechnologien anhand von fiktiven Paketen geben. Für Inhalte, die nicht vor Ort gezeigt werden konnten, wie die Aufgabe und Auslieferung von Paketen, wurden vorab erstellte Videoclips genutzt. Ebenfalls zuvor produzierte Interviews mit den Organisationsleitern schilderten an verschiedenen Stellen während der Demonstration die Besonderheiten der postalischen Lieferkette. Das entwickelte Konzept wurde mit den französischen Partnern abgestimmt und auf dem gemeinsamen Konsortiumstreffen am 11. und 12. Dezember 2014 in Paris vorgestellt. Abbildung 19 zeigt einige Bilder des Demonstrator Events in Deutschland.

Abbildung 18: Bilder Demonstrator Event in Frankreich

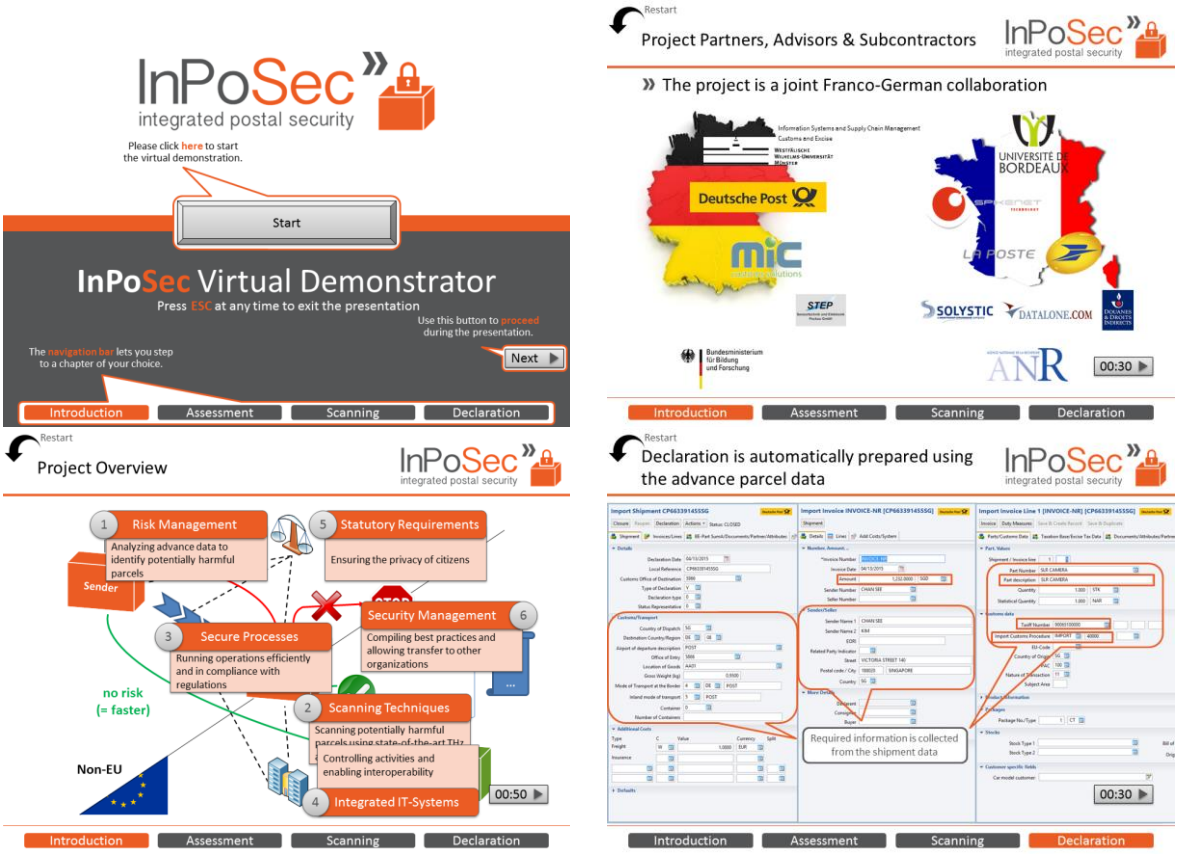
Abbildung 19: Bilder Demonstrator Event in Deutschland

2.1.7.2 UAP 8.2 Demonstration und Validierung des Gesamtkonzepts

Der Demonstrator hat alle Teilaspekte des Projekts in ein Gesamtkonzept integriert, um dieses einem breiten Publikum aus Wirtschaft, Forschung und Regierung zu präsentieren. Dabei haben alle Partner ihre Lösungen vorgestellt, um einen Gesamteindruck zu vermitteln. Die WWU war hierbei besonders bei der Organisation des physischen Testaufbaus und der Live-Demonstration beteiligt. Hierzu wurde eine einstündige Präsentation vorbereitet, welche in verschiedenen Szenarien die Ankunft von risikofreien, risikohaften und zollpflichtigen Sendungen unter Verwendung von Testpaketen schildert (siehe Abbildung 19 unten rechts). Hierdurch konnte der Lösungsansatz von InPoSec anschaulich wiedergegeben werden. Rechtliche Fragestellungen

hinsichtlich Datenschutz und Postgeheimnis wurden in den Präsentationen und Plakaten hervorgehoben.

Zusätzlich wurde ein virtueller Demonstrator entworfen und implementiert, der das Gesamtkonzept dem Anwender vorstellt (Abbildung 20 Bild 2-3) und ihm ermöglicht, selbst im Prozess zur Auswahl und Prüfung potentiell gefährlicher Sendungen aktiv zu werden. Hierzu wurde eine interaktive Präsentation erstellt, welche auf Eingaben und Entscheidungen des Anwenders reagiert. Dabei wird dem Anwender eine Reihe von zufällig gewählten Sendungen und deren Daten präsentiert, aus denen er möglichst die Sendung selektiert, die eine Gefahr enthält (Abbildung 20 Bild 4-5). Das gewählte Paket kann mit den im Projekt untersuchten Technologien virtuell gescannt werden. Die Risikoanalyse und die Technologien werden hierzu dem Anwender schnittweise erklärt, bevor ihm das Ergebnis der Überprüfung präsentiert wird (Abbildung 20 Bild 6). Der Anwender kann dabei solange andere Technologien oder Pakete wählen, bis er die Gefahr entdeckt hat, oder eine falsche Entscheidung getroffen hat. Der virtuelle Demonstrator soll so den Ablauf schildern und die Problematik der Identifikation risikoreicher Sendungen und der Auswahl der Untersuchungstechnologien verdeutlichen. Die interaktive Präsentation wurde im Rahmen des Demonstrators ausgestellt und konnte Vorort ausprobiert werden. Zusätzlich wurde den geladenen Gästen und weiteren Interessierten ein Download bereitgestellt, unter dem die Präsentation und andere Materialien im Rahmen des Demonstrators bereitgestellt wurden.



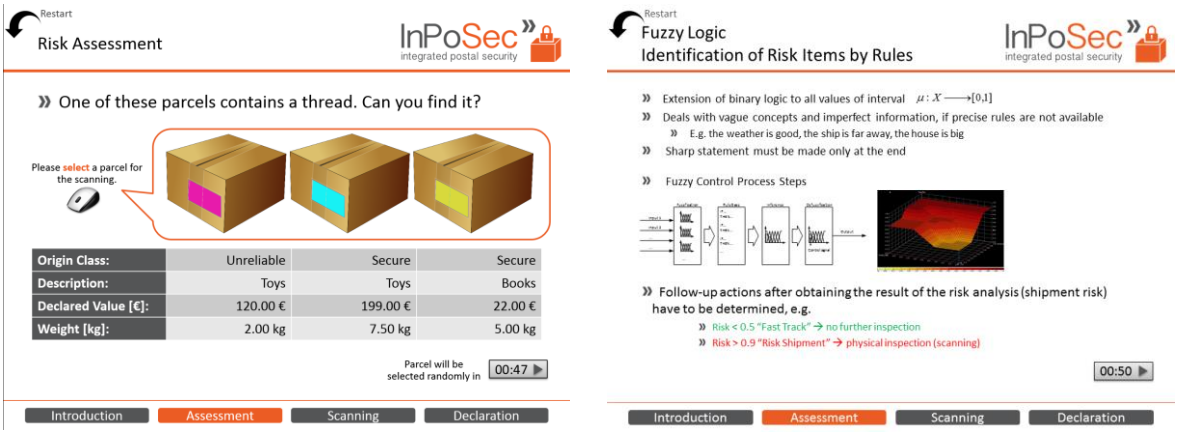


Abbildung 20: Virtueller Demonstrator Screenshots

2.1.8 AP 9 Kommunikation

2.1.8.1 UAP 9.2 Workshop

Im Rahmen der Öffentlichkeitsarbeit im Projekt wurde ein Workshop geplant, auf dem das Projekt und die erzielten Ergebnisse dem Fachpublikum (e. g. Postgesellschaften, Zollbehörden etc.) vorgestellt wurden. Dieser fand im Rahmen der 12. International Petersberg Conference des Bundesverbands Deutscher Postdienstleister (BvDP) am 25.06.2014 in Bonn statt, wo das relevante Fachpublikum aus Wirtschaft und Verwaltung angesprochen werden konnte. In diesem Workshop wurden die erarbeiteten Ergebnisse dem Publikum vorgestellt und in einer Podiumsdiskussion kritisch geprüft und diskutiert, um so weitere Erkenntnisse für die Weiterentwicklung und die Verwertung zu gewinnen.

2.1.8.2 UAP 9.3 Wissenschaftliche Veröffentlichungen und Konferenzen

Im Rahmen der 8. Future Security Konferenz des Fraunhofer-Instituts für Naturwissenschaftlich-Technische Trendanalysen INT vom 17. bis 19. September 2013 in Berlin wurde die in AP 2 entwickelte Modellierungsmethode der Secure Logistics Processes (SLP) Methodology veröffentlicht.

- Böhle, C., Hellingrath, B., Middelhoff, M., Deuter, P. (2013). Modeling and Analyzing Secure Business Processes in Logistics. Proceedings of the 8th Future Security Conference, Berlin, pp. 175-184.

Im Rahmen der 15. ASIM Fachtagung Simulation in Produktion und Logistik des Heinz Nixdorf Instituts Paderborn vom 9. bis 11. Oktober 2013 in Paderborn wurde die Konzeption des Simulationsmodells aus AP 2 basierend auf einem exemplarischen Vergleich von Screening-Technologien vorgestellt.

- Hellingrath, B.; Böhle, C.; Middelhoff M.: Simulation of a Logistics Network to Import Goods with Unknown Risk to Increase the Security in the Supply Chain. In: Proceedings of the ASIM 2013. Paderborn, 2013

Im Rahmen der 12. International Petersberg Conference des Bundesverbands Deutscher Postdienstleister (BvDP) am 25.06.2014 in Königswinter wurde vor Vertretern der Fachbranche das Projekt vorgestellt und anschließend im Rahmen einer Podiumsdiskussion diskutiert. Auch ein Vertreter des französischen Konsortiums war dafür anwesend.

Im Rahmen des Interdisciplinary Workshop on Global Security (WISG) am 22.-23.01.2013 und 30.-31.01.2014 in Troyes, Frankreich, wurde das Projekt gemeinsam mit den französischen Partnern durch ein Poster vorgestellt.

2.2 Die wichtigsten Positionen des zahlenmäßigen Nachweises

- Personalkosten
  - Wissenschaftliche Mitarbeiter: 531.334,61 €
  - Studentische Hilfskräfte: 35.463,50 €
- Reisekosten: 22.013,42 €
- Geräte: 14.591,45 €
- Unteraufträge: - €

2.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Der Verlauf der Arbeit im Projekt folgte der im Projektantrag formulierten Planung. Alle im Arbeitsplan formulierten Aufgaben wurden erfolgreich bearbeitet, es waren keine zusätzlichen Ressourcen für das Projekt nötig.

2.4 Darstellung des voraussichtlichen Nutzens

Wirtschaftliche Erfolgsaussichten

Die Westfälische Wilhelms-Universität verfolgt als Projektpartner primär wissenschaftliche Ziele.

Wissenschaftliche und/oder technische Erfolgsaussichten

Die gewonnenen wissenschaftlichen Erkenntnisse wurden zielgruppengerecht aufbereitet und allen Interessierten sowie als wichtig erachteten Personen und Institutionen zugänglich gemacht. Hierzu wurden Vorträge auf wissenschaftlichen Konferenzen gehalten und Publikationen erstellt. Zur Ansprache eines eher wirtschaftlichen Adressatenkreises wurde ein Workshop auf der 12. International Petersberg Conference des Bundesverbands Deutscher Postdienstleister (BvDP) am 25.06.2014 in Königswinter veranstaltet und es hat ein Treffen mit Microsoft am 07.10.2014 in Köln zur Vorstellung der entwickelten Modellierungs- und Evaluationsplattform gegeben. Studenten konnten von dem Projekt profitieren indem sie mittels Seminaren, Projektseminaren und Abschlussarbeiten eingebunden wurden und somit frühzeitig die angewandte Forschung kennen lernten und die Chance bekamen, sich selbst mit Ideen einzubringen, was wiederum der Förderung des wissenschaftlichen Nachwuchses dient. Auch die Anfertigung von Dissertationsschriften durch die am Projekt beteiligten wissenschaftlichen Mitarbeiter wurde verfolgt und im Anschluss an das Projekt fortgesetzt.

Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

Aus wissenschaftlicher Sicht ist neben den erzielten Ergebnissen die langfristige Perspektive interessant. Dies erklärt sich dadurch, dass viele der Innovationen nicht kurzfristig evaluiert werden können, wie etwa die Auswirkungen des Sicherheitsmanagementkonzepts oder rechtliche Änderungen. Daher kann die wissenschaftliche Betrachtung des Themas nicht mit der Projekt-laufzeit enden und muss über einen längeren Zeitraum fortgesetzt werden. Unter anderem

beschäftigen sich mehrere Dissertationsarbeiten mit logistischen und rechtlichen Fragestellungen über das Projekt hinaus. Dabei ist besonders die Übertragung der Erkenntnisse in andere Bereiche relevant. Darüber hinaus ist Sicherheit ein Thema in der gesamten globalen Lieferkette, z.B. auch im Containerverkehr, der Luftfracht und europaweiten Straßentransporten. Bei der Entwicklung der im Projekt entworfenen Plattform wurde auf eine möglichst generalisierbare Umsetzung geachtet, um diesen Transfer sowohl zwischen Postgesellschaften als auch auf weitere vergleichbare Anwendungsbereiche zu unterstützen. Die erarbeiteten Modellierungssprachen und -methoden sowie Verfahren zur Evaluation und die entsprechenden Tools wurden ebenfalls vor dem Hintergrund der Generalisierbarkeit auf vergleichbare Problemdomänen entworfen. Über den Kontakt zum EU-Projekt SAFEPOST wurde in mehreren Treffen die Möglichkeit einer Kooperation in einem Folgeprojekt diskutiert. SAFEPOST endet planmäßig 2016 und sowohl bei der WWU als auch bei SAFEPOST besteht Interesse gemeinsam in einem Folgeprojekt die Ergebnisse weiter zu entwickeln.

Die enge Kooperation mit den beteiligten Postunternehmen sichert die Umsetzung der im Arbeitspaket 6 entwickelten rechtlichen Ergebnisse. Damit bilden die Ergebnisse die unverzichtbare Grundlage für die Entwicklung und die wirtschaftliche Verwertbarkeit der von den anderen Projektpartnern erbrachten logistischen und technischen Lösungen.

2.5 Fortschritte auf dem Gebiet des Vorhabens bei anderen Stellen

Im Zuge der Arbeiten wurden kontinuierlich bekannte Projekte im thematischen Umfeld des Vorhabens beobachtet, um wichtige Erkenntnisse Dritter aufgreifen zu können. Zudem wurden regelmäßig Internet-Recherchen zum Thema des Vorhabens durchgeführt, um über Neuerungen informiert zu sein.

Auf Einladung des SAFEPOST-Konsortiums hat eine Delegation des InPoSec-Projekts am SAFEPOST Postal Security Forum am 28. und 29.11.2013 in Vilnius teilgenommen. SAFEPOST ist ein im FP7 gefördertes europäisches Projekt, das sich ebenfalls mit der Gestaltung sicherer postalischer Lieferketten beschäftigt. Daher existieren Überschneidungen in den Zielen beider Projekte. Aus den durch SAFEPOST präsentierten Inhalten konnten jedoch keine Erkenntnisse identifiziert werden, die für das InPoSec-Projekt nutzbar waren und in der weiteren Planung hätten berücksichtigt werden müssen. Die präsentierten Inhalte aus InPoSec wurden mit großem Interesse seitens SAFEPOST aufgenommen. Die Projekte unterscheiden sich in Ihrer Arbeitsweise in Hinblick auf die von InPoSec vollzogene integrierte Betrachtung der Prozesse und der rechtlichen Rahmenbedingungen im Sinne des Privacy-by-Design.

2.6 Erfolgte oder geplante Veröffentlichungen der Ergebnisse

- Siehe auch vergangene Zwischenberichte
- Im Rahmen der 8. Future Security Konferenz des Fraunhofer-Instituts für Naturwissenschaftlich-Technische Trendanalysen INT vom 17. bis 19. September 2013 in Berlin wurde die in AP 2 entwickelte Modellierungsmethode der Secure Logistics Processes (SLP) Methodology veröffentlicht.
    - Böhle, C., Hellingrath, B., Middelhoff, M., Deuter, P. (2013): Modeling and Analyzing Secure Business Processes in Logistics. In: Proceedings of the 8th Future Security Conference, Berlin, pp. 175-184.

- Im Rahmen der 15. ASIM Fachtagung Simulation in Produktion und Logistik des Heinz Nixdorf Instituts Paderborn vom 9. bis 11. Oktober 2013 in Paderborn wurde die Konzeption des Simulationsmodells aus AP 2 basierend auf einem exemplarischen Vergleich von Screening-Technologien vorgestellt.
    - Hellingrath, B., Böhle, C., Middelhoff, M. (2013): Simulation of a Logistics Network to Import Goods with Unknown Risk to Increase the Security in the Supply Chain. In: Proceedings of the ASIM 2013. Paderborn.
- Im Rahmen der 8. Multikonferenz Wirtschaftsinformatik vom 26. bis 28. Februar 2014 in Paderborn wurde eine Erweiterung der Modellierungsmethode der Secure Logistics Processes (SLP) Methodology für informatorische Sicherheit veröffentlicht.
    - Middelhoff, M., Böhle, C., Hellingrath, B. (2014): Modeling and Analyzing Information Security in Secure Logistics Business Processes. In: Kundisch, D., Suhl, L., & Beckmann, L. (Eds.), Tagungsband Multikonferenz Wirtschaftsinformatik, Paderborn, pp. 1924-1936.
- Am 22. Oktober 2013 wurde das InPoSec Projekt bei PostEurop präsentiert.
- Am 5. November 2013 wurde das InPoSec Projekt der Bundesfinanzdirektion Nord präsentiert.
- Am 28. November 2013 wurde das InPoSec Projekt bei SAFEPOST präsentiert.
- Im Rahmen des Interdisciplinary Workshop on Global Security (WISG) am 22.-23.01.2013 in Troyes, Frankreich, wurde das Projekt gemeinsam mit den französischen Partnern durch ein Poster vorgestellt.
- Im Rahmen des Interdisciplinary Workshop on Global Security (WISG) am 30.-31.01.2014 in Troyes, Frankreich, wurde das Projekt gemeinsam mit den französischen Partnern durch ein Poster vorgestellt.
- Im Rahmen der 12. International Petersberg Conference des Bundesverbands Deutscher Postdienstleister (BvDP) am 25.06.2014 in Königswinter wurde vor Vertretern der Fachbranche das Projekt vorgestellt und anschließend im Rahmen einer Podiumsdiskussion diskutiert. Auch ein Vertreter des französischen Konsortiums war dafür anwesend.
- Am 7. Oktober 2014 wurden Teile des InPoSec Projekts (v.a. die Modellierungs- und Evaluationsplattform) Microsoft in Köln vorgestellt.
- Vom 19.-20. Jänner 2015 nahmen Vertreter des InPoSec Projekts an der ITOM Konferenz in Rotterdam teil und präsentierten die bisherigen Ergebnisse des Projekts.
- Am 27. Mai 2015 wurde das InPoSec Projekt bei einem Treffen des EU-Projekts DOGGIES präsentiert.
- Die Endergebnisse wurden außerdem bei den beiden Abschlussveranstaltungen präsentiert:
    - 17. März 2015 Französischer Demonstrator in Paris
    - 6. Mai 2015 Deutscher Demonstrator in Troisdorf/Bonn
- „Safety First“ in: Postal Technology International, September 2015

3 Referenzen

Becker J, Kugeler M, Rosemann M (Hrsg.): Prozessmanagement. Ein Leitfaden Zur Prozessorientierten Organisationsgestaltung. Springer Verlag, 2008.

Dieke, A. K., Junk, P., & Zauner, M. (2010). Netzzugang und Zustellwettbewerb im Briefmarkt. Bad Honnef.

Europäische Kommission: Authorised Economic Operator (AEO). http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/aeo/index_en.htm. Letzter Zugriff: 15.03.2012, 2006.

Hempsch, C. K. (2010). Optimierung postalischer Vorlaufnetzwerke. RWTH Aachen.

Hermann, P. and Hermann, G. (2006). Security Requirement Analysis of Business Processes. Electronic Commerce Research 6(3-4), pp. 305-335.

Jakoubi, S., Tjoa, S., Goluch, G. and Quirchmayr, G. (2009). A Survey of Scientific Approaches Considering the Integration of Security and Risk Aspects into Business Process Management. Proceedings of the 20th International Workshop on Database and Expert Systems Application, pp. 127-132.

Nüttgens, Markus; Rump Frank J.: Syntax und Semantik Ereignisgesteuerter Pro-zessketten (EPK). In: Desel J (ed) Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen – Promise, Bonn, 2002.

OMG (2011). Business Process Model and Notation (BPMN) – Version 2.0. http://www.omg.org/spec/BPMN/2.0/

Srivatanakul, T., Clark, J. A. and Polack, F. (2004). Effective Security Requirements Analysis: HAZOP and Use Cases. Information Security: 7th International Conference, Lecture Notes in Computer Science Vol. 3225. Palo Alto, CA: Springer, pp. 416-427.

Transported Asset Protection Association TAPA EMEA Transported Asset Protection Association. www.tapaemea.com. Accessed 15.03.2012, 2012.

United States Customs and Border Protection C-TPAT Overview. http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_overview.xml, Letzter Zugriff: 15.03.2012, 2007.

Van der Lijn, N., Meijer, A., Bas, P. de, Volkerink, B., & Kok, H. (2005). Development of competition in the European postal sector. Rotterdam.

Walsh, Tim: The European Mail Manifesto.

White, Steven A.: Introduction to BPMN. In: BPTrends, S. 1–11, 2004.