Schlussbericht zu Nr. 8.2

ZE: FIS Flug- und Industriesicherheit Service- und Beratungs-GmbH	Förderkennzeichen: 13N10406

Vorhabenbezeichnung: Elektromagnetischer Schutz für Verkehrsinfrastrukturen – (EMSIN)

Teilvorhaben: Anforderungsanalyse und grundlegende Untersuchung der Einsatzmöglichkeiten von Schutzsystemen

Laufzeit des Vorhabens: 01.04.2010 – 31.03.2013

Projektleitung:

Dipl.-Kfm. Benjamin Cimander

Innovationsmanagement

Flug- und Industriesicherheit Service- und Beratungs- GmbH

Langer Kornweg 19

65451 Kelsterbach

Telefon: 06107 - 308 6 - 36

Fax: 06107 - 308 6 - 99

E-Mail: b.cimander@fisgmbh.de

I. Kurze Darstellung zu

1. **Aufgabenstellung**
2. **Voraussetzungen, unter denen das Vorhaben durchgeführt wurde,**
3. **Planung und Ablauf des Vorhabens,**
4. **wissenschaftlichem und technischem Stand, an den angeknüpft wurde, insbesondere**
    - **Angabe bekannter Konstruktionen, Verfahren und Schutzrechte, die für die Durchführung des Vorhabens benutzt wurden,**
    - **Angabe der verwendeten Fachliteratur sowie der benutzten Informations- und Dokumentationsdienste,**
5. **Zusammenarbeit mit anderen Stellen**

II. Eingehende Darstellung

1. **der Verwendung der Zuwendung und des erzielten Ergebnisses im Einzelnen, mit Gegenüberstellung der vorgegebenen Ziele,**
2. **der wichtigsten Positionen des zahlenmäßigen Nachweises,**
3. **der Notwendigkeit und Angemessenheit der geleisteten Arbeit,**
4. **des voraussichtlichen Nutzens, insbesondere der Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplans,**
5. **des während der Durchführung des Vorhabens dem ZE bekannt gewordenen Fortschritts auf dem Gebiet des Vorhabens bei anderen Stellen,**
6. **der erfolgten oder geplanten Veröffentlichungen des Ergebnisses nach Nr. 11**

I.1 Kurze Darstellung zur Aufgabenstellung

Das Gesamtziel des Verbundvorhabens EMSIN war der technische und organisatorische Schutz von kritischen Verkehrsinfrastrukturen vor Störungen und Zerstörungen durch bewusst erzeugte elektromagnetische Felder. Diese elektromagnetischen Felder können eine Funktionsstörung, einen Ausfall oder die Zerstörung einzelner Systemelemente einer IT-Infrastruktur bewirken und damit zu erheblichen Störungen des Betriebablaufes oder auch zu katastrophalen Unfällen führen. Vor Beginn des Projektes gab es für die Detektion eines HPM-Angriffs keine technischen Möglichkeiten. Es würden im Ernstfall nur die Auswirkungen bemerkt werden, z.B. ein defekter Computer, aber die Ursachen hierfür wären nicht erkennbar.

Das Projekt EMSIN untersuchte die Verwundbarkeit eines Flughafens gegenüber böswillig herbeigeführten elektromagnetischen Gefährdungen. Unter aktiver Beteiligung von unterschiedlichen öffentlichen und privaten Forschungsstellen und Anwendern sollte ein integrierter Ansatz, bestehend aus technologischen und organisatorischen Maßnahmen, entwickelt werden, um die Leistung und Funktion kritischer Infrastruktureinrichtungen der Luftfahrt (Flughäfen, Flugleitung etc.) im Falle elektromagnetischer Angriffe und Anschläge zu gewährleisten. Insbesondere sollte ein Sensor zur unmittelbaren Detektion, Analyse und Ortung von Angriffen mit elektromagnetischen Impulsen erarbeitet werden, der durch Erkennen von abweichendem Normverhalten im Rahmen der ortsüblichen elektromagnetischen Ausstrahlungen eine zeitnahe Detektion einer Bedrohung und Empfehlungen von Sofortmaßnahmen nach einem elektromagnetischen Angriff ermöglicht.

Moderne Kommunikationstechnologien und IT-Infrastrukturen sind notwendige Voraussetzungen für die sichere und reibungslose Abwicklung des Betriebes einer kritischen Infrastruktur. Schnelle Informationsübermittlung, durchgängiger Zugriff auf Datenbanken sowie die Leitung des Verkehrsablaufes mit Hilfe vernetzter IT-Systeme (IT-Netze) sind für den effektiven und sicheren Betriebsablauf entscheidend. Daher sollten im Rahmen des Projektes Wirkungsmechanismen und Schädigungen modelliert, analysiert sowie geeignete Schutzkonzepte entwickelt werden. Elektronische Komponenten für den Systemschutz sowie Detektoren zur Identifizierung von Angriffen sollten untersucht werden.

Besonderes Augenmerk sollte dabei auf der späteren wirtschaftlichen Verwertung der Ergebnisse in heimischen Märkten und im Export liegen. Aufbauend auf den in der wissenschaftlichen Literatur veröffentlichten Ergebnissen von Untersuchungen an einzelnen Komponenten und Baugruppen sollte die Verwundbarkeit moderner elektrischer Schaltkreise und IT-Netze gegenüber elektromagnetischen Feldern hoher Leistung experimentell und theoretisch untersucht werden.

In einem zweiten Arbeitsschritt sollte eine Analysemethode erarbeitet werden, die es ermöglicht, die elektromagnetische Gefährdung in einer kritischen Infrastruktur unter Einbeziehung aller Randbedingungen zu analysieren. Hierzu war es notwendig, sowohl die beobachteten Wirkungsmechanismen, als auch die Ausbreitung der Wirkungen und Schädigungen in geeigneter Weise zu erfassen.

Basierend auf den gewonnenen Erkenntnissen sollten Konzepte für den Schutz kritischer Infrastrukturen vor elektromagnetischen Bedrohungen erarbeitet werden. Diese Schutzkonzepte sollten von vornherein die technischen Mittel (Designrichtlinien, Schutzelemente, Schirmung, Detektion etc.) mit den organisatorischen Erfordernissen der Prozessabläufe (Monitoring, Zugangsbeschränkungen, etc.) so integrieren, dass sie in ihrer Gesamtheit zur Prävention, Abwehr und Bewältigung elektromagnetischer Stör- und Schadwirkungen geeignet sind.

Auf der Grundlage des Wissens über die elektromagnetische Bedrohung und der erarbeiteten Konzepte zum Schutz kritischer Infrastrukturen sollte ein Sensornetzwerk aufgebaut werden. Das Sensornetzwerk sollte der Detektion und der Lokalisierung der Gefahrenquelle, ebenso wie der Einleitung einer schnellen und effektiven Reaktion im Fall einer elektromagnetischen Stör- und Schadwirkung, dienen. Die Untersuchung und anschließende Modellierung der elektronischen Infrastruktur sollte anhand einer in Betrieb befindlichen Anlage (deutscher und/oder israelischer Flughafen) erfolgen und der Identifikation von Schwachstellen in den bestehenden Sicherheitssystemen dienen. Neben dem Aufbau eines Testnetzwerkes sollten Empfehlungen zur strukturellen Auslegung von Netzwerken basierend auf Simulationsergebnissen und Messungen am Testnetzwerk geliefert werden.

Mit dem Sensorsystem sollte erstmalig ein Mittel konzipiert werden, um einen elektromagnetischen Angriff zu entdecken. Mit der Entdeckung des Angriffs sollte das Sensorsystem eine Lokalisierung des Wirkmittels durchführen. Nach der Ermittlung und Meldung der Position könnten Folgemaßnahmen eingeleitet werden. Die Erarbeitung dieser Maßnahmen war ebenfalls Teil des Vorhabens EMSIN. Außerdem sollten Strategien und Lösungsansätze für die Risikobewertung und Gefahrenabwehr ausgearbeitet und die Lösungsansätze auf gesellschaftliche Akzeptanz sowie rechtliche Umsetzbarkeit geprüft werden.

Die Verwertung der Ergebnisse des Projektes EMSIN sollte hauptsächlich in zwei Teile gegliedert werden. Auf der einen Seite sollte soweit möglich das entstandene Wissen als Dienstleistung und Consulting vermarktet werden und auf der anderen Seite sollte der konzipierte Sensor nach Vorhabensabschluss als Produkt weiterentwickelt und auf den Markt gebracht werden.

Das Anliegen des Bereichs Dienstleistung und Consulting war es, die durch das vermehrte Auftreten elektromagnetischer Wirksysteme notwendig gewordene Härtung und den Schutz sensibler Kommunikations- und IT-Netze sowie elektronischer Schaltkreise und Steuerungen vor HPM-Angriffen voranzutreiben und sicherzustellen. Diese Angriffe sind in den letzten Jahren zur Bedrohung geworden, da die Bauanleitungen für HPM-Wirkmittel im Internet verfügbar sind und von Personen mit technischem Grundverständnis genutzt werden können.

Sowohl die zunehmende Verbreitung und Verfügbarkeit geeigneter elektromagnetischer Waffen (HPEM-Quellen), als auch die beobachtbare Abnahme der Störfestigkeit marktgängiger elektrischer Schaltkreise und Infrastrukturen gegenüber Mikrowellenfeldern charakterisieren die wesentlichen technischen Herausforderungen, die die Entwicklung des Sensors begleiten.

Der Sensor sollte für die Detektion, die Lokalisierung und die effektive Reaktion bei einem elektromagnetischen Angriff erarbeitet werden. Auf der israelischen Seite sollte die Firma Netline die Hardware und die Kontroll- und Managementsoftware des Überwachungssensors bearbeiten. Die deutschen Partner haben Kenntnisse über die HPM-Wirkmittel und Ortungsmethoden. Die Zusammenarbeit beider Seiten sollte es ermöglichen ein Ortungssystem für die HPM-Wirkmittel zu konzipieren.

Die Reaktion von IT-Systemen auf die Einkopplung elektromagnetischer Störgrößen besteht in Fehlfunktionen wie der fehlerhaften Verarbeitung von Daten und dem Ausfall von Komponenten. Die Erwartungen des Nutzers an die Zuverlässigkeit, Bedienbarkeit und Verfügbarkeit des Sensorsystems sowie dessen Einbindung in das Gesamtsystem Luftverkehr stellen sowohl Herausforderungen an die Qualität des Schutzes als auch die Randbedingungen bezüglich technischer und organisatorischer Begrenzungen.

Der Hauptzweck des zu erarbeitendem Sensorsystems ist das Detektieren und Orten elektromagnetischer Störungen, die durch terroristische Aktivitäten hervorgerufen werden. Des Weiteren werden durch die Entwicklung besonderer technischer und organisatorischer Konzepte die Weiterführung des regulären Betriebs sowie die Minimierung der Folgeschäden abgesichert. Im besten Fall sind Folgeschäden rein wirtschaftlicher Natur, aber die Wahrscheinlichkeit ist hoch, dass sich der Ausfall der technischen Systeme auch in Personenschäden auswirken kann.

Bisher unterliegt der Besitz jedweder Geräte, die in der Lage sind elektromagnetische Störungen zu verursachen, keiner strafrechtlichen Verfolgung. Wenn man die Konsequenzen, die beabsichtigte elektromagnetische Störungen mit sich bringen in Betracht zieht, erscheint eine Neubewertung des rechtlichen Hintergrundes im Rahmen des Projektes zwingend. Die Untersuchungen hinsichtlich des Besitzes einer HPM-Störquelle sollten im Laufe des Projektes auf rechtliche Fragestellungen, die mit dem Gebrauch dieser Geräte zusammenhängen, ausgeweitet werden.

Bisher ist das Aussenden elektromagnetischer Interferenzen nur ein Verstoß gegen EMV-Vorschriften und gegen das Telekommunikationsgesetz. Der Angriff auf Infrastrukturen mit elektromagnetischen Feldern ist deshalb mit dem illegalen Betrieb eines Senders gleichgestellt. Und selbst dies greift nur, wenn vorgeschriebene Grenzwerte übertreten werden. Es ist sehr gut möglich, dass Interferenzen von HPM-Störquellen diese Grenzwerte nicht überschreiten und deshalb der Betrieb eines solchen Gerätes nicht strafrechtlich verfolgt werden kann. Möglichkeiten, diese Situation zu ändern, sollten in diesem Zusammenhang erörtert werden.

Schließlich sollte untersucht werden, welche Möglichkeiten für den Betreiber einer kritischen Infrastruktur bestehen, Maßnahmen gegen einen Angreifer zu ergreifen, nachdem ein elektromagnetischer Angriff entdeckt wurde. Es sollte diskutiert werden, ob weitergehende Möglichkeiten über das Hausrecht hinaus eingeführt werden sollen. Des Weiteren ist für den Betreiber der Infrastruktur die Frage, ob eine Höhere-Gewalt-Klausel angewandt werden kann, wenn ein elektromagnetisches Feld entdeckt wurde, von Interesse. In diesem Zusammenhang sollten auch Haftungsfragen diskutiert werden.

Das Gesamtziel des Teilprojekts „Anforderungsanalyse und grundlegende Untersuchung der Einsatzmöglichkeiten von Schutzsystemen“ war die endanwenderseitige Unterstützung der technischen Arbeiten zum Aufbau eines Sensorsystems zum Schutz der Netzwerke von Flughäfen und anderen kritischen Infrastrukturen vor elektromagnetischen Angriffen sowie die Erstellung von Konzepten zur Anwendung des Systems, insbesondere im Bereich Prävention, Abwehr und Bewältigung von Stör- und Schadwirkungen.

Grundlage für die Erarbeitung eines Systems zum Schutz vor elektromagnetischen Angriffen war die Analyse des aktuellen Baustandes elektronischer Infrastruktur am Beispiel Flughafen sowie die Erfassung der dort verfügbaren Sicherheitssysteme. Im weiteren Projektverlauf sollten Empfehlungen zur strukturellen Auslegung von Netzwerken erarbeitet werden und im Rahmen der Verifikation des fertigen Systems für den Praxiseinsatz die Benutzerschnittstelle validiert werden. Anschließend sollten die rechtlichen Grundlagen, die für das zu erarbeitende Schutzsystem relevant sind, begutachtet werden.

Das Gesamtziel des Teilprojekts gliederte sich in die folgenden Arbeitspakete:

- Analyse der Gefährdung
- Verfahren zur Analyse der Gefährdung und der Schadensausbreitung
- Empfehlungen zur strukturellen Auslegung von Netzwerken (technische Schutzkonzepte)
- Kontroll- und Management-Software für das Spektrumüberwachungssensornetz
- Bewertung anwenderrelevanter Fragestellungen inklusive Zuständigkeiten und rechtlicher Rahmenbedingungen

Die Verwertung der Ergebnisse des Projektes EMSIN sollte durch die Vermarktung des entstandenen Wissens als Dienstleistung und Consulting sowie dadurch erfolgen, dass der Sensor gemeinsam mit den Partnern zum Produkt weiterentwickelt und auf den Markt gebracht wird.

Ein wichtiges Umsetzungsziel seitens der FIS sollte das Angebot von entsprechenden Konzepten und deren Realisierung zum Schutz der Infrastrukturen sein. Der Sensor sollte für die Detektion, die Lokalisierung und die effektive Reaktion bei einem elektromagnetischen Angriff zum Einsatz gebracht werden. Die Umsetzung der Ergebnisse sollte überwiegend in Deutschland erfolgen, die Kunden sollten nach Möglichkeit international aufgestellt sein.

I.2 Kurze Darstellung zu den Voraussetzungen, unter denen das Vorhaben durchgeführt wurde,

Dem Verbundvorhaben lagen Szenarien asymmetrischer Bedrohungspotenziale auf Basis elektromagnetischer Wirkmittel (HPEM-Quellen) zugrunde, die sich gewollt und geplant (Anschlag, Sabotage, kriminelle Handlung) auf elektronische Bestandteile kritischer Verkehrsinfrastrukturen auswirken. Darüber hinaus werden auch beabsichtigte und unbeabsichtigte elektromagnetische Störungen bei den Szenarien mitberücksichtigt und untersucht.

HPEM-Waffen können mit einfachen Mitteln hergestellt und in Einsatz gebracht werden. Sie durchdringen physikalische Barrieren wie Zäune oder Wände. Man kann deshalb in Zukunft von einem vermehrten Einsatz ausgehen. Eine „normale“ EMV-Einwirkung wird in der Mehrzahl aller Fälle zu Funktionsstörungen und nicht zur kompletten Zerstörung von elektronischen Komponenten und Geräten führen.

Im Fall von HPM kann es aufgrund bedeutend höherer elektrischer und magnetischer Feldstärken beziehungsweise Strömen und Spannungen zu Zerstörungen elektronischer Geräte und Anlagen, zumindest aber zu irreversiblen Veränderungen von Bauteileparametern, kommen. Auf diese Weise könnten zum Beispiel die Elektronik von Computern, Kraftfahrzeugen, Flugzeugen und Kontrollzentren von Infrastrukturen usw. angegriffen werden. Dabei können einzelne elektrische oder elektronische Baugruppen, Schaltkreise sowie vernetzte und nicht vernetzte elektrische und elektronische Systeme einschließlich IT- und Kommunikationsnetzen betroffen sein. HPEM-Angriffe könnten unter Umständen bis zum Zusammenbruch übergeordneter Netze, wie dem Luftverkehr oder sogar intermodal gekoppelter Verkehre (Luft, Wasser, Land) führen.

HPM-Angriffe hinterlassen üblicherweise keine bleibenden Beweise und die Auswirkungen können sich von ärgerlich bis katastrophal bewegen. Verbrecher und Terroristen können HPM als wirksame Antielektronikwaffen benutzen, um die Elektronik von Computern, Kraftfahrzeugen, Flugzeugen und Kontrollzentren von Infrastrukturen usw. erfolgreich anzugreifen. HPM-Waffen sind in der Lage, diese elektronischen Systeme in einem nicht zu erkennenden Angriff zu beschädigen mit all ihren gefährlichen direkten Auswirkungen und Folgeschäden. Momentan gibt es keine technischen und organisatorischen Möglichkeiten, die Störquelle zu identifizieren und den Täter mithilfe eines geeigneten Krisenreaktionsplans dingfest zu machen.

Daher sollte im Rahmen dieses Projektes die Verwundbarkeit moderner elektrischer Schaltkreise und IT-Netze gegenüber elektromagnetischen Feldern hoher Leistung experimentell und theoretisch untersucht werden. Des Weiteren sollte eine Analysemethode erarbeitet werden, die die elektromagnetische Gefährdung in einer kritischen Infrastruktur unter Einbeziehung aller Randbedingungen analysiert. Basierend auf den gewonnenen Erkenntnissen sollten Konzepte für den Schutz kritischer Infrastrukturen vor elektromagnetischen Bedrohungen erarbeitet werden sowie ein Sensornetzwerk zur Detektion und Lokalisierung der Gefahrenquelle aufgebaut werden.

Mit Hilfe des Sensornetzwerkes sollte es möglich sein, sowohl die Gefahrenquelle zeitnah zu detektieren, als auch Sofortmaßnahmen einzuleiten, die zur Ergreifung des Täters führen können. Somit ergibt sich erstmals die Möglichkeit, in diesem Bereich einen entscheidenden Beitrag zur zivilen Sicherheit zu leisten, da es zukünftig nicht mehr möglich sein wird, unerkannt und unbestraft Angriffe mit HPM-Waffen durchzuführen. Zu diesem Zweck sollten im Rahmen dieses Projektes elektromagnetische Bedrohungen durch High power microwave (HPM) sowie durch beabsichtigte und unbeabsichtigte elektromagnetische Störungen untersucht werden.

Zunehmende Aufmerksamkeit ist den sogenannten HPM-Quellen (HPM-Waffen) zu widmen (HPM: High Power Microwave, oder HPEM: High Power Electromagnetics), deren Bedeutung und Entwicklung relativ jung sind, wie die einschlägigen Veröffentlichungen belegen. Es handelt sich hierbei um leistungsstarke elektromagnetische Strahlung emittierende Quellen, die über eine eingeschränkte Reichweite verfügen und ein definiert begrenztes Gebiet betreffen können. Gemäß dem 3. Gefahrenbericht der Schutzkommission beim Bundesminister des Innern geht von den HPEM-Quellen eine zunehmende Gefährdung elektronischer Systeme für zivile Einrichtungen aus. Es wird in diesem Zusammenhang bereits von „Elektromagnetischem Terrorismus“ gesprochen, der zu einer Gefährdung der öffentlichen Ordnung führen kann. Die Schutzkommission beim BMI weist deshalb ausdrücklich daraufhin, dass zurzeit ein Schutz gegen HPEM-Angriffe generell noch nicht existiere.

High Power Microwave-Waffen können relativ einfach und ohne aufwendige Kosten von Zivilpersonen aus handelsüblichen Komponenten gefertigt und zu Sabotage- oder Erpressungszwecken eingesetzt werden. Der Angriff erfolgt nach der Aktivierung des HPM-Wirkmittels. Die durch den Angriff freigesetzte elektromagnetische Welle mit der darin enthaltenen Energie breitet sich aus, durchdringt die Wände und erreicht die elektronischen Geräte beispielsweise Computer und Netzwerkkomponenten. Je nach Entfernung des HPM-Wirkmittels zu den elektronischen Geräten, des Aufbaus des Wirkmittels und der Beschaffenheit der Wände wird der Effekt von nicht wahrnehmbar bis zu einem Funktionsausfall des Gerätes führen. Eine weitere Möglichkeit ist der leitungsgebundene Angriff. Das Wirkmittel wird hierbei zum Beispiel an eine vorhandene Steckdose angeschlossen und ausgelöst. Die freigewordene Energie breitet sich über die Netzleitungen aus und kann so ihre zerstörende Wirkung entfalten. HPM-Wirkmittel können in der Nähe einer IT- Infrastruktur ausgelöst werden. Das Szenario für einen Angriff kann auch für Rechenzentren, Energieunternehmen und Finanzsysteme angewendet werden. Bei unserem israelischen Partner ist die Detektion und Lokalisierung von beabsichtigten und unbeabsichtigten elektromagnetischen Störungen ein weiterer Schwerpunkt. Das Sensorsystem wird hier ebenso für die Detektion, die Lokalisierung und die effektive Reaktion bei einer elektromagnetischen Störung konzipiert.

Mit Hilfe des zu entwickelnden Sensornetzwerkes sollte es möglich sein, sowohl die Gefahrenquelle zeitnah zu detektieren, als auch Sofortmaßnahmen einzuleiten, die zur Ergreifung des Täters führen können. Somit ergibt sich erstmals die Möglichkeit, in diesem Bereich einen entscheidenden Beitrag zur zivilen Sicherheit zu leisten, da es zukünftig nicht mehr möglich sein wird, unerkannt und unbestraft Angriffe mit HPM-Waffen durchzuführen.

I.3 Kurze Darstellung zu Planung und Ablauf des Vorhabens

Für eine erfolgreiche Projektdurchführung war eine enge Zusammenarbeit innerhalb des Verbundes unerlässlich. Der Verbund bestand auf der deutschen Seite aus drei Forschungseinrichtungen:

- Gottfried Wilhelm Leibniz Universität Hannover (LUH),
- Fachhochschule Hannover (FHH) sowie dem
- Wehrwissenschaftlichen Institut für Schutztechnologien (WIS).

und zwei Unternehmen:

- Thales (THA) und
- Flug- und Industriesicherheit Service- und Beratungs- GmbH (FIS).

Im Unterauftrag bei der Leibniz Universität Hannover erfolgte die rechtliche Begleitforschung durch Frau Dr. Aigner-Hof.

Des Weiteren war ein Unternehmen aus Israel am Projekt beteiligt:

- Netline Communications Technologies Ltd. (NCT)

Die Zusammenarbeit erfolgte im Rahmen von insgesamt neun Arbeitspaketen:

- Analyse der Gefährdung
- Testnetzwerk
- Verfahren zur Analyse der Gefährdung und der Schadenausbreitung
- Empfehlungen zur strukturellen Auslegung von Netzwerken
- Spektrumüberwachungssensornetz
- Kontroll- / Managementsoftware für das Spektrumüberwachungssensornetz
- TDOA-basierte Ortung der Bedrohung
- Technische Schutzelemente
- Bewertung anwenderrelevanter Fragestellungen inklusive Zuständigkeiten und rechtlicher Rahmenbedingungen

Die Arbeitspakete waren in diverse Unterarbeitspakete unterteilt und wurden in enger Zusammenarbeit der beteiligten Partner bearbeitet.

Zur Optimierung der Zusammenarbeit der Verbundpartner dienten regelmäßige Projekttreffen. Zu den Treffen waren auch die Mitglieder des Projektbeirates eingeladen. Die Treffen dienten der Zusammenführung sämtlicher Ergebnisse und der Bewertung der gewonnenen Daten und Erkenntnisse durch die Experten aus der Praxis.

Die Arbeitsteilung der Projektpartner sowie ihre Zusammenarbeit sind in der folgenden Übersicht dargestellt:

Workpackage		Partner	2010				2011				2012				
No	Name		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
1	**Analyse der Gefährdung**	**LUH**													
1.1	Auswertung der technischen Fachliteratur	FHH													
1.2	Analyse des aktuellen Baustandes elektronischer Infrastruktur														
1.2.1	Bestandaufnahme an Flughäfen	FIS													
1.2.2	Identifikation kritischer Baugruppen und Messung ihrer Störfestigkeit	LUH													
1.3	Analyse der elektromagnetischen Gefährdung														
1.3.1	Analyse der charakteristischen elektromagnetischen Umgebung	FHH													
1.3.2	Definition möglicher Störer	WIS													
1.4	Erfassung verfügbarer Sicherheitssysteme	FIS													
2	**Testnetzwerk**	**WIS**													
2.1	Aufbau eines Testnetzwerkes	WIS													
2.2	Vermessung der Störfestigkeit	WIS													
2.2.1	Vermessung der Störfestigkeit gegenüber leitungsgeführten Störungen	WIS													
2.2.2	Vermessung der Störfestigkeit gegenüber gestrahlten Störungen	WIS													
2.3	Klassifizierung der Störungen	WIS													
3	**Verfahren zur Analyse der Gefährdung und der Schadensausbreitung**	**LUH**													
3.1	Modellierung der Wirkungen und Effekte in Netzwerk	LUH													
3.1.1	Modellierung der elektromagnetischen Wirkungsmechanismen	LUH													
3.1.2	Modellierung der Schadensverteilung	LUH													
3.2	Methode zur Gefährdungsanalyse von Netzwerken	FHH													
3.2.1	Ableitung eines geeigneten methodischen Ansatzes	FHH													
3.2.2	Analyse des Testnetzwerkes	LUH													
3.2.3	Analyse eines bestehenden IT-Netzes	LUH													
4	**Empfehlungen zur strukturellen Auslegung von Netzwerken (technische Schutzkonzepte)**														
4.1	Erfassung organisatorischer und technischer einschränkender Randbedingungen	FIS													
4.2	Erarbeitung von Empfehlungen zur strukturellen Auslegung von Netzwerken	WIS													
4.3	Erarbeitung von Maßnahmen zur Abwehr eines Angriffes	THA													
4.4	Konzeptvorschläge für Schulung und Krisenreaktion	FIS													
5	**Spektrumüberwachungssensornetz**	NCT													
5.1	Festlegung der Spezifikationen für einen robusten Überwachungssensor des elektromagnetischen Spektrums	NCT													
5.2	Sensorentwicklung	NCT													
5.3	Entwicklung eines Spektrumüberwachungsnetzes	NCT													
5.4	Integration der Überwachung u. der Bedrohungserkennung in den Sensor	NCT													
6	**Kontroll- und Management-Software für das Spektrumüberwachungssensornetz**	**NCT**													
6.1	Software Konzeption	NCT													
6.2	Validierung Benutzerschnittstelle	FIS													
7	**TDOA-basierte Ortung der Bedrohung**	**THA**													
7.1	Überwachung	LUH													
7.2	Erkennen von Bedrohungen	LUH													
7.3	Ortung nach dem TDOA-Prinzip (Time Difference Of Arrival), um auffällige Richtantennen zu vermeiden	THA													
7.4	Integration mit dem Sensornetz	THA													
8	**Technische Schutzelemente**	**WIS**													
8.1	Leistungsspezifikation technischer Schutzelemente	WIS													
8.2	Konstruktive Umsetzung / Auswahl technischer Schutzelemente	LUH													
8.3	Bau von Technologiedemonstratoren / Nachweisführung	WIS													
9	**Bewertung anwenderrelevanter Fragestellungen inklusive Zuständigkeiten und rechtlicher Rahmenbedingungen**	**FIS**													
9.1	Zusammenstellung der einschlägigen Vorgaben und Regelwerke	LUH/ FIS													
9.2	Anlage einer tabellarischen Übersicht zu den der rechtlichen Bewertung zugrunde liegenden Ausgangslagen, Standardsituationen und deren Modifikationen. Erste rechtliche Bewertung der Ausgangslagen	LUH/ FIS													
9.3	Übersicht der relevanten Kompetenzverteilung zwischen öffentlichen und privaten Stellen. Beurteilung von Standardsituationen	LUH/ FIS													
9.4	Erstellung einer Übersicht zum verfügbaren rechtlichen Instrumentarium an Hand der bis dahin beurteilten Ausgangslagen und Standardsituationen (Eingriffsbefugnisse, Ansprüche u.ä.)	LUH/ FIS													
9.5	Rechtliche Beurteilung von Ausgangslagen, Standardsituationen und ihren Modifikationen im Hinblick auf Privatrecht, Öffentliches Recht, Strafrecht unter Einbeziehung von Telekommunikationsrecht und Datenschutzrecht.	LUH/ FIS													
9.6	Gesamtbeurteilung unter Einbeziehung von speziellen technikrechtlichen, von Vorgaben des Europarechts und des internationalen Rechts	LUH/ FIS													
9.7	Abschließende rechtliche Beurteilung an der Hand der bis dahin vorgelegten Ergebnisse der anderen Arbeitsgruppen	LUH/ FIS													

Abbildung 1: Projektplan „EMSIN“

I.4 Kurze Darstellung zum wissenschaftlichen und technischen Stand an den angeknüpft wurde, insbesondere

- **Angabe bekannter Konstruktionen, Verfahren und Schutzrechte, die für die Durchführung des Vorhabens benutzt wurden,**
- **Angabe der verwendeten Fachliteratur sowie der benutzten Informations- und Dokumentationsdienste**

In den letzten zehn Jahren wurden zahlreiche Informationen über die Entwicklung von leistungsstarken Mikrowellenquellen (HPM-Quellen) veröffentlicht. Die physikalisch-technischen Prinzipien, die grundsätzlichen konstruktiven Konzepte und die erforderlichen Materialien und Komponenten sind ohne Beschränkung verfügbar. Diese hohe Verfügbarkeit und die geringen Kenntnisanforderungen zur Realisierung machen HPM-Quellen zu einer besonders gefährlichen asymmetrischen Waffe.

Deshalb erscheint es notwendig, künftig von Anwendungen in den Bereichen Terrorismus, Sabotage, Erpressung und anderer Kriminalität auszugehen. Für alle Täterkreise ist der Einsatz von HPM-Systemen in vielerlei Hinsicht vorteilhaft. HPM-Quellen sind vor Inbetriebnahme nicht detektierbar, da sich ihre Elemente von Standardelektronik nicht unterscheiden. Nach erfolgtem Anschlag kann derzeit aus der Art der Störung oder Zerstörung nicht unmittelbar auf die Art des Angriffes rückgeschlossen werden. Dem Täter bietet sich so die Möglichkeit der unerkannten Flucht sowie der Spuren- wie Tatmittelbeseitigung.

Für das Sensorsystem bedeutet dies, dass die Detektion und Lokalisierung der HPEM-Quelle bis zum Auslösen eines Alarms, nur wenige Sekunden beanspruchen darf. Angestrebt ist eine Zeitspanne unter 10 Sekunden. Anders als bei Angriffen mit Spreng- oder Gefahrenstoffen besteht bei der Ausführung der Tat keine Gefahr für die Gesundheit des Täters.

Nach aktueller Rechtslage sind Beschaffung, Besitz und das Mitführen von HPM-Quellen zulässig. Gezielte rechtswissenschaftliche Untersuchungen zu diesem Komplex liegen nicht vor und sollen deshalb ebenfalls im Vorhaben EMSIN erarbeitet werden.

In den USA wurde diese Bedrohung für die nationale Sicherheit erkannt und ist Gegenstand der Arbeit verschiedener Kommissionen und Hearings. Schon im Jahr 1999 wurde durch die Vollversammlung der URSI (Union Radio - Scientifique Internationale) die „Resolution of Criminal Activities using Electromagnetic Tools“ verabschiedet, in welcher auf die Gefährdung durch die kriminelle Nutzung elektromagnetischer (EM) Wirksysteme hingewiesen wird. Die URSI Resolution empfahl darüber hinaus zusätzliche Forschungsaktivitäten zur Sicherstellung einer ausreichenden elektromagnetischen Härtung sowie die Erforschung von Methoden und Techniken zum Schutz vor elektromagnetischen Angriffen und die Bereitstellung geeigneter Methoden zum Schutz der Öffentlichkeit vor den Auswirkungen eines EM-Angriffs.

In den letzten Jahren wurde international für die Bedrohung durch EM Angriffe der Begriff „Intentional Electromagnetic Interference“ geprägt. In Folge der Resolution wurden die Wirkmechanismen und die durch elektromagnetische Felder hoher Leistung hervorgerufenen Effekte auf einige wichtige militärische Systeme untersucht.

Vergleichbare Untersuchungen für zivile Systeme liegen nur in ungenügendem Maße vor. National wurden derartige Forschungsarbeiten im Rahmen von Studien durch die WTD 812 und das WIS initiiert. Generell zeigt sich, dass die für eine gravierende Funktionsstörung (Mission Kill) benötigten Feldstärken und Leistungspegel bereits heute durch frei verfügbare HPM Quellen erzeugt werden können.

Im Rahmen eines elektromagnetisch verträglichen Aufbaus von IT-Netzwerken gehört der Schutz gegenüber der Einkopplung ungewollter Störsignale aus umgebenden elektromagnetischen Feldern zum Bestandteil praktizierter Technik. Je nach geforderter Standkraft werden die Teilsysteme eines Netzwerkes mit Schutzelementen, Filtern, Schirmen und galvanischen Trennungselementen versehen.

Forschungsarbeiten der vergangenen Jahre haben jedoch gezeigt, dass der durch die EMV gegebene Grundschutz für eine Abwehr eines bewussten EM-Angriffes bei weitem nicht ausreicht. Die Defizite beim Aufbau von wichtigen IT-Netzwerken liegen heute darin begründet, dass lediglich die klassischen Störsignale im Bereich der Elektromagnetischen Verträglichkeit (EMV) betrachtet werden.

Diese klassischen EMV-Störsignale sind von den Feldstärken her begrenzt und auch oft schmalbandig, so dass beispielsweise mit entsprechenden Filtern oder ähnlichen Maßnahmen gearbeitet werden kann. Eingangschutzelemente im klassischen EMV-Bereich sind beispielsweise im Frequenzbereich nach oben beschränkt. HPEM-Störsignale zeichnen sich aber gerade dadurch aus, dass sie meist stark breitbandig sind und durch extrem steile Anstiegszeiten auch sehr hohe Frequenzanteile besitzen. Diese schnellen Pulse können beispielsweise von den klassischen Schutzelementen nicht unterdrückt werden. Zusätzlich erfordern die in der Regel weit höheren Feldstärke-Spitzenwerte von HPEM-Störquellen auch eine angepasste Auslegung von Schutzelementen.

Aufgrund dieser Defizite und der veränderten Bedrohungsform ist es notwendig, vorhandene Schutzkonzepte zu überdenken, zu verbessern oder neu zu entwerfen. Ebenso ist es notwendig neuartige Schutzelemente zu konstruieren, die auf die HPEM-Bedrohungsparameter zugeschnitten sind. Dies wurde im Rahmen der Arbeitspakete in das Verbundvorhaben aufgenommen.

Im Zuge vorheriger und andauernder Untersuchungen des WIS zeigte sich bereits, dass klassische Schutzelemente über Schaltzeiten verfügen, welche für eine wirkungsvolle Abblockung der eingekoppelten Störsignale zu langsam sind. Weiterhin werden diese durch die eingekoppelten hohen Spannungspegel zerstört. Umfangreiche Erkenntnisse wurden durch den Projektpartner WIS in das Verbundvorhaben EMSIN eingebracht. Als entscheidendes Mittel einer Gefahrenabwehr hat die Technik bisher keinen für den Nutzer wirtschaftlich und praxisgerecht einsetzbaren Detektor oder Ortungssensor hervorgebracht.

Die Erkennung schneller Pulse war bisher sehr teuer und nur wissenschaftlichem Personal mit Hilfe komplizierter Labortechnik vorbehalten. Zur Bewertung der Verwundbarkeit von elektronischen Systemen sind in der Fachliteratur keine Methoden zu finden, welche dazu geeignet wären, ein IT-Netzwerk in seiner gesamten Komplexität zu analysieren. So scheitern messtechnisch basierte Verfahren an der Ausdehnung des Netzwerkes und der Notwendigkeit umfangreicher Messungen vor Ort. Das Projekt „EMSIN“ sollte daher einen Beitrag leisten die entsprechenden messtechnisch basierten Verfahren zu verbessern.

Die derzeit genutzte Technologie zur Funkpeilung (meist für militärische Anwendungen), ermöglicht nur eine begrenzte Genauigkeit bei der Lokalisierung von modernen Störszenarien. Die meisten Lösungen bestehen aus einigen Fahrzeugen oder aus ortsfesten Installationen, GPS-Synchronisationshardware und drahtlosen digitalen Kommunikationskanälen, die die Anwendung von Ortungs-Algorithmen ermöglichen. Die gegenwärtig angewandten Lösungen sind in dieser Form nicht für eine 24/7-Überwachung ausgelegt. Sie werden hauptsächlich dazu benutzt, einen Sender zu lokalisieren, nachdem ein Problem aufgetreten ist. Dies ist der Stand der Technik in Deutschland und Israel.

Die vorgeschlagene Lösung wird eine Echtzeit-, Rund-um-die-Uhr-Überwachung des betreffenden Spektrums ermöglichen. Nur durch die gleichzeitige Peilung mehrerer Kanäle, wird das System ein reales Echtzeit-Warn- und -Ortungssystem. Das System wird aus mehreren Sensoren an verschiedenen Positionen im Flughafengelände bestehen. Durch den Einsatz dieser kostengünstigen Sensoren wird ein äußerst robustes System mit verbesserter Genauigkeit erstellt.

Es sind keine Patente bekannt, die einer Verwertung der hier erzielten Ergebnisse im Wege stehen würden. Es wird während der Projektbearbeitung regelmäßig eine Überprüfung der Patentsituation geben und wesentliche, in diesem Projekt gewonnene, Innovationen werden patentrechtlich geschützt werden.

I.5 Kurze Darstellung zur Zusammenarbeit mit anderen Stellen

Bei Thales (THA) werden im Bereich JC4I seit über 20 Jahren Systeme zur Detektion, Ortung und Aufklärung elektromagnetischer Strahlungen entwickelt. Eine Spezialisierungsrichtung der Aufklärungsexpertise sind sensorsignalverarbeitende Algorithmen für Echtzeitanwendungen in Verbindung mit vollautomatischen Signalklassifikatoren. Eingesetzt werden diese in Überwachungssystemen zur Alarmierung und gegebenenfalls automatischen Einleitung von Gegenmaßnahmen. Weitere ergänzende Themenschwerpunkte von Thales in diesem Bereich sind:

- Aktive Jammer in verschiedenen Frequenzbereichen
- Maßnahmen und Systeme gegen Aufklärung und Jamming
- IT-Security, Sicherheitskonzepte und Härtung von IT-Komponenten, Funksysteme, insbesondere störresistente Wellenformen

Die Firma Thales war Projektkoordinator des Projektes EMSIN und untersuchte im Rahmen des Projektes die Ortungssysteme, integrierte sie im Sensornetz und erarbeitete Empfehlungen zur strukturellen Auslegung von Netzwerken.

Am Institut für Grundlagen der Elektrotechnik und Messtechnik der Leibniz Universität Hannover (LUH) werden seit vielen Jahren elektronische Systeme und Komponenten aus dem militärischen Bereich auf ihre Empfindlichkeit gegenüber elektromagnetischen Einkopplungen untersucht. Auftraggeber dieser Studien, in deren Verlauf eine große Anzahl nationaler und internationaler Veröffentlichungen entstanden, sind Institutionen des Bundes und private Unternehmen. Schwerpunkt der Forschungsarbeiten des Institutes ist die elektromagnetische Feldtheorie verbunden mit dem Messen und Erzeugen von elektromagnetischen Feldern. Die Betrachtung von EMV-Problemen großer, heterogener Systeme gewinnt zunehmend an Bedeutung.

Im Rahmen des Projektes EMSIN erarbeitete die LUH Verfahren zur Analyse der Gefährdung und der Schadensausbreitung. Außerdem führte sie die Analyse eines bestehenden IT-Netzes am Beispiel Flughafen durch und unterstützte die WIS bei der Erstellung von technischen Schutzelementen. Im Unterauftrag der LUH führte Frau Dr. Aigner-Hof die rechtliche Begleitforschung zum Projekt EMSIN durch.

An der Fachhochschule Hannover (FHH) liegt der Schwerpunkt der Forschungsaktivitäten auf der Störfestigkeit von Luftfahrzeugen gegen elektromagnetische Felder. Zu dieser Thematik wurde ein Projekt im Auftrag der Luftfahrtindustrie bearbeitet. Weitere Expertise besteht beispielsweise im Bereich der elektrischen Schirmungseigenschaften von Baumaterialien und Baukörpern sowie im Bereich der Einkopplung schneller elektromagnetischer Impulse in elektronische Systeme beziehungsweise im Bereich der Entwicklung impulsabstrahlender Antennen.

Die Fachhochschule Hannover erarbeitete im Projekt EMSIN die theoretischen Grundlagen der Analyse und Modellierungen von Netzwerken. Unter anderem erfolgte in diesem Zusammenhang die Analyse der charakteristischen elektromagnetischen Umgebung.

Beim Wehrwissenschaftlichen Institut für Schutztechnologien - ABC-Schutz (WIS) ist der Tätigkeitsschwerpunkt „Schutz vor elektromagnetischen Feldern“ in den Geschäftsfeldern „High-Power Microwave (HPM)-Simulation“ (GF 320) und „Elektromagnetische Wirkungen“ (GF 330) angesiedelt. Die Empfindlichkeit und der Schutz von elektronischen Systemen gegen schmalbandige HPM-Felder bilden den Arbeitsschwerpunkt des GF 320. Mit Hilfe experimenteller und theoretischer Verfahren werden Einkoppelwege, Schadensmechanismen und Schadenseffekte untersucht, um die Qualität von Schutzmaßnahmen bewerten zu können. In den vergangenen Jahren lag der Schwerpunkt der Forschungsarbeiten auf der Untersuchung von Flugkörpern und Komponenten von zivilen und militärischen IT-Systemen. Das GF 330 „Elektromagnetische Wirkungen“ testet Bundeswehrsysteme (unter anderem EF2000, TIGER) auf ihre Härte gegenüber den Wirkungen des Nuclear Electromagnetic Pulse (NEMP) sowie gegenüber nichtnuklearen elektromagnetischen Wirksystemen (UWB). Die Wirkungen von NEMP- und UWB-Impulsen auf elektronische Komponenten und mögliche Schutzmaßnahmen werden vermessen, analytisch beschrieben und weiterentwickelt.

Das Wehrwissenschaftliche Institut für Schutztechnologien – ABC-Schutz (WIS) war im Rahmen des Projektes EMSIN für den Aufbau des Testnetzwerks zuständig. Darüber hinaus wurden am WIS die technischen Schutzelemente definiert.

Seit 1998 entwickelt und produziert die israelische Firma Netline (NCT) voll programmierbare HF-Kommunikations-Jamming- und Ortungslösungen für militärische Kunden, Polizei und Behörden. Netline bietet eine breite Palette von Systemen an, von kostengünstigen Low-End-Standalone-Produkten bis High-End-Netzwerk-Installationen, die große Einrichtungen abdecken. Das Produktsortiment umfasst mehrere Generationen von HF-Signal-Quellen, Breitband-Spektralanalysatoren und Signalverarbeitung, jeweils optimiert für eine spezifische Anwendung. Netline ist an verschiedenen Forschungsprogrammen des israelischen “Chief Scientist" beteiligt. In diesem Rahmen wurde beispielsweise ein auf neuen Technologien basierender Signal Generator (WRBS) entwickelt. Dieser Signal Generator ist ein allgemeiner Signal Generator Baustein, welcher leicht in die verschiedensten Systeme eingebunden werden kann. So wurde er unter anderem in der neuen Produktfamilie der Netline-Störer eingesetzt.

Die Firma Netline Communications Technologies Ltd. führte im Rahmen des Projektes EMSIN die Entwicklung des Spektrumüberwachungssensors durch und sollte diesen in den Ortungsserver der Firma THALES implementieren. Außerdem programmierte sie eine Kontroll- und Managementsoftware für das Sensornetzwerk.

Die FIS GmbH ist ein leistungsstarkes, im europäischen Verbund agierendes Unternehmen der Flug- und Industriesicherheit, das in seinen Geschäftsfeldern eine führende Marktposition einnimmt. Unter dem Dach und im Netzwerk des global ausgerichteten Sicherheitskonzerns ICTS Europe entwickelt die FIS individuelle und nachhaltige Sicherheitslösungen. Die ICTS Europe ist in 24 Ländern mit insgesamt 77 Standorten und etwa 11.000 Mitarbeitern vertreten.

Die Flug- und Industriesicherheit Service- und Beratungs-GmbH – kurz FIS GmbH – wurde 1988 mit Hauptsitz in Kelsterbach bei Frankfurt am Main gegründet. An neun Airport-Standorten in Deutschland beschäftigt die FIS GmbH zurzeit über 1.400 Mitarbeiterinnen und Mitarbeiter. Das Produkt- und Dienstleistungsangebot umfasst das Spektrum von der Passagier- und Gepäckkontrolle über Personal-, Waren-, Fracht- und Dokumentenkontrolle bis hin zum Objektschutz. Zudem sichert die FIS GmbH kritische Infrastrukturen sowie Großveranstaltungen. Auftraggeber sind hauptsächlich Behörden, Flughafenbetreiber und Luftverkehrsgesellschaften.

Die Firma FIS leistete in Zusammenarbeit mit dem Flughafen und der DFS die endanwenderseitige Unterstützung bei der technischen Entwicklung des Sensorprodukts sowie bei der Erstellung von Konzepten zur Systemanwendung. Dabei analysierte sie den aktuellen Baustand elektronischer Infrastruktur am Beispiel Flughafen und erfasste die dort verfügbaren Sicherheitssysteme. Darüber hinaus war sie für die Validierung der Benutzerschnittstelle sowie für die Begutachtung anwenderseitiger Fragestellungen verantwortlich.

Dem Verbund stand ein Beirat zur Verfügung, der mit umfangreicher themenbezogener Erfahrung die Forschungsarbeit begleitete. Der Beirat sollte zusätzlich die Sichtweise der Endnutzer in das Projekt einbringen. Er nahm an Projektsitzungen teil und überprüfte Vorgehensweisen und Lösungswege welche den Flughafen betreffen. Es wurden beispielsweise Hinweise bei der Bestandaufnahme der Infrastruktur oder bei der Überprüfung von Konzepten und Maßnahmen zur Bewältigung von Schadenereignissen gegeben sowie bei erweiternden Fragestellungen weitere Kontakte zu Organisationseinheiten und Abteilungen am Flughafen und zu anderen Endnutzern hergestellt. Folgende Unternehmen begleiteten das Projekt im Beirat:

- DFS Deutsche Flugsicherung
- Flughafen Hannover-Langenhagen
- Flughafen Paderborn Lippstadt
- Ben Gurion Airport

Zur Einbindung der Endanwender sollte ein Workshop mit Flughafenvertretern und der DFS organisiert werden. Dazu sollten Vertreter der größten deutschen Flughäfen, schwerpunktmäßig aus den Bereichen Sicherheit und IT, eingeladen werden. Im Vordergrund sollten vor allem die Anforderungen der Endanwender an die Funktionalitäten des Systems, die Bedienbarkeit und die Anbindung an das gesamte Sicherheitssystem der jeweiligen Infrastrukturen stehen. Außerdem sollte mit den Flughafenvertretern abgeklärt werden, ob es Ergänzungen beziehungsweise Modifikationen bezüglich der bereits erfassten typischen IT-Installationen gibt. Auf diese Weise sollte gewährleistet werden, dass die Auslegung der Systeme den Anforderungen der Endanwender genügt und die Ergebnisse nach Projektende erfolgreich umgesetzt werden können. Aufgrund von negativer Berichterstattung während der Projektlaufzeit wurde jedoch darauf verzichtet einen solchen Workshop zu veranstalten. Stattdessen wurde die Zusammenarbeit mit den Beiratsmitgliedern in den entsprechenden Themengebieten intensiviert.

II.1 Eingehende Darstellung der Verwendung der Zuwendung und des erzielten Ergebnisses im Einzelnen, mit Gegenüberstellung der vorgegebenen Ziele

Im Rahmen dieses Projektvorhabens wurden die Arbeitspakete Analyse der Gefährdung, Testnetzwerk, Verfahren zur Analyse der Gefährdung und der Schadensausbereitung, Empfehlungen zur strukturellen Auslegung von Netzwerken, Spektrumüberwachungssensornetz, Kontroll- und Management- Software für das Spektrumsüberwachungssensornetz, TDOA-basierte Ortung der Bedrohung, Technische Schutzelemente sowie Bewertung anwenderrelevanter Fragestellungen inklusive Zuständigkeiten und rechtlicher Rahmenbedingungen bearbeitet. Im Folgenden ein Überblick über die Verteilung der Arbeitspakete über die Projektlaufzeit:

Workpackage		Partner	2010				2011				2012				
No	Name		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
1	**Analyse der Gefährdung**	**LUH**													
1.1	Auswertung der technischen Fachliteratur	FHH													
1.2	Analyse des aktuellen Baustandes elektronischer Infrastruktur														
1.2.1	Bestandaufnahme an Flughäfen	FIS													
1.2.2	Identifikation kritischer Baugruppen und Messung ihrer Störfestigkeit	LUH													
1.3	Analyse der elektromagnetischen Gefährdung														
1.3.1	Analyse der charakteristischen elektromagnetischen Umgebung	FHH													
1.3.2	Definition möglicher Störer	WIS													
1.4	Erfassung verfügbarer Sicherheitssysteme	FIS													
2	**Testnetzwerk**	**WIS**													
2.1	Aufbau eines Testnetzwerkes	WIS													
2.2	Vermessung der Störfestigkeit	WIS													
2.2.1	Vermessung der Störfestigkeit gegenüber leitungsgeführten Störungen	WIS													
2.2.2	Vermessung der Störfestigkeit gegenüber gestrahlten Störungen	WIS													
2.3	Klassifizierung der Störungen	WIS													
3	**Verfahren zur Analyse der Gefährdung und der Schadensausbreitung**	**LUH**													
3.1	Modellierung der Wirkungen und Effekte in Netzwerk	LUH													
3.1.1	Modellierung der elektromagnetischen Wirkungsmechanismen	LUH													
3.1.2	Modellierung der Schadensverteilung	LUH													
3.2	Methode zur Gefährdungsanalyse von Netzwerken	FHH													
3.2.1	Ableitung eines geeigneten methodischen Ansatzes	FHH													
3.2.2	Analyse des Testnetzwerkes	LUH													
3.2.3	Analyse eines bestehenden IT-Netzes	LUH													
4	**Empfehlungen zur strukturellen Auslegung von Netzwerken (technische Schutzkonzepte)**														
4.1	Erfassung organisatorischer und technischer einschränkender Randbedingungen	FIS													
4.2	Erarbeitung von Empfehlungen zur strukturellen Auslegung von Netzwerken	WIS													
4.3	Erarbeitung von Maßnahmen zur Abwehr eines Angriffes	THA													
4.4	Konzeptvorschläge für Schulung und Krisenreaktion	FIS													
5	**Spektrumüberwachungssensornetz**	NCT													
5.1	Festlegung der Spezifikationen für einen robusten Überwachungssensor des elektromagnetischen Spektrums	NCT													
5.2	Sensorentwicklung	NCT													
5.3	Entwicklung eines Spektrumüberwachungsnetzes	NCT													
5.4	Integration der Überwachung u. der Bedrohungserkennung in den Sensor	NCT													
6	**Kontroll- und Management-Software für das Spektrumüberwachungssensornetz**	**NCT**													
6.1	Software Konzeption	NCT													
6.2	Validierung Benutzerschnittstelle	FIS													
7	**TDOA-basierte Ortung der Bedrohung**	**THA**													
7.1	Überwachung	LUH													
7.2	Erkennen von Bedrohungen	LUH													
7.3	Ortung nach dem TDOA-Prinzip (Time Difference Of Arrival), um auffällige Richtantennen zu vermeiden	THA													
7.4	Integration mit dem Sensornetz	THA													
8	**Technische Schutzelemente**	**WIS**													
8.1	Leistungsspezifikation technischer Schutzelemente	WIS													
8.2	Konstruktive Umsetzung / Auswahl technischer Schutzelemente	LUH													
8.3	Bau von Technologiedemonstratoren / Nachweisführung	WIS													
9	**Bewertung anwenderrelevanter Fragestellungen inklusive Zuständigkeiten und rechtlicher Rahmenbedingungen**	**FIS**													
9.1	Zusammenstellung der einschlägigen Vorgaben und Regelwerke	LUH/ FIS													
9.2	Anlage einer tabellarischen Übersicht zu den der rechtlichen Bewertung zugrunde liegenden Ausgangslagen, Standardsituationen und deren Modifikationen. Erste rechtliche Bewertung der Ausgangslagen	LUH/ FIS													
9.3	Übersicht der relevanten Kompetenzverteilung zwischen öffentlichen und privaten Stellen. Beurteilung von Standardsituationen	LUH/ FIS													
9.4	Erstellung einer Übersicht zum verfügbaren rechtlichen Instrumentarium an Hand der bis dahin beurteilten Ausgangslagen und Standardsituationen (Eingriffsbefugnisse, Ansprüche u.ä.)	LUH/ FIS													
9.5	Rechtliche Beurteilung von Ausgangslagen, Standardsituationen und ihren Modifikationen im Hinblick auf Privatrecht, Öffentliches Recht, Strafrecht unter Einbeziehung von Telekommunikationsrecht und Datenschutzrecht.	LUH/ FIS													
9.6	Gesamtbeurteilung unter Einbeziehung von speziellen technikrechtlichen, von Vorgaben des Europarechts und des internationalen Rechts	LUH/ FIS													
9.7	Abschließende rechtliche Beurteilung an der Hand der bis dahin vorgelegten Ergebnisse der anderen Arbeitsgruppen	LUH/ FIS													

Abbildung 2: Projektplan „EMSIN“

Das Arbeitspaket 1 „Analyse der Gefährdung“ wurde von der LUH koordiniert und hatte folgende Unterpakete: Auswertung der technischen Fachliteratur, Analyse des aktuellen Baustandes elektronischer Infrastruktur, Analyse der elektromagnetischen Gefährdung sowie Erfassung verfügbarer Sicherheitssysteme.

Das Unterpaket 1.1 „ Auswertung der technischen Fachliteratur“ wurde von der FHH bearbeitet. Es sollte eine ergänzende Auswertung der technischen Fachliteratur durchgeführt werden, da es im Bereich Intentional Electromagnetic Interference zwar grundlegende Publikationen gibt, die sich aber eher mit den physikalischen Phänomenen beschäftigen. Die meisten Untersuchungen an konkreten Flughäfen berühren sofort sicherheitsempfindliche Aspekte und sind damit öffentlich sehr schwer zugänglich. Konkrete Aussagen können daher nur aus den verschiedenen Arbeitspapieren der Normungsausschüsse (z.B. IEC SC77C, IEEE TC-5 High Power Electromagnetics oder TC 7 Nonsinusoidal Fields Technical Committees) abgeleitet werden. Der Zugang zu diesen Gremien war über die Projektpartner gegeben. Aktuelle Änderungen und Ergänzungen der technischen Fachliteratur in Bezug auf die Modellierung und Analyse von IT-Netzwerken sowie den Schutz von Anlagen, die mit Flughäfen vergleichbar sind, vor elektromagnetischen Bedrohungen sollten kontinuierlich gesichtet und ausgewertet werden. Insbesondere war dabei zu überprüfen, wie die publizierten Ergebnisse auf die Situation am Flughafen übertragen werden können. Dies sollte mit Hilfe der Anwender bewertet werden.

Das Unterpaket 1.2 „Analyse des aktuellen Baustandes elektronischer Infrastruktur“ war in die beiden Gliederungspunkte 1.2.1 „Analyse des Aufbaus typischer IT-Netze und Kommunikationsfrequenzen an Flughäfen“ sowie 1.2.2 „Identifikation kritischer Baugruppen und Messung ihrer Störfestigkeit“ unterteilt.

Die „Analyse des Aufbaus typischer IT-Netze und Kommunikationsfrequenzen an Flughäfen“ wurde von der FIS koordiniert. Am Beispiel Flughafen sollten die für Verkehrsinfrastrukturen typischen Installationen einschließlich der zum Flughafenbetrieb notwendigen Frequenzbänder aufgenommen und charakterisiert werden. Die Baustandsaufnahme sollte als Basis für den Aufbau eines Testnetzwerkes (Arbeitspaket 2) und die Analyse in späteren Arbeitsschritten (Arbeitspakete 1.3.1, 3.3.1, 3.2.1, 4.1) dienen.

Die LUH koordinierte die „Identifikation kritischer Baugruppen und Messung ihrer Störfestigkeit“. In diesem Zusammenhang sollten die Komponenten der in Arbeitspaket 1.2.1 identifizierten Komponenten, Subsysteme und Baugruppen einer ersten Bewertung hinsichtlich ihrer Störsensitivität zugeführt werden. Anhand funktionaler Bewertungen sollten die Baugruppen und Subsysteme identifiziert werden, deren Funktion für die Leistungsfähigkeit des Netzwerkes von wesentlicher Bedeutung sind. In Vorarbeiten wurden statistisch basierte Methoden zur Vermessung der Störfestigkeit von Baugruppen entwickelt. Diese Methoden sollten auf die Vermessung der identifizierten Baugruppen und Subsysteme übertragen werden. Als Ergebnis dieses Arbeitspaketes sollten die Beschreibungen der Breakdown-Failure-Rate für ausgewählte Geräte geliefert werden.

Das Unterpaket 1.3 „Analyse der elektromagnetischen Gefährdung“ wurde von der WIS koordiniert und war in die beiden Gliederungspunkte 1.3.1 „Analyse der charakteristischen elektromagnetischen Umgebung“ sowie 1.3.2 „Definition möglicher Störer“ unterteilt.

Die „Analyse der charakteristischen elektromagnetischen Umgebung“ wurde von der FHH koordiniert. In diesem Zusammenhang sollte die Bewertung der in 1.2.1 charakterisierten Umgebung in Bezug auf die in 1.2.2 bestimmten Störschwellen erfolgen und vorhandene Schwachstellen identifiziert werden.

Die „Definition möglicher Störer“ wurde von der WIS koordiniert. Hier sollten aus den bestimmten Störschwellen von Baugruppen (1.2.2) als auch anhand der abgeschätzten Empfindlichkeit des Gesamtsystems (1.3.1) technische Parameter (Leistungspegel, Feldstärkewerte, Signalform, Frequenzbereich) von als kritisch einzustufenden Störern abgeleitet werden. In den nachfolgenden Arbeitsschritten sollten die abgeleiteten technischen Parameter als Referenz für die angenommene Bedrohung dienen.

Der gewählte Weg der Definition eines für Netzwerke kritischen Störers besitzt gegenüber einer Marktsichtung und der Verwendung vorhandener Störquellen die Vorteile der Unabhängigkeit von vorhandenen Quellen sowie der Wirksamkeit des Schutzes auch gegenüber zukünftigen Störquellen, als auch der Auslegung des Schutzes gegen die schlimmstmögliche Bedrohung. In diesem Kontext sollten auch kritische Störer im Bezug auf Flugfunk, Radar etc mitbetrachtet werden.

Das Unterpaket 1.4 „Erfassung verfügbarer Sicherheitssysteme“ wurde von der FIS koordiniert und diente der Ermittlung und Analyse der bestehenden Sicherheitskontrollen und der zugehörigen Sicherheitssysteme. Die Einsatzmöglichkeiten und Leistungsparameter der Sicherheitssysteme sollten ermittelt werden sowie die Schwachstellen in Bezug auf die Einbringung einer HPM-Quelle analysiert werden.

Das Arbeitspaket 2 „Testnetzwerk“ hatte die Unterpakete: Aufbau eines Testnetzwerkes, Vermessung der Störfestigkeit und Klassifizierung der Störungen. Alle Unterpunkte sowie das Gesamtpaket wurden vom WIS koordiniert.

Im Rahmen des Unterpakets 2.1 „Aufbau eines Testnetzwerkes“ sollte basierend auf den Ergebnissen des Arbeitspaketes 1.2 ein generisches Testnetzwerk beim WIS aufgebaut werden, das typische Installationsmerkmale von Netzwerken an Flughäfen nachbildet. Mit Hilfe des Netzwerkes sollten intensive messtechnische Untersuchungen durchgeführt werden, ohne in den Betrieb eines Flughafens eingreifen zu müssen.

Das Unterpaket 2.2 „Vermessung der Störfestigkeit“ war in die beiden Gliederungspunkte 2.2.1 „Vermessung der Störfestigkeit gegenüber leitungsgeführten Störungen“ sowie 2.2.2 Vermessung der Störfestigkeit gegenüber gestrahlten Störungen“ unterteilt.

Im Rahmen der „Vermessung der Störfestigkeit gegenüber leitungsgeführten Störungen sollte das in Arbeitspaket 2.1 aufgebaute Testnetzwerk hinsichtlich der Störfestigkeit gegenüber auf Leitungen (Stromversorgungs- und Datenleitungen) eingekoppelten elektrischen Störgrößen untersuchen werden. Die Parameter der eingekoppelten Störungen sollten aus den in Arbeitspaket 1.3.2 definierten Parametern kritischer Störer abgeleitet werden. Der Testaufbau sollte basierend auf genormten Testaufbauten für EMV-Untersuchungen in einem speziellen beim WIS vorhandenen Laborraum realisiert werden. Anhand der gewonnenen Ergebnisse sollten die Parameter kritischer Störer angepasst und erweitert werden. Durch Variation der Störparameter sollte der für die auftretenden Effekte und Störungen maßgebliche Parametersatz (z.B. Amplitude, Energie, Signalform, Bandbreite) ermittelt werden.

Des Weiteren sollte bei der „Vermessung der Störfestigkeit gegenüber gestrahlten Störungen“ das in Arbeitspaket 2.1 aufgebaute Testnetzwerk hinsichtlich der Störfestigkeit gegenüber gestrahlten elektrischen Störgrößen untersucht werden. Die Parameter der eingekoppelten Störungen sollten aus den in Arbeitspaket 1.3.2 definierten Parametern kritischer Störer abgeleitet werden und im Rahmen der Vermessung sollten die auf Leitungen (Stromversorgungs- und Datenleitungen) eingeprägten Störgrößen aufgenommen und den Ergebnissen des Arbeitspaketes 2.2.1 gegenübergestellt werden. Anhand der gewonnenen Ergebnisse zur Störfestigkeit gegenüber gestrahlten Pulsen, sollten die notwendigen Leistungsparameter kritischer Störer angepasst und erweitert werden. Durch Variation der Störparameter sollte der für die auftretenden Effekte und Störungen maßgebliche Parametersatz (z.B. Amplitude, Energie, Signalform, Bandbreite) ermittelt werden.

Im Rahmen des Arbeitspaketes 2.3 „Klassifizierung der Störungen“ sollten die im Rahmen der Vermessung des Testnetzwerkes beobachteten Störungen und Effekte hinsichtlich ihrer Wirkung auf die Funktion des beaufschlagten Teilsystems (Effekt Level) als auch hinsichtlich ihrer Wirkung auf die Leistungsfähigkeit des Gesamtsystems bewertet und klassifiziert werden.

Das Arbeitspaket 3 „Verfahren zur Analyse der Gefährdung und der Schadensausbreitung“ wurde von der LUH koordiniert und hatte die Unterpakete Modellierung der Wirkungen und Effekte im Netzwerk sowie Methode zur Gefährdungsanalyse von Netzwerken.

Das Unterpaket 3.1 „Modellierung der Wirkungen und Effekte im Netzwerk“ war in die beiden Gliederungspunkte 3.1.1 „Modellierung der elektromagnetischen Wirkungsmechanismen und 3.1.2 „Modellierung der Schadensverteilung“ gegliedert. In diesem Arbeitspaket sollte die Ausbreitung der Störeffekte im Netzwerk diskutiert werden und als Ergebnis die erwartete Störgröße am Störobjekt angegeben werden.

Die „Modellierung der elektromagnetischen Wirkungsmechanismen“ wurde von der LUH koordiniert und hier sollten basierend auf den Ergebnissen des Arbeitspaketes 1.1 und den Ergebnissen der Vermessung des Testnetzwerkes (Arbeitspaket 2.2) die elektromagnetischen Wirkungsmechanismen in parametrisierten Modellen dargestellt werden.

Die technische Herausforderung dieses Arbeitsschrittes lag darin, dass das Netzwerk in seiner Gesamtheit unter Einbeziehung seiner Umgebung zu berücksichtigen war. Auch war es nicht das Ziel, die jeweilige Störgröße (Strom, Spannung, Feldstärke) mit hoher mathematischer Genauigkeit zu bestimmen. Im Gegensatz zu etablierten numerischen und analytischen Berechnungsverfahren sollte vielmehr ein Modellierungsansatz verfolgt werden, der eine mehr statistisch basierte Aussage über das Eintreten eines Effektes ermöglicht (Eintrittswahrscheinlichkeit).

Die „Modellierung der Schadensverteilung“ wurde ebenfalls von der LUH koordiniert. In diesem Zusammenhang sollte anhand der im Arbeitspaket 2.2 beobachteten Effekte und Schadensereignisse sowie unter Nutzung des im Arbeitspaket 3.1.1 hergeleiteten Modells die Ausbreitung der Effekte und Schäden im Netzwerk modelliert werden. Hierbei sollten neben den elektromagnetischen Wirkungsmechanismen auch Schadenseffekte auf vernetzte Systemarchitekturen und ihre Anwendungen in geeigneter Weise mit einbezogen werden. Ziel waren Aussagen der Verteilung von Effekten, Leistungseinbrüchen und Schäden auf der Anwendungsschicht.

Das Unterpaket 3.2 „Methode zur Gefährdungsanalyse von Netzwerken“ wurde von der FHH koordiniert und war in die drei Gliederungspunkte: 3.2.1 „Ableitung eines geeigneten methodischen Ansatzes“, 3.2.2 „Analyse des Testnetzwerkes“ und 3.2.3 „Analyse eines bestehenden IT-Netzes“ unterteilt. In diesem Arbeitspaket sollten Methoden zur Beschreibung der Störfestigkeit und deren messtechnischer Nachweis abgeleitet werden.

Die „Ableitung eines geeigneten methodischen Ansatzes“ wurde von der FHH koordiniert. Hier sollte unter Einbeziehung der in den Arbeitspaketen 3.1.1 und 3.1.2 gewonnenen Ergebnisse ein methodischer Ansatz entwickelt werden, mit dessen Hilfe die Gefährdung real vorhandener Netzwerke analysiert werden kann. Die zu entwickelnde Methode sollte hierbei sowohl die Parameter eines kritischen Störers (Arbeitspaket 1.3.2) als auch die Umgebungsbedingungen des Netzwerkes (Arbeitspakete 1.2.1, 1.3.1) berücksichtigen. Die Dimensionen der typischen Netzwerke auf Flughäfen (Stromversorgungsnetz, Flugsicherheitsnetz, Kommunikationsnetz usw.) kombiniert mit der extrem großen Komplexität dieser Netzwerke durch gegenseitige Durchdringung führt dazu, dass sie mit bisher existierenden analytischen, numerischen und messtechnischen Ansätzen nur unzureichend betrachtet werden können.

In Vorarbeiten zu diesem Vorhaben wurde ein Verfahren aus der Funktionalen Sicherheit erarbeitet, welches die Störwahrscheinlichkeit großer Systeme angeben kann. Die besondere Herausforderung in diesem Arbeitspaket bestand darin, die Ausfallfunktionen nach Arbeitspaket 3.1.2 mit den elektrischen Schaltplänen und der räumlichen Situation des Flughafens zu verknüpfen.

Die „Analyse des Testnetzwerkes“ wurde durch die LUH koordiniert und im Rahmen dieses Arbeitspaketes sollte die im Arbeitspaket 3.2.1 erarbeitete Analysemethode anhand des im Arbeitspaket 2.1 aufgebauten Testnetzwerkes verifiziert und optimiert werden.

Die „Analyse eines bestehenden IT-Netzes“ wurde von der LUH koordiniert. In diesem Zusammenhang sollte das IT-Netzwerk eines Flughafens mit Hilfe der im Arbeitspaket 3.2.2 erarbeiteten Analysemethode in Bezug auf die Gefährdung durch elektromagnetische Störer bewertet werden. Die Ergebnisse sollten mit den im Arbeitspaket 3.2.1 durchgeführten Abschätzungen verglichen werden. Die Erarbeitung der Analyse und die Klärung der entsprechenden Punkte sollten in Zusammenarbeit mit dem Flughafen und der DFS (Deutsche Flugsicherung) erfolgen.

Das Arbeitspaket 4 “Empfehlungen zur Strukturellen Auslegung von Netzwerken (technische Schutzkonzepte)“ war in die folgenden Unterpakete gegliedert: Erfassung organisatorischer und technischer einschränkender Randbedingungen, Erarbeitung von Empfehlungen zur strukturellen Auslegung von Netzwerken, Erarbeitung von Maßnahmen zur Abwehr eines Angriffes sowie Maßnahmen zur Bewältigung von Schadensereignissen.

Das Unterpaket 4.1 „Erfassung organisatorischer und technischer einschränkender Randbedingungen“ wurde gemeinsam von FIS und THA bearbeitet. Es sollten organisatorische und technisch einschränkende Randbedingungen erfasst werden, die eine Grundlage für die zu erarbeitenden Empfehlungen zur strukturellen Auslegung von Netzwerken darstellen. Die FIS sollte die Erfassung der organisatorisch einschränkenden Randbedingungen übernehmen. Dabei sollte insbesondere geklärt werden, welche Organisationsstrukturen der Konzeption von Netzwerken einschränkend entgegenstehen beziehungsweise bei der Neukonzeption eines solchen Netzwerkes beachtet werden müssen. Damit sollte gewährleistet werden, dass das Netzwerk den Anforderungen der zukünftigen Arbeitsumgebung entspricht und die Ergebnisse nach Projektende erfolgreich umgesetzt werden können. Die technisch einschränkenden Randbedingungen sollten durch THALES bearbeitet und dargestellt werden. Technische Randbedingungen können der physikalische Aufbau der Wände im Flughafen, infrastrukturelle Voraussetzungen zur Installation des Sensornetzwerks oder auch die Spannungsversorgung etc. sein.

Im Rahmen des Unterpaketes 4.2 „Erarbeitung von Empfehlungen zur strukturellen Auslegung von Netzwerken“ welches durch die WIS koordiniert wurde, sollten aufgrund der gewonnenen Erkenntnisse und Ergebnisse über den gegenwärtigen Bau- bzw. Konstruktionsstand von IT-Netzen in Flughäfen (Arbeitspaket 1.2) und der gemessenen klassifizierten Störempfindlichkeiten an einem generischen Netzwerk (Arbeitspaket 2.3) Empfehlungen zur strukturellen Auslegung von Netzwerken unter elektromagnetischen Schutzaspekten erarbeitet werden. Das Beachten dieser Empfehlungen für neu zu errichtende Netzwerke auf Flughäfen kann bereits zu einer erheblichen Reduzierung der Empfindlichkeit gegenüber transienten elektromagnetischen Störgrößen führen.

Die „Erarbeitung von Maßnahmen zur Abwehr eines Angriffes“ erfolgte im Unterpaket 4.3 und wurde von THALES, FIS und WIS bearbeitet. Hier sollten Konzepte zu passiven und aktiven Schutzmaßnahmen bei existierenden Netzen sowie zur Detektion und Ortung von durchgeführten Angriffen entwickelt und maximale Detektions- und Reaktionszeiten unter Berücksichtigung der Bezahlbarkeit definiert werden.

Das Unterpaket 4.4 „Maßnahmen zur Bewältigung von Schadensereignissen“ wurde von der FIS koordiniert. Damit eine angemessene Reaktion im Fall von Gefahr gezeigt werden kann, sollten Schulungskonzepte für das Sicherheitspersonal sowie Konzepte zur Alarmierung, Fehlerkorrekturmaßnahmen, Maßnahmen zur Bewältigung von Schadensereignissen und Konzepte für den automatischen Wiederanlauf vorhanden sein. Basierend auf den vorangegangenen Arbeitspaketen und deren Ergebnissen sollten Empfehlungen beziehungsweise Vorschläge für geeignete Schulungs- und Krisenreaktionsmaßnahmen erarbeitet werden.

Das Arbeitspaket 5 „Spektrumüberwachungssensornetz“ wurde von Netline koordiniert und war in die Unterpakete Festlegung der Spezifikationen für einen robusten Überwachungssensor des elektromagnetischen Spektrums, Sensorentwicklung, Entwicklung eines Spektrumüberwachungsnetzes durch Integration von Sensoren in einem robusten LAN-Netzwerk sowie Integration der Überwachung und der Bedrohungserkennung in den Sensor untergliedert.

Im Rahmen des Unterpaketes 5.1 sollten die Spezifikationen für einen robusten Überwachungssensor des elektromagnetischen Spektrums durch Netline und Thales definiert werden.

Die Entwicklung eines Spektrumüberwachungssensors basierend auf Breitbandempfängern, die in der Lage sind verschiedene Arten von elektromagnetischen Signalen (zum Beispiel Mobiltelefone, Radio-Dienste, Piratensender, etc.) im Frequenzbereich von 20 MHz - 3 GHz zu erkennen, sollte im Arbeitspaket 5.2 durch Netline erfolgen. Die wichtigste innovative Herausforderung dieser Arbeit besteht in der Konzeption von Sensoren, welche eine zeitliche Synchronität besitzen, um eine Ortung auf Basis vom Signallaufzeiten (TDoA, Time Difference of Arrival) durchzuführen. Des Weiteren müssen die Sensoren robust gegenüber HPEM und dennoch empfindlich genug sein, um bei einer gerichteten Antenne Signale außerhalb der Richtwirkung zu erfassen. Im Rahmen des Vorhabens „EMSIN“ wird die grundsätzliche Möglichkeit der Ortung festgestellt.

Im Zusammenhang mit dem Arbeitspaket 5.3 widmete sich Netline der Entwicklung eines Spektrumüberwachungsnetzes durch Integration von Sensoren in einem robusten LAN-Netzwerk.

Während in Arbeitspaket 5.4 die Integration der Überwachung und der Bedrohungserkennung in den Sensor durch Netline und die LUH vorgenommen werden sollte. Hier sollte die Integration der Algorithmen aus den Arbeitspaketen 7.1 und 7.2 in den Sensor erfolgen. Nach dieser Integration sollte der Sensor in der Lage sein, eine Bedrohung zu erkennen und zu detektieren.

Das Arbeitspaket 6 „Kontroll- und Management-Software für das Spektrumüberwachungssensornetz“ wurde ebenfalls von Netline koordiniert und war in die beiden Gliederungspunkte Softwarekonzeption und Validierung der Benutzerschnittstelle unterteilt.

Im Rahmen des Arbeitspaketes 6.1 „Softwarekonzeption“ sollte die Erarbeitung einer Kontroll- und Management-Software für das Sensor-Netzwerk erfolgen. Die Software sollte die Flughafenkarte mit einem Überblick über die verschiedenen Bereiche des Flughafens und mit dem Zustand der einzelnen Gebiete darstellen (zum Beispiel grüne Meldeleuchte für normalen Zustand und rot bei Alarmsituationen). Im Falle einer Alarmmeldung sollte ein Dialogfenster mit dem Gebiet, in dem der Alarm ausgelöst wurde, erscheinen, das den Status aller installierten Sensoren in der Umgebung anzeigt. Darüber hinaus sollten detaillierte Messwerte der Alarmursache zur weiteren Analyse dargestellt werden.

Im Arbeitspaket 6.2, welches von FIS koordiniert wurde, sollte die Validierung Benutzerschnittstelle erfolgen. Hierzu sollten die Spezifikationen der Benutzerschnittstelle analysiert und das fertige System für den späteren Praxiseinsatz verifiziert werden. Hierbei sollten insbesondere die Bedienerfreundlichkeit und die Akzeptanz des Sicherheitspersonals und der Flughafenbetreiber beachtet werden und darüber hinaus auch arbeitsmedizinische und arbeitsprozessbezogene Aspekte sowie die rechtlichen Anforderungen aus dem Datenschutz berücksichtigt werden.

Das Arbeitspaket 7 „TDOA-basierte Ortung der Bedrohung“ wurde von Thales koordiniert und war in die Unterpakete Überwachung, Erkennen von Bedrohungen, Ortung nach dem TDOA-Prinzip (Time Difference of Arrival) sowie Integration mit dem Sensornetz unterteilt.

Im Unterpaket 7.1 „Überwachung“, koordiniert von der LUH, sollten anhand der für diese Art von Störern charakteristischen Parameter nach Arbeitspaket 1.3.2 die Leistungsdaten eines realisierbaren High Power Electromagnetic / Ultrawide Band – Pulse (HPEM/UWB)-Warnsensors abgeleitet werden. Eine besondere Herausforderung stellen dabei die extrem breitbandigen, transienten UWB-Impulse dar. Einerseits müssen die zu entwickelnden Antennen diese Signale aufnehmen können und andererseits dürfen die transienten Eigenschaften der Signale nicht signifikant verändert werden, damit eine Identifikation nach Arbeitspaket 1.3.2 möglich ist.

Das Unterpaket 7.2 „Erkennen von Bedrohungen“ wurde ebenfalls von der LUH koordiniert. In diesem Zusammenhang bestand die wesentliche innovative Herausforderung in der breitbandigen Erfassung der für HPEM/UWB-Bedrohungen typischen Parameter und die sichere Trennung von für Flughäfen typischen Feldsignalen (Handy, Radar, Funkdienste) im Normalbetrieb und einem Angriff. Aus den Arbeitspaketen 1.2.1, 1.3.1 und 1.3.2 sollten diese Daten vorliegen. Die hierfür benötigten mathematischen Operationen (Signalanalyse) sollten in Software und/oder Hardware abgebildet und auch auf eine Ortung eines identifizierten Störers ausgerichtet werden. Der störungsarme Betrieb in der elektromagnetischen Umgebung eines Flughafens als auch die Bedienung durch nicht fachkundiges Personal waren weitere Randbedingungen der Entwicklung.

Koordiniert durch Thales sollte im Unterpaket 7.3 „Ortung nach dem TDOA-Prinzip (Time Difference Of Arrival)“ die Entwicklung des Ortungsalgorithmus in einer Multisensorumgebung erfolgen. Der Ortungsalgorithmus muss robust und präzise mit den verschiedensten Bedingungen umgehen können, u.a. Signalreflexionen oder Störungen. So ergibt eine Messungenauigkeit oder Verfälschung von 10 ns einen Ortungsfehler von ca. 3 m. In diesem Zusammenhang sollte eine Software zur Kontrolle und Einstellung des Ortungsservers erarbeitet werden. Die Definition der Positionierung der Sensoren und der Abdeckung in Abhängigkeit von der Umgebung sollte ebenfalls durchgeführt werden.

Das Unterpaket 7.4 „Integration mit dem Sensornetz“ wurde von Thales koordiniert. Im Rahmen dieses Arbeitspaktes sollten die Integration des Algorithmus mit den Sensoren und die Kopplung mit der Management-Software des Ortungssystems erfolgen. Des Weiteren die Ortung der erkannten Sender, die eine Bedrohung darstellen. In diesem Zusammenhang sollen die Positionen an die Kontroll- und Managementsoftware (Arbeitspaket 6) übergeben werden. Ebenso wie die Darstellung der Position des identifizierten Verursachers.

Das achte Arbeitspaket „Technische Schutzelemente“ wurde von der WIS koordiniert und beinhaltete die Unterpakete: Leistungsspezifikation technischer Schutzelemente, Konstruktive Umsetzung / Auswahl technischer Schutzelemente sowie Bau von Technologiedemonstratoren / Nachweisführung.

Im Unterpaket 8.1 „Leistungsspezifikation technischer Schutzelemente“ welches von der WIS koordiniert wurde, sollten basierend auf dem im Arbeitspaket 4 erarbeiteten technischen Schutzkonzept und unter Einbeziehung der Ergebnisse der Arbeitspakete 2.2 und 2.3 technische Anforderungen an zum Bespiel Schaltzeiten oder Stromspitzenwerte für Schutzelemente zum Schutz vor leitungsgeführten und gestrahlten Störungen abgeleitet werden. Die Vorgaben sollten in Bezug auf eine spätere Verwertbarkeit hin optimiert werden.

Das Unterpaket 8.2 „Konstruktive Umsetzung / Auswahl technischer Schutzelemente“ wurde von der LUH koordiniert. Basierend auf den in den Arbeitspaketen 1.2.2 und 3.1.2 identifizierten empfindlichen Baugruppen und Geräten sowie den nach Arbeitspaket 3.1.1 bekannten Störgrößen am Objekt, sollte in diesem Zusammenhang ein angepasster Schutz für diese sensitiven Elemente erarbeitet werden.

Im Rahmen des Arbeitspaketes 8.3 „Bau von Technologiedemonstratoren / Nachweisführung“ welches durch die WIS koordiniert wurde, sollten für die im Arbeitspaket 5.2 erarbeiteten Schutzelemente Demonstratoren gefertigt werden. Die Schutzwirkung sollte anhand von Messungen am generischen Testnetz (Arbeitspaket 2) nachgewiesen werden. Am Beispiel eines existierenden Netzwerkes sollte die Integrierbarkeit in reale Netzwerke untersucht werden.

Das Arbeitspaket 9 „Bewertung anwenderrelevanter Fragestellungen inklusive Zuständigkeiten und rechtlicher Rahmenbedingungen“ wurde von der FIS koordiniert und von Frau Dr. Aigner-Hof (Unterauftragnehmerin der LUH) bearbeitet.

Der Projektplan sah für dieses Arbeitspaket folgende Gliederungspunkte vor: Zusammenstellung der einschlägigen Vorgaben und Regelwerke; Anlage einer tabellarischen Übersicht zu den der rechtlichen Bewertung zugrunde liegenden Ausgangslagen, Standardsituationen und deren Modifikationen. Erste rechtliche Bewertung der Ausgangslagen; Übersicht der relevanten Kompetenzverteilung zwischen öffentlichen und privaten Stellen. Beurteilung von Standardsituationen; Erstellung einer Übersicht zum verfügbaren rechtlichen Instrumentarium an Hand der bis dahin beurteilten Ausgangslagen und Standardsituationen (Eingriffsbefugnisse, Ansprüche u.ä.); Rechtliche Beurteilung von Ausgangslagen, Standardsituationen und ihren Modifikationen im Hinblick auf Privatrecht, Öffentliches Recht, Strafrecht unter Einbeziehung von Telekommunikationsrecht und Datenschutzrecht; Gesamtbeurteilung unter Einbeziehung von speziellen technikrechtlichen, von Vorgaben des Europarechts und des internationalen Rechts sowie die abschließende rechtliche Beurteilung anhand der bis dahin vorgelegten Ergebnisse der anderen Arbeitsgruppen.

Im Teilprojekt „Anforderungsanalyse und grundlegende Untersuchung der Einsatzmöglichkeiten von Schutzsystemen“ war es die Vorgabe, dass nach 18 Monaten Projektlaufzeit das prozess- und technologieseitige Anforderungsprofil an das zu erstellende System, an die Benutzerschnittstelle und an den entsprechenden Sicherheitsprozess formuliert ist.

Im Rahmen dieses Teilprojektvorhabens wurden Teile der Arbeitspakete Analyse der Gefährdung, Verfahren zur Analyse der Gefährdung und der Schadensausbreitung, Empfehlungen zur strukturellen Auslegung von Netzwerken (technische Schutzkonzepte), Kontroll- und Management-Software für das Spektrumüberwachungssensornetz sowie Bewertung anwenderrelevanter Fragestellungen inklusive Zuständigkeiten rechtlicher Rahmenbedingungen bearbeitet. Im Folgenden ein Überblick über die Verteilung der Arbeitspakete über die Projektlaufzeit:

1. Jahr				2. Jahr				3. Jahr			
Q1	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.2.1											
1.4											
							3.2.3				
	4.1										
						4.3					
						4.4					
				6.2							
9.1											
	9.2										
		9.3									
			9.4								
				9.5							
								9.6			
										9.7	

Abbildung 3: Projektplan FIS GmbH

Im Einzelnen wurden in diesem Teilprojekt folgende Arbeitspakete bearbeitet:

- AP 1.2.1 Bestandsaufnahme IT-Netze
- AP 1.4 Erfassung verfügbarer Sicherheitssysteme
- AP 3.2.3 Analyse eines bestehenden IT-Netzes
- AP 4.1 Erfassung organisatorischer und technischer einschränkender Randbedingungen
- AP 4.3 Erarbeitung von Maßnahmen zur Abwehr eines Angriffes
- AP 4.4 Konzeptvorschläge für Schulung und Krisenreaktion
- AP 6.2 Validierung Benutzerschnittstelle
- AP 9.1 Zusammenstellung der einschlägigen Vorgaben und Regelwerke
- AP 9.2 Anlage einer tabellarischen Übersicht zu den der rechtlichen Bewertung zugrunde liegenden Ausgangslagen, Standardsituationen und deren Modifikationen. Erste rechtliche Bewertung der Ausgangslagen
- AP 9.3 Übersicht der relevanten Kompetenzverteilung zwischen öffentlichen und privaten Stellen. Beurteilung von Standardsituationen
- AP 9.4 Erstellung einer Übersicht zum verfügbaren rechtlichen Instrumentarium an Hand der bis dahin beurteilten Ausgangslagen und Standardsituationen (Eingriffsbefugnisse, Ansprüche u.ä.)
- AP 9.5 Rechtliche Beurteilung von Ausgangslagen, Standardsituationen und ihren Modifikationen im Hinblick auf Privatrecht, Öffentliches Recht, Strafrecht unter Einbeziehung von Telekommunikationsrecht und Datenschutzrecht
- AP 9.6 Gesamtbeurteilung unter Einbeziehung von speziellen technikrechtlichen, von Vorgaben des Europarechts und des internationalen Rechts
- AP 9.7 Abschließende rechtliche Beurteilung anhand der bis dahin vorgelegten Ergebnisse der anderen Arbeitsgruppen

Nachfolgend die Aufzählung der wichtigsten Ergebnisse:

Im Rahmen des Arbeitspaketes 1 „Analyse der Gefährdung“ wurde das Unterpaket 1.2.1 „Bestandsaufnahme des Aufbaus typischer IT-Netze und Kommunikationsfrequenzen an Flughäfen“ bearbeitet. In diesem Zusammenhang wurde im Kontext des Unterarbeitspaketes 1.2 „Analyse des aktuellen Baustandes elektronischer Infrastruktur“ in Zusammenarbeit mit den technischen Projektpartnern, sowie ausgewählten Endanwendern, eine Bestandsaufnahme der an Flughäfen typischen IT-Netze und Kommunikationsfrequenzen erstellt.

Am Beispiel Flughafen wurden die für Verkehrsinfrastrukturen typischen Installationen einschließlich der zum Flughafenbetrieb notwendigen Frequenzbänder aufgenommen und charakterisiert. Die Bestandsaufnahme diente als Basis für den Aufbau eines Testnetzwerkes (Arbeitspaket 2) und für die Analyse in späteren Arbeitsschritten (Arbeitspakete 1.3.1, 3.2.1, 4.1).

Zu diesem Zweck wurden durch die technischen Partner Messungen am Flughafen durchgeführt. Ziel der Messkampagne waren die Ermittlung und Aufnahme des vorhandenen Spektrums, Feldmessungen, Messungen am Niederspannungsversorgungsnetz und die Messung der Mantelströme von Netzwerk und Telekommunikationsnetz. Des Weiteren wurden mit Hilfe der Messungen die typischen Installationen und die zum Flughafenbetrieb notwendigen Frequenzbänder aufgenommen.

Ergänzend zu den Messungen wurden IT-Netze und kritische Infrastruktursysteme erfasst, die durch unbeabsichtigte und beabsichtigte elektromagnetische Störungen in ihrem Betrieb beeinträchtigt werden könnten und deren Ausfall oder Störung einen negativen Einfluss auf die reibungslosen Abläufe am Flughafen hätte. Bei der Entwicklung von Bedrohungsszenarien im weiteren Projektverlauf wurde auf diese Komponenten ein besonderes Augenmerk gerichtet.

Die FIS GmbH fungierte in diesem Zusammenhang als Bindeglied zwischen den Projektpartnern und den Endanwendern im Projektbeirat. Auf diese Weise konnten die Fragen- und Checklisten der technischen Partner bezüglich der relevanten Komponenten der typischen IT-Netze abgearbeitet werden. Die Mitglieder des Beirats standen den Projektpartnern während der gesamten Projektlaufzeit und insbesondere während der Projekttreffen, aber auch im Rahmen von speziellen Ortsbesichtigungen und Experteninterviews, zur Klärung offener Fragen zur Verfügung.

Auf die Organisation zweier ursprünglich geplanter Workshops zur Einbindung weiterer Endanwender wurde aufgrund zwischenzeitlich negativer Berichterstattung über das Projekt verzichtet. Stattdessen wurde die direkte und zielgerichtete Zusammenarbeit mit den Mitgliedern des Projektbeirates intensiver gestaltet als ursprünglich geplant. Im Vordergrund standen vor allem die Anforderungen der Endanwender an die Funktionalitäten des Systems, die Bedienbarkeit und die Anbindung an das gesamte Sicherheitssystem der Infrastruktur. Auf diese Weise sollte gewährleistet werden, dass die Auslegung der Systeme den Anforderungen der Endanwender genügt und die Ergebnisse nach Projektende erfolgreich umgesetzt werden können.

Des Weiteren wurde im Rahmen des Arbeitspaketes 1 „Analyse der Gefährdung“ das Unterpaket 1.4 „Erfassung verfügbarer Sicherheitssysteme“ bearbeitet. Im diesem Kontext wurden die in den Flughafenbereichen angewendeten Luftsicherheitsmaßnahmen prozess- und technologieseitig systematisch erfasst und auf Leistungsparameter inklusive Schwachstellen bezüglich der Einbringung einer HPM-Quelle hin analysiert. Mit Hilfe dieser Vorgehensweise sollte der Bedarf an Verbesserungsnotwendigkeiten vorhandener Luftsicherheitssysteme deutlich gemacht werden, insbesondere sollten damit aber Anforderungen an zukünftige Sicherheitssysteme abgeleitet werden.

Zu diesem Zweck wurden die Kontrollmaßnahmen gemäß § 5 Luftsicherheitsgesetz (LuftSiG), es handelt sich hierbei um die Passagier- und Handgepäckkontrollen, und die Sicherheitsmaßnahmen gemäß § 8 LuftSiG, hierbei handelt es sich um die Personal- und Warenkontrollen sowie die Streifengänge des Sicherheitspersonals, genauer betrachtet. Des Weiteren erfolgte eine detaillierte Unterscheidung und Betrachtung der Sicherheitsmaßnahmen im öffentlichen Bereich sowie der Sicherheitsmaßnahmen im nicht öffentlichen Bereich eines Flughafens.

Im Rahmen der Erarbeitung eines Pflichtenheftes wurden die verschiedenen Layouts der Passagier- und Handgepäckkontrollstellen erfasst. Neben dem Layout wurden auch die Aufgaben der unterschiedlichen Positionen (Einweiser, Personenkontrollkraft, Monitorkontrollkraft und Nachschaukraft) erläutert. Des Weiteren wurden die verschiedenen Kontrollstellenlayouts der Personal- und Warenkontrolle erfasst und die Aufgaben der unterschiedlichen Positionen erläutert. Am Beispiel der Personal- und Warenkontrolle wurden außerdem die verschiedenen Prozessschritte im Einzelnen beschrieben. Zudem wurde die bei den Kontrollmaßnahmen eingesetzte Technik dargelegt sowie der rechtliche Ordnungsrahmen dargestellt und Aspekte der Arbeitsmedizin beziehungsweise Arbeitssicherheit aufgeführt.

Da nicht nur die Möglichkeit besteht eine HPM-Quelle durch Überwindung einer Sicherheitskontrollstelle in den Sicherheitsbereich einzubringen, sondern auch durch Überwindung der Einfriedung des Flughafens, wurden zusätzlich die Streifengänge des Sicherheitspersonals auf dem Flughafengelände in die Betrachtung einbezogen und die Randbedingungen dieser Sicherheitsmaßnahme beleuchtet.

Das erarbeitete Pflichtenheft wurde an alle Projektpartner verteilt und im Rahmen der Projekttreffen erfolgte eine fortlaufende Rückkopplung der Erkenntnisse mit allen am Verbundprojekt beteiligten Partnern. Die Arbeitspakete 1.2.1 und 1.4 wurden entsprechend der ursprünglichen Planung abgeschlossen und im weiteren Projektverlauf fortlaufend ergänzt und überarbeitet.

Im Rahmen der weiteren projektbezogenen Arbeiten stellte die WIS einen HPM-Koffer zur Verfügung mit dessen Hilfe getestet werden konnte inwieweit die Möglichkeit besteht, dass ein HPM-Koffer die Sicherheitskontrollen an einem Flughafen überwinden und unbeachtet in den Sicherheitsbereich eingebracht werden kann. Daher wurde das Pflichtenheft um die Röntgenbilder eines HPM-Koffers sowie dessen Realbilder und die entsprechenden sicherheitsrelevanten Bewertungen ergänzt.

In diesem Zusammenhang wurde deutlich, dass im Rahmen der Röntgenkontrolle mit Hilfe der Gepäckprüfanlage, die über unterschiedliche Bilddarstellungsarten zur Identifizierung von gefährlichen Gegenständen verfügt, beim Durchleuchten des HPM-Koffers, aufgrund der materiellen Beschaffung der typischerweise in einer HPM-Quelle verwendeten Komponenten, ein signifikantes Röntgenbild entsteht. Aufgrund dieses Röntgenbildes und der geltenden Sicherheitsbestimmungen müssen auf jeden Fall weitergehende Untersuchungen des HPM-Koffers eingeleitet werden und somit kann das unerkannte Einbringen eines HPM-Koffers in den Sicherheitsbereich ausgeschlossen werden.

Wie geplant erfolgte keine direkte Beteiligung der FIS am Arbeitspaket 2 „Testnetzwerk“. Im Rahmen des Arbeitspaketes 3 „Verfahren zur Analyse der Gefährdung und Schadensausbreitung wurde im Kontext von Unterarbeitspaket 3.2.3 die „Analyse eines bestehenden IT-Netzes“ unterstützt. Hierzu wurde das bestehende IT-Netzwerk eines Flughafens mit Hilfe der im Arbeitspaket 3.2.2 erarbeiteten Analysemethode in Bezug auf die Gefährdung durch elektromagnetische Störer bewertet. Die Ergebnisse wurden dann mit den im Arbeitspaket 1.2.3 durchgeführten Abschätzungen verglichen.

Im Rahmen der Durchführung der Analyse, die auf den Erkenntnissen aus Arbeitspaket 1.2.1 basierte und mit Hilfe der erarbeiteten Analysemethode durch die Projektpartner anhand eines bestehenden IT-Netzwerks des Flughafens bezüglich der Gefährdung hinsichtlich elektromagnetischer Störer durchgeführt wurde, ergaben sich weitergehende wichtige Fragen und Klärungspunkte, die systematisch erfasst wurden. Durch die FIS GmbH erfolgte in Zusammenarbeit mit den Endanwendern aus dem Beirat die Klärung der offenen Punkte ähnlich wie in AP 1.2.1 bereits geschehen durch die Übermittlung von Fragebögen sowie die Durchführung von Ortsbesichtigungen und Experteninterviews.

So musste beispielsweise geklärt werden, welche Netze auf Flughäfen verfügbar sind und ob das EMSIN-Sensorsystem in vorhandene Netzwerke eingebunden werden darf. Des Weiteren war zu klären, welche Netzwerktechnologien flächendeckend an Flughäfen vorhanden sind und welche Datenübertragungskapazitäten für das EMSIN-Sensorsystem verfügbar sind. Zudem musste geklärt werden inwieweit das EMSIN-Sensorsystem an einem sicherheitskritischen Netz betrieben werden kann und ob Reserven bei den Netzwerkleitungen vorhanden sind, die für das EMSIN-Sensornetz genutzt werden können. Abschließend mussten noch Fragen bezüglich der an Flughäfen verwendeten Baumaterialien und deren Leitfähigkeit geklärt werden.

Im Rahmen der Experteninterviews, der Beantwortung der Fragebögen und der entsprechenden Ortstermine erfolgte außerdem die Rückkopplung mit den Beiratsmitgliedern bezüglich einer Einschätzung der eventuell von einer elektromagnetischen Störung betroffenen Systeme an Flughäfen. Auf eine genaue Beschreibung der Ergebnisse wird an dieser Stelle aus Sicherheitsgründen verzichtet. Das Arbeitspaket 3.2.3 wurde planungsgemäß abgeschlossen.

Im Arbeitspaket 4 „Empfehlungen zur strukturellen Auslegung von Netzwerken (technische Schutzkonzepte) erfolgte eine Beteiligung der FIS in den Unterarbeitspaketen 4.1 „Erfassung organisatorischer und technischer einschränkender Randbedingungen“, 4.3 „Erarbeitung von Maßnahmen zur Abwehr eines Angriffes“ und 4.4 „Konzeptvorschläge für Schulung und Krisenreaktion“.

Im Rahmen des Arbeitspaketes 4.1 erfolgte die „Erfassung organisatorischer und technischer einschränkender Randbedingungen“, die eine Grundlage für die zu erarbeitenden Empfehlungen zur strukturellen Auslegung von Netzwerken darstellen, wobei die FIS die Erfassung der organisatorisch einschränkenden Randbedingungen übernahm und Thales für die Erfassung der technisch einschränkenden Randbedingungen verantwortlich war.

Bei der Erfassung der organisatorisch einschränkenden Randbedingungen musste insbesondere geklärt werden, welche Organisationsstrukturen der Konzeption von Netzwerken einschränkend entgegenstehen beziehungsweise bei der Neukonzeption eines solchen Netzwerkes beachtet werden müssen. Damit wurde gewährleistet, dass das Netzwerk den Anforderungen der zukünftigen Arbeitsumgebung entspricht und die Ergebnisse nach Projektende erfolgreich umgesetzt werden können.

Besondere Berücksichtigung bei der Erfassung der organisatorisch einschränkenden Randbedingungen durch die FIS fanden daher unter anderem die vorhandenen Organisationsstrukturen, in die sich das neu konzipierte System einfügen muss. Hierbei sind beispielsweise die Kommunikationswege zwischen dem Sicherheitspersonal und den zuständigen öffentlichen Organen (wie zum Beispiel der Bundespolizei) zu nennen sowie die unterschiedlichen Zuständigkeiten von verschiedenen Sicherheitsorganen am Flughafen zu beachten. Zu diesem Zweck wurden im Zusammenhang mit der Bearbeitung dieses Arbeitspaketes verschiedene Szenarien entwickelt, die innerhalb und außerhalb eines Flughafens stattfinden können und begründet durch die organisatorischen und technischen sowie insbesondere gesetzlichen Randbedingungen unterschiedliche Herausforderungen an die involvierten Sicherheitsorgane und die verwendete Technik stellen.

Hierbei sind neben den spezifischen Anforderungen des späteren Einsatzbereichs sowie den spezifischen Anforderungen an die Technikkomponenten und das Prozessdesign auch die Anforderungen aus den mitarbeiterbezogenen Themenfeldern zu beachten. In diesem Zusammenhang ist vor allen Dingen die Mensch-Maschine-Schnittstelle des neuen Sensorsystems entscheidend. Neben dem Arbeits- und Gesundheitsschutz sind auch Themen wie Aus- und Weiterbildung sowie Gewährleistung von Sicherheitsstandards zu klären. Bei der Entwicklung des EMSIN-Sensorsystem war hier vor allen Dingen darauf abzuzielen, dass eine schnelle und präzise Ortung der Störquelle beziehungsweise des Störers durch den Sensor und das Sicherheitspersonal aber ohne Beeinträchtigung von unbeteiligten Personen von statten geht und auf diese Weise das EMSIN-Sensorsystem einen Beitrag zur Erhöhung des Sicherheitsniveaus leisten kann.

Ein besonderes Augenmerk muss auf die spätere Bedienbarkeit des Systems gerichtet werden. Vorrangig muss eine neue Technologie- beziehungsweise Sicherheitsprozessinnovation eine zuverlässige Arbeit des Sicherheitspersonals gewährleisten. Dennoch sollte es nach Möglichkeit auch zu einer Steigerung der Effizienz und der Wirtschaftlichkeit bei allen Systempartnern kommen. Vor allen Dingen sollte daher im Zusammenhang mit der Technologieinnovation auf die Ausgestaltung der Mensch-Maschine-Schnittstelle geachtet werden, denn nur wenn die Bedienerfreundlichkeit gewährleistet ist, kann die Technik zuverlässig arbeiten. Je komplizierter die eingesetzte Technologie oder der durchzuführende Prozess ist, desto schwieriger wird es für das Sicherheitspersonal, zuverlässig zu arbeiten.

Durch Beachtung der einschränkenden organisatorischen Randbedingungen wird gewährleistet, dass das Sicherheitsnetzwerk im zukünftigen Einsatzgebiet optimal genutzt werden kann. Nur unter Berücksichtigung aller einschränkenden Randbedingungen kann eine optimale Verwertung gewährleistet werden.

Hierzu zählen neben den organisatorisch einschränkenden Randbedingungen auch die technisch einschränkenden Randbedingungen. Die technisch einschränkenden Randbedingungen für den Schutz und für die Maßnahmen zur Abwehr eines Angriffes wurden von Thales erfasst. Hierbei können zum Beispiel die benutzten Flughafenfrequenzen, die geografische Anordnung der schutzwürdigen Bereiche, der physikalische Aufbau der Wände im Flughafen, die infrastrukturellen Voraussetzungen zur Installation des Sensornetzwerks oder auch die Spannungsversorgung am Flughafen etc. unter Umständen eine einschränkende Rolle spielen.

Basierend auf den Erkenntnissen aus dem Arbeitspaket 4.1 erfolgte im Rahmen des Arbeitspaketes 4.3 die „Erarbeitung von Maßnahmen zur Abwehr eines Angriffes“. Es wurde analysiert, wie ein Sensornetzwerk zur Detektion und Ortung von durchgeführten Angriffen in einem Flughafen aufgebaut sein muss, damit es optimal angewendet werden kann. Die Erkenntnisse der Positionierung und der räumlichen Abdeckung der Sensoren aus dem Arbeitspaket 7.3 flossen hier ebenso mit ein wie die Feststellungen aus Arbeitspaket 4.1. Es wurde eine Schätzung durchgeführt, welcher Aufwand bei einer Realisierung entsteht. Ebenso wurden die Detektions- und Reaktionszeiten bei der Konzeption des Sensornetzwerkes berücksichtigt.

Im Rahmen des Arbeitspaketes 4.3 erfolgte durch die FIS die Erarbeitung von Konzeptvorschlägen zu passiven und aktiven Schutzmaßnahmen. Zu diesem Zweck haben die FIS und Frau Dr. Aigner-Hof anhand unterschiedlicher Szenarien theoretische Ansatzpunkte und die sich daraus ergebenden rechtlichen, sicherheitsrelevanten und für Mitarbeiterschulungen dringlichen Fragestellungen mit den Projektpartnern analysiert und Ansatzpunkte für präventive Maßnahmen im Falle einer Bedrohung kritischer Infrastrukturen entwickelt.

Damit die entwickelten Szenarien allgemeinverbindlich Anwendung finden können wurden die Szenarien anhand eines Modellflughafens definiert. Die theoretischen Ergebnisse der technischen Projektpartner fanden ebenfalls Berücksichtigung bei der Erarbeitung der Konzeptvorschläge zu passiven und aktiven Schutzmaßnahmen.

Neben den rechtlichen Fragestellungen war die bauliche und infrastrukturelle Beschaffenheit des Flughafens ein sehr wichtiger Faktor bei der Entwicklung, Analyse und Bewertung von entsprechenden Szenarien. Anhand der sich daraus ergebenden Erkenntnisse wurden Handlungsempfehlungen und Maßnahmen zur Vorbeugung beziehungsweise zur Vermeidung eines HPM-Angriffs entwickelt.

Anhand des Modellflughafens wurden entsprechende Handlungsempfehlungen und Vorbeugemaßnahmen für verschiedene Bereiche am Flughafen entwickelt. Hierbei wurden neben dem öffentlich zugänglichen Bereich, die sicherheitsempfindlichen Bereiche, der Sicherheitsbereich sowie das Umfeld des Flughafengeländes in die Betrachtung einbezogen. Die Handlungsempfehlungen und Vorbeugemaßnahmen basieren dabei auf verschiedenen möglichen zukünftigen Szenarien wie zum Beispiel der Aktivierung einer HPM-Störquelle am Flughafen. Es wurden verschiedene Maßnahmen, die zur Abwehr eines Angriffs mit einer HPM-Quelle beitragen können, definiert. Die Maßnahmen wurden in präventive Maßnahmen, Reaktions- und Interventionsmaßnahmen, Sanktionsmöglichkeiten, technische Maßnahmen, organisatorische Maßnahmen und personelle Maßnahmen unterschieden. Als präventive Maßnahmen zählen beispielsweise die erhöhte Präsenz von Sicherheitskräften und der Einsatz von Sensoren im Innen- und Außenbereich. Während die Erweiterung der Liste der verbotenen Gegenstände (§ 11 LuftSiG) sowie das Erarbeiten und Anwenden eines Notfallhandlungsplans beim Einsatz des Sensors beispielsweise zu den Reaktions- und Interventionsmaßnahmen gezählt wird. Zu den Sanktionsmöglichkeiten zählt unter anderem das Eingreifen der Bundespolizei oder anderer Organe im Falle des Feststellens einer Gefährdung oder Bedrohung durch den Einsatz einer HPM-Störquelle. Technische Maßnahmen sind zum Beispiel das Anbringen von speziellen Steckdosenabdeckungen im öffentlichen Bereich oder der Einsatz von Schutzfolien. Zu den organisatorischen Maßnahmen zählt zum Beispiel die Überarbeitung der Zugangsregelungen, während personelle Maßnahmen zum Beispiel durch den Einsatz spezielle geschulter Sicherheitskräfte zum Tragen kommen können.

Aus Sicherheitsgründen wird auf die Darlegung der Maßnahmen im Einzelnen verzichtet, lediglich auf einige der Maßnahmen soll nachfolgend genauer eingegangen werden. So gibt es beispielsweise Möglichkeiten der magnetischen Abschirmung, sowohl durch die Verwendung unterschiedlicher Folienarten, als auch durch Beschichtungen, können schützenswerte Geräte sowie Bauteile nach Angaben gegen elektromagnetische Strahlungen, je nach der Höhe ihrer Frequenz, abgeschirmt werden. Zu den elektronischen Schutzmaßnahmen gehören neben den aktiven Schutzmaßnahmen, dies sind technische Lösungen wie zum Beispiel Funkgeräte mit Frequenzsprungverfahren (Frequency hopping) beziehungsweise die Verwendung von gehärteten elektronischen Geräten, auch passive Schutzmaßnahmen wie Funkdisziplin. Aber auch elektronische Gegenmaßnahmen wie Störsender (Jamming) zum Neutralisieren der Störquelle sind geeignet als Gegenmaßnahme zur Abwehr eines HPM-Angriffs. Auch die Verwendung von absorbierenden Materialien, die eine Schädigung durch „Verzögerungstechnik“ eingrenzen, zum Beispiel durch Beschichtungen oder besondere Farbanstriche, sind als Abwehrmaßnahme geeignet.

Im Rahmen von separaten Ortsterminen bei der WIS und bei THALES wurde auch der Themenbereich Schutzelemente behandelt. Es wurde bei dieser Gelegenheit darauf hingewiesen, dass die extrem kurzen Anstiegszeiten von einigen Störsignalen, deren Nachweis erschweren und diese Störsignale von Schutzelementen noch nicht wahrgenommen werden können. Die Arbeitspakete 4.1 und 4.3 wurden planmäßig abgeschlossen und fortlaufend, in Abhängigkeit von den Forschungsergebnissen der technischen Projektpartner, ergänzt.

Die FIS GmbH fungierte in diesem Zusammenhang als Bindeglied zwischen den Projektpartnern und den Endanwendern im Projektbeirat. Auf diese Weise konnten die Ergebnisse mit den Endanwendern besprochen, abgestimmt und deren Verbesserungsvorschläge und Ideen in das Projekt einfließen sowie die die spätere Einsetzbarkeit und die Akzeptanz beim Endanwender optimiert beziehungsweise sichergestellt werden. Die Mitglieder des Beirats standen den Projektpartnern während der gesamten Projektlaufzeit und insbesondere während der Projekttreffen, aber auch im Rahmen von speziellen Ortsbesichtigungen und Experteninterviews, zur Klärung offener Fragen zur Verfügung.

Auf die Organisation zweier ursprünglich geplanter Workshops zur Einbindung weiterer Endanwender wurde aufgrund zwischenzeitlich negativer Berichterstattung über das Projekt verzichtet. Stattdessen wurde die direkte und zielgerichtete Zusammenarbeit mit den Mitgliedern des Projektbeirates intensiver gestaltet als ursprünglich geplant. Im Vordergrund standen vor allem die Anforderungen der Endanwender an die Funktionalitäten des Systems, die Bedienbarkeit und die Anbindung an das gesamte Sicherheitssystem der Infrastruktur. Auf diese Weise sollte gewährleistet werden, dass die Auslegung der Systeme den Anforderungen der Endanwender genügt und die Ergebnisse nach Projektende erfolgreich umgesetzt werden können.

Im Rahmen des Arbeitspaketes 4.4 wurden von der FIS GmbH basierend auf den vorangegangenen Arbeitspaketen und deren Ergebnissen Empfehlungen beziehungsweise Vorschläge für geeignete Schulungs- und Krisenreaktionsmaßnahmen erarbeitet. Diese sind für die spätere Anwendbarkeit von entscheidender Wichtigkeit. Ein System kann nur effizient arbeiten, wenn auf eintretende Gefahren angemessen reagiert wird. Um dies zu gewährleisten, sind Krisenreaktionspläne und Schulungen der Mitarbeiter bezüglich der Bedienung des Systems und der Umsetzung der Reaktionspläne notwendig.

Damit eine angemessene Reaktion im Fall von Gefahr gezeigt werden kann, müssen Schulungskonzepte für das Sicherheitspersonal sowie Konzepte zur Alarmierung, Fehlerkorrekturmaßnahmen, Maßnahmen zur Bewältigung von Schadensereignissen und Konzepte für den automatischen Wiederanlauf vorhanden sein.

Aufgrund der Verzögerung bei den technischen Entwicklungsarbeiten zur exakten Lokalisierung einer HPM-Störquelle durch den zu entwickelnden Sensor und deren praktischer Umsetzung, wurde die Bearbeitung des Arbeitspakets zunächst auf theoretischer Basis durchgeführt.

Dieses Arbeitspaket wurde in Verbindung mit dem Arbeitspaket 9.5 (Rechtliche Beurteilung von Ausgangslagen, Standardsituationen und deren Modifikationen anhand von Privatrecht, öffentlichem Recht, Strafrecht unter Einbeziehung von Telekommunikationsrecht und Datenschutzrecht) behandelt, da bei der Konzeption von Schulungen der Mitarbeiter und auch bei der Entwicklung von Modellen zur Handhabung von Krisenreaktionen unter anderem arbeitsrechtliche Gesichtspunkte aber auch rechtliche Beurteilungen hinsichtlich der Zuständigkeiten und Eingriffsmöglichkeiten eine wichtige Rolle spielten. Daher fand in diesem Zusammenhang zwischen der FIS und Frau Dr. Aigner-Hof ein reger Informationsaustausch statt.

Um aussagefähige und praxistaugliche Konzeptvorschläge für Schulung und Krisenreaktion zu entwickeln, wurden offene Fragen mit den technischen Projektpartnern geklärt. Hierzu wurde unter anderem ein Fragenkatalog zur Beantwortung an die technischen Projektpartner übermittelt. Da sich die Erprobung eines einsatzfähigen Sensors von Seiten der Projektpartner verzögerte, war die Bearbeitung des Arbeitspaketes 4.4 zunächst auf theoretische Grundlagenforschung und Literaturrecherche beschränkt. Vorbereitende Arbeiten, wie beispielsweise die Entwicklung unterschiedlicher Szenarien unter Einbeziehung der rechtlichen Fragestellungen, auf deren Grundlage die weiteren Untersuchungen erfolgen sollten, wurden durchgeführt. Sobald die durch die technischen Partner erzielten Ergebnisse eindeutige Schlussfolgerungen zugelassen haben und die an die Partner gestellten Fragen zufriedenstellend beantwortet worden waren, konnten die entsprechenden aktiven und passiven Schutzmaßnahmen sowie präventive Maßnahmen weiter ausgearbeitet werden. Berücksichtigt werden mussten in diesem Zusammenhang auch betriebsrechtliche und betriebswirtschaftliche Gesichtspunkte.

Abschließend wurde wie folgt zwischen organisatorischen und technischen Schutzmaßnahmen unterschieden:

Als organisatorische Schutzmaßnahmen beziehungsweise Maßnahmen, die im Zusammenhang mit der Einführung der organisatorischen Schutzmaßnahmen beziehungsweise im Rahmen der Implementierung des EMSIN-Sensorsystems ergriffen werden müssen, wurden beispielsweise folgende Aktivitäten definiert: der Einsatz von Sensoren zur Ortung und Beweisführung; das Abschirmen beziehungsweise Beschichten von gefährdeten Infrastrukturen; die Modifizierung bestehender Rechtsvorschriften; die Implementierung einer mobilen Einsatztruppe zur Schadensminimierung und Einleitung von alternativen Handlungsmodulen; die Erstellung eines Notfallhandlungsplanes auch zur Panikvermeidung; die Durchführung von Spezialschulungen zur Sensibilisierung des Sicherheitspersonals und von Flughafenmitarbeitern; die Erfassung arbeitsmedizinischer und arbeitsprozessbezogener Aspekte sowie die Gestaltung des Arbeitsplatzes für die Mitarbeiter, die mit dem Sensorsystem arbeiten; die Erstellung von Schulungskonzepten für das Sicherheitspersonal; die Entwicklung von Prozessabläufen nach einem HPM-Angriff; der Einsatz von zusätzlichem Personal für zusätzliche Kontrollmaßnahmen beziehungsweise Streifengänge sowie die Erweiterung der Eingriffsermächtigungen für Sicherheitspersonal beziehungsweise Flughafenmitarbeiter.

Als technische Schutzmaßnahmen beziehungsweise Maßnahmen, die im Zusammenhang mit der Einführung der technischen Schutzmaßnahmen beziehungsweise im Rahmen der Implementierung des EMSIN-Sensorsystems ergriffen werden müssen, wurden beispielsweise folgende Aktivitäten definiert: Realisierung von Verzögerungsmechanismen in technischen Geräten etc., die einen sofortigen Totalausfall verhindern; Einführung eines visuellen und „technischen“ Alarmsignals an zentrale Krisenstelle; Aufschaltung der gesamten Überwachungstechnik der Infrastruktur; Spezialsicherung der für nicht Beschäftigte zugänglichen elektrischen Infrastruktur (Steckdosen); Entwicklung von Prozessabläufen nach einem HPM-Angriff; Erstellung eines Protokolls zum Nachweis eines HPM-Angriffs und zur Ermittlung der Schäden; Installation von präventiven Messtechniken und Meldesystemen für den Notfall sowie die Konzeption der Benutzerschnittstelle.

Aufgrund der sich verzögernden Entwicklung eines einsatzfähigen Sensors durch die technischen Projektpartner wurden von der FIS theoretische Modelle zur Schulung und Krisenreaktion erarbeitet. Ziel wird es sein, diese Modelle bei erfolgreicher Entwicklung des Sensors in praxistaugliche Konzeptvorschläge zu transferieren. Das Arbeitspaket 4.4 wurde planungsgemäß abgeschlossen.

Im Zusammenhang mit dem Arbeitspaket 5 „Spektrumüberwachungssensornetz“ erfolgte gemäß Projektplan keine Beteiligung der FIS GmbH. Das Arbeitspaket 6 „Kontroll- und Management- Software für das Spektrumüberwachungssensornetz“ war unterteilt in die Unterarbeitspakete 6.1 „Softwarekonzeption“ und 6.2 „Validierung Benutzerschnittstelle“. Das Arbeitspaket 6 wurde vom israelischen Partner Netline koordiniert und bearbeitet. Eine Beteiligung der FIS GmbH erfolgte am Unterarbeitspaket 6.2 im Rahmen der Validierung der Benutzerschnittstelle.

Ziel dieses Arbeitspaketes war die Validierung der Benutzerschnittstelle. Hierzu sollten die Spezifikationen der Benutzerschnittstelle analysiert und das fertige System für den späteren Praxiseinsatz verifiziert werden. Da es im Projektverlauf zu Verzögerungen bei der Entwicklung des Sensorsystems gekommen ist, konnte keine Bewertung des fertigen Systems stattfinden. Stattdessen wurden aufgrund theoretischer Überlegungen und anhand der Ergebnisse der vorangegangenen Arbeitspakete insbesondere unter Einbeziehung der in den Arbeitspaketen 4.3 und 4.4 erarbeiteten Maßnahmen zur Abwehr eines Abgriffes und den erarbeiteten Maßnahmen zur Bewältigung von Schadensereignissen die entsprechenden Benutzer sowie die Anforderungen an die zugehörigen Benutzerschnittstellen definiert. Die endgültige Verifizierung kann natürlich erst nach Fertigstellung des Systems erfolgen. Es wurden grundlegende Arbeiten durchgeführt, auf deren Basis die spätere Verifizierung des fertigen Systems für den zukünftigen Praxiseinsatz erfolgen soll.

Bei der Definition und der Ausgestaltung der Benutzerschnittstelle war insbesondere darauf zu achten, dass das Sicherheitspersonal im Kontrollraum zielgerichtet mit der in Arbeitspaket 6.1 entwickelten Software arbeiten kann. Hierbei galt es auch die Bedienerfreundlichkeit und die Akzeptanz des Sicherheitspersonals und der Flughafenbetreiber zu beachten. Darüber hinaus waren auch arbeitsmedizinische und arbeitsprozessbezogene Aspekte sowie die rechtlichen Anforderungen zum Beispiel aus dem Datenschutz zu berücksichtigen.

Die Benutzerschnittstelle ist für den späteren Praxiseinsatz des EMSIN-Sensorsystems von hoher Wichtigkeit. Neben den angesprochenen Aspekten ist bei der Konzeption auch auf die spätere internationale Anwendbarkeit zu achten. So kann beispielsweise eine graphisch gestaltete Benutzeroberfläche unter Umständen große Vorteile gegenüber einer sprachbasierten Oberfläche bieten.

Die im Rahmen des EMSIN-Sensorsystems verwendeten Lagebilder für die Anordnung der Sensoren sind daher besonders geeignet, um im späteren Einsatz die genaue Ortung der Störquelle zu unterstützen. Es ist denkbar, dass die entsprechenden Lagebilder an mobile Einsatzkräfte weitergeleitet werden. Gegebenenfalls ist auch eine Kopplung mit Videokamerabildern möglich. Auf diese Weise kann der Einsatz des Sicherheitspersonals optimiert und ein zeitnahes Eingreifen gewährleistet werden.

Auf Grundlage der aktuellen Entwicklungsarbeiten wurde ebenfalls eine Einschätzung bezüglich der Erfüllung der organisatorischen und technischen Randbedingungen aus Arbeitspaket 4.1 insbesondere hinsichtlich der erarbeiteten Schnittstellen getroffen. Nach heutigem Kenntnisstand wird der Arbeitsschutz und Gesundheitsschutz für Sicherheitsmitarbeiter beziehungsweise alle anderen beteiligten Personen durch den Einsatz des Sensors nicht negativ beeinträchtigt. Allerdings müssen beide Aspekte bei der Erarbeitung von Krisenreaktionsmaßnahmen Berücksichtigung finden. Aufgrund der bedienerfreundlich gestalteten Benutzeroberfläche hält sich der Aus- und Weiterbildungsbedarf des Sicherheitspersonals in Grenzen. Auf diese Weise wird eine weitere einschränkende Randbedingung entschärft.

Durch die Erweiterung der Liste der verbotenen Gegenstände, die nicht im Handgepäck mitgeführt werden dürfen, könnte die Suche nach einer HPM-Quelle beziehungsweise deren Komponenten im Rahmen der Sicherheitskontrolle von Passagieren und Personal vereinfacht werden. Durch den Einsatz des Sensors wird die schnelle und präzise Ortung der Störquelle beziehungsweise des Störers durch den Sensor und das Sicherheitspersonal ohne Beeinträchtigung von unbeteiligten Personen möglich und auf diese Weise die Sicherheit gewährleistet.

Zu klären bleibt noch, wie die Kommunikation zwischen Sicherheitspersonal und öffentlichen Organen (wie zum Beispiel der Bundespolizei) im Fall der Ortung einer Bedrohung zu organisieren ist. Des Weiteren sind die baulichen Voraussetzungen für den Einsatz der Sensortechnologie zu klären. Hierzu sind allerdings die endgültigen Parameter des EMSIN-Sensorsystems nötig, so dass eine abschließende Klärung erst stattfinden kann, wenn sich das EMSIN-Sensorsystem in der finalen Entwicklungsphase befindet. Die abschließende Bewertung der Benutzerschnittstelle konnte nicht mehr in der Projektlaufzeit stattfinden, da die entsprechenden Informationen zum Projektabschluss noch nicht vorlagen. Zu beachten ist dabei auch, ob der Sensor vorwiegend im Außen- oder Innenbereich eingesetzt werden soll, dies würde eine andere Bearbeitung der Schutzmaßnahmen zur Folge haben und ebenso die Ausgestaltung der Benutzerschnittstelle beeinflussen.

Die Benutzerschnittstelle ist die Stelle oder Handlung, mit der ein Mensch mit einer Maschine in Kontakt tritt. Im einfachsten Fall ist dies ein Lichtschalter: Er gehört weder zum Menschen, noch zur „Maschine“ (Lampe), sondern ist die Schnittstelle zwischen beiden. Damit eine Benutzerschnittstelle für den Menschen nutzbar und sinnvoll ist, muss sie auf seine Bedürfnisse und Fähigkeiten angepasst sein.

Der Erfolg eines technischen Produktes hängt nicht nur von den Faktoren Preis, Zuverlässigkeit und Lebensdauer ab, sondern auch vom Faktor Handhabbarkeit beziehungsweise Bedienungsfreundlichkeit. Idealerweise erklärt sich eine Benutzerschnittstelle intuitiv von selbst, also ohne Schulungsaufwand. Die Norm EN ISO 9241 ist ein internationaler Standard, der Richtlinien der Interaktion zwischen Mensch und Computer beschreibt. Die Teile 11-17 und 110 behandeln Aspekte der Software-Ergonomie.

Der wichtigste Gegenstandsbereich der Software-Ergonomie im engeren Sinne ist die zu optimierende Softwarenutzung an Arbeitsplätzen. Allgemein befasst sie sich mit Grundregeln und Methoden zum Entwurf sowie zur Bewertung von interaktiver Software, die möglichst optimal an die Bedürfnisse der Benutzer und die Erfordernisse der Arbeitsaufgabe anzupassen ist. Die Belastungsminderung und Handlungsunterstützung durch das System stehen im Vordergrund. Nicht ergonomisch gestaltete Programme können zu psychischen Belastungen (zum Beispiel Stress, Frustration etc.) bei den Benutzern führen.

Im Rahmen der Validierung der Benutzerschnittstelle (MMI) des EMSIN-Sensorsystems wurde vor allen Dingen auf die Benutzerschnittstelle der Firma THALES Bezug genommen. Allerdings ist diese als Test-MMI beziehungsweise Entwicklungs-MMI konzipiert, nicht für die spätere Anwendung. Aufbauend auf dieser Entwicklungs-MMI wurden in Zusammenarbeit mit THALES fünf verschiedene Anwender-MMI definiert. Bei den fünf Anwendern, die jeweils über eine gemäß den Besonderheiten ihrer Aufgabe gestalteten MMI verfügen sollten, handelt es sich um die Einsatzkraft, den Nutzer in der Leitstelle, den Administrator in der Leitstelle, Mitarbeiter für Service / Wartung sowie Mitarbeiter für Installation / Kalibrierung.

Im Rahmen der Arbeiten zum Arbeitspaket 6.2 wurden nicht nur die Anwender definiert, sondern auch ihre Aufgaben und Eigenschaften sowie ihre Funktionen bei der Erarbeitung von Empfehlungen zur Ausgestaltung der jeweiligen Benutzerschnittstellen berücksichtigt. Die entsprechenden Ergebnisse können als Leitfaden bei der Ausgestaltung der finalen Benutzerschnittstellen dienen.

Für den späteren Einsatz des Sensors ist es von großer Bedeutung, dass durch die Signalgebung beziehungsweise die Benutzerschnittstelle die Bedienerfreundlichkeit und die Akzeptanz beim Sicherheitspersonal gewährleistet werden. So kann beispielsweise das gleichzeitige Auftreten verschiedener Signale die Arbeit mit dem Gerät erschweren und so die Wahrscheinlichkeit des Erkennens von Gefahren negativ beeinflussen.

Deshalb ist bei der Konzeption der Mensch-Maschine-Schnittstelle auf eine möglichst einfache Signalgebung zu achten. Die Bedienerfreundlichkeit des Sensorsystems soll zu einer nahezu fehlerfreien Auswertung des Signals durch das Gerät beziehungsweise den Bediener beitragen. Die Auswertung der Signale muss zuverlässig, mit geringem Zeitaufwand und hoher Detektionsrate erfolgen, denn nur auf diese Weise kann zu einer Erhöhung der Sicherheit beigetragen werden. Zu viele Fehlalarme oder fehlerhafte Ortungen wirken sich negativ auf die Akzeptanz des Systems beim Sicherheitspersonal aus.

Das Arbeitspaket 6.2 wurde planungsgemäß abgeschlossen.

Im Rahmen von Arbeitspaket 7 „TDOA-basierte Ortung der Bedrohung und Arbeitspaket 8 „Technische Schutzelemente“ erfolgte planungsgemäß keine Beteiligung der FIS GmbH. Im Rahmen des Arbeitspaketes 9 erfolgte durch Frau Dr. Aigner-Hof in Zusammenarbeit mit der FIS GmbH die „Bewertung der anwenderrelevanten Fragestellungen inklusive Zuständigkeiten und rechtlicher Rahmenbedingungen“.

Das Arbeitspaket 9 war in die folgenden sieben Unterarbeitspakete unterteilt: Zusammenstellung der einschlägigen Vorgaben und Regelwerke; Anlage einer tabellarischen Übersicht zu den der rechtlichen Bewertung zugrunde liegenden Ausgangslagen, Standardsituationen und deren Modifikationen. Erste Rechtliche Bewertung der Ausgangslagen; Übersicht der relevanten Kompetenzverteilung zwischen öffentlichen und privaten Stellen. Beurteilung von Standardsituationen; Erstellung einer Übersicht zum verfügbaren rechtlichen Instrumentarium an Hand der bis dahin beurteilten Ausgangslagen und Standardsituationen (Eingriffsbefugnisse, Ansprüche u.ä.); Rechtliche Beurteilung von Ausgangslagen, Standardsituationen und ihren Modifikationen im Hinblick auf Privatrecht, Öffentliches Recht, Strafrecht unter Einbeziehung von Telekommunikationsrecht und Datenschutzrecht; Gesamtbeurteilung unter Einbeziehung von speziellen technikrechtlichen, von Vorgaben des Europarechts und des internationalen Rechts; Abschließende rechtliche Beurteilung an der Hand der bis dahin vorgelegten Ergebnisse der anderen Arbeitsgruppen.

Im Rahmen der Gesamtbewertung wurden unter anderem die Straf- und Ordnungswidrigkeitsbestände zusammengestellt und die Befugnisse privater Stellen von denen öffentlicher Stellen abgegrenzt. Zudem wurde auch die Organisationsstruktur über das Zusammenwirken von privaten und staatlichen Stellen untersucht. Insbesondere galt es zu klären, inwieweit die verschiedenen Stellen über Kompetenzen verfügen, Maßnahmen zur Eindämmung eines konkreten elektromagnetischen Angriffs zu ergreifen. Darüber hinaus galt es mögliche Schadensersatzansprüche der Störer gegen private und staatliche Maßnahmen sowie die möglichen Abwehr- und Schadensersatzansprüche gegen Störer zusammenzustellen.

Es erfolgte eine Darstellung des Gesetzes über die elektromagnetische Verträglichkeit sowie eine Begutachtung der Relevanz des Vorhabens hinsichtlich der geplanten Nachfolgeregelung der EG-Verordnung Nr. 2320/2002 als neuer zentraler europäischer Luftsicherheitsvorschrift. Des Weiteren erfolgte eine Begutachtung der Kompetenzverteilung zwischen der EG, dem Bund und den Ländern bezüglich der für das Vorhaben relevanten Rechtsgebiete.

Die FIS GmbH leistete im Rahmen des Arbeitspakets 9 zum einen Zuarbeiten bei den rechtlichen Regelungen, die sich mit den für das Projekt relevanten sicherheitsspezifischen Anforderungen befassen. Hierbei galt es beispielsweise zu klären, welche Institution für den Schutz vor elektromagnetischen Angriffen zuständig ist. Zum anderen erfolgt die Mit- beziehungsweise Zuarbeit der FIS GmbH bei der Erstellung einer Übersicht über die Kompetenzverteilung zwischen öffentlichen und privaten Stellen (Arbeitspaket 9.3). In diesem Zusammenhang wurden verschiedene mögliche Bedrohungsszenarien betrachtet. Hierbei galt es insbesondere zu klären, welche Aufgaben von den einzelnen Sicherheitsakteuren ausgeübt werden dürfen. Dies war insbesondere für die Erstellung der Konzepte zur Gefahrenabwehr entscheidend. Denn damit Notfallpläne effizient greifen können, muss bereits bei der Erstellung der Notfallpläne klar geregelt sein, welche Stelle für welche Maßnahmen verantwortlich ist. Bei der Gesamtbeurteilung in Arbeitspaket 9.6 musste hinsichtlich der Erstellung der verschiedenen Eingriffsbefugnisse nicht nur die Situation in Deutschland beachtet werden, sondern auch die speziellen Vorgaben des EU- und internationalen Rechts, da diese eventuell von der nationalen Gesetzgebung abweichende Lösungsmöglichkeiten hinsichtlich der Eingriffsbefugnisse bieten.

Im Rahmen des Arbeitspaketes 9.1 „ Zusammenstellung der einschlägigen Vorgaben und Regelwerke“ erfolgte sowohl die systematische Zusammenstellung der einschlägigen rechtlichen Vorgaben und Regelwerke als auch die Sammlung einschlägiger Literatur durch die Unterauftragnehmerin Frau Dr. Aigner-Hof. Im Rahmen des vorbereitenden Zuarbeitens wurden Frau Dr. Aigner-Hof von Seiten der FIS GmbH die sicherheitsrelevanten Gesetze und Regelwerke zur Verfügung gestellt und von Frau Dr. Aigner-Hof um weitere relevante Regelwerke ergänzt. Die zusammengestellten Regelwerke zu den verschiedenen Sachgebieten wurden in Bundesrecht, Ländergesetze, europäisches Recht und internationales Recht untergegliedert. Dabei wurde auch die Rechtsprechung zum Beispiel zum Arbeitsschutz, zum Luftsicherheitsgesetz und zur Vorratsdatenspeicherung wie auch die einschlägige Literatur (Monographien, Kommentare, Aufsätze in Fachzeitschriften) berücksichtigt.

Im Rahmen von Arbeitspaket 9.2 „Anlage einer tabellarischen Übersicht zu den der rechtlichen Bewertung zugrunde liegenden Ausgangslagen, Standardsituationen und deren Modifikationen. Erste rechtliche Bewertung der Ausgangslagen“ wurden von der FIS GmbH Frau Dr. Aigner-Hof einige Standardsituationen für Analysezwecke zur Verfügung gestellt. Es handelt sich dabei um Standardsituationen, die tagtäglich an den Passagier- und Handgepäckkontrollen an Flughäfen vorkommen können. Diese Szenarien wurden unter anderem im Pflichtenheft und während der Präsentationen im Rahmen der Projekttreffen dargelegt und den Projektpartnern vermittelt. Neben diesen tatsächlich zurzeit an deutschen Flughäfen vorkommenden Szenarien wurden zukünftig mögliche Szenarien unter Berücksichtigung des Einsatzes von HPM-Störquellen definiert. Für diese Szenarien gibt es noch keine rechtlichen Grundlagen bezüglich der Durchführung von Kontrollen. Besonders problematisch ist die Rechtslage bei verdächtigen Personen im öffentlichen Bereich innerhalb und außerhalb kritischer Infrastrukturen wie zum Beispiel Flughäfen. Frau Dr. Aigner-Hof war hier mit der Untersuchung der rechtlichen Ausgangslage und der Ermittlung von möglichen Änderungen betraut.

Im Rahmen von Arbeitspaket 9.3 „Übersicht der relevanten Kompetenzverteilung zwischen öffentlichen und privaten Stellen. Beurteilung von Standardsituationen“ wurden durch die FIS GmbH die Befugnisse privater und öffentlicher Stellen in Sicherheitsbelangen abgrenzt und die Organisationsstruktur über das Zusammenwirken der verschiedenen Sicherheitsakteure untersucht und in diesem Zusammenhang die Kompetenzen der verschiedenen Stellen herausgearbeitet.

Insbesondere musste im Rahmen der rechtlichen Bewertung geklärt werden, inwieweit die verschiedenen Stellen beziehungsweise Sicherheitsakteure berechtigt sind, Abwehrmaßnahmen zur Eindämmung eines konkreten elektromagnetischen Angriffs zu ergreifen. Die Erstellung der Übersicht über die Kompetenzverteilung zwischen öffentlichen und privaten Stellen erfolgte durch Frau Dr. Aigner-Hof unter Berücksichtigung verschiedener möglicher Bedrohungsszenarien, die bereits im Rahmen der Zuarbeiten zu Arbeitspaket 9.2 von der FIS GmbH an Frau Dr. Aigner-Hof übermittelt wurden.

Während des Arbeitspaketes 9.3 erfolgte die detailliertere Ausarbeitung der Standardsituationen. In enger Zusammenarbeit zwischen Frau Dr. Aigner-Hof und der FIS GmbH sind verschiedene Szenarien einer HPM-Bedrohung weiterentwickelt worden. Zur abschließenden rechtlichen Beurteilung dieser Standardsituationen wurden die Ergebnisse der WIS und von THALES bezüglich des effizienten Einsatzes eines Sensornetzwerks berücksichtigt. Frau Dr. Aigner-Hof und die FIS entwickelten Szenarien und Lösungsansätze auf theoretischer Basis, die bei praktischer Anwendung des Systems modifiziert werden können.

Das Arbeitspaket 9.4 „Erstellung einer Übersicht zum verfügbaren rechtlichen Instrumentarium an Hand der bis dahin beurteilten Ausgangslagen und Standardsituationen“ wurde durch die FIS GmbH durch die Erstellung einer Übersicht zum verfügbaren rechtlichen Instrumentarium an Hand der bis dahin beurteilten Ausgangslagen und Standardsituationen aus Endanwendersicht unterstützt. Auf Grund des verfügbaren rechtlichen Instrumentariums erfolgte durch Frau Dr. Aigner-Hof die Erstellung eines Risikomanagementmodells mit rechtlichen Komponenten, das bei Standardsituationen flexibel eingesetzt werden kann.

Vorläufiges Ergebnis dieses Arbeitspaketes: Aus rechtlicher Sicht ist es notwendig, einerseits das Gesamtrisiko einer Störung durch elektromagnetische Quellen und andererseits die vorbeugenden und die Störquelle aufspürenden und gegebenenfalls beseitigenden Gegenmaßnahmen in einzelne Risiken und Risikofaktoren aufzuteilen. Danach erfolgt aus juristischer Sichtweise eine: Risikoerkennung, Risikoanalyse und Risikobewertung.

Im Rahmen des Arbeitspaketes 9.5 „Rechtliche Beurteilung von Ausgangslagen, Standardsituationen und deren Modifikationen an Hand von Privatrecht, öffentliches Recht, Strafrecht unter Einbeziehung von Telekommunikationsrecht und Datenschutzrecht“ wurde die rechtliche Beurteilung aus Endanwendersicht unterstützt.

Durch den Einsatz von Sensoren soll festgestellt werden, ob bei einer bestimmten Person oder bestimmten Gegenständen wie z.B. Gepäckstücken Indizien für eine Sicherheitsgefahr bestehen. Auch insoweit ist bei den möglichen Gegenmaßnahmen und bei deren Schutzwirkung für Personen oder Gegenständen zu differenzieren.

Zur rechtlichen Beurteilung des Einsatzes von Störquellen und der Verantwortlichkeit des Störers, der eine elektromagnetische Quelle einsetzt, müssen zunächst die tatsächlichen Gegebenheiten beantwortet werden. Dabei ist zu beachten, dass die rechtliche Beurteilung auch mögliche Auswirkungen auf unterschiedliche Rechtsträger zu berücksichtigen hat. Ferner ist hinsichtlich der Störquellen und der eventuellen Gegenmaßnahmen zwischen Luftfahrzeugen, Fluggästen, Personal und unbeteiligten Dritten und deren Rechtsgütern zu differenzieren.

Hauptzweck des zu entwickelnden Sensorsystems ist das Orten elektromagnetischer Störungen, die durch terroristische Aktivitäten hervorgerufen werden. Auch sollen durch die Entwicklung spezifischer technischer und organisatorischer Gegenmaßnahmen die Weiterführung des regulären Betriebes sowie die Minimierung der Folgeschäden erreicht werden. Ferner sind die Voraussetzungen einer Haftung zu prüfen.

Die Bearbeitung der Arbeitspakete 9.6 „Gesamtbeurteilung unter Einbeziehung von speziellen technikrechtlichen, von Vorgaben des Europarechts und des internationalen Rechts“ sowie 9.7 „Abschließende rechtliche Beurteilung an der Hand der bis dahin vorgelegten Ergebnisse der anderen Arbeitsgruppen“ wurde durch die FIS GmbH endanwenderseitig unterstützt. Damit auch die Ergebnisse der anderen Arbeitsgruppen aus der Projektendphase in die abschließende rechtliche Beurteilung, die durch Frau Dr. Aigner-Hof vorgenommen wurde, einfließen konnten, erfolgte die Finalisierung der abschließenden rechtlichen Beurteilung in den sechs Monaten im Anschluss an die eigentliche Projektlaufzeit.

Alle Arbeitspakete wurden planungsgemäß abgeschlossen. Somit wurde nicht nur das Meilensteinziel nach 18 Monaten erreichen sondern auch das Teilprojekt erfolgreich abgeschlossen. Aufgrund der Ergebnisse der abgeschlossenen Arbeitspakete 1.2.1 und 1.4 sowie der Ergebnisse aus den Arbeitspaketen 4.1 und 6.2 wurde das Meilensteinziel erreicht. Dieses bestand darin, das prozess- und technologieseitige Anforderungsprofil an das zu erstellende System, an die Benutzerschnittstelle und an den entsprechenden Sicherheitsprozess zu formulieren.

Das Teilvorhaben „Anforderungsanalyse und grundlegende Untersuchung der Einsatzmöglichkeiten von Schutzsystemen“ ist im Rahmen des Gesamtprojektes „Elektromagnetischer Schutz für Verkehrsinfrastrukturen“ (EMSIN) während des Berichtszeitraums gemäß der ursprünglichen Planung im Zeitplan fortgeschritten. Kurzfristig aufgetretene zeitliche Verzögerungen konnten kompensiert werden.

Durch regelmäßige Partnertreffen von Frau Dr. Aigner-Hof und Mitarbeitern der FIS wurden die entsprechenden Themen, auch unter Einbeziehung der WIS und von THALES, sowie des Flughafen Hannovers und der DFS, bearbeitet. Da sich die Entwicklung und Erprobung eines einsatzfähigen Sensorsystems von Seiten der

Projektpartner verzögert hat, war die Bearbeitung der Arbeitspakete 4.3, 4.4 und 6.2 größtenteils auf theoretische Grundlagenforschung und Literaturrecherche beschränkt. Ebenso war die Bearbeitung der Arbeitspakete 9.1 bis 9.7 größtenteils auf die theoretischen Ergebnisse der technischen Partner beschränkt und es mussten daher die Szenarien anhand eines Modellflughafens definiert werden.

Zwei geplante große Workshops mit Endanwendern fanden nicht statt, da sich die technischen Entwicklungen verzögert haben und es des Weiteren negative Berichterstattung wegen der angeblichen militärischen Fokussierung des Projektes gegeben hatte und weitere gegebenenfalls negative Berichterstattung vermieden werden sollte. Die Meinung der Endanwender wurde im Projekt stattdessen von den Beiratsmitgliedern, der Flughafen Hannover GmbH und der Deutschen Flugsicherung GmbH, rückgekoppelt. Außerdem hatte sich die AirITSystems GmbH, die als Tochterfirma des Flughafens Hannover die IT-Infrastrukturen am Flughafen verantwortet, bereit erklärt, technische Fragen der Projektpartner zu beantworten. Die für den Workshop budgetierten Mittel wurden stattdessen für die Abstimmungsarbeiten mit dem Beirat sowie für die theoretischen Grundlagenarbeiten und die Literaturrecherche verwendet, die nötig wurden, da zum Beispiel die Szenarien nicht anhand des entwickelten Sensors konzipiert werden konnten, sondern aufgrund der Verzögerungen bei der Sensorentwicklung, auf theoretischer Grundlage anhand eines Modellflughafens konzipiert werden mussten.

Die Rückkopplung der Ergebnisse der Teilprojekte erfolgte auf den Projekttreffen, die regelmäßig alle 6 Monate stattfanden und an denen alle Projektpartner teilnahmen. Neben den Projekttreffen gab es regelmäßige Arbeitstreffen innerhalb der Arbeitspakete. Hier sind besonders die regelmäßigen Arbeitstreffen mit Frau Dr. Aigner-Hof im Rahmen der Bearbeitung des Arbeitspaketes 9 sowie Arbeitstreffen mit WIS und Thales hervorzuheben. Des Weiteren gab es zwei Treffen mit dem israelischen Partner Netline in Tel Aviv. Diese Treffen fanden am Rande der dortigen Homeland Security Conference (2010 und 2012) sowie des deutsch-israelischen Workshop zum Thema Kooperation in der zivilen Sicherheitsforschung (2012) statt.

Der Konferenzbesuch insbesondere die Vorträge zum Thema „New Generation Airport Security – Ben Gurion International Airport Security“ und „Airports of 2015“ haben dazu beigetragen, die Sicherheitsarchitektur am Ben-Gurion Flughafen kennenzulernen und die Analyse der Möglichkeiten zur Einbringung einer HPM-Waffe in den Flughafen Ben Gurion ermöglicht. Somit konnte das Arbeitspaket 1.4 „Erfassung verfügbarer Sicherheitssysteme“ um die entsprechenden Einschätzungen ergänzt werden. Aufgrund der verschärften Sicherheitsvorkehrungen kann ausgeschlossen werden, dass eine entsprechende HPM-Störquelle in den Sicherheitsbereich des Flughafens Ben Gurion eingebracht werden kann. Der Möglichkeit durch die Aktivierung einer HPM-Störquelle im Umfeld des Flughafens eine Beeinträchtigung hervorzurufen, kann nur durch den Einsatz des EMSIN-Sensorsystems entgegengearbeitet werden.

II.2 Eingehende Darstellung der wichtigsten Positionen des zahlenmäßigen Nachweises

Im Rahmen dieses Teilprojektvorhabens wurden die Arbeitspakete Bestandsaufnahme IT-Netze, Erfassung verfügbarer Sicherheitssysteme, Analyse eines bestehenden IT-Netzes, Erfassung organisatorischer und technischer einschränkender Randbedingungen, Erarbeitung von Maßnahmen zur Abwehr eines Angriffes, Konzeptvorschläge für Schulung und Krisenreaktion, Validierung Benutzerschnittstelle und Bewertung anwenderrelevanter Fragestellungen bearbeitet. Im Folgenden die Verteilung der Arbeitspakete und Ressourcen über die Projektlaufzeit:

1. Jahr				2. Jahr				3. Jahr			
Q1	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
1.2.1											
1.4											
							3.2.3				
	4.1										
						4.3					
						4.4					
				6.2							
9.1											
	9.2										
		9.3									
			9.4								
				9.5							
								9.6			
										9.7	

Abbildung 4: Arbeitsplan FIS GmbH

Arbeitspaket	**Dauer der Arbeitspakete**	**Mensch-Monate**
1.2.1 Bestandsaufnahme IT-Netze	12 Monate	6 MM
1.4 Erfassung verfügbarer Sicherheitssysteme	6 Monate	3 MM
3.2.3 Analyse eines bestehenden IT-Netzes	15 Monate	3 MM
4.1 Organisatorische und technische Randbedingungen	27 Monate	8 MM
4.3 Erarbeitung von Maßnahmen zur Abwehr eines Angriffes	12 Monate	4 MM
4.4 Konzeptvorschläge für Schulung und Krisenreaktion	12 Monate	7 MM
6.2 Validierung Benutzerschnittstelle	12 Monate	7 MM
9 Bewertung anwenderrelevanter Fragestellungen	36 Monate	6 MM
Gesamt		**44 MM**

Abbildung 5: Ressourcenverteilung FIS GmbH

Die inhaltliche Ausgestaltung der einzelnen Arbeitspakete wurde bereits im vorangegangenen Kapitel II.1 beschrieben. Neben den mit der Bearbeitung einhergehenden Personalkosten wurden lediglich Reisekosten im zahlenmäßigen Nachweis erfasst, da im Rahmen des Teilprojektes keine Materialkosten beziehungsweise F+E-Fremdleistungen angefallen sind. Die ursprünglich geplanten Budgets für die Personal- und Reisekosten wurden in der Summe eingehalten.

Auf die Organisation zweier ursprünglich geplanter Workshops zur Einbindung weiterer Endanwender wurde aufgrund der Verzögerungen bei der Entwicklung des EMSIN-Sensorsystems und aufgrund zwischenzeitlich negativer Berichterstattung über das Projekt verzichtet. Stattdessen wurde die direkte und zielgerichtete Zusammenarbeit mit den Mitgliedern des Projektbeirates intensiver gestaltet als ursprünglich geplant. Im Vordergrund standen vor allem die Anforderungen der Endanwender an die Funktionalitäten des Systems, die Bedienbarkeit und die Anbindung an das gesamte Sicherheitssystem der Infrastruktur. Auf diese Weise sollte gewährleistet werden, dass die Auslegung der Systeme den Anforderungen der Endanwender genügt und die Ergebnisse nach Projektende erfolgreich umgesetzt werden können. Entsprechend budgetierte Mittel wurden daher nicht als sonstige unmittelbare Vorhabenkosten abgerufen. Stattdessen wurden weitere Personalkosten für die Abstimmungsarbeiten mit dem Projektbeirat angesetzt.

II.3 Eingehende Darstellung der Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die Notwendigkeit und Angemessenheit der geleisteten Arbeiten ist vor allen Dingen in der endanwenderseitigen Betreuung des Projektes zu begründen. Gesamtziel des Projektes war die endanwenderseitige Unterstützung der technischen Arbeiten zum Aufbau eines Sensorsystems zum Schutz der Netzwerke von Flughäfen und anderer kritischer Infrastrukturen vor elektromagnetischen Angriffen sowie die Erstellung von Konzepten zur Anwendung des Systems. Grundlage für die Erarbeitung des Systems zum Schutz vor elektromagnetischen Angriffen war die Analyse des aktuellen Baustandes elektronischer Infrastruktur am Beispiel Flughafen sowie die Erfassung der dort verfügbaren Sicherheitssysteme. Im weiteren Projektverlauf wurden Empfehlungen zur strukturellen Auslegung von Netzwerken erarbeitet. Im Rahmen der Verifikation des Systems für den Praxiseinsatz wurde die Benutzerschnittstelle validiert. Anschließend wurden rechtliche Grundlagen, die für das Schutzsystem relevant sind, begutachtet. Im Rahmen des Gesamtprojektes konnte ein Demonstrator entwickelt werden. Mit diesem können HPM-Störquellen, die im Bereich der Sensoren zum Einsatz gebracht werden, geortet werden. Besonders wichtig für die Entwicklung des Demonstrators waren neben der Kenntnis der technischen und organisatorischen Randbedingungen auch die Kenntnisse der Anforderungen, die bezüglich der rechtlichen Rahmenbedingungen beziehungsweise bezüglich späterer Anwendung gestellt werden. Für die optimale Entwicklung des EMSIN-Sensorsystems wurden im Rahmen der bereits beschriebenen Arbeitspakete die endanwenderseitigen Erkenntnisse eingearbeitet. Die ausführliche Beschreibung der Arbeitspakete und die Beschreibung der durchgeführten Arbeiten finden sich in Kapitel II.1.

II.4 Eingehende Darstellung des voraussichtlichen Nutzens, insbesondere der Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplans

Die wirtschaftlichen Erfolgsaussichten untergliederten sich in die folgende Bestandteile: Dienstleistungen und Consulting, sowie die Vermarktung des Produktes. Ergebnisse des Projektes in Hinblick auf die Verwertung sind: Härtung elektronischer Ausrüstung, Planung störresistenter IT-Systeme sowie Konstruktion von Detektions- und Peilsensoren.

Das Wissen über HPEM/EM Bedrohungen ist selten oder nicht existent. Es existieren einige Firmen, die im Bereich EMV arbeiten, aber bislang fehlt das Know-How mit HPEM/EM- Risiken umzugehen. Es zeichnete sich daher ab, dass mit dem Projekt EMSIN hier ein entscheidender Vorteil für solche Lösungen aufgebaut wird. Der wesentliche Vorteil ist der allgemeine Lösungsansatz mit dieser Bedrohung umzugehen: die theoretischen Ansätze, um allgemein Infrastrukturen auf diese Bedrohung hin zu analysieren, die Konzeption der Schutzelemente, um einen Schutz zu erwirken sowie das Sensorsystem, um einen Angriff zu detektieren, den Angreifer zu lokalisieren und Gegenmaßnahmen einzuleiten.

Nach Abschluss des Projekts EMSIN war geplant, dass THALES die gewonnenen Erkenntnisse nutzt, um als Planungsbüro oder Consultant für Flughäfen oder Betreiber anderer kritischer Infrastrukturen Sicherheitskonzepte zu entwickeln und diese bei der Installation von kundenspezifischen Lösungen gegen elektromagnetische Bedrohungen zu beraten. Über THALES und FIS sollten die Partner bei Bedarf eingebunden werden.

Dienstleistungen und Consulting sollten die Entwicklung und Unterstützung bei der Härtung der elektronischen Ausrüstung und die Konzeption von störresistenten IT-Systemen für kritische Infrastrukturen beinhalten. Basierend auf den erarbeiteten Konzepten sollten Handlungsempfehlungen und Vorgehensweisen entwickelt werden, die unter Berücksichtigung der vorhandenen Infrastruktur der Standortspezifika, der operationellen Notwendigkeiten und der Umweltbedingungen eine Analyse der elektromagnetischen Verletzlichkeit der kritischen Infrastrukturen aufzeigen. Auf der Grundlage des aus den exemplarisch untersuchten Systemen erworbenen Wissens sollten technische Konzepte für den Schutz der Infrastruktur gegen elektromagnetische Bedrohungen entwickelt werden. Die wirtschaftliche Nutzung dieses Konzeptes sollte in Form von Beratungsleistungen der Projektpartner THALES, Universität Hannover und FIS stattfinden.

Zusätzlich sollten allgemeine Leitlinien für die Einsetzung von Schutztechnik gegen elektromagnetische Bedrohungen, wie auch für die Übernahme marktfähiger Komponenten entwickelt werden. Diese Leitlinien sollten dann von Projektpartnern THALES, Universität Hannover, WIS und FIS in Seminaren und einschlägigen Veröffentlichung genutzt werden. Es war angedacht diese Aktivitäten nach dem Projektende zu beginnen.

Ihm Rahmen der Arbeiten sollte ein Sensor für die Detektion, die Lokalisierung und die effektive Reaktion bei einer elektromagnetischen Bedrohung konzipiert werden. Spektrumüberwachungssensoren, die bisher zur Anwendung kommen, sind hochpreisige Einzelsysteme (~100 K Euro). Es ist klar, dass in zivilen Anwendungen und vor allem bei Verkehrsinfrastrukturen wie Flughäfen ein Netz von Sensoren in wesentlich größeren Mengen benötigt wird. Daher ist eine zukünftige Entwicklung von kleinen Low-Cost-Sensoren erforderlich. Bei der zukünftigen Serienentwicklung werden die gewonnenen Erkenntnisse des Vorhabens einfließen, um kostengünstige, kleine vernetzte Sensoren für zivile Anwendungen zu entwickeln.

Das System soll auf gepulste RF- und Mikrowellensignale (HPM) sowie sehr kurze Einzelpulse (z.B. UWB) ansprechen, als auch bei Abweichungen vom Regelbetrieb. Derzeit gibt es weder ein solches System, noch eine andere Möglichkeit sichere Angaben über den Standort des Angreifers eines elektromagnetischen Angriffs zu erhalten. Derzeit wird jede Unterbrechung mit allgemeinen technischen Störungen, Phänomenen in der Atmosphäre oder Softwareproblemen erklärt.

Das EMSIN-Sensorsystem zur Detektion soll mithilfe von statistischen und anderen Prozeduren zwischen böswilligen Angriffen und uns normal umgebenden elektromagnetischen Feldern unterscheiden und so Falschalarme vermeiden. Das Gerät selbst muss gegen elektromagnetische Interferenz gehärtet werden. Die frühzeitige Detektion elektromagnetischer Angriffe erlaubt es dem Betreiber der Infrastruktur geeignete Gegen- und Schutzmaßnahmen zu ergreifen und erhöht die Wahrscheinlichkeit den Eindringling zu identifizieren/ergreifen. Die zu ergreifenden operationellen Maßnahmen basieren auf Notfallplänen, die individuell passend zu den jeweiligen Kundenbedürfnissen erstellt werden. Idealerweise sollte das Gerät bei jeder kritischen Infrastruktur, nicht nur im Luftverkehr, genutzt werden. Eine sichere und effektive Handhabung durch weitgehende Automatisierung ist möglich. Die erwartete große Anzahl benötigter Systeme erlaubt eine wirtschaftlich optimierte Produktion der Detektionssensoren. Herstellung und Vermarktung des Systems soll durch die Projektpartner THALES, Netline und FIS durchgeführt werden. Die Verwertung des Systems durch Thales und FIS sollte hauptsächlich in Deutschland stattfinden. Die weltweite Verwertung wird in Absprache mit Netline erfolgen.

Für dieses am Anfang stehende Geschäftsfeld muss der Kunde erst sensibilisiert werden, da er sich der Bedrohung noch nicht bewusst ist und da bisher noch kein HPEM-Angriff öffentlich bekannt wurde. Aber für kritische Infrastrukturen rechtfertigt allein die Möglichkeit eines HPEM/EME Angriffes diese Investition, um Menschenleben zu schützen oder finanzielle Verluste zu vermeiden. Deshalb wird nach einer Anlaufzeit ein regelmäßiges Wachstum des Geschäftsfeldes angenommen.

Potentielle Kunden für Dienstleistungen und Consulting sind Hersteller von IT-Geräten und Systemen für zum Beispiel Flughafensicherheit und Betreiber kritischer Infrastrukturen. Potentielle Kunden für die Sensoren zur Detektion und Peilung von HPEM/EME Bedrohungen sind Flughäfen, Kernkraftwerke, Energieunternehmen und Finanzsysteme.

Im Projekt EMSIN sollte Wissen bezüglich beabsichtigter elektromagnetischer Störungen (engl.: Intentional Electromagnetic Interference(IEMI)) erarbeitet werden. Diese Kenntnisse über den Ursprung, die Ausbreitung und die Auswirkung beabsichtigter elektromagnetischer Störungen werden zu überragendem Spezialwissen führen. Zum einen die Fähigkeit IEMI-Angriffe zu detektieren und zum anderen das Spezialwissen über die Härtung und den Schutz der elektronischen Geräte und Systeme vor diesen Bedrohungen. Beide Fähigkeiten konnten bislang an anderer Stelle nicht realisiert werden. Das Know-how in diesem Bereich stellt ein Alleinstellungsmerkmal für die teilnehmenden Institutionen und Firmen dar.

Direkt nach dem Abschluss des Projektes EMSIN werden Publikationen vorbereitet, die das Bewusstsein für diese Gefahr wecken, und zum Schutz der kritischen Infrastruktur „Flughafen“ detaillierte Informationen liefern werden. Weiterhin sind Publikationen der Ergebnisse auf internationalen Konferenzen und in wissenschaftlichen Journalen wie IEEE -Transactions on EMC geplant. Die Ergebnisse sollen durch folgende Maßnahmen der Öffentlichkeit zugänglich gemacht werden: Publikationen auf nationalen und internationalen Kongressen z.B. AMEREM, IEEE EMC Conference, EMC Europe usw.; Publikationen in nationalen und internationalen Journalen z. B.: IEEE Transactions on EMC, IET Electronic Letters usw. sowie Workshops zum Thema Schutz kritische Infrastruktur bei IEMI-Bedrohung. Durch Mitarbeit in nationalen und internationalen Normungsgremien sollen die erarbeiteten Verfahren und Methoden etabliert werden.

Nach der Markteinführung der Produkte werden zusätzliche Kundenanforderungen und weitergehende Erkenntnisse zu einer weiteren Sensorsystemgeneration führen. An diese werden die Dienstleistungen und Consulting angepasst. Die Verbreitung dieser Technologie wird zwangsläufig zu einer Erweiterung des Einsatzes auch auf weniger kritische Infrastrukturen führen (Industrie und Transport). In diesem Zusammenhang ist es erforderlich, dass die technischen Parameter wie zu überwachende Frequenzbereiche und Bandbreiten diesen neuen Erfordernissen angepasst werden. Dadurch entsteht neuer Forschungs- und Entwicklungsbedarf von Universitäten und Instituten. Neue mögliche Märkte für Detektion und Peilung/Ortung könnten in den Bereichen Logistik, RFID (Funkfrequenzidentifikation) und Teile-/Güterverfolgungssysteme entstehen. Die Anforderungen dieser neuen Märkte müssen analysiert und bestimmt werden. Diese Anforderungen werden die technische Realisierung des Sensors sowie die Management-Software, die die neuen Arbeitsprozesse begleiten muss, beeinflussen. Dies könnte zu spezialisierten und kleineren Sensoren führen.

Die FIS wird im Rahmen ihrer bisherigen Tätigkeiten im Bereich der Sicherheitsberatung von Flughäfen und kritischen Infrastrukturen in Zusammenarbeit mit den Projektpartnern die Ergebnisse von EMSIN bei der Erstellung von Sicherheitskonzepten einbinden und so die Vermarktung unterstützen. Basierend auf den erarbeiteten Konzepten werden Handlungsempfehlungen und Vorgehensweisen entwickelt, die unter Berücksichtigung der vorhandenen standortspezifischen Infrastruktur, der operationellen Notwendigkeiten und der Umweltbedingungen eine Analyse der elektromagnetischen Verletzlichkeit der kritischen Infrastrukturen aufzeigen.

Auf der Grundlage des aus den exemplarisch untersuchten Systemen erworbenen Wissens werden technische Konzepte für den Schutz der Infrastruktur gegen elektromagnetische Bedrohungen entwickelt. Die wirtschaftliche Nutzung dieses Konzeptes wird in Form von Beratungsleistungen der Projektpartner THALES, Universität Hannover und FIS stattfinden. Zusätzlich werden allgemeine Richtlinien für den Einsatz von Schutztechnik gegen elektromagnetische Bedrohungen wie auch für die Übernahme marktfähiger Komponenten entwickelt. Diese Richtlinien können dann von Projektpartnern THALES, Universität Hannover, WIS und FIS in Seminaren und einschlägigen Veröffentlichungen genutzt werden.

Des Weiteren ist im Anschluss an das Projekt geplant, dass die FIS Konzepte zur Mitarbeiterschulung zum Umgang mit dem Sensorprodukt ausarbeiten wird und im Rahmen der deutschlandweiten Aktivitäten aber auch mithilfe des durch die ICTS Europe bestehenden europäischen Netzwerkes die Konzepte in Zusammenarbeit mit den Projektpartnern vermarkten wird. Die Verwertung durch die FIS erfolgt überwiegend in Deutschland, die Vermarktung wird weltweit angestrebt.

Im Rahmen der Arbeiten sollte ein Sensor für die Detektion, die Lokalisierung und die effektive Reaktion bei einer elektromagnetischen Bedrohung erarbeitet werden. Das technische Design und die Konzeption des Sensors werden aus dem Ergebnis des Technologiedemonstrators für ein Detektions- und Ortungsgerät, das in Echtzeit elektromagnetische Angriffe auf kritische Infrastrukturen detektiert, wiedergibt und aufzeichnet, erarbeitet. Die zu ergreifenden operationellen Maßnahmen basieren auf Notfallplänen, die individuell passend zu den jeweiligen Kundenbedürfnissen erstellt werden. Idealerweise sollte das Gerät bei jeder kritischen Infrastruktur, nicht nur im Luftverkehr, genutzt werden. Eine sichere und effektive Handhabung durch weitgehende Automatisierung ist möglich. Die erwartete große Anzahl benötigter Systeme erlaubt eine wirtschaftlich optimierte Produktion der Detektionssensoren. Herstellung und Vermarktung des Systems werden durch die Projektpartner THALES und Netline durchgeführt, wobei sämtliche weiterführenden Forschungs- und Entwicklungsarbeiten bezüglich des Sensors sowie dessen Produktion in Deutschland stattfinden werden. Zusätzlich wird die FIS das Sensorprodukt in ihr Portfolio aufnehmen und mithilfe des europäischen Netzwerkes und den Kontakten zu Flughäfen und kritischen Infrastrukturen bei der weltweiten Vermarktung unterstützen.

Die prinzipielle Realisierbarkeit des EMSIN Sensor-System wurde durch die Arbeiten der beteiligten Projektpartner bereits gezeigt. Im Rahmen dieses Projektes blieb allerdings noch zu klären, inwieweit die Nachweisbarkeit verbessert werden kann. Des Weiteren ist der Herstellungsprozess noch derart zu optimieren, dass die Sensoren auch unter industriellen Bedingungen eingesetzt werden können. Erst wenn diese beiden Punkte realisiert worden sind, können die bereits erläuterten Vermarktungsstrategien Anwendung finden.

Eine separate Vermarktung von beispielsweise Krisenreaktionsmodellen und Technologie ist nur hinsichtlich der Technologie möglich, aber nicht sinnvoll. Das Sensorsystem wird nur in Kombination die volle Wirkung entfalten. Das hier erstellte Sensorsystem muss in das Gesamtsystem Flughafen oder entsprechend in einer kritischen Infrastruktur eingebunden werden.

Die derzeitigen Rahmenbedingungen erlauben keinerlei zusätzliche Komplikationen, sondern verlangen vielmehr nach intelligenten Beiträgen zur Effizienz- und Servicesteigerung. Das bedingt für die Integration des hier entwickelnden Sensorsystems ein Höchstmaß an Prozessinnovation, um den Rahmenbedingungen im Sicherheitsbereich zu genügen. Zudem ist vielfältigen nationalen, supranationalen und internationalen rechtlichen Rahmenbedingungen wie zum Beispiel dem deutschen Luftsicherheitsgesetz sowie den entsprechenden nationalen Luftsicherheitsregulierungen der anderen Staaten und den Vorgaben der Europäischen Union zu genügen und die Akzeptanz und Zulassung der nationalen Regulierungsbehörden und der späteren Nutzer ist zu erwirken.

II.5 Eingehende Darstellung des während der Durchführung des Vorhabens dem ZE bekannt gewordenen Fortschritts auf dem Gebiet des Vorhabens bei anderen Stellen

Während der Projektlaufzeit wurden dem Zuwendungsempfänger keine Fortschritte auf dem Gebiet des Vorhabens bei anderen Stellen bekannt.

Das im Projekt „EMSIN“ entwickelte Sensorsystem ist einzigartig und wurde noch nicht von anderen Stellen realisiert.

II.6 Eingehende Darstellung der erfolgten / geplanten Veröffentlichungen des Ergebnisses nach Nr.11

Ziel des Teilprojektes war die endanwenderseitige Unterstützung der technischen Arbeiten zum Aufbau eines Sensorsystems zum Schutz der Netzwerke von Flughäfen und anderer kritischer Infrastrukturen vor elektromagnetischen Angriffen sowie die Erstellung von Konzepten zur Anwendung des Systems, insbesondere im Bereich Prävention, Abwehr und Bewältigung von Stör- und Schadwirkungen.

Da die einzelnen Arbeitspakete sicherheitsrelevante Informationen enthalten, die nicht veröffentlicht werden dürfen, wurde im Rahmen des Teilprojektes auf die Veröffentlichung von Ergebnissen verzichtet und lediglich die Veröffentlichung der Ergebnisse der anderen Teilprojekte beziehungsweise die Veröffentlichung der Ergebnisse des Gesamtprojektes unterstützt.