Ansatz und Risikoanalyse für ein Smart Object Network im Krankenhaus

Martin Sedlmayr[1], Andreas Becker[1], Ulli Münch[2], Fritz Meier[2], Hans-Ulrich Prokosch[1], Thomas Ganslandt[1]

Lehrstuhl für Medizinische Informatik
Friedrich-Alexander Universität Nürnberg Erlangen
Krankenhausstraße 12
91054 Erlangen
martin.sedlmayr@imi.med.uni-erlangen.de

Fraunhofer-Arbeitsgruppe für Technologien der Logistik-Dienstleistungswirtschaft ATL
Zentrum für Intelligente Objekte
Dr. Mack-Straße 81
90762 Fürth

Abstract: Radio Frequency Identification (RFID) ist eine etablierte Technologie zum Identifizieren und Lokalisieren von Objekten. Drahtlose Sensornetzwerke gehen einen Schritt weiter, indem sie über Sensoren aktiv ihre Umwelt wahrnehmen und Informationen weitervermitteln können. Dieser Beitrag beschreibt die Entwicklung eines Sensornetzwerks zum Einsatz im Krankenhaus. Dabei soll auf Basis derselben Infrastruktur (Hardware, Schnittstellen, Software) verschiedene Einsatzszenarien unterstützen werden, so dass der Nutzen der Technologie maximiert und die Investition gerechtfertigt werden können. Am Beispiel zweier Szenarien (Gerätemanagement, Bluttransfusionen) wird die Flexibilität des Ansatzes demonstriert. Ein besonderer Schwerpunkt wird auf die Risikoanalyse des Systems gelegt.

1 Einleitung

Durch die zunehmende Marktorientierung von Kliniken und Krankenhäusern wächst der Bedarf, Arbeitsabläufe und den Einsatz von Betriebsmitteln im Hinblick auf eine Steigerung der Effizienz und Qualität kontinuierlich zu optimieren. Von besonderem Interesse sind hierbei Materialien, deren Einsatz mit Risiken verbunden ist (z.B. Fehltransfusion oder bakterielle Kontamination von Blutprodukten) sowie mobile medizintechnische Geräte, deren Lokalisierung innerhalb des Krankenhauses für Wartungs- und Einsatzzwecke mit einem hohen personellen Aufwand verbunden ist. So werden durchschnittlich 30 Minuten einer Schicht des medizinischen Personals für die Suche nach benötigten Geräten verwendet. Jährlich bleiben dabei bis zu 10% des Inventars unauffindbar [Gl04]. Von 4,5 Millionen Blutspenden werden bis zu 5% wegen Fehlplanungen oder Unbrauchbarkeit entsorgt, weil beispielsweise die Einhaltung der Kühlkette eines Blut-

beutels, der zwischen 100 und 400 Euro kosten kann, nicht ausreichend nachgewiesen werden kann [Ki06]. Zudem werden mit einer Häufigkeit von 1:400-1:10.000 die Empfänger von Konserven verwechselt, wobei jede dritte Verwechslung gefährlich inkompatibel ist [Sh07, Dz07a]. Eine eindeutige Identifikation der Blutkonserven und die verbesserte Dokumentation der Rücknahme ausgegebener Blutkonserven könnten einen wesentlichen Beitrag zur Senkung von Fehltransfusionen und Erhöhung der Wiederverwendung leisten.

RFID ist eine etablierte Technologie zur Identifizierung und Lokalisierung von Objekten, die in vielerlei Hinsicht zur Optimierung von Logistikprozessen beigetragen hat [MM05]. Einen Schritt weiter gehen mobile Sensornetze, bei denen intelligente Objekte ihre Umgebung mit Sensoren wahrnehmen und aktiv kommunizieren können. Den sich daraus ergebenden Möglichkeiten stehen jedoch auch Risiken bezüglich Sicherheit, Vertraulichkeit und Integrität der Daten gegenüber [Vi08].

Ziel des Projektes OPAL (Optimierte und sichere Prozesse durch mobile und intelligente Überwachung und Lokalisierung von Betriebsmitteln) ist die Entwicklung eines Sensornetzwerkes zur Verbesserung des Gerätemanagements und dem optimierten Umgang mit Blutkonserven. Der Lösungsansatz von OPAL besteht darin, Ressourcen mit so genannten „Smart Objects“, d. h. kleinen mobilen und intelligenten IT-Einheiten, auszustatten und in die vorhandene IT-Infrastruktur einzubinden. So können stets aktuelle Informationen über Standort, Zustand und Wartungszeitpunkt oder auch über Temperatur und Bewegung ermittelt werden. Ein Schwerpunkt des Projektes liegt auch in der Analyse der Risiken und Gegenmaßnahmen beim Einsatz eines Sensornetzwerkes im Umfeld OP und Intensivstation.

Der Beitrag ist wie folgt aufgebaut: Zunächst wird die zugrundeliegende RFID und Sensortechnologie und deren heutige Anwendung im Krankenhaus vorgestellt. Anschließend werden der in OPAL verfolgte Ansatz und relevante Arbeitsschritte der Umsetzung beschrieben. Da mit der neuen Technologie auch neue Risiken einhergehen, war die Risikoanalyse ein wesentlicher Schritt, der besonders gewürdigt wird. Eine Zusammenfassung und Bewertung schließt den Beitrag ab.

2 Stand der Technik

Bei RFID verwenden sogenannte Tags oder Transponder elektromagnetische Wellen um Objekte zu identifizieren und Daten zu kommunizieren [ES07]. Im Gegensatz zu Barcodes benötigt RFID dadurch keine Sichtlinie zum Auslesen der Daten und ist auch weniger anfällig gegenüber Verschmutzung oder Beschädigungen an den Aufklebern. RFID Technologie wird grob in zwei Gruppen, der aktiven und der passiven, unterschieden. Bei *passiven RFID Tags* wird die zum Auslesen benötigte Energie von außen induziert [We09], was jedoch nur auf verhältnismäßig kurze Distanz möglich ist. Zudem können aufgrund der benötigten Energiemenge medizintechnische Geräte gestört werden [To08]. Im Gegensatz dazu besitzen *aktive RFID Tags* eine eingebaute Energiequelle (Batterie), so dass die Knoten kontinuierlich Daten verarbeiten und mit geringerer Energieleistung über größere Reichweiten kommunizieren können. *Sensornetzwerke* nutzen

Tags, die mit verschiedenen Sensoren und einer lokalen Recheneinheit ausgestattet werden [Ak02]. Häufig können die Tags untereinander kommunizieren (Multi-Hop Verfahren), so dass auch unter widrigen Umständen mit geringsten Sendeleistungen fest installierte Ankerknoten erreicht werden können. Aufgrund der lokalen Intelligenz spricht man auch von Smart Object Tags bzw. Netzwerken. Ein entscheidender Vorteil gegenüber aktivem RFID besteht in der vom Tag selbst initiierten Kommunikation, während RFID Tags immer erst durch ein Lesegerät explizit aktiviert werden müssen, was beispielsweise eine kontinuierliche Lokalisation verhindert.

Hunderte Ansätze und Projekte zum Einsatz von RFID im Krankenhaus demonstrieren anschaulich die Anwendbarkeit der dieser Technologie [Wi08]. Dabei werden vier Funktionen genutzt: die Verfolgung von Objekten (Tracking), die Identifizierung und Authentifizierung, die Kommunikation von Daten sowie die Überwachung (Sensing). Diese Funktionen kommen vor allem in vier klinischen Anwendungsgebieten zum Einsatz: Patientensicherheit und Qualität der Versorgung, Management von Beständen bzw. Nachschub, pharmazeutische Anwendungen sowie Unterstützung von Patienten. Wir fokussieren im Weiteren auf zwei Gebiete, welche die spezifischen Funktionen von RFID Technologie nutzen: Bestandsmanagement (für mobile, medizinische Geräte) und Transfusionssicherheit.

Beim Bestands- bzw. Gerätemanagement hat RFID bereits seine Vorteile klar bewiesen [MM05]. Die Zeit, die zum Auffinden eines medizinischen Gerätes aufgewendet werden muss, kann durch das aktive Tracking deutlich verringert werden [Gl04]. Während passive Tags für den Warenein- und -ausgang verwendet werden, können aktive Tags auch zur kontinuierlichen Verfolgung verwendet werden. Dabei gibt es verschiedene Ansätze: Bei [Na06] werden nur wenige Objekte mit besonderem Interesse (z.B. kostspielige oder wichtige Instrumente wie Infusionspumpen oder OP-Besteck) getagged. Im großen Stil werden bei [Gl04] insgesamt 12.000 mobile Objekte mit aktiven RFID Sensoren versehen, von medizinischen Geräten bis zu Schlüsseln; den Sensorstückkosten von $15 standen dabei Einsparungen von $200.000 im ersten Jahr gegenüber.

Bei der Transfusionssicherheit liegt der Nutzen des Einsatzes von RFID in den Identifikations- und Messmöglichkeiten der Sensorknoten [Dz07a]. RFID ist hier eine Alternative zu Barcodes, die anfällig für Verschmutzungen und Beschädigungen wie Knicke und Kratzer sind [Sa06]. Beispielsweise können stationäre Lesegeräte in OP-Tische eingebaut werden, die die passiven Transponder eines Patientenarmbandes bzw. einer Blutkonserve lesen und damit den Matchingprozess unterstützen [Dz07b]. Aktive Sensorknoten könne darüber hinaus ständig die Temperatur einer Blutkonserve messen, wobei das in [Ki06] vorgestellte System wiederum den Matchingprozess nicht unterstützt.

Zusammenfassend existieren vielfältige Beispiele für den Einsatz von passiver und aktiver RFID Technologie im Krankenhaus. Jedoch werden nur spezifische Einsatzszenarien unterstützt, d.h. es gibt noch keine generische Plattform für mehrere Dienste. Zudem ist die Nutzung von RFID auf den Einsatz von Lesegeräten oder –stationen beschränkt, da eine proaktive, kontinuierliche Kommunikation nicht möglich ist. All dies kann durch Sensornetzwerke realisiert werden, die bisher jedoch noch nicht eingesetzt werden.

3 Ansatz

Im Projekt OPAL wird auf Basis eines Smart Object Netzwerks eine Serviceplattform entwickelt, die verschiedenste Dienste mit derselben Hardware und Infrastruktur realisiert. Smart Objects sind aktive Sensorknoten, die an Geräten, Material oder Patienten angebracht werden können und sich selbstständig in einem drahtlosen Netzwerk organisieren. Die Sensorknoten sind mit verschiedenen Sensoren, z.B. für Temperatur oder Bewegung, bestückt, und übermitteln ihre Werte an fest installierte Ankerknoten, welche den Übergang zum Krankenhausnetzwerk herstellen. Die Sensorknoten – und damit auch die Objekte, an denen sie angebracht wurden – können über zellenbasierte und triangulationsbasierte Algorithmen lokalisiert werden [Ro05].

Abbildung 1: Sensorknoten und Anbringung an einem Beatmungsgerät

Der OPAL Prototyp wird im OP und der Intensivstation des Universitätsklinikums Erlangen für die Szenarien Gerätemanagement und Transfusionssicherheit evaluiert werden. Die Spezifikation der Hard- und Software ist abgeschlossen und ab Sommer 2009 werden 700 Sensorknoten für mobile medizinische Geräte, Blutkonserven und Patienten ausgebracht (Abbildung 1).

Im Folgenden wird auf die Aspekte der Prozessintegration, der Gestaltung des Netzwerkes sowie die Systemarchitektur eingegangen. Dem wichtigen Aspekt der Risikoanalyse ist Kapitel 4 gewidmet.

3.1 Prozessanalyse

Zuerst wurden die bestehenden Arbeitsprozesse der beiden Szenarien, dem „Management von Blutkonserven“ und dem „Management von medizinischen Geräten“, mit Anwendern in der transfusionsmedizinischen und hämostaseologischen Abteilung und der anästhesiologischen Klinik vor Ort aufgenommen und analysiert. Für jeden Prozess wurden die beteiligten menschlichen Akteure und IT-Systeme identifiziert und die Räumlichkeiten in den jeweiligen klinischen Abteilungen besichtigt.

In einem zweiten Schritt wurden die Anforderungen an eine sensornetzwerkbasierte Lösung mit den jeweiligen Ansprechpartnern definiert und daraus die nötigen Änderungen der Arbeitsprozesse ermittelt.

Beim Szenario "Management von Blutkonserven" wurden 6 von 11 Prozessen verändert, beispielsweise wurde für das Programmieren und Anbringen der Tags an den Blutbeuteln ein neuer Arbeitsschritt eingefügt. Eine ebenfalls neue Aktivität ist die Prüfung der Richtigkeit der Zuordnung einer Blutkonserve zu einem Patienten vor der Transfusion der Konserve mit Hilfe der Smart Objects. Eine weitere Prozessänderung ergab sich durch die Möglichkeit der Temperaturmessung von Blutkonserven (Eskalation von Alarmen).

Beim Szenario Gerätemanagement ergaben sich 5 Änderungen an den insgesamt 10 identifizierten Prozessen. Ein neuer Arbeitsprozess für das Anbringen und Programmieren der Tags wurde ebenfalls benötigt. Eine weitere Prozessänderung ergab sich durch die Möglichkeit einer raumgenauen Ortung von medizintechnischen Geräten mit Hilfe der Tags.

3.2 Raumtechnische Randbedingungen und Gehäusedesign

Um die funktechnischen Eigenschaften der Räumlichkeiten zu untersuchen, wurden zwei Messreihen durchgeführt, denn Tische, Geräte oder sogar Stahltüren verhindern die Ausbreitung der Radiowellen und können Reflexionen und Interferenzen verstärken. Aufgrund der Ergebnisse konnten die Position der Ankerknoten und die Größe bzw. Geometrie der Antennen bestimmt werden. Insbesondere die Energieleistung der Sender kann auf ein unkritisch geringes Niveau eingestellt werden. Dadurch wurde auch der Einsatz batteriebetriebener, mobiler Ankerknoten möglich, was den organisatorischen Aufwand der Befestigung erheblich reduziert, denn feste Montagen finden aus hygienischen Gründen typischerweise nur einmal jährlich gebündelt statt.

Die Anforderungen und Möglichkeiten für die Gestaltung der Sensorknotengehäuse wurden erhoben. Die Gehäuse dürfen beispielsweise die normale Verwendung der Geräte nicht stören, Patientenarmbändern müssen komfortabel aber im Notfall entfernbar sein, und im Allgemeinen desinfizierbar bzw. sterilisierbar sein. Gerätetags müssen wartungsfrei bis zu zwei Jahre laufen, damit sie im normalen Prüfrhythmus der Geräte gewartet werden können. Die Gehäuse müssen so klein wie möglich sein, wobei die Größe der Batterie und der Antenne hier Grenzen setzen.

Es wurden verschiedene Gehäuseformen unter dem Aspekt wie diese an Geräten wie Beatmungsmaschinen, Patientenmonitoren und Infusionspumpen angebracht werden können diskutiert. Ergänzend wurden 10 Exemplare eines Gehäuses mit verschiedenen Montagetechniken im OP und Aufwachstation an Geräten befestigt und über 6 Wochen im Alltag beobachtet. Während die Montage an den meisten Geräten unkritisch war, stellten sich vor allem moderne, d.h. kleine, Spritzenpumpen im Rack als problematisch heraus, da kein Platz für zusätzliche Objekte vorhanden ist. Während man im speziellen Fall eine Möglichkeit über ein anderes Gehäuse schaffen konnte, wäre zukünftig die

Zusammenarbeit mit den Herstellern notwendig, um Optionen der Integration in die Gehäuse oder die Anbringung von Zusätzen (z.B. wie Kensington Lock) zu schaffen.

3.3 Systemarchitektur

Neben Anpassungen der Prozesse und dem Design der Sensorknoten sind auch Infrastrukturmaßnahmen erforderlich, um die aktiven Komponenten in das Netzwerk einzubinden und über Schnittstellen mit den IT-Systemen des Klinikums zu verbinden.

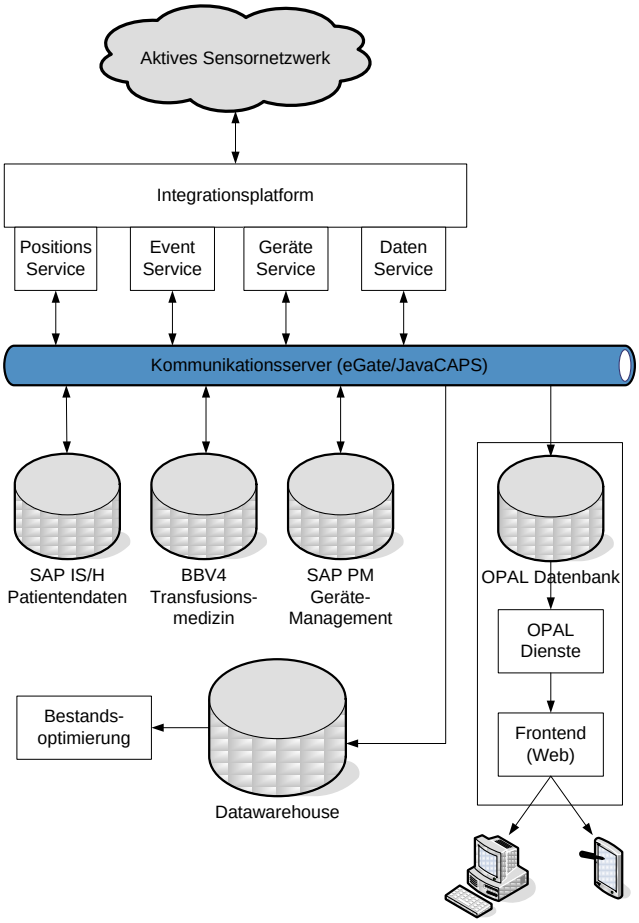

Abbildung 2: OPAL System Architektur

Insbesondere ist eine bidirektionale Kommunikation verschiedener klinischen Informationssysteme mit dem Sensornetzwerk vonnöten. Beispielsweise können Ortsinformationen im Gerätebuch aktualisiert werden oder Temperaturwerte einer Blutkonserve in die Chargendokumentation eingehen. Umgekehrt werden Zuordnungen eines Tags zu einem Gerät von der Benutzerschnittstelle auf den Sensorknoten propagiert. Abbildung 2 zeigt

die Architektur und deren Module des OPAL Systems. Jede dieser Komponenten wird im Folgenden kurz beschrieben:

- Das Smart Object Netz besteht aus intelligente Sensorknoten, die an medizinische Geräte, Blutkonserven und Patienten angebracht werden. Dies ermöglicht eine Unterstützung der beschriebenen Prozesse und die Identifizierung, Aufzeichnung und Übermittelung von Umfelddaten sowie eine relative Bestimmung der Position innerhalb des Smart Object Netzes. Fest installierte Anker- und Gatewayknoten stellen die Brücke zum Klinikumsnetzwerk bzw. der Integrationsplattform her.

- Die Integrationsplattform ist für die Kommunikation zwischen der OPAL Datenbank und dem Smart Object Netz zuständig. Hierbei werden die im Smart Object Netz generierten Nachrichten mit Informationen angereichert und via SOAP (Service Oriented Architecture Protocol) Nachrichten an die OPAL-DB übermittelt. Die Integrationsplattform bietet weiterhin die Möglichkeit, Anweisungen und Informationen an das Smart Object Netz zu übermitteln. Somit kann eine bidirektionale Kommunikation zwischen OPAL-DB und Smart Object Netz realisiert werden.

- Der Kommunikationsserver ist die zentrale Drehscheibe für Daten innerhalb des Klinikums. Das Universitätsklinikum Erlangen nutzt hierfür das Produkt eGate/JavaCAPS [We98], welches einen nachrichtenbasierten und serviceorientierten Ansatz verfolgt. Innerhalb des Projektes wird der Kommunikationsserver als Anbindung an andere Softwarekomponenten durch die OPAL-DB benutzt. Somit können Informationen aus anderen Bereichen des Klinikums leicht in das System integriert werden.

- Klinische Informationssysteme unterstützen verschiedenste Prozesse innerhalb der Klinik. Für das Projekt werden die Systeme SAP IS/H (Patientendaten), SAP PM (Bestandsmanagement, Gerätebuch) und BBv4 (Transfusionsmedizin) angebunden. Dabei werden verschiedene Kommunikationsstandards genutzt: SAP-BABI Verbindungen für Geräte, HL7 für Patientendaten und eine direkte Datenbankanbindungen an das BBv4-System für Blutbeutelinformationen.

- Die OPAL Datenbank zeichnet alle relevanten Events auf, die im Smart Object Netz generiert werden. Hierunter fallen z.B. Position, Temperatur, Matching von Blutkonserven mit einem Patienten, und das Verheiraten von Smart Objects mit medizinischen Geräten, Blutbeuteln oder Patienten. Weiterhin stellt diese die Verbindung zu anderen klinischen Informationssystemen her und bezieht dadurch Informationen, die für den einwandfreien Gebrauch des Systems notwendig sind. Um Latenzzeiten des Gesamtsystems zu minimieren und Verbindungsabbrüchen zu den anderen klinischen Informationssystemen vorzubeugen werden die benötigten Objektdaten zwischengespeichert. Regeln auf der Datenbank überwachen Grenzwerte und können Alarme eskalieren (z.B. Email oder SMS versenden).

- Das Frontend besteht aus Webseiten, die von Arbeitsstationen und mobilen Endgeräte aufgerufen werden können. Diese dienen neben der Visualisierung auch der Steuerung des OPAL-Systems und gibt dem Klinikpersonal die Möglichkeit nach mobilen Geräten zu suchen bzw. deren momentane Position anzeigen zu lassen und Informationen über die Smart Objects abzurufen.

- Ziel der intelligenten Bestandsoptimierung ist es, die Gerätebestände aus übergeordneter Sicht (Sicht des gesamten Klinikums) möglichst gering zu halten, ohne jedoch Einbußen an der Verfügbarkeit der einzelnen Geräte hinzunehmen (Qualitätslevel bleibt erhalten). Dies kann durch ein proaktives, dynamisches Ausbalancieren der reduzierten Gerätebestände erreicht werden.

- Die Warenrückverfolgung von Blutkonserven ist ein weiteres Module welches zu der Abschlussprüfung der Bluttransfusion Informationen beisteuern kann. Dies geschieht durch eine lückenlose Dokumentation der Blutbeutel von der Ausgabe in der Blutbeutelbank hin zur Transfusion.

Das OPAL System wird über eine serviceorientierte Architektur realisiert. Hierbei wird jedes Modul als Web-Service [Ne02] implementiert und seine Schnittstellen durch die Beschreibungssprache WSDL (Web Service Description Language) spezifiziert. Diese Vorgehensweise bei der Realisierung des Gesamtsystems ermöglicht die Skalierbarkeit und Übertragbarkeit auf andere Anwendungsfälle bzw. Projektpartner.

4 Risikoanalyse

Bei der Integration einer neuen Technologie in bestehende Geschäftsprozesse bzw. IT-Landschaften ist der Sicherheitsaspekt nicht zu vernachlässigen. Zwar ist eine vollständige Absicherung aufgrund der Vielfältigkeit des Themas nicht möglich, jedoch können die relevantesten Risiken und Gegenmaßnahmen identifiziert und bei der Realisierung berücksichtigt werden [BSI05]. Die in OPAL durchgeführte Risikoanalyse bestand aus drei Phasen:

- Phase 1: Identifikation von möglichen Risiken

- Phase 2: Bewertung der einzelnen Risiken und die Auswahl der Primärrisiken

- Phase 3: Identifikation von möglichen Gegenmaßnahmen und Auswahl der umzusetzenden Gegenmaßnahmen

In Phase 1, der Identifikation von möglichen Risiken, wurde ein morphologischer Kasten [Ri98] erzeugt um möglichst strukturiert alle Risiken zu identifizieren (Abbildung 3). Zwei Hauptkategorien (Angreifer und Opfer) betrachten die Risiken aus zwei Blickwinkeln. Die Angreifer-Sicht zeigt die unterschiedlichen Quellen von Risiken, die Angriffspunkte und die Angriffsarten. Die Opfer-Sicht zeigt die Auswirkungen und die damit verbundenen Sicherheitsziele. Folgende drei Sicherheitsziele sind von besonderer Rele-

vanz: Vertraulichkeit der Informationen; Integrität der Informationen; und Verfügbarkeit des Systems und damit die Funktionssicherheit.

Quelle	Höhere Gewalt	Organisatorische Mängel	Menschliche Fehler	Technisches Versagen	Vorsätzliche Fehlhandlungen	Angreifer
Angriffspunkt	Sensorknoten	Luftschnittstelle	human Interface	Middleware/Anwendungssystem		
Angriffsart	Abtrennen	Abhören und Auslesen	Deaktivieren / Blocken / Stören	Inhalt fälschen	Zerstören	
Sicherheitsziel	Verfügbarkeit	Vertraulichkeit	Integrität	Rechtssicherheit		Opfer
Auswirkung	Rechtliche Konsequenzen	Gefahr für Leib und Leben	Umweltschäden	Finanzielle Schäden	Volkwirtschaftliche Schäden	Ruf und Wahrnehmung

Abbildung 3: Morphologischer Kasten zur Strukturierung möglicher Risiken

Wenn der Schutz dieser Ziele nicht gewährleistet ist und es durch technisches oder menschliches Versagen, durch höhere Gewalt oder gar durch den bewussten Angriff böswilliger Dritter zu Verletzungen der Ziele kommt, können Unterschiedliche Folgen für die verschiedenen Akteure entstehen. Zum Beispiel der Verlust von Vertrauen bzw. Ruf und negative Wahrnehmung in der Öffentlichkeit, finanzielle Schäden, rechtliche Konsequenzen oder gar Gefahr für Leib und Leben.

Zerstören

R10 Manipulation/Zerstörung von IT-Geräten oder Zubehör		
Sicherheitsziel		• Aus verschiedenen Beweggründen könnte ein böswilliger Dritter versuchen, das System durch Zerstören oder Manipulieren von IT-Geräten zu schädigen. Zum Beispiel kann durch eine starke elektromagnetische Welle die Sensorknoten zerstört werden. Neben dem finanziellen Verlust durch die zu ersetzende Hardware kann dadurch auch die Aufgabenerfüllung beeinträchtig werden.
Verfügbarkeit		
Auswirkung		
Finanzielle Schäden		
Risikoberechnung		
Auftretens-wahrscheinlichkeit	8,13	
Entdeckungs-wahrscheinlichkeit	2,75	
Bedeutung	2,75	
Risikowert	**3,95**	
Gegebene Antworten: 5-1-5-7101059888-1154-542111-Gew_222222		
Quelle:	siehe BSI IT-Grundschutz	

Sammlung von möglichen Gegenmaßnahmen						
		Typ	A	E	B	R
			8,13	2,75	2,75	3,95
	Tamper Resistenz		0,2			0,03
	Schulung Mitarbeiter			0,5		0,25
	Managementsystem			0,5		0,25
	Backupprozesse				0,8	0,42
	Hilfsprozesse			0,5		0,25

Abbildung 4: Beschreibung eines Risikos

Um sicherzustellen, dass alle Risiken die diese Ziele verletzten könnten identifiziert werden, wurde für jede Kombination aus Quelle, Angriffspunkt und Angriffsart nach tatsächlichen Risiken gesucht. Im Rahmen von zwei Workshops und vorangehende Literatur- und Fallstudienrecherche wurden ca. 400 Risiken identifiziert und beschrieben, die einer dieser Kombinationen zugeordnet werden konnten (Abbildung 4).

Diese 400 Risiken wurden in der zweiten Phase bewertet. Dazu wurde die Fehlermöglichkeits- und Einflussanalyse (FMEA) verwendet [IEC06]. Diese Methode hilft dabei jedem Risiko eine Risikoprioritätszahl (RPZ) zuzuordnen und damit Risiken vergleichbarer zu machen. Die RPZ wird gebildet in dem für jedes Risiko folgende drei Kennzahlen bestimmt werden: Auftrittswahrscheinlichkeit, Entdeckungswahrscheinlichkeit und Bedeutung. Jeder dieser Kennzahlen wird ein Wert zwischen 1 und 10 zugeordnet. Dabei bedeutet 1 bei der Auftrittswahrscheinlichkeit, dass dieses Risiko so gut wie nie auftreten kann. Eine 10 bedeutet, dass dieses Risiko garantiert auftreten wird. Bei Entdeckungswahrscheinlichkeit bedeutet eine 1, dass ein Auftreten des Risikos sofort und völlig offensichtlich erkannt wird, eine 10 würde bedeuten, dass ein Auftreten niemals erkannt werden würde. Eine 1 bei Bedeutung bedeutet ein Auftreten des Risikos hätte kaum bis gar keine Folgen, eine 10 würde eine Gefahr für Leib und Leben oder die Existenz des ganzen Projektes bedeuten. Das Produkt aus diesen drei Kennzahlen ergibt die RPZ. Daraus ergibt sich ein möglicher Wertebereich zwischen 1 und 1000. Risiken mit einem Wert von größer als 150 sollten auf alle Fälle weiter betrachtet werden. Die Bewertung ergab 19 Top Risiken für die im ersten Schritt passende Gegenmaßnahmen gesucht wurden (Abbildung 5).

Bedrohung	Auftretensws.	Entdeckungsws.	Bedeutung	Risikowert
R12 Bewusste Manipulation von Information auf dem Sensorknoten bzw. im Backend IT-System	6,4	8,8	10,0	8,23
R08 Mutwilliges Beschreiben des Tags mit falschen Daten	4,3	8,8	10,0	7,19
R11 Abhören bzw. Auslesen über das Human Interface	6,1	10,0	6,0	7,16
R05 Verhinderung von Diensten	5,6	7,0	5,0	5,82
R04 Abtrennen des Sensorknotens und an anderen Objekt anbringen	6,5	7,8	3,3	5,47
R07 Nachrichten fälschen	4,4	8,3	4,3	5,36
R03 Abtrennen des Sensorknotens	7,3	6,0	3,0	5,08
R01 Abhören des Datenaustausches über die Luftschnittstelle	4,4	10,0	2,8	4,94
R06 Entfernen der Batterie oder abtrennen der Antenne	7,1	3,3	5,0	4,88
R13 Abtrennen des Sensorknotens	6,0	6,0	3,0	4,76
R10 Manipulation/Zerstörung von IT-Geräten oder Zubehör	8,1	2,8	2,8	3,95
R16 Gefährdung durch Reinigungs- oder Fremdpersonal	6,6	3,3	2,8	3,90
R18 Tippfehler bei der Eingabe	3,9	7,3	2,0	3,83
R14 Gefährdung durch Reinigungs- oder Fremdpersonal	6,3	3,5	2,5	3,80
R15 Fahrlässige Zerstörung von Gerät oder Daten	6,5	2,8	2,8	3,66
R19 Kein ordnungsgemäßer PC-Benutzerwechsel	4,0	8,0	1,5	3,63
R17 Versehentlich abgeschirmt	7,4	4,3	1,5	3,61
R02 Kompromittierung kryptographischer Schlüssel				

Abbildung 5: Bedrohungen (nach Risikowert sortiert)

Dazu wurden in Phase 3 zu jedem Top Risiko mindestens 10 passenden Gegenmaßnahmen identifiziert, diese senken entweder die Wahrscheinlichkeit, dass ein Risiko eintritt, die Bedeutung wenn ein Risiko eintritt oder die Gegenmaßnahme erhöht die Entdeckungswahrscheinlichkeit. Gegenmaßnahmen müssen nicht unbedingt technischer Natur sein, es gibt auch Gegenmaßnahmen wie die bewusste Gestaltung der Prozesse oder Richtlinien des Managements. Ein Beispiel für solche ist der Verzicht auf Speicherung von personenbezogenen Informationen wenn nicht ausreichend für die Sicherung der Vertraulichkeit gesorgt werden kann. Für jede Gegenmaßnahme wurde der Nutzen bestimmt. Der Nutzen einer Gegenmaßnahme ist in diesem Fall das Senken einer der drei Kennzahlen (Auftrittswahrscheinlichkeit, Entdeckungswahrscheinlichkeit und Bedeutung) im ersten Schritt für einzelne Risiken und im zweiten Schritt der addierte Einzelnutzen über alle Risiken. Neben dem Nutzen hat jede Gegenmaßnahme auch Kosten, dabei kann man verschiedene Kostenarten unterscheiden wie beispielsweise höhere Investitionskosten für einzelne Komponenten, höhere Betriebskosten, die Überwindung von Vorbehalten oder der Verzicht auf Nutzenpotenziale.

	Gegenmaßnahme	Kosten	Kosten-Nutzen
G08	Sensitive Daten auf dem Sensorknoten reduzieren	1,57	20,96
G05	Daten zwischen Sensorknoten und Tag oft synchronisieren	1,57	8,15
G07	Mitarbeiter aus- und weiterbilden	1,71	6,93
G04	Backupprozesse definieren	2,43	5,13
G01	Tamper Evident	2,00	3,66
G29	Datenübertragung über die Funkschnittstelle verschlüsseln	2,29	3,59
G30	Hash Funktionen, Checksummen und Signaturen zum Sicherstelle der Integrität und der Authentizität von Nachrichten bzw. Speicherinhalten	1,71	3,36
G10	Bedeutungsvolle Identifikationsnummer am/im SK	1,00	3,00
G17	Verändern der Informationen auf dem Tag nur über autorisierte Basisgeräte	1,71	2,98
G13	Erweiterte Funktionalitäten in der Basisstation bzw. Backend	2,00	2,75
G39	Pufferspeicher in den Komponenten und passende Synchronisationsalgorithmen	1,29	2,72
G41	Managementsystem	1,57	2,68
G25	Signierte bzw. Verschlüsselte Identifikationsnummern	2,00	2,44
G28	Informationen auf dem Sensorknoten verschlüsseln	2,29	2,42
G19	Verändern von Informationen ist unmöglich bzw. nur einmal möglich	4,57	2,04
G42	Sessionverwaltung	1,29	1,81
G09	Sicheres Entsorgen von Sensorknoten	1,57	1,77
G36	Schreibschutz durch Passwort bzw. Authentifizierung und Rollen	1,29	1,66
G03	Hilfsprozesse hinzufügen	4,00	1,26
G02	Tamper Resistenz	2,00	1,22
G38	Authentifizierung und Autorisierung von Benutzern	1,29	1,21
G34	Physische Sicherheitsverfahren	3,00	1,17
G24	Bedeutungslose und wirklich zufällige Identifikationsnummer am/im SK	1,86	1,16
G14	Sichere Umgebungen schaffen	2,00	0,94
G15	Verschiedene kryptografische Schlüssel für jede Komponente	1,71	0,94
G16	Periodisches Verändern von kryptografische Schlüssel	1,71	0,94
G32	Abhören von Nachrichten durch Abschirmung erschweren	1,57	0,91
G12	Sichere Passwörter	1,86	0,91
G31	Valide Schreib- bzw. Leseaktivitäten protokollieren	1,57	0,81
G22	Sensorknoten mit Hardware Unique IDs einsetzen	2,29	0,69
G18	Verändern der Informationen auf dem Tag mit eingeschränkten technischen Verfahren	2,29	0,65
G37	Sensitive Information auf dem Human Interface reduzieren	4,14	0,47
G33	Kodierung bzw. Pseudonymisierung der Kommunikation bzw. Informationen im Speicher	3,29	0,46
G43	Technische Maßnahmen die Abhören/Stören der Funkschnittstelle erschweren	2,29	0,38

Abbildung 6: Identifizierte Gegenmaßnahmen in ihrer Kosten-Nutzen Relation

Aus dem Verhältnis zu Kosten-Nutzen ergaben sich aus den 50 betrachteten Gegenmaßnahmen, 20 Gegenmaßnahmen die den höchsten Nutzen bei den geringsten Kosten versprachen (Abbildung 6). Aus dem Ergebnis der strukturierten Ermittlung von Primärrisiken und passenden Gegenmaßnahmen wurden funktionale und nicht-funktionale Anforderungen ermittelt, die von den Entwicklern der einzelnen Komponenten des Gesamtsystems beachtet werden müssen.

5 Diskussion

Der Einsatz drahtloser Sensornetzwerke in klinischen Szenarien ist ein neues Thema, so dass bisher kaum Erfahrungen existieren. Neben technischen Herausforderungen gilt es auch das Management durch verlässliche Zahlen und operative Hilfestellungen zu unterstützen [FM08, Mu06].

Eine der größten Hindernisse sind die direkten Kosten der Einführung, die sich auf bis zu eine halbe Million Dollar pro Krankenhaus belaufen können [Pa07], ohne dass der Return on Investment vorab errechnet werden kann. Fallbeispiele legen jedoch eine dreijährige Amortisationszeit nahe [Wi08, Na06]. Um diese Kosten zu relativieren sollte daher die eingesetzte Technologie möglichst mehrere Dienste (mehr Vorteile bei konstanten Kosten) auf derselben Plattform (günstige Massenproduktion) anbieten. Allerdings sollten die Ziele und die Umsetzung bewusst geplant werden, da industrielle Standardprodukte nicht ohne weiteres im klinischen Umfeld eingesetzt werden können und die Erwartungen oftmals enttäuscht wurden [FM08].

Insbesondere die Nutzung neuer Möglichkeiten zur Umstellung etablierter Prozesse erfordert ein adäquates Change Management. Beispielsweise erleichtert eine stets aktuelle Übersicht über die Standorte und Einsätze medizintechnischer Geräte die gemeinsame Nutzung (Anschaffung, Lagerhaltung, Betrieb) von Geräten durch mehrere Abteilungen. Die nutzungsgerechte Abrechnung von Geräteeinsätzen (Kostenträgerrechnung) oder neue Betreibermodelle (z.B. Betriebsgesellschaft) werden dadurch erst ermöglicht.

Der objektive Schutz von sensiblen, patientenbezogenen Daten muss genauso beachtet werden, wie die subjektiven Ressentiments von Anwendern und Patienten bezüglich „funkender Kästchen“ [FM08], auch wenn diese geringer sind als vielfach angenommen [KR09]. In OPAL wurde daher schon früh eine umfangreiche Risikoanalyse durchgeführt, welche in das Systemdesign eingeflossen ist. Beispielsweise wurde die Menge der Daten auf einem Sensorknoten gering gehalten, auch wenn dadurch einige der Vorteile aktiver Sensornetze (die lokale Verarbeitung der Daten) nicht realisiert werden konnten. Zusätzlich wurden von Beginn an Endanwender in die Anforderungsanalyse eingeschlossen und der Entwurf mehrfach mit Anwendern und anderen relevanten Stellen wie dem Sicherheitsbeauftragtem oder dem Datenschutzbeauftragtem abgestimmt.

Einige der heutigen Beschränkungen werden mit zukünftigen Generationen der Hardware hinfällig. Innerhalb des ersten Projektjahres von OPAL fiel der Preis für die Hardware um 30% auf 25 Euro pro Sensorknoten während die Leistungsfähigkeit des verwendeten Prozessors um 400% stieg. In Verbindung mit leistungsfähigeren Batterien

werden starke Verschlüsselungsalgorithmen für die Speicherung und Kommunikation patientenbezogener Daten möglich werden, so dass einige der heutigen Beschränkungen wegfallen werden.

Ein bisher offener Punkt ist das Gehäusedesign der Sensorknoten. Zwar lassen sich fachliche und technische Anforderungen an einen Sensorknoten definieren und erfüllen, aber die schiere Menge an medizinischen Gerätetypen, Einbau- und Umbaumöglichkeiten sowie deren Einsatzmöglichkeiten macht ein generisches Design nahezu unmöglich. Spezifische Gehäuse verteuern jedoch den Preis pro Sensorknoten, so dass man idealerweise die Zusammenarbeit mit den Geräteherstellern suchen sollte.

Der serviceorientierte Ansatz auf Basis etablierter Webtechnologien (SOA, XML, Webservices) hat die Integration in die klinische IT-Landschaft einfach gemacht. Die Übertragbarkeit auf andere Häuser wie auch die Skalierbarkeit ist gegeben.

6 Zusammenfassung und Ausblick

Als bewährte Technologie im Logistikbereich findet RFID im Krankenhausmarkt zunehmend Verbreitung. Aktive Sensornetzwerke gehen noch einen Schritt weiter, indem sie die Basis für mobile und ubiquitäre Dienste bilden. Die Möglichkeit zur zeitnahen Lokalisierung und Identifizierung von Objekten wie Gerätschaften oder Blutkonserven kann zu neuen Diensten und Geschäftsmodellen führen.

Die Herausforderung besteht in der Schaffung einer generischen Plattform, auf der verschiedenste Dienste aufsetzen können. Heutige Ansätze konzentrieren sich vor allem auf spezifische Anwendungsszenarien. In OPAL Health wird ein Smart Object Netzwerk realisiert mit dem bei gleicher Hardware sehr verschiedene Szenarien abgedeckt werden können. Neben der technologischen Herausforderung, sind Fragen zum Einsatz vor allem auch bezüglich der Sicherheit zu beantworten.

Der Einsatz eines morphologischen Kastens und der FMEA Analyse hat sich als Grundlage der Risikoanalyse bewährt. Hier konnten Anwender und Techniker gemeinsam Risiken identifizieren, bewerten und geeignete Gegenmaßnahmen wählen. Durch die frühzeitige Durchführung der Risikoanalyse konnte diese in das Systemdesign einfließen. Deswegen konnten jedoch nicht alle technischen Möglichkeiten des Sensornetzwerkes ausgeschöpft werden, weil beispielsweise personenbezogene Daten aufgrund beschränkter Batteriekapazitäten noch nicht adäquat auf dem Chip bzw. während der Kommunikation verschlüsselt werden können.

Danksagung

Das Projekt OPAL-Health wird vom Bundesministerium für Wirtschaft und Technologie im Rahmen des Programms „SimoBIT – sichere Anwendung der mobilen Informationstechnik (IT)“ gefördert (FKZ 01MB07017).

Literaturverzeichnis

[Gl04] Glabman, M.: Room for tracking. RFID technology finds the way. In Mater Manag Health Care, 2004, 13; S. 26-8, 31-4, 36 passim.

[Ki06] Kim, S.-J. et al.: Smart Blood Bag Management System in a Hospital Environment: Personal Wireless Communications, 2006; S. 506–517.

[Sh07] SHOT, T. S. H. o. T. S. G.: SHOT Annual Report 2007. "http://www.shotuk.org".

[Dz07a] Dzik, W. H.: New technology for transfusion safety. In Br J Haematol, 2007, 136; S. 181–190.

[MM05] Michael, K.;.McCathie, L.: The pros and cons of RFID in supply chain management. International Conference on Mobile Business, 2005. ICMB 2005, 2005.

[Vi08] Vilamovska, A-M. et. al.: Deliverable 1: Scoping and identifying areas for RFID deployment in healthcare delivery. In: Study on the requirements and options for RFID application in healthcare. RAND Europe, Brussels, 2008.

[ES07] Egan, M. T.; Sandberg, W. S.: Auto identification technology and its impact on patient safety in the Operating Room of the Future. In Surg Innov, 2007, 14; S. 41-50; discussion 51.

[We09] Wessel, R.: German Clinic Uses RFID to Track Blood. RFID Journal, 2009.

[To08] van der Togt, R. et al.: Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment. In JAMA, 2008, 299; S. 2884–2890.

[Ak02] Akyildiz, I. F. et al.: Wireless sensor networks: a survey. In Computer Networks, 2002, 38; S. 393–422.

[Na06] Nagy, P. et al.: Radio frequency identification systems technology in the surgical setting. In Surg Innov, 2006, 13; S. 61–67.

[Sa06] Sandler, S. G. et al.: Bar code and radio-frequency technologies can increase safety and efficiency of blood transfusions. In Labmedicine, 2006, 37; S. 436–439.

[Dz07b] Dzik, S.: Radio frequency identification for prevention of bedside errors. In Transfusion, 2007, 47; S. 125S-129S; discussion 130S-131S.

[Ro05] Roth, J.: Mobile Computing: Grundlagen, Technik, Konzepte. Dpunkt-Verlag, Heidelberg, 2005.

[We98] Wentz, B. et al.: The Erlangen university hospital communication hub-proprietary and standardised communication. In Stud Health Technol Inform, 1998, 52 Pt 2; S. 995–998.

[Ne02] Newcomer, E.: Understanding Web Services: XML, WSDL, SOAP, and UDDI. Addison-Wesley, Boston, 2002.

[BSI05] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz Kataloge, 2005.

[Ri98] Ritchey, T.: General Morphological Analysis - A general method for non-quantified modelling. Adapted from a paper presented at the 16th Euro-Conference on Operational Analysis, Brussels, 1998.

[IEC06] International Electrotechnical Commission: IEC60812: Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA). 2006

[FM08] Fisher, J. A.; Monahan, T.: Tracking the social dimensions of RFID systems in hospitals. In International Journal of Medical Informatics, 2008, 77; S. 176–183.

[Mu06] Murphy, D.: Is RFID right for your organization? In Mater Manag Health Care, 2006, 15; S. 28–33.

[Pa07] Page, L.: Hospitals tune in to RFID. In Mater Manag Health Care, 2007, 16; S. 18–20.

[KR09] Katz, J. E.; Rice, R. E.: Public views of mobile medical devices and services: a US national survey of consumer sentiments towards RFID healthcare technology. In Int J Med Inform, 2009, 78; S. 104–114.