

# Sichere Warenketten durch RescueIT<sup>1</sup>

Michael Clasen<sup>2</sup>, Kai Fischbach<sup>3</sup>, Rafael Pietrowski<sup>3</sup>, Andreas Schaad<sup>4</sup>

<sup>2</sup>Fakultät IV Wirtschaft und Informatik  
Fachhochschule Hannover, Ricklinger Stadtweg 120, 30459 Hannover  
michael.clasen@fh-hannover.de

<sup>4</sup>SAP Research  
Vincenz-Priessnitz-Str. 1, 76131 Karlsruhe  
andreas.schaad@sap.com

<sup>3</sup>Seminar für Wirtschaftsinformatik und Informationsmanagement  
Universität zu Köln, Pohligstr. 1, 50969 Köln  
fischbach@wim.uni-koeln.de  
pietrowski@wim.uni-koeln.de

**Abstract:** In diesem Beitrag wird das Projekt RescueIT vorgestellt, welches sich mit der Entwicklung einer verteilten, serviceorientierten IT-Infrastruktur für die kontinuierliche und robuste Überwachung von Warenketten beschäftigt. Innovatives Element ist die Einrichtung einer Risikodatenbank. Mit Hilfe dieser Informationen sollen sich Informationsnetze selbständig nach Angriffen oder Ausfällen regenerieren können. Es werden die Projektziele, die Architektur und die geplante Vorgehensweise vorgestellt.

## 1 Einleitung

Die Sicherheit in Warenketten hat in den letzten Jahren einen erheblichen Bedeutungszuwachs erfahren [Jü03]. Gründe hierfür waren u.a. Fälle von Maul- und Klauenseuche und BSE der letzten Jahre [Jü05, Po08]. Dies führte dazu, dass sich auch die Wissenschaft verstärkt mit dem Thema Rückverfolgung von Lebensmitteln beschäftigt hat [Ga05, Ho05, Jo05, Po08].

Waren- und Informationsketten, die in der Realität eher als Netze zu bezeichnen sind, werden in der heutigen Zeit durch einen komplexen und heterogenen Verbund aus Informations- und Kommunikationstechnologien und darauf aufbauenden Anwendungssystemen der Warenkettenpartner realisiert. Diese Systeme koordinieren die Warenflüsse sowie Produktions-, Lager- und Logistikprozesse. Aufgrund der hohen Komplexität können Ausfälle einzelner Systeme negative Auswirkungen auf andere Kettenpartner oder sogar auf die gesamte Kette haben. Dieser Aspekt wurde bei vielen bisherigen Untersuchungen vernachlässigt.

---

<sup>1</sup> Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministerium für Bildung und Forschung unter dem Förderkennzeichen 13N10965 gefördert. Die Verantwortung für den Inhalt liegt bei den Autoren.

Um diese komplexen Systeme möglichst robust gegenüber Störungen zu gestalten, setzt RescueIT (Robustes und verfügbares SCM – Unterstützende IT-Plattform) auf selbstheilende Prozesse und kontinuierliche Verbesserungen durch Erstellung einer Expertendatenbank. Der hohen Komplexität dieser Warenketten wird mit verteilten Systemen und serviceorientierter Programmierung entgegengetreten. Die Verwendung standardisierter und offener Protokolle und Schnittstellen soll helfen, die Kommunikation zwischen den heterogenen Systemen entlang der Warenkette weiter zu vereinfachen. Die geplante Architektur und Vorgehensweise werden im Folgenden dargestellt.

## **2 Architektur**

Neu am Projekt RescueIT ist, dass nicht nur die Produktivphase (Phase B) unterstützt wird, sondern es schon davor in der Designphase (Phase A) ansetzt. Darüber hinaus werden mögliche Ausfallrisiken vorgedacht und in einer Risikodatenbank abgespeichert. Dieses Expertenwissen steht sowohl in der Phase A beim Design neuer Rückverfolgungssysteme zur Verfügung als auch in einer Ausfall- oder Störsituation (Phase C), in der automatisiert eine Selbstheilung ausgelöst wird. Das folgende Referenzszenario verdeutlichen die Projektinnovationen der drei Phasen (Abbildung 1).

Phase A beschäftigt sich mit der Planung und Analyse einer Waren- und Informationskette. Hier können die einzelnen Partner kollaborativ eine gemeinsame Sicht ihrer Warenkette(n) modellieren. Eine Risikodatenbank unterstützt bei der Analyse möglicher logischer und physischer Schwachstellen. Risiken und Sicherheitsanforderungen werden in den Prozessmodellen grafisch dargestellt und Prüfbedingungen definiert.

Phase B beschreibt die Aufgaben der RescueIT-Plattform zur Laufzeit. Basierend auf dem modellgetriebenen Ansatz (Phase A) werden die in den Prozessmodellen festgelegten Prüfbedingungen automatisch überwacht. Hierzu stehen Daten aus den lokalen Warenwirtschaftssystemen der Partner sowie Sensordaten entlang der Warenkette zur Verfügung. Abweichungen vom definierten Sollzustand meldet die RescueIT-Plattform ihren Partnern unverzüglich, so dass Maßnahmen (Phase C) eingeleitet werden können.

In Phase C geht es um die Handhabung von Problemsituationen wie Ausfall und Wiederherstellung. Kommt es zu einem Ausfall von Sensoren, IT-Diensten oder manuellen Schritten, werden weitestgehend automatisiert kompensierende Maßnahmen getroffen. Dabei stellt die RescueIT-Plattform die erforderlichen Methoden zur Verfügung. Die Plattform unterstützt die Wiederherstellung des Originalzustands der Systeme und überwacht die einheitliche Verwaltung der Daten. Neuartige Angriffs- und Abwehrmuster werden zur Abwehr zukünftiger Gefahren in der Risikodatenbank gespeichert. Somit kann eine kontinuierliche Verbesserung der RescueIT-Plattform sichergestellt werden.

Entlang dieser Warenkette müssen alle auszuführenden und durch die IT unterstützten (Geschäfts-)Prozesse sicher, verfügbar und robust gegenüber Störungen ausgelegt sein. Hardwareseitig wird die Einbindung von Sensoren oder RFID-Tags zur Gewinnung von Daten und Informationen über die Prozesse eine wichtige Rolle spielen. Somit können beispielsweise defekte Komponenten entdeckt und ausgetauscht bzw. kurzfristig auf noch funktionsfähige umgeschaltet werden.

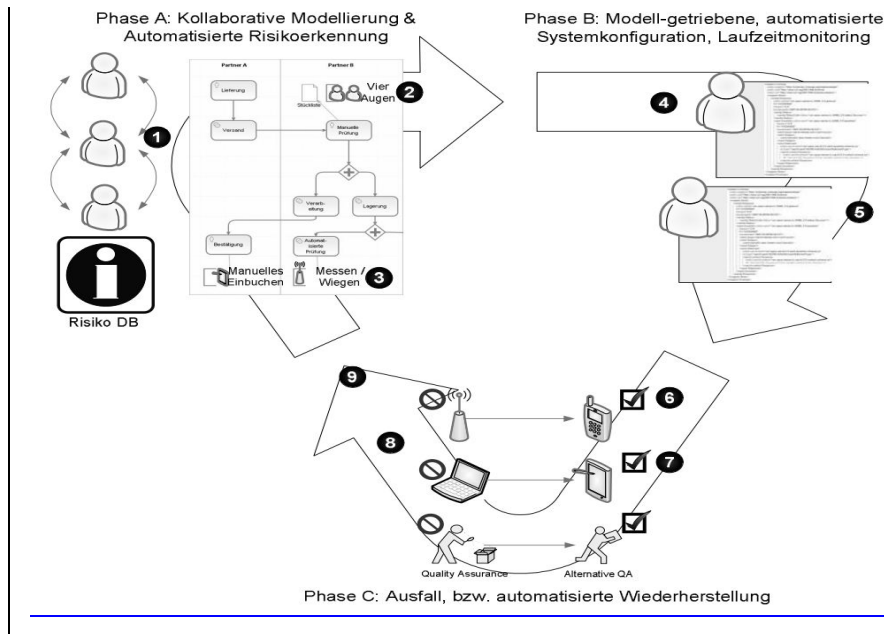


Abbildung 1: Referenzszenario<sup>2</sup>

Softwareseitig steht ein zentrales Repository zur Verfügung, welches sowohl zur Entwicklungs- als auch zur Ausführungs- und Änderungszeit alle notwendigen Informationen über die verfügbaren Dienste in der Infrastruktur enthält. Sollte also ein Service temporär nicht verfügbar sein, kann automatisch ein vergleichbarer Service alternativ eingebunden werden.

Die unterschiedlichen Systeme der Partner entlang der Warenkette (z.B. Supply Chain Management (SCM)-, Customer Relationship Management (CRM)-Systeme) werden an die Integrations-Komponente durch entsprechende Adapter angeschlossen, die etwa die Abbildung zwischen unterschiedlichen Schnittstellentechnologien (z.B. Webservices, native APIs) leisten. Als Grundlage für z.B. Analysen zur Früherkennung von Risiken werden durch die Datenintegrations-Komponente die unterschiedlichen Datenmodelle in einem einheitlichen Datenmodell integriert, das ebenfalls der Risiko-Datenbank zu Grunde liegt.

<sup>2</sup> Quelle: <http://www.sichere-warenketten.de>.

## 4 Vorgehensweise

Basierend auf dem Gedanken der Szenarioorientierung werden als Basis für das Projekt zusammen mit den Partnerunternehmen mögliche Anwendungsszenarien erstellt. Durch die Analyse von konkreten Anwendungsfällen sollen die Anforderungen der Endnutzer und KMUs ermittelt werden. Diese Szenarien werden von der juristischen Begleitforschung untersucht und bilden die Basis für die Arbeitsgruppen der technischen Umsetzung. Eine periodische Evaluation der Entwicklung aus Anwendersicht stellt ihre spätere Einsetzbarkeit sicher.

Die analysierten Anwendungsszenarien bilden ebenfalls die Basis für die Erstellung der Geschäftsprozesssicht, der Risikodatenbank sowie einer definierten Anzahl an Diensten. Hier erfolgen also die service- und sicherheitsorientierte Modellierung von Waren- und Prozessen sowie die Erarbeitung von Konzepten zur Abbildung der Modelle auf den Code der Zielsysteme. Hierzu gehört auch die Einbeziehung der Sicherheit der Plattform als auch der eingebundenen Dienste. Auf Basis der Risikodatenbank soll es möglich sein, im Schadensfall neue benötigte Dienste sicher in die Warenkette zu integrieren. Die Integration der Dienste sowie die Visualisierung der Sicherheitsanforderungen werden auf Basis der vorhergehenden Ergebnisse erfolgen. Des Weiteren muss im Falle eines Schadens die Möglichkeit bestehen, sicher Daten auszutauschen bzw. anonyme Vergleiche zu ermöglichen.

## Literaturverzeichnis

- [Ga06] Gampel, B.: Rückverfolgung von Lebensmitteln. Eine empirische Analyse kettenübergreifender Informationssysteme. Cuvillier Verlag, Göttingen 2006.
- [Ho05] Hobbs, J., Bailey, D., Dickinson, D., Haghiri, M.: Traceability in the Canadian Red Meat Sector: Do Consumers Care? In: Canadian Journal of Agricultural Economics, Vol. 53, No. 1, 2005, S. 47-65.
- [Jo05] Jones, P., Clarke-Hill, C., Comfort, D., Hillier, D., Shears, P.: Radio Frequency Identification and Food Retailing in the UK. In: British Food Journal, Vol. 107, No. 6, 2005, S. 356-360.
- [Jü03] Jüttner, U., Peck, H., Christopher, M.: Supply Chain Management: Outlining an Agenda for Future Research. In: International Journal of Logistics: Research and Applications, Vol. 6, No. 4, 2003, S. 197-210.
- [Jü05] Jüttner, U.: Supply Chain Risk Management: Understanding the Business Requirements from a Practitioner Perspective. In: International Journal of Logistics Management, Vol. 16, No. 1, 2005, S. 120-141.
- [Po08] Pouliot, S., Sumner D.: Traceability, Liability, and Incentives for Food Safety and Quality. In: American Journal of Agricultural Economics, Vol. 90, No. 1, 2008, S. 15-27.
- [Th03] Theuvsen, L.: Rückverfolgbarkeit von Lebensmitteln: Herausforderungen und Lösungsansätze aus organisatorischer Sicht. In: Berichte über Landwirtschaft, Bd. 81, 2003, S. 555-581.