



International Research Project

RescueIT

Funded By



Bundesministerium
 für Bildung
 und Forschung

Towards Resiliency in Food Supply Chains

RescueIT was a German/French research project started in 2010 and successfully completed in 2014. With focus on the security in food supply chains, the objective was the development of a supply-chain-wide IT-Platform that enables tracking and tracing as well as resilient processes. The major goal was the continuous improvement of the security in food supply chains.

Food supply chains are vulnerable to both unintended as well as intended disruptions due to their complex and global nature. They are often based on heterogeneous collections of information and communication technologies and different information systems. The extensive coordination of flows of goods as well as production, storage, and logistics processes may lead to additional risks.

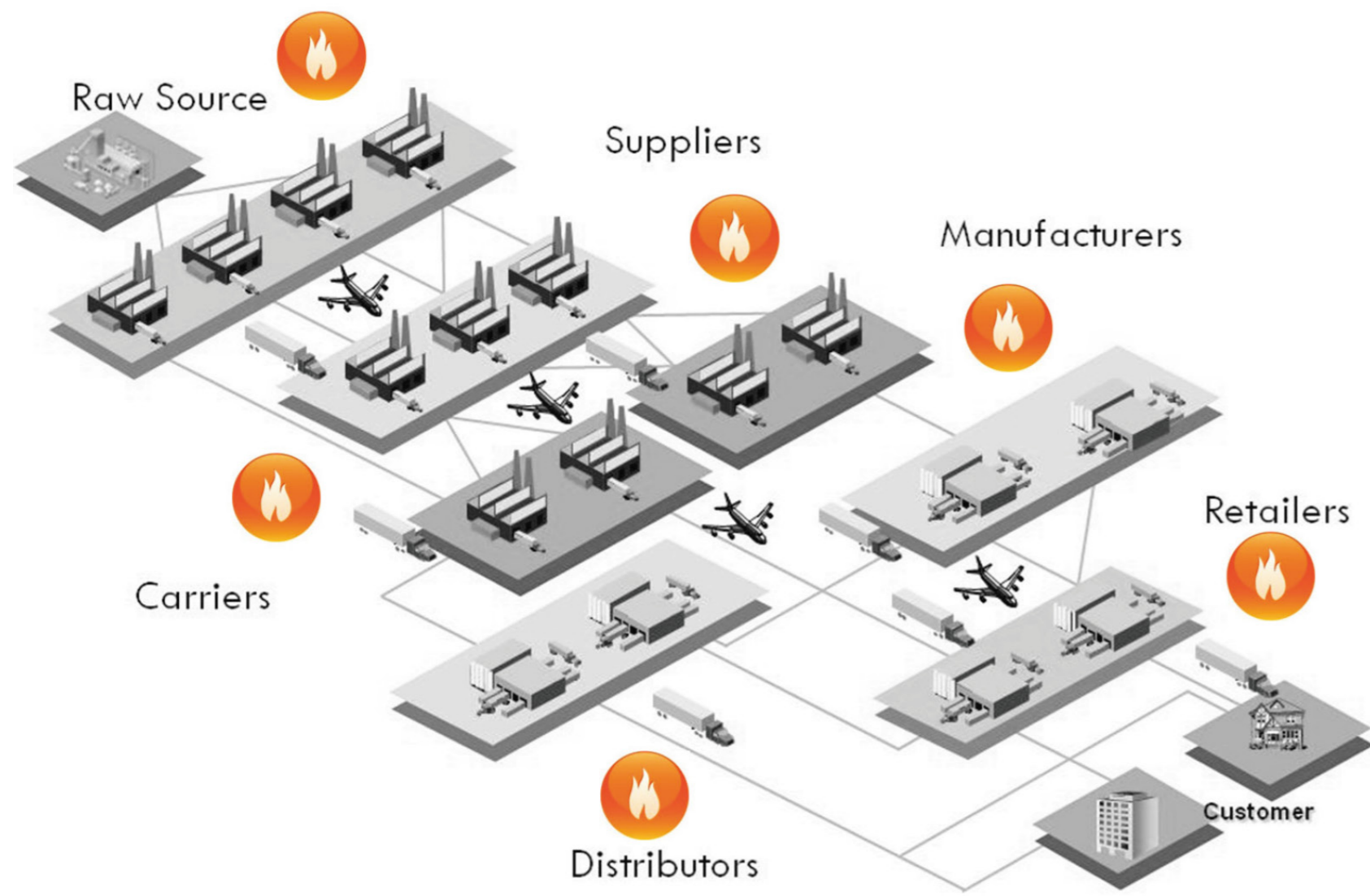


Figure 1: Food supply chain

Given the broad nature of food supply chains, creating both, secure (e.g. supply chains that maintain advanced security procedures) and resilient food supply chains (e.g. supply chains that are able to react quickly and restore operations when unexpected disruptions occur), is of utmost importance and the main goal of RescueIT.

Our Approach: Scenario-Driven Research

The project RescueIT makes use of a scenario-driven approach. Three overall scenarios are considered, which address the current topics in food supply chains concerning risks, threats and the safety of the population.

Contamination

In the past there were many cases of contamination, which can be roughly categorized into radioactive cases, chemical cases and biological cases. A complex harmonized effort is necessary to enable rapid tracing of contaminated products backwards and forward through the supply network. Close collaboration of supply chain partners is necessary to find the source of contamination but also for immediate removal of products from all levels of the supply chain.

Cyber Attack

Recently, the frequency of cyber attacks has increased dramatically. Targets are not only governments anymore, but also companies. Possible attack points especially in the food supply chain include systems that are commonly used in the industry and the standardized information exchange between partners. Another possible attack could be directed towards very specific systems for recipe/mixture management and cause the inclusion of not declared allergens into foods for example.

Breakdown of Critical Infrastructures

Recent statistics show that about once a year an extensive natural disaster occurs in Germany/France. The example of the Elbe Food Water in August 2002 supports this. More than 337.000 people were affected by the flooding. At least 1880 streets, 94 railway bridges and 400 km of rails were destroyed. This resulted in huge damages in agriculture, industry, and retail and enormous failures of infrastructure facilities in almost every other sector. It gets even worse when natural disasters destroy critical infrastructures. These organizations and institutions are essential for the functioning of society and economy. Especially the food provision is dependent on many critical infrastructures like energy, water, and transportation.

Our Goal: Continuous Improvement through Comprehensive Integration

RescueIT follows an unique integrated approach to assist supply chain and risk managers not only in the productivity phase (phase B), but also before in the design phase (phase A) and after in the recovery phase (phase C). Potential risks are kept in a so-called Risk Database. This expert knowledge can be used in phase A when designing supply chains as well as in case of an incident in the recovery phase (phase C), where automated self-healing processes get initiated.

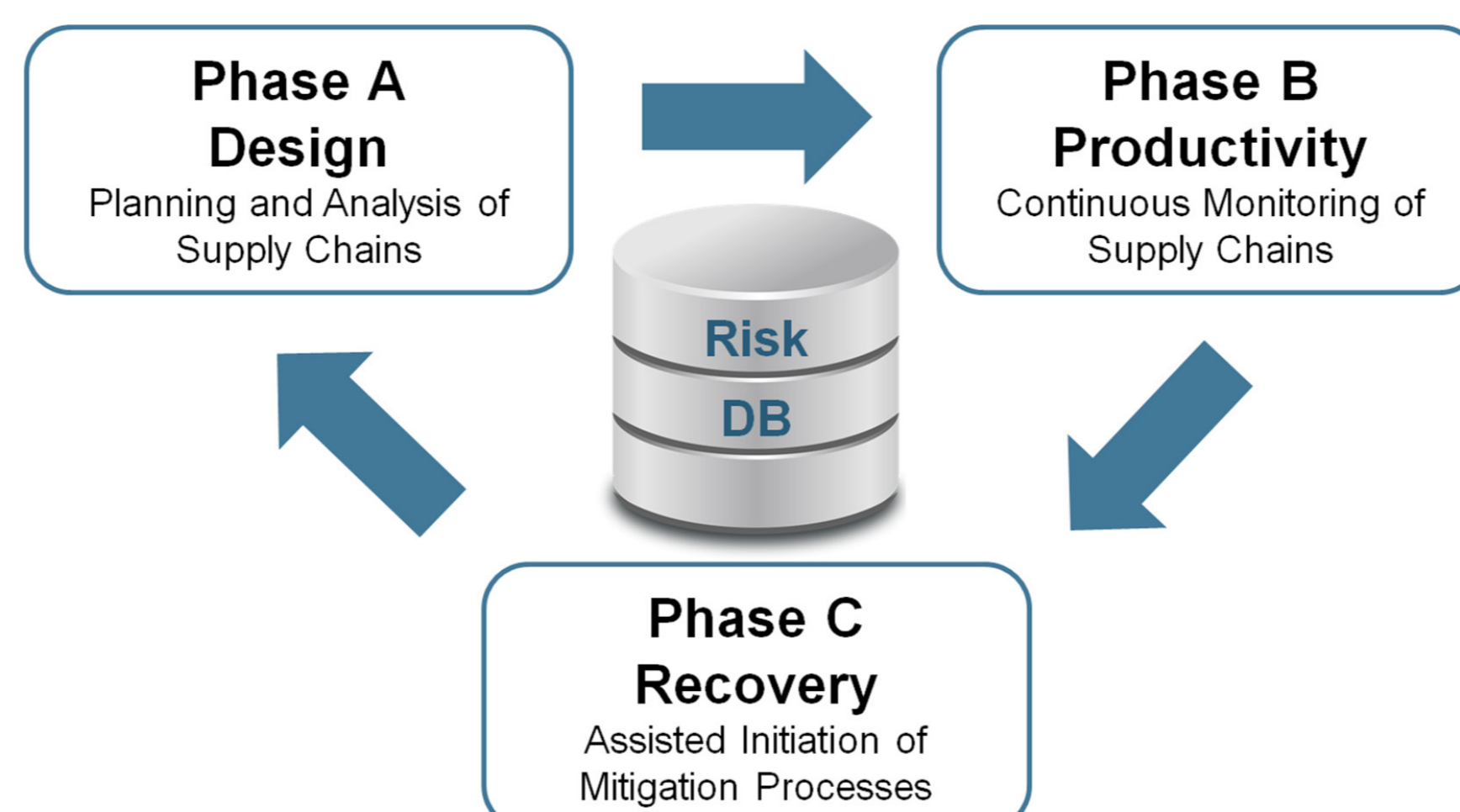


Figure 2: Integrated approach to assist supply chains

German-French Business Award 2011 in the Category „Innovation“ 2nd Place



Contact

Dipl.-Wirt.-Inf. Puja Abbassi
 abbassi@wim.uni-koeln.de
 Tel.: +49 221 470-5396



Dipl.-Wirt.-Inf. Rafael Pietrowski
 pietrowski@wim.uni-koeln.de
 Tel.: +49 221 470-5318

