Concepts for the Improvement of

Supply Chain Efficiency and Security

Johan Scholliers, Sirra Toivonen, Antti Permala, Karri Rantasila
VTT Technical Research Centre of Finland,
P.O.Box 1300, FI-33101 Tampere, Finland,
tel. +358207223642, johan.scholliers@vtt.fi
Lea Hannola
Lappeenranta University of Technology,
P.O. Box 20, FI-53851 Lappeenranta, Finland
Tel. +358 40 822 3982, lea.hannola@lut.fi

ABSTRACT

Modern supply chains have a large number of transport phases and actors involved, and face many security risks. This paper presents a discussion and new concepts for management of the multimodal supply chains and transport unit security. The paper will assess how companies can benefit from the investments in security technology, and discuss the possibilities of the use of monitoring technology.

Keywords: logistics, supply chain security, innovation, tracking

1. INTRODUCTION

The Finnish national LogProof project aims to develop comprehensive operations models based on security solutions and services for logistic multi-stakeholder networks, as well as methods for security and safety management. The project develops, evaluates and pilots operations models produced by the value network based on new technologies and service packages internationally. In addition, the project aims to identify potential business opportunities and ideas for security and safety management in a network of supply chain management business, and develop new business models for commercialization of new products and services. The projects research results are used in several industry cases related to comprehensive operations models in logistics networks.

This paper presents a discussion and new concepts of mobile solutions to manage global supply chain and transport unit security and product safety. Even though solutions to track and trace vehicles with stationary mounted devices are already steadily used, the use of mobile

devices still scarce. The technology may be thought as immature or expensive for global supply chain purposes or the business model is not profitable from the operator's point of view.

2. RISK MANAGEMENT

The aim of logistics is to execute the delivery process productively, on-time, economically securely and safely, taking into account the client's requirements. "Undesirable" events include late (or too early) delivery, non-delivery (the chain breaks), damaged, obsolescent, incorrect amount of products, or delivery to wrong location. The product damages are often caused by interaction of various factors and damage mechanisms may be complex. A disturbance free supply chain is efficient, reliable, visible, resilient and economical. This means that the supply chain is able to deliver the shipments as planned and not deteriorating the quality of goods. These economical and operational advantages can be achieved by utilizing state of the art monitoring technologies. Vulnerability of one point will decrease the total performance of the supply chain and it should be viewed in the overall context of the business needs [1].

The aim of the risk management can be modelled as to identify the sources of risk, magnitude of risk and its relationship to business objectives and threat of disruption in supply chains [2].

The frequency of security incidents as well as their consequences is increasing. Typically the most vulnerable phases in multimodal supply chains are slowing, stopping and parking en route on the road transport, moving through dangerous geographical areas, loading and unloading, change of transport vehicles or transport modes and static points along the routes (warehouses, terminals, ports, borders, etc.) [3]. The total loss of value caused by theft of cargo and freight vehicles is about 8.2 Billion each year in Europe, or about 6.7 Euro per loaded trip [4]. The management of supply chain security is a topic which is hence high on the agenda of logistics operators and governmental agencies [5], [6].

Supply chain risk assessment's objectives are to identify and assess those risks and vulnerabilities in the supply chain process and route that can affect the quality of the delivery process. Several security risk assessment and management methods for supply chains and container freight have been developed in recent years [5],[7], [8]. The ways of assessing risks are selected according to the required objectives. In order to manage the security in supply chains and logistics, technologies and knowledge for building monitoring and emergency systems capabilities is implemented. The constant changes of processes, business practices and economic power in the global business environment have generated the need for the security management approach to enterprise resiliency [9].

The value of the increased security measures and monitoring of the supply chain can be found e.g. in improved product safety and supply chain processes, in increased supply chain visibility and delivery speed as well as in resilience improvements, which include better anticipation and reaction to the undesired occurrences in the supply chain [10].

3. INNOVATION FROM SECURITY

New innovations, innovative security solutions and services are needed to enhance the competitive advantage of companies operating in logistic networks. Tidd et al. [11] define *innovation* as a process of turning opportunity into new ideas and of putting these into widely used practice. According to Trott [12], the term innovation is a very broad concept that can be understood in a variety of ways, and he introduces the notion that innovation is a process with number of distinctive features that have to be managed. Thus, Trott defines innovation as the management of all the activities involved in the process of idea generation, technology development, manufacturing and marketing of a new (or improved) product or manufacturing process or equipment. Specht [13] defines all the stages from fundamental research to product and market introduction as innovation management.

The literature features numerous innovation process models and business decision models that describe how companies develop or should develop new products or services. According to Trott [12], to many people new products are the outputs of the innovation process, where the new product development (NPD) process is a sub-process of innovation. Koen et al. [14] suggest that the innovation process can be divided into three areas: the front end of innovation (FEI), the new product development process, and commercialization, as depicted in Figure 1. Kim and Wilemon [15] define the front end as a period between when an opportunity is first considered and when it is judged ready for development. The actual product development is the process of transforming business opportunities into tangible products [12], and commercialization is a set of activities associated with preparing the market into which an innovation will be launched [11].

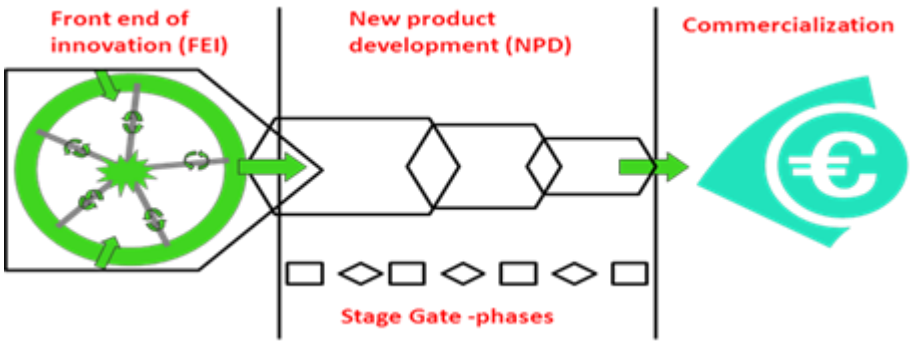

Figure 1: The innovation process (Modified from Koen et al. 2002 [14])

When building new security solutions or services in supply chains, the FEI is regarded as one of the most important steps in the innovation process. Problems in the front end phase have an impact on customer dissatisfaction with delivered solutions, e.g. if the actual customer needs are not taken into account or they are interpreted in a wrong way in the final solution. Khurana and Rosenthal [16] define the core responsibilities of a development team in FEI, such as a) identifying customer needs and competitive situations; b) performing technology

evaluation of current capabilities and requirements, as well as alignment with existing business and technology plans; c) identifying core product requirements; d) testing the concept; e) specifying the resources needed to complete the project; and f) identifying key risks and challenges.

According to Tuominen et al. [17], in order to be able to develop innovations a company must have an innovation management system that takes the *customer needs*, the company's *strategies* as well as *technological opportunities* and the company's *resources* into account. Customer needs and requirements vary depending on the different actors in the supply chain and the related industry-specific factors. Therefore, several perspectives, e.g. those of service and technology providers, logistic solution providers and cargo owners have to be taken into account in customer needs assessment phase of the innovation process. In addition, many other stakeholders are involved in global multimodal supply chains: authorities, private persons, transport operators, terminal operators, infrastructure keepers and insurance companies. The creation, development and commercial success of new security innovations require a great deal of input from a variety of specialist sources. Technology and technology-oriented companies are traditionally more influenced by new technologies than other companies, especially in business-to-business environment [18]. The development of more sophisticated and complex technologies have created business opportunities for safety and security service providers in supply chains.

However, the introduction of new innovations and security solutions is not enough in the field of security business in supply chains. The actual benefits and additional value for customers of new technological solutions have to be identified and justified for the customers. A previous study [19] identifies and prioritizes the key value drivers of security and safety management in supply chains, which can be utilized in the development of security solutions for customers.

In addition, in a networked business environment, the value for the customer is no longer tied up to a certain service or process, but the service forms an entity that helps the customer achieve its goals easier and more cost-effectively. According to Lampela [20], to produce innovations effectively, organizations need to operate in networks, and networking in organizations and especially in the area of innovations has increased due to several reasons. The need for satisfying various customer requirements has increased the complexity of products and services, which means for the organizations an integration of broad set of specialized skills, and complementary strengths are often sought from partners as each organization is concentrating on core competencies. Lampela [20] mentions other reasons for the increase of networking in innovation, such as leveraging the often high risks in innovation activities and possibilities to learn from partners, gaining access to new knowledge, resources and markets.

This paper provides as an example how ITS technology can be used to improve supply chain security. Starting from the stakeholder requirements, a high level architecture regarding the

information to be collected and to be exchanged between the different stakeholders is developed. The suitable technology is selected and the complete system is designed, including design or tailoring of the software and, if needed, required organisational changes and co-operation contracts. In the next phase the system is implemented, training is provided to the personnel involved, as well as concrete guidelines for service personnel on how to react on the information provided on exceptions by the monitoring system.

4. SELECTION OF THE MONITORING SOLUTION

The most appropriate monitoring solution both in terms of information exchange, performance and economics, depend on the specific demands of information exchange.
Different models can be identified [21]:

- Black box model: no information is shared between the supply chain partners during transport or other logistics processes. Problems are noticed and actions are taken with a significant delay. No major technologies are utilized in the black box model, and all actions related to identification and other logistics processes are conducted manually.
- Notification model. Notifications (advising) and other exchange of information are based on manual data input at nodal points of the supply chain (related to handling of goods). The notification model alarms about deviations only just when an anomality has been identified (e.g. a seal is broken, part of consignment is missing at destination).
- ID-model, which uses identification technologies (OCR, barcode, RFID) to enable collection and transmission of tracking and monitoring information. GS1 EPCglobal has developed a whole suit of specifications and standards starting from the actual air interface of the tag and the data content of the tag to the EPCIS information services.
- Continuous monitoring model. Real time wireless communication together with sensor technologies enables significant development of the supply chain monitoring and tracking solutions. New technologies can further facilitate the improvement of business processes and can speed up the growth of e-logistics.

5. CONCEPT FOR THE MANAGEMENT OF EXCEPTIONS IN SUPPLY CHAINS

Tracking and monitoring systems on the market are mainly used in supply chains covered by a single vehicle. Multimodal consignments pose challenges both to the monitoring unit as well as to the collection of information from partners. Through measurement of location and of the environmental conditions during transport, and by real-time communication with a background system, the complete supply chain can be monitored from origin to destination.
Critical issues in the monitoring of consignments moving through the supply chain are the identification of exceptions and the efficient reaction on exceptions (e.g. search of misplaced products, attempt to recover stolen products). Exception management consists of monitoring, diagnosis, and resolution that are involved in the process of keeping track of logistics

activities, checking the cause of the exception, and applying the solution for the exception [22]. An efficient resolution of exceptions is critical, since without effective response measures, which allow normalizing the situation or at least mitigating the damage, without unnecessary delays the overall impact remains limited. Procedures for exception resolution involving security personnel in nodal points of the supply chain should be put in place to optimise exception mitigation and goods recovery.

Efficient detection of exceptions requires not only monitoring technologies, but also a proper understanding of the exceptions and the actions needed to manage them. For the correct identification and diagnosis of exceptions, the information from monitoring equipment has to be fused with other available data, such as:

- shipment plan. Documents regarding the shipment, such as the waybill, packing list, expected route and timing; Changes in the transport plans (e.g. rerouting, unexpected time delays) should be informed. Hence, involvement of all supply chain actors is desired and training of all personnel which will be in contact with the technology is important.
- environmental data, such as meteorological data, road traffic and road weather conditions, news (special events, strikes,…)
- in terminal areas, information from CCTV and imaging systems.

By combining all relevant data, knowledge is gained on the actual status of the consignment (location, transport mode and process, such as loading and discharging…). Also the lack of information can raise an alert, e.g. if the back end software notices that no location information is received, this may be due to an obstruction of the tracking device (e.g. moved to a location where there is no cellular network), to failure of the tracking device or to jamming of the communication network by criminals. Figure 2 shows the concept for monitoring goods in multimodal supply chains.

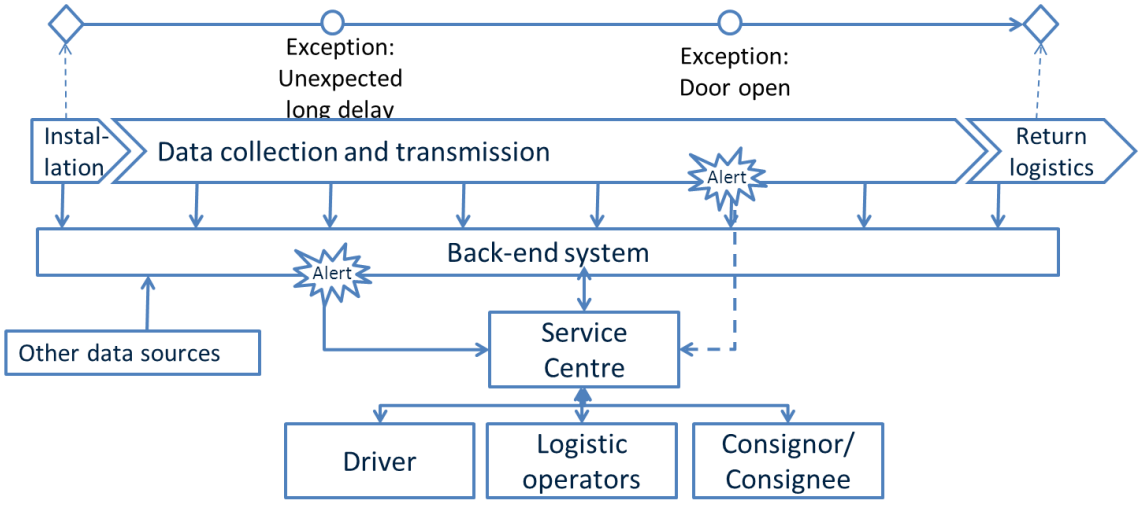

Figure 2: Concept for real-time monitoring of shipments

Monitoring equipment is attached to the goods, the vehicle or the transport unit. Alerts can be

generated by the monitoring equipment or by the back-end system, which combines the data with the other available data. A service centre, hosted by the partner responsible for the security of the supply chain, takes care for real-time follow-up of shipments, and reacts on identified exceptions.

The selection of the asset, to which the devices are attached and the movement of which is monitored, depends on the needs and the possibilities of the actors involved. In order to track single goods of high value, the tracking unit should preferably be directly attached to the unit. For consignments containing many different parcels, the transport unit may be a more appropriate asset to follow. The actor in charge of security may however not have the possibility to attach the equipment to the asset of interest, for instance if he does not have access to the asset, or due to size or performance limitations of suitable devices (e.g. battery limitations, transport in metal enclosure). Tracking equipment is widely used in vehicles, where they can be easily attached permanently to the electric supply, which eases maintenance and management of the devices. Tracking equipment is available for containers, which have special requirements regarding the position of the antennas, but leasing conditions (no holes can be made in the container) and the global loop (difficulties in return logistics and Customs acceptance of add-on equipment to containers) put challenges to the use of the technology. If the asset, to which the tracking unit is attached, is not the asset of interest (e.g. the vehicle in which the asset is transported is tracked instead of the asset), the data is not valid anymore when unit and asset of interest are separated, either through theft or through missing data (e.g. there is no information on the moment that the asset has been discharged from the vehicle).

In addition to exception management, the monitoring equipment also creates possibilities for improving the efficiency of supply chains, e.g. through more accurate estimates of the time of delivery, and a more accurate inventory of transport resources [23]. In addition there are many foreseen impacts of monitoring solutions on supply chain quality indicators such as service level quality.

Monitoring of shipments facilitates increased automation, reduces costs and lead time, and enables possibilities to react on deviations. For example, re-scheduling and re-routing can be done faster when deviations are recognized in real-time. Finally, monitoring may be required because of the nature of transported goods. In these cases, sensors are applied in order to collect information about the conditions (e.g. temperature, humidity, shocks) during logistics operations. For example, Raab et al. [24] have agreed that monitoring of optimal temperature is a prerequisite for cold chain management. Only efficient monitoring ensures the quality, safety, and economic viability of the supply chain.

6. MONITORING TECHNOLOGIES

The following ITS technologies can be added to cargo and load units:

- RFID-(Radio Frequency Identification) tags for identification of cargo, load units and vehicle at reading points. RFID is an affordable and standardised technology, which allows automatic reading in free flow at discrete spots [25]. Passive UHF RFID technology allows reading distance of 4-6 meter; active technologies, such as ISO 18000-7 allow several hundreds of meter. A major drawback in tracking is that there is no information if the tag does not pass near the reading units. Standards have been developed for use of RFID in supply chains, but a business case for RFID in open chains has not yet been found.
- RFID-based sensor devices, e.g. RFID seals. These devices allow assessing the integrity of load units at nodal points. Standards have been developed for electronic seals, such as ISO 18185, but have not been taken up by industry.
- Tracking devices for vehicle, transport unit, load unit or cargo. These devices have location and (long-range) communication capabilities, and possibly environmental condition sensors. Monitoring of vehicles is already much in use, through on-board installed fleet management equipment, which transmits location to a back end server. These units can follow the cargo from origin to destination and provide information on the transport conditions (such as temperature, shock, humidity) to the background system of the service provider [26]. The complexity of tracking devices varies from simple location devices, which send location on demand, to advanced sensor systems, which sense load unit conditions (door status, temperature…) continuously and report to back end system in real time.
- Container security devices (CSDs), which detect opening of the load unit and/or intrusions and transfers the data to a control centre. The device does not directly prevents opening of the door, only informs of door opening. The device is either a single unit or consists of a set of wireless devices. The communication between the CSD unit and the control centre can be based on (a combination of): cellular communication, satellite communications and short range communications (e.g. RFID based on ISO 18000-7). Procedures have to be put in place to distinct authorised from non-authorised opening, and all actors (including Customs) have to be trained to comply with the security procedures.

7. CONCLUSION

Management of the security in complex logistics systems requires innovative monitoring solutions that enable real time tracking of logistics processes and reacting deviations. Increasing security allows also improving the transparency and efficiency of the supply chain, and offers possibilities to supply chain stakeholders and third parties for new business concepts and value-added services.

Different stakeholders in the supply chain have different requirements regarding security, and make independent decisions, which complicates the management of the complete supply

chain security. Potential solutions may involve transfer of information at nodal points using e.g. RFID, or real-time tracking of consignments, using advanced tracking equipment with sensors. The use of monitoring devices, containing location sensors, cellular or satellite communications and possible additional environmental sensors, allow real-time detection and diagnosis of exceptions – if information is fused with other data sources – and hence make it possible to mitigate threats. This requires however that the data are followed on a 24/7 basis and that follow-up actions are well described. Hence, security improvement requires the collaboration of all actors in the supply chain.

8. REFERENCES

[1] CIPS, "Supply Chain Vulnerability," CIPS, 2006.

[2] R. Narasimhan and S. Talluri, "Perspectives on Risk Management in Supply Chains," *Journal of Operations Management,* 2008.

[3] FreightWatch International, "FreightWatch International Global Threat Assessment," 2011.

[4] A. van den Engel and E. Prummel, "Organised theft of commercial vehicles and their loads in the European Union," Brussels, 2007.

[5] H. Salmela, S. Toivonen and J. Scholliers, "Enhancing supply chain security with vulnerability management and new technology," *IET Intelligent Transport Systems,* vol. 4, no. 4, pp. 307-317, 2010.

[6] L. Urciuoli, Security in Physical Distribution Networks- A Survey study of Swedish transport operators, Lund: Lund University, 2010.

[7] J. Boukachour, C.-H. Fredouet and M. B. Gningue, "Building an Expert-System for Maritime Container Security Risk Management," *International Journal of Applied Logistics,* vol. 2, no. 1, pp. 35-56, 2011.

[8] N. Papas, "Combining EA techniques with Bow-Tie Diagrams to enhance European Port Security," in *International Conference on Paperless Freight Transport Logistics. 10-11.5.2011*, Munich, 2011.

[9] L. Ritter, J. Barrett and R. Wilson, Securing total Transportation networks. A total security management approach., New York: McGraw-Hill, 2007.

[10] B. Peleg-Gillai, G. Bhat and L. Sept, "Innovators in Supply Chain Security: Better Security Drives Business Value," *The Manufacturing Innovation Series,* 2006.

[11] J. Tidd, J. Bessant and K. Pavitt, Managing Innovation: Integrating Technological, Market and Organizational Change, Chichester, England: John Wiley & Sons Ltd, 2005.

[12] P. Trott, Innovation Management and New Product Development, Essex, England: Pearson Education Limited, 2005.

[13] G. Specht, F&E Management: Kompetenz im Innovationsmanagement, Stuttgart, Germany: Schäffer-Poeschel, 2002.

[14] P. Koen, G. Ajamian, S. Boyce, A. Clamen, E. Fisher, S. Fountoulakis, A. Johnson, P. Puri and R. Seibert, "Fuzzy front end: effective methods, tools, and techniques," in *The PDMA ToolBook for New Product Development*, New York, USA, John Wiley & Sons, Inc., 2002.

[15] D. Kim and D. Wilemon , "Focusing the fuzzy front end in new product development," *R&D Management,* vol. 32, no. 4, pp. 269-279, 2002.

[16] A. Khurana and S. Rosenthal, "Towards holistic "Front Ends" in new product development," *Journal of Product Innovation Management,* vol. 15, no. 1, pp. 57-74, 1998.

[17] M. Tuominen, P. Piippo, T. Ichimura and Y. Matsumoto, "An analysis of innovation management systems' characteristics," *Int. J. Production Economics,* Vols. 60-61, pp. 135-143, 1999.

[18] A. Brem and K.-I. Voigt, "Integration of market pull and technology push in the corporate front end and innovation management – Insights from the German software industry," *Technovation,* vol. 29, no. 5, pp. 251-367, 2009.

[19] L. Hannola, V. Ojanen, S. Toivonen and T. Kässi, "Value drivers in supply chain security, the IEEE International Conference on Industrial Engineering and Engineering Management, December 10 – 13, 2012, Hong Kong, ISBN: 978-1-4673-2944-6.," Hong Kong, 2012.

[20] H. Lampela, "Inter-organisational learning within and by innovation networks," Lappenranta University of Technology, Lappeenranta, 2009.

[21] E. Pilli-Sihvola, K. Rantasila, A. Permala and J. Huhtaniemi, "Solutions for monitoring multimodal supply chain," in *e-Freight 2012. e-Freight, International Conference on Paperless Freight Transport Logistics, 9-10.5.2012*, Delft, The Netherlands, 2012.

[22] D. Xua, C. Wijesooriyaa, Y.-G. Wanga and G. Beydounb, "Outbound logistics exception monitoring: A multi-perspective ontologies' approach with intelligent agents," *Expert Systems with Applications,* vol. 38, no. 11, p. 13604–13611, 2011.

[23] A. Permala, E. Pilli-Sihvola, K. Rantasila and J. Scholliers, "RFID–a supporting technology for paperless logistics," in *International Conference on Paperless Freight Transport Logistics. 10-11.5.2011*, Munich, 2011.

[24] V. Raab, B. Petersen and J. Kreyenschmidt, "Temperature monitoring in meat supply chains," *British Food Journal,* vol. 113, no. 10, pp. 1267-1289, 2011.

[25] A. Permala and J. Scholliers, "Freight transport visibility provided by RFID," in *The 16th World Congress and Exhibition on Intelligent Transport Systems and Services, 21-25.9.2009*, Stockholm, Sweden, 2009.

[26] J. Scholliers, S. Toivonen, A. Permala and T. Lahtinen, "A Concept for Improving the Security and Efficiency of Multimodal Supply Chains," *International Journal of Applied Logistics,* vol. 3, no. 2, April-June 2012.