Developing a Security Event Management System for Intermodal Transport

Rainer Müller

Information Logistics
Institute of Shipping Economics and Logistics
Universitätsallee GW 1 Block A
28359 Bremen
mueller@isl.org

Abstract: Bremen, Federal State of Germany, is planning to set up a headquarter for GMES - Global Monitoring of Environment and Security. One goal of the Institute of Shipping Economics and Logistics (ISL) is to develop services for GMES to improve the security in intermodal container transport with emphasis on the maritime sector.
ISL is developing a Security Event Management System which takes care of all security related events in the intermodal chain. The security system registers the schedule and transport information of a container and assigns a corridor for its transport.
During the transport the system receives events which will be used for computing a security risk factor for each container, by considering restrictions like position with respect to the assigned corridor, duration of standstill and others. According to the value of the security risk factor the user will be informed using web services, EDI, or email.

1 Introduction

The optimisation of container transportation relies primarily on a system of trust, where sealed containers move unimpeded through the supply chain (noted in [AP03]). Most of the containers will be transported by vessel which are endangered for terrorist acts.

This paper describes a project of ISL to develop a demonstrator in order to increase the security of container transport chains, decreasing the risk of threats for vessels and for hinterland transportation.

First the result of a former project of ISL will be introduced, which had the goal to develop a Logistics Event Manager which has a lot of similarities to the new Security Event Manager. Afterwards the new concept of this software and the needed security related events will be described.

After discussing several ways how to generate those events and their restrictions, the calculation of a security factor will be described.

2 Logistics Event Manager

The intermodal transport of a container is accompanied by so-called events, which fall into two categories: On the one hand there are expected events such as loading and unloading messages. These and the sequence of their occurrence are clearly defined and can easily be monitored. On the other hand there are events which occur unexpectedly and which may allude to problems such as delay messages or a notice indicating a technical defect.

Nowadays there are Track & Trace systems where a controller is able to get informed about the current events of a shipped container. The disadvantages of such systems are:

- The user gets updated information only on request based on manual interactions
- Users have to contact several sources (e.g. terminals, shipping lines, railways) to get information about the complete chain
- A controller who is responsible for a huge amount of containers has to manually review all these data although he is just interested in transports where something is going wrong.

A better solution instead of those passive Track & Trace systems are SCEM (Supply Chain Event Management) systems, which are well known in the production industry.

ISL has developed such a SCEM system for logistic purposes to evaluate how SCEM concepts can be used for intermodal container transports covering several sub-transports performed by different transport modes (e.g. imports using ocean shipping to one of the big North Sea ports, rail transport into the hinterland, final distribution to the receiver by truck).

This SCEM system, called Logistics Event Manger, compares the expected events with the current events and decides on appropriate pre-configured actions, e.g. to inform the user in case (and only in case) of problems. Problems can be coped with soon after their occurrence and before they cause a severe impact to the transport process. Thus, an optimisation of the transport chains will become feasible.

For each event there are decision rules which examine its occurrence on time, delay or total absence. Depending on the result of these examinations, the SCEM system is able to initiate appropriate actions in a flexible way. It can send emails or SMS which can notify their receivers about the occurrence of a specific event. In addition, the user's computer system can be affected for example such that containers originally associated to a cancelled voyage are marked so they can for example be re-scheduled to another voyage.

3 Security Event Manager

ISL is now about to use the SCEM concept for security purposes as well. Of course there are logistic events which could be also interesting for security issues, e.g. a delayed arrival of the container at a terminal could also be a consequence of a disruption. Nevertheless most events which are important for the security of a transport are not directly bound to logistic processes.

The main idea is to adapt the SCEM concept to security related events. First of all there was an analysis which security related information and events are interesting for an intermodal container supply chain.

3.1 Security related data and events

For a security system we have to differ between static information and events which occur dynamically.

Static information which are interesting for a security system are:

- Value of goods: The higher the value the higher is the risk of theft.
- Type of cargo: dangerous goods could be used for acts of terrorism.
- Destination: There are locations which are more interesting for terrorism acts like others, e.g. terminals.
- Companies: The kind of companies involved in the transport has a great impact on the security, e.g. if they are screened and certified. The more companies are involved in an intermodal transportation the higher the risk of theft or terrorism acts.

In addition to these static data there are events occuring during a transport which could be notified by different systems and persons.

3.2 Automatical messaging of events

By using smart units or smart containers events could be messaged automatically. For example these devices are able to detect breaking the door by light and contact sensors. Furthermore they can notify changes inside the container which could indicate a disruption using shock, fire, smoke and temperature sensors. Some units are able to transmit these data by GSM/GPRS to a security system or use RFID technology to track the container position at important locations. There are also smart units and smart containers equipped with a GPS Module which could be used for permanent position tracking.

But as a matter of fact, due to the high initial and maintenance costs of these devices, their application is feasible in case of containers with high-value goods or dangerous cargo only.

To solve this problem, ISL has developed a low-price solution which can be used on the vehicle, like train, truck, or barge. A standard mobile phone and a GPS receiver (or Galileo in the future) is used to track the vehicle while it is transporting the container

which has to be monitored. A small Java application on the mobile phone is receiving the GPS position from the GPS receiver and sends it via web services to a server. The users are able to track the current position using a Google Maps application.

The current position of the container can be used for generating events, which is one functionality of the Logistics Event Manager and will also be implemented in the new Security Event Manger.

In the Logistics Event Manager, an event will be generated when a transported container enters or leaves a defined area, e.g. a terminal. The user is able to define the position and the radius of locations (like terminals or motorway junctions) as well as the type of event which should be generated by entering or leaving the defined circle.

Figure 1 Generating events by entering area

The server receives the GPS position and detects if a container enters or leaves a defined area and generate appropriate events (see figure 1). The Logistic Event Manager receives the event and decide by using a rule machine to send an e-mail or to use EDI to inform the user. The system is also able to inform the user about standstills of the transport.

This functionality will also be used in the Security Event Manager to generate security related events.

In addition, the user of the system could assign a detailed description of the container´s route, which will be used as a security corridor. By comparing the current position and the security corridor the system can identify a deviation and create an event if necessary, e.g. if a truck is leaving the motorway before it was planned (see figure 2).

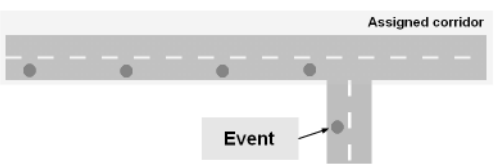

Figure 2 Generating events in case the assigned corridor is left

Beside the comparison of the current position and the planned security corridor the algorithm also has to evaluate the probability of a possible threat. This probability is lower e.g. if the driver of the truck is leaving the motorway in the case of a congestion. There are several countries where TMC (Traffic Message Channel) is available and can be used for retrieving information about congestions. The Security Event Manager should be able to use this information to calculate the chance of a threat.

On the other hand the system will be able to recognize standstills when the carrier is not changing its position for a longer time. There are several restrictions concerning such standstills:

- A standstill somewhere in a forest is more dangerous than on a motorway service area
- The longer the time of standstill the higher the chance of a disruption
- A standstill during the night could be more dangerous than in the daytime

The system also has to take care of events which occurred in the past, because e.g. the chance of a disruption is high if the container has left the assigned security corridor one hour ago and it is not moving anymore.

3.3 Generating events manually

It is desirable to generate events in an automatical manner, but there are events which could only be detected by humans. Furthermore not every container will be equipped with a smart unit.

By using software and hardware clients, especially mobile clients, workers could send messages to the Security Event Manager which has to evaluate if an event should be created. Security related events could be:

- Changed goods, which could be detected by opening the container during a customs check
- False, missing or broken seal
- The carrier, chassis or driver is a different one than the planned one
- High security level of a terminal (in cause of ISPS)
- Nervousness of the driver

3.4 Security factor

The Security Event Manager has to calculate a security factor assessing the current threat level of a transport. This factor will range from 0 to 100, where 100 means the highest threat level.

The factor's range will be divided into three categories: OK, low risk and high risk; which could be used for visualisation purposes.

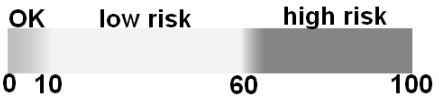

Figure 3 Security factor and categories

Following the SCEM idea security factor itself will be used for generating messages, e.g. Mail or EDI messages, to inform the user proactively.

The calculation of the security factor will base mainly upon the security relevant data (e.g. dangerous cargo, value of goods) and the occurred events.

The user will have the option to declare a container transport to be endangered itself, as a result of circumstances, e.g. a high-value container. This would change the threshold in the algorithm which will increase the security factor accordingly.

4 Conclusions

Security Event Management is a good application for SCEM, but it is necessary to identify the ways how to generate the security related events.

Using synergies of the Logistics Event Manger and identifying the security related events can help to create a new application to increase the security of intermodal transport.

Instead of a small number of logistic events there are a lot of security related events having several restrictions. ISL is about to develop an algorithm to compute a security factor which indicates the threat level which will be used in the Security Event Manager.

5 References

[AP03] APL Logistics, 2003, Adding Security and Value to the Supply chain, http://www.apl.com/news/documents/security_white_paper.pdf

[IM03] International Maritime Organisation, 2003, The International Ship and Port Security Code, 2003 Edition

[CO05] Collins, J., 2005: IBM, Maersk Developing Cargo Tracker, RFID Journal Sept. 22, 2005, http://www.rfidjournal.com/article/articleview/1884/1/1/

[SA] Savi, http://www.savi.com