# Risk Assessment for Container Security – CONTAIN

Pontus Svenson, Joel Brynielsson, Andreas Horndahl, Pontus Hörling, Thomas Jansson, Farzad Kamrani

FOI Swedish Defence Research Agency, SE 164 90 Stockholm, Sweden

***Abstract*—We briefly describe the CONTAIN project, with emphasis on the architecture for risk assessment for customs and logistics.**

## I. Introduction And Background

Each year, there are more than 240 million container moves, representing 70% of world-wide cargo shipments. Container security is thus a vital problem for the European Union. In this paper, we briefly describe the CONTAIN project [1]. The aim of CONTAIN is to specify and demonstrate a European Shipping Containers Surveillance system encompassing regulatory, policy and standardisation recommendations, new business models and advanced container security management capabilities.

CONTAIN will perform demonstrations in the ports of Bologna, Genova and Valencia. Pilot versions of the demonstrations will be conducted starting January 2014, with final demonstrations planned for the period December 2014 to March 2015. The main innovations that will be demonstrated are enhanced positioning devices for containers using EGNOS and Container Security Device; secure and standardized information exchange between all involved stakeholders, including enterprise as well as government authorities; optimization of logistics processes by taking advantage of the information collected for security purposes; risk assessment for logistics, enabling supply chain operators to quickly detect thefts and other illegal actions; and risk assessment for customs, enabling customs to select which containers to inspect for the presence of illegal substances

Here we focus on the risk assessment parts. The tools for risk assessment for logistics and customs share a common architecture, shown in Figure 1, and based on the FOI fusion framework platform [2,3]. Information that is relevant for the risk assessment is transferred from the CONTAIN platform to the risk assessment tools. Risks are then computed using any of a number of different computation modules implemented in the platform.

## II. Container risk assessment for logistics

The user interface for the risk assessment for logistics tool is shown in Figure 2. The seal of a contain in transit through Europe has been broken and the security operators are made aware of this as well as the consequenses of it. The are several important differences between the risk assessment for logistics and risk assessment for customs tools. They are of course based on different kinds of data, where the customs are interested in all available information about the contents of containers, while the logistics tool needs sensor information about where a container is and what is happening to it.

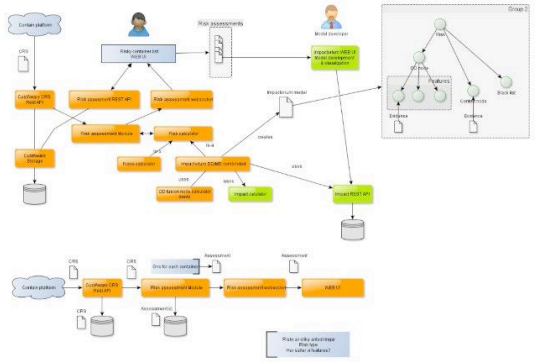

**Figure 1. The architecture of the risk assessment tools developed in CONTAIN.**

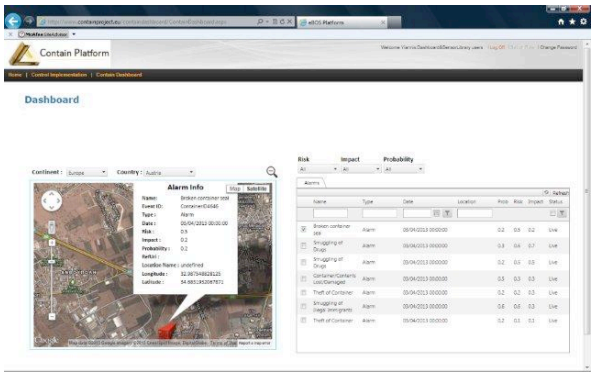


**Figure 2 User interface for the risk assessment for logistics tool.**

Once a risk has been identified, it is important to try to prevent if or else mitigate the consequences of it. A tool for this based on multi-hypothesis management [4] and analysis of competing hypotheses [5] will be tested in CONTAIN.

## References

[1] CONTAIN project web site, http://www.containproject.com/

[2] Pontus Svenson, Tomas Berg, Pontus Hörling, Michael Malm and Christian Mårtenson, Using the impact matrix for predictive situational awareness, In Proceedings of the Tenth International Conference on Information Fusion (FUSION 2007)

[3] Robert Forsgren, Lisa, Kaati, Christian Mårtenson, Pontus Svenson and Edward Tjörnhammar,.An overview of the impactorium tools 2008, In Proceedings of the Second Skövde Workshop on Information Fusion Topics (SWIFT 2008),

[4] Tove Gustavi, Maja Karasalo, Christian Mårtenson, A tool for generating, structuring, and analyzing multiple hypotheses in intelligence work, In Proceedings EISIC 2013

[5] Lisa Kaati and Pontus Svenson, Analysis of competing hypothesis for investigating lone wolf terrorist In 2011 Proceedings of the European Intelligence and Security Informatics Conference (EISIC 2011)