

Baltic Sea Information Motorways

BaSIM



Final Report

Work Package 2



Project part-financed
by the European Union



Work Package 2

Deliverable No.: 7
 Version: 1.0
 Status: Final
 Date: 31.12.2007
 Editor: Horst Pahl
 Author: Horst Pahl

History				
Version	Date	Change	Pages	Author
1.0	31.12.2007	1 st Version	17	HP

Index

Final Report.....	1
The BaSIM Project	4
Work Package 2: BSR Port and Supply Chain Security	5
The strategic focus	5
Regulations and their Implementation.....	6
Objectives.....	6
Regulations.....	7
Methodological Approach	8
Impact of the Regulations.....	9
Fields of Work Package 2 Activities	10
IT Solutions	11
Alarm and Communication Management.....	11
Area Monitoring	12
Hinterland and Chain Security	13
E-Learning (Employee Training).....	15
Impact of the Work Package.....	16
Sustainability	16
Recommendations	17
Annexes.....	17

The BaSIM Project

One of the key elements in the Northern Dimension transport market is the concept of the Baltic Sea Motorways aiming at promotion of maritime transport, multimodality covering also hinterland and logistics in general. Aim of the Baltic Sea Motorways is to make transport in the BSR more competitive. Baltic Sea Motorways is a future vision carried by most of the Baltic Sea countries, including Russian Federation, to enhance co-operation and to optimise logistics systems of the BSR. The necessity is evident when looking at the rates transport and logistics services have risen in the BSR in the recent years and it is forecasted to rise at the same speed also in the next years.

The vision and the first steps have been implemented by BaSIM, under the TEDIM umbrella. BaSIM shall create a sustainable basis for investments in the future aiming at solving existing and coming up bottlenecks in BSR and transnational communication and co-operation.

Therefore BaSIM emphasized simultaneous actions which are needed to develop both physical and information infrastructure within BSR, for an overall improvement of logistics productivity and competitiveness.

The project was divided into four integrated work packages (WP):

WP 1: Standardised ICT architecture: Improvement of BSR short-sea transportation network by collaborative information exchange based on international architecture and standards.

WP 2: BSR Port and Supply Chain Security: Supporting new processes and procedures based on laws and regulations of Port and Supply Chain Security with ICT solutions shown in Best Practice and transferred to an implemented demonstrator.

WP 3: Maritime Transport Corridor Development: Innovative maritime transport corridor concepts and strategies to create the frame for efficient maritime transport and thus facilitate sustainable economic growth in the BSR demonstrated in practical scenario analysis.

WP 4: Supporting information services: Needed to simplify and speed up the implementation phase of new logistics applications and processes between partners in the BSR and also to a wider market including an implemented demonstrator.

Work Package 2

Work Package 2: BSR Port and Supply Chain Security

The strategic focus

The strategic focus of work package 2 lied in the improvement of security of transport and logistics processes by integrated ICT solutions according international security laws, regulations and standards.

Planned results were:

- Overview on worked out processes according new security regulations in the BSR.
- Best Practice Concept on telematic solutions improving security by telematic integration and support in ports and logistics chains, based on evaluation and conclusions of the partners.
- Implemented telematic demonstrator(s) supporting security.

The above shown results which were planned for work package 2 also give the flow of the work to be done:

- Get accompanied with laws, regulations and standards which handle security aspects (mainly ISPS Code (International Ship and Port Security Code), SOLAS convention and IMO regulations)
- Evaluate and give an overview on the implemented processes in ports and at logistics services providers based on the above mentioned regulations
- Evaluate areas where information technologies (IT) can support these processes and enhance security at the same time
- Conclude the areas with the involved partners and companies and describe the possible solutions in a Best Practice Concept
- Draw up a Fine Concepts for the concluded areas on basis of the Best Practice Concept in close coordination with the partners
- Implement demonstrators for the concluded areas on basis of the Fine Concepts
- Test the demonstrators under real life conditions

The following chapters give a short overview on content and surrounding matters. Detailed descriptions can be found in the equivalent documents / handbooks of the IT solutions (outputs of work package 2) attached as annexes which are part of the Final Report.

Work Package 2

Regulations and their Implementation

The following chapters will give a short overview on the regulations and their implementation in general in order to give background knowledge. The objective is not to describe the different national laws and transfers but to show in short the basis on which the further work in work package 2 was installed.

Objectives

The amendments to SOLAS (International Convention for the Safety of Life at Sea), the ISPS Code, were decided 12.12.2002 and entered into force in July 2004. The overall aim of this code is to establish a new international framework of measures to enhance maritime security, through which ships and port facilities can co-operate to detect and deter acts, which threaten security in the maritime transport sector.

It shall reach these aims by defining and fulfilling the following objectives, which are

1. to establish the international framework by involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade;
2. to establish the respective roles and responsibilities of the Contracting Governments, Government agencies, local administrations and the shipping and port industries, at the national and international level for ensuring maritime security;
3. to ensure the early and efficient collection and exchange of security-related information;
4. to provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels; and
5. to ensure confidence that adequate and proportionate maritime security measures are in place.

The ISPS code embodies several functional requirements, which include

1. gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments;
2. requiring the maintenance of communication protocols for ships and port facilities;
3. preventing unauthorized access to ships, port facilities and their restricted areas;

Work Package 2

4. preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities;
5. providing means for raising the alarm in reaction to security threats or security incidents;
6. requiring ship and port facility security plans based upon security assessments; and
7. requiring training, drills and exercises to ensure familiarity with security plans and procedures.

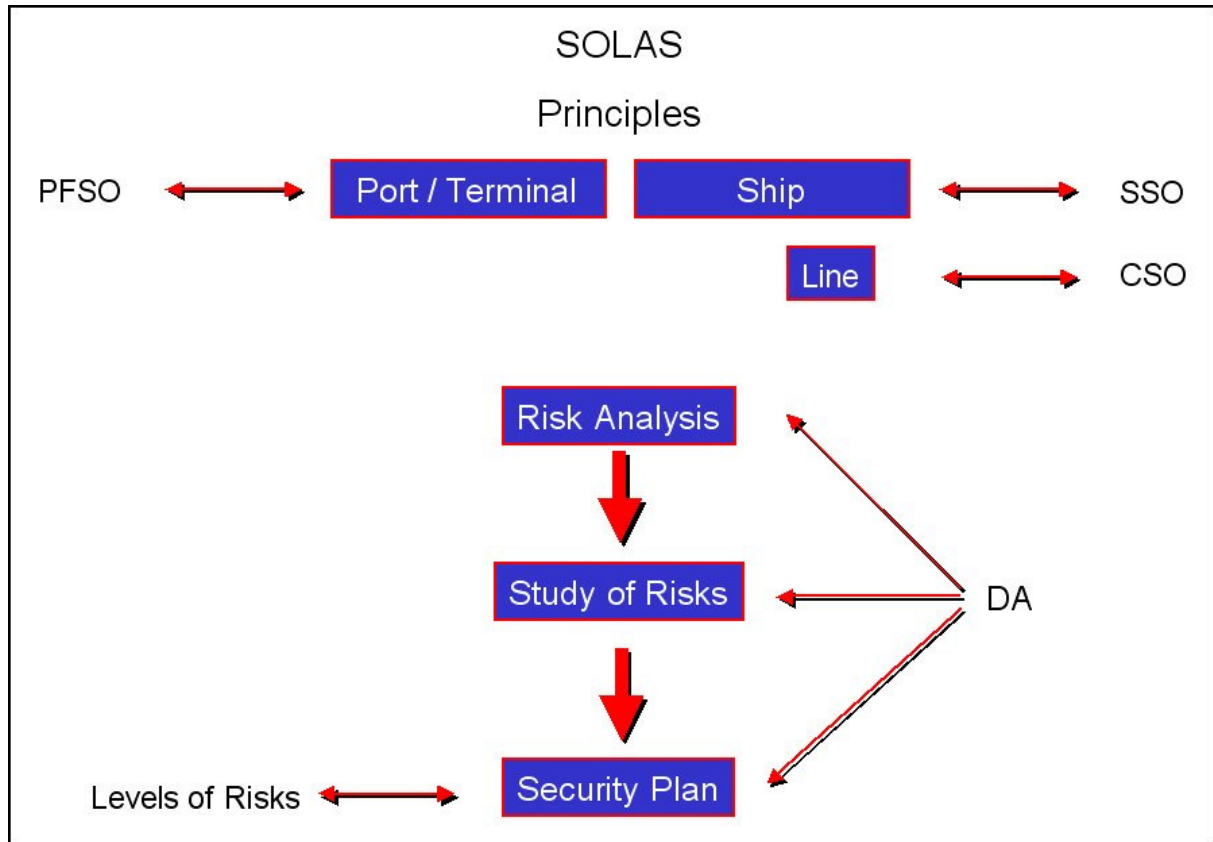
Regulations

To participate in this ISPS regulation framework, ports and companies have to go through different levels of processes for getting the necessary certification.

- Estimation of security + risk of ships and port facilities.
- Generating an appropriate security plan.
- Verification and approval of this plan.
- Verification of the security systems aboard and on land

The regulations, which require changes and improvements in processes within the companies and ports as also perhaps constructional changes and enhancements in IT systems, are mainly concentrated within the security plan.

It bases on three security levels and addresses the necessary steps and activities within each level and concerning the switching between them.



Methodological Approach

In general the implementation of all these requirements meant and still means changes and enhancements to existing processes and facilities, in all meanings, as organisational changes, structural changes and enhancements and technical improvements or implementation of IT support.

In order to find out the general but also the individual impact of the new regulations different ways were gone:

- Questionnaires were worked out and sent to
 - selected partners of the BaSIM Project
 - partners of the work package
 - selected companies, authorities and institutions
- Expert meetings and interviews were held with
 - Port Facility Security Officers (PFSO)
 - Company Security Officers (CSO)
 - Ship Security Officers (SSO)
 - Members of Port Authorities or equivalent units
 - Members of Port- and Terminal Operators
 - Members of ISPS Code and security related units

Work Package 2

Close relation to the BSR and its ports was one of the fundamental items while selecting the partners.

The results of the questionnaires, meetings and interviews were analysed and put down in the document “**Overview on new Processes in the Baltic Sea Region based on new Security Regulations**” (published February 2005, see annex to this Final Report).

These results were taken to find out the impact of the regulations made to the authorities, institutions and companies on one side. On the other side the results were taken to evaluate the areas where IT technology is either missing or urgently needed to support and enhance security processes.

Impact of the Regulations

The following types of impact were separated on basis of the evaluation:

Organisational:

- National organisation, like “point of contact”
- Regional organisations, like “designated authorities”
- Local organisation like “port facility security officer” (PFSO) or “company security officer” (CSO)
- Training of the security personnel
- Implementing communication channels and networks for security issues on regional and national levels
- Employ more security personal

Structural:

- Prohibiting access by fences, controlled access points, etc.
- Setting up restricted areas
- Extending the electronic equipment for monitoring of security relevant areas.

Technical:

- New or enhanced communication lines.
- Video control equipment.
- Electronically supported access control.

These are only the basic elements of possible changes which were given on two different questionnaires, during expert interviews and project meetings. It had to be considered, that the specific implementations were done individually at each port regarding the given boundary conditions and the estimation of security and risk within that port, from which derives the security plan, which was and is not opened to the public.

Work Package 2

The requirements occurring from the security regulations also have impact to planning procedures as they were handled in work package 3 of the BaSIM Project. Therefore the results of this part of work package 2 were discussed and transferred to work package 3.

Fields of Work Package 2 Activities

The above-mentioned impact had influences on existing processes and created also the demand for IT enhancement or new IT processes.

On basis of the given answers to the questionnaires and from single meetings and talks with PFSOs and CSOs (mentioned above), the following main fields were decided as important in the sense of the BaSIM Project, work package 2, meaning possible IT support.

These were in general:

- Alarm and Communication Management
- Area Monitoring
- Hinterland and Chain Security
- Employee Training via E-Learning

Alarm and Communication Management focuses on the necessary steps for notifying any involved persons and initiating necessary actions in consideration of the security plans in the cases of level changes or other dangerous situations.

Area Monitoring focuses on the necessary functionality for controlling the area by managing patrols, checkpoints and related status information and on all managing activities related.

Hinterland and Chain Security focuses on the transport activities from sender to port acting with new technologies like sensors, GPS, GPRS and RFID in order to enhance security along the chain and with this in ports and on ships.

Employee Training focuses on the training of the personnel, to sensitise them for security issues and to teach them the necessary security guidelines, derived from the security plan.

Looking on these points, there were several possible approaches where modern IT solutions may support the existing and new processes. The solutions were discussed with the partners and had been defined as follows.

IT Solutions

In the following a short overview is given on the solutions decided according the activity fields described above.

Detailed descriptions were first published in the official output “**Best Practice Concept**” (published: August 2005, see annex to this Final Report) and can be found in the different documentations to the different solutions (see annexes to this Final Report).

The concepts and the concrete solutions were first discussed with the partners. During implementation prototyping meetings were arranged with the future users in order to involve them from a very early stage of work. This way of implementation ensured that the envisaged solutions and also the final products get a very high level of acceptance, which leads to a great sustainability.

Alarm and Communication Management

With the “**Alarm Management System (AMS)**” implemented during the BaSIM Project the local communication and activity processes, starting with the information from the Designated Authority to the PFSO or CSO and ending up with defined activities, are handled in a most extensive automatic way. These processes happen within a port region in case of any alert. The activities which have to follow up can be divided in two categories:

- The notification of all involved persons, as so called “*communication branch*”
- The initiating of security activities depending on the security level, as “*activity branch*”.

In case of level change or alert the following general procedure is followed: The Designated Authority gives information to the PFSO, SSO or CSO. The decision-makers then meet and start several the necessary activities according level and security plan. The kind of alert, the reached security level will make it necessary to notify different groups of people and to initiate different types of activities. This all will differ from situation to situation, from terminal to terminal, from ship to ship. All these activities are done in a more or less manual way and using papers to a great extent.

The security plan used is individually harmonised with each port, ship or company. It should contain the phone numbers of people who might be notified, it should contain a definition of who has to be informed in which case, it has to contain all possible activity instructions for the different kind of security levels and situations.

The AMS will not only ease up the different tasks, but also will make them safer in the sense of avoiding mistakes. The system mirrors the workflow in case of calamity as described above. It gives the future users a wide range of administrative functionality in order to prepare real time usage. It gives the possibility of the usage of automatic and technical solutions when starting and monitoring processes according ISPS code and security plan.

Work Package 2

AMS allows adopting the security plan individually for each port, its terminals, ship or company. It integrates communication lines for notification and an integrated functionality to combine persons, processes and activities.

It can provide the user (decision-maker) with automated notifications and can show the necessary steps in that specifically given situation, which was entered by the user before and it helps the user to monitor them or to give him final status information.

Features are:

- Adopting the workflow of the internal security plan
- Differentiation between e.g. terminals in one port
- Entering and editing of basic data (people, alarm, activities...)
- Grouping of contact persons, alerts, activities...
- Association of different persons to groups or different groups to a board
- Entering of different types of alarm
- Choosing automatically the persons to be notified or processes to be started
- Sending email, fax, sms automatically, with appropriate content defined beforehand
- Providing an appropriate list of activities, selected automatically from the security plan in an appropriate order according to the workflow given
- Initiating activities on mouse click, if electronically possible (e.g. increase illumination of specific areas)
- Gathering and showing current status of activities provided by connected systems as port information systems, area access control systems, staff patrol mechanisms, ...

AMS is implemented on basis of Service Oriented Architecture (SOA) and with this follows the newest technology. It has open interfaces and possibilities for creating own, individual procedures within the framework of the security plan.

Area Monitoring

In any of the three possible security levels it is necessary to have control on relevant and important areas. This overview needs to be intensified when increasing the security level. Therefore e.g. in port areas patrolling security staff controls fences, gates, doors and security relevant places, video equipment monitors specific gates and areas, and illumination is used in specific places.

In higher security level, the period between patrol rounds and monitoring increases. In which way this has to be done is fixed in the security plan. The necessary checkpoints are listed there, and also the necessary steps for the further monitoring.

Work Package 2

Possible is would be a system that has a wireless interface to the electronic security plan, to other existing systems and to communication lines, that helps coordinating the patrols.

Features could be:

- generating random routes for patrols by changing the order of checkpoints to avoid traceable behaviour
- sending route info to data handhelds used by patrolling guards
- logging patrolled route by receiving the controlled checkpoints from the data handheld terminals
- providing last status information about checkpoints in case at last visit there was something unusual
- giving information of problems automatically to the PFSO or CSO for starting further activities
- controlling the adjustment of noticed and reported problems

After the project break several discussions with the partners took place and after restarting work it was decided to drop the planned activities according “Area Monitoring”. The necessity did not exist anymore because time has overcome the envisaged solution.

It was decided to have new technologies (SoA and sensors) in the fields “Alarm and Communication Management” and “Hinterland and Chain Security” instead.

The equivalent chapters in “Best Practice Concept” show the envisaged solution.

Hinterland and Chain Security

Port security is tightly connected with the traffic and cargo coming from sea or from the hinterland. Sea traffic has either been controlled already in the counter port or the level of security is upgraded. Hinterland transportations are the main issues for the processes of security in the port or port terminals. The problems which occur are:

- Assurance of the security of the incoming trucks and trailers, meaning no risky cargo has been placed into the trailer during the voyage or meaning the truck or trailer has not been manipulated itself etc.
- Identify of the incoming trucks and trailers to a high level, meaning the truck or trailer is that which has been booked.
- Avoidance of bottlenecks in gate control and the port traffic while checking the truck or trailer as intensive as possible, meaning to have equivalent information as quick as possible and in an easy accessible and clear readable way.

In addition to the problems mentioned the fact of the different players (forwarder, trucking company, stevedore, shipping line) involved in the chain does not ease up the possible solution.

Work Package 2

It was decided to use modern telematic technologies to try to solve the mentioned problems to a high extent. These are:

- RFID (Radio Frequency Identification) tags and readers
- GPS/GPRS transponders together with intelligent server software
- Sensors for different purposes

The used sensors were especially developed for the BaSIM Project. The used sensors are able to communicate with each other. They build up a small local area network and with one sensor being the so called “head sensor” they are also able to communicate to the outside.

By using these innovative technologies the work package 2 stepped into new area of mobile techniques, especially by using all features together in one “security package”.

The whole scenario was built up as follows:

- The company “Mobile Objects” provided the work package with two GPS transponder including the necessary equipment. A manual and electronic access to the monitoring server was installed by the company. The transponder should monitor truck and trailer along the route from address “end loading until the gate of the port.
- TraDaV ordered sensors especially built for the demonstrator scenario. These sensors had the functionality
 - Electronic seal for doors
 - Measurement of distance between truck and trailer
 - Measurement of movements inside the trailer

In addition to the mentioned functionality the sensors were able to build up an internal small network in order to communicate with each other. The head sensor was able to send data via the GPS transponder to the GPS server. The sensors were paid by TraDaV.

- The company “Securitas” provided the work package with one RFID Reader, one RFID handheld reader and ten RFID tags. This equipment was installed to assure 100% identification.
- TraDaV and Lübecker Hafen-Gesellschaft (Port of Lübeck) implemented an application which in case of event accesses the GPS server and reads the data according the read RFID tagnumber, interprets them and displays the results in an online application for the gate personnel. These applications were installed at the Lübecker Hafen-Gesellschaft (Port of Lübeck) at in the system of the Port of Turku.
- In Germany a truck of “BTL NORD GmbH” (a 100% daughter of Schenker) was equipped with a GPS transponder. At the back of the cabin of the truck one sensor was installed in order to measure the distance between truck

Work Package 2

and trailer. The sense was to recognize if the trailer was disconnected from the truck.

- The truck driver was provided with the other sensors. At the status “end loading” the driver installed the seal sensors at the back doors of the trailer and the movement sensor inside the trailer.
- At status “end loading” the personnel of BTL typed in the planned route in order to build up “route fencing”. The transponder and the server always will give alarm as soon the truck left the planned route.
- During the voyage transponder and sensors send data to the server. The sensors only in case of abnormal status, the transponder in decided intervals. The server was comparing route and GPS data and with this checks the “route fencing”.
- Arrived at the port gate the RFID reader reads the RFID tag at the trailer, proves it according the booking lists, and builds up a connection via Internet to the GPS server. The data according the identified transport are collected, interpreted and the result is displayed to the gate personnel.
- If any of the results shows “red” the gate personnel have to check truck and trailer, the entrance to the port is denied.

The described hardware, scenarios and activities were installed and done parallel in Finland, also organised by TraDaV and supported by the Port of Turku and “Schenker Finland Oy”.

Parallel to the tests data have been exchanged between Lübeck and Turku in order to follow and identify the oncoming transports. These data were, besides normal travel data, in special the RFID tag ID, the access data for the GPS server etc. With this requirements came up to enhance data exchange, better to say special messages, as handled in work package 1 has to be enhanced. This was discussed and it was found that after these data will be fixed an enhancement could easily be done, meaning an adjustment of existing messages.

The whole scenario for the first time shows the possibility of the interaction of different innovative technologies like RFID, sensors, GPS, GPRS and different inhouse-systems. It was tested in Germany and Finland during the last months in 2007. The main focus was to show the practicability and not only the feasibility.

Detailed information including also pictures is given in an extra document which is attached as annex.

E-Learning (Employee Training)

According the ISPS regulations the staff has to be trained regularly to know about the security plan and to be sensitised about security issues within the relevant area. To replace the standard training, which is expensive and brings a lot of organisational work, an electronic training system can be used instead.

Work Package 2

It was discussed that a possible system should have the functionalities as listed below:

- Flexible according different types of content (html, .ppt, etc.).
- The necessary topics will easily to adapt changes.
- Tests will prove the gathered knowledge.
- Types of questions and answers vary.
- The answers will be electronically stored.
- Current status per user is stored.
- The training can be made at work with storing and verifying the answers automatically, providing / registering the user as certificated.
- The training can be made at home, delivering the answers later, stored at floppy or sent by email.

It was decided to develop a system which is based on the SCORM standard. This standard is accepted and used as international standard and gives the opportunities of having different types of data as input and of having the possibility defining own content, questions, test etc.

Such system provides the necessary flexibility to avoid organisational work and also fixed and unwanted breaks in daily working routine, because the training can be done when working processes allow it.

Detailed information is given in an extra document which is attached as annex.

Impact of the Work Package

Due to the fact that the envisaged and the implemented solutions were oriented to practical use the interest at the involved project partners and at the partners who supported the work was very high.

Already in the evaluation phase the interest for the Alarm Management System was remarkable, which turned into first demands for prototype implementations at two companies involved in ISPS regulations. Also further areas to be dealt with the system were suggested.

The part of Hinterland Chain Security showed the first time the combined functionality of sensor technology, RFID technology, GPS/GPRS technology and the technology of inhouse-systems. Besides that traffic tracking was shown even during border crossing and modality change.

E-Learning is a future technology to be used especially from the economic viewpoint of education of the personnel. Therefore the choice of implementing an frame for E-Learning purposes was the right choice of the partners of WP 2.

Sustainability

Work Package 2

Already during the final test phases possible future users raised their interest mainly for the “Alarm Management System (AMS)” and the item “E-Learning”.

A first installation of AMS took place already in January 2008. After first work suggestions came up for further enhancement of the system in direction of dangerous cargo accident handling or other exceptional events. The system will also be upgraded with the possibility of having different languages available.

It is awaited that the AMS will be an interest product on the market. It is planned to have marketing events around the Baltic Sea Region for a start.

Actions to be taken with the E-Learning frame are nearly the same as mentioned with AMS. The frame will be used within the Logistics Portal of the Lübeck region. Contacts will be built up with other companies to provide adequate contents, like dangerous cargo handling or transport security.

According Hinterland Chain Security meetings in Turku and Lübeck will be held with the partners in order to discuss the frame and functionality of future using of the equipment and experiences gathered during WP 2 work.

Recommendations

The problem of cost and benefit occurred especially at the Hinterland Chain Security area. The cost for the equipment of truck and trailer lies to the forwarder, whereas the benefit; security according ISPS, lies to the port operator. So the goal should be to give also the forwarder some benefit or the put strength into the reducing of costs at the equipment side. Also making other data sources available for security and monitoring aspects like the German Maut.

Annexes

The following annexes are part of this Final Report:

- “Alarm Management System”, Final Documentation
- “Hinterland Chain Security”, Final Documentation
- “E-Learning”, Final Documentation