

# SIT Seminar



## Perspectives and Issues for European Freight Transport Security Policy

*Jolly Hotel • Brussels, Belgium • 15 June 2004*

### **The Safe and Secure Intermodal Transport (SIT) Thematic Network**

Peter Colon - BCI, SIT Project Coordinator

### **Crime Incidents in Transport**

Ton van der Lee, Dutch National Police Agency

### **Global Supply Chain Security Initiatives**

Susan Evans, Director of Business Development EMEA, SAVI Technology

### **Security from a European Shipper's Perspective**

Andrew Traill, Head of Rail Freight, Maritime and Air Cargo Policy (FTA), European Shippers' Council



**Buck  
Consultants  
International**



For more information please contact:

Mariana Andrade  
ERTICO - ITS Europe  
Avenue Louise 326  
B-1050 Brussels, Belgium  
Tel +32 (0)2 400 0782  
Fax +32 (0)2 400 0701  
m.andrade@mail.ertico.com





---

## The Safe and Secure Intermodal Transport Thematic Network

*Peter Colon - SIT Project Coordinator - BCI*

The Safe and Secure Intermodal Transport project was initiated in January of 2003 and has a duration of 3 years. It is a thematic network, which means that it is not embarking in any new research, but rather, seeks to create a basis for consensus amongst relevant actors in the field of safety and security, on the nature of the problems and the direction in which to seek solutions.

It is an International Forum where the different players in the area of safe and secure intermodal transport can exchange knowledge on innovative technologies, research results and commercial activities.

SIT has three partners:

- Buck Consultants International - the project coordinator,
- ERTICO - dissemination coordinator and cluster leader for the Container Security and Crime Incidents in Transport clusters, and
- ENO Transportation Foundation who is the project's link to activities in the US.

The project also has 6 members who actively participate in cluster activities and in expanding the SIT network. They are:

- Thomas Miller & Co Ltd.
- KLPD (Dutch National Police Agency)
- Europlatforms (European Association of Freight Villages)
- European Community Shipowners' Associations
- International Road Transport Union
- Ilim - The Polish Institute for Warehousing and Logistics

There is currently no overall European approach to intermodal safety and security. The intermodal market is strongly modally driven and heavily based on national developments and regulations. So the SIT project was created to look at the different opportunities to harmonize safety and security standards and to create a seamless information exchange between the different transport modes and between the stages in the supply chain.

This, however, needs to be done on a wider level than Europe because the US, as we all know, are very concerned about security and have created many new initiatives.

That is why SIT is funded by the European Commission under DG TREN, with the support of the US Department of Transportation.

The objectives of the network are to:

- Identify RTD gaps,
  - Make policy recommendations for an intermodal safety and security approach and
  - Provide an information base regarding safety and security, available on the project website.
-



Last year's project activities revolved around 5 different clusters. Research on current issues related to these topics were conducted by experts in the field and reports with a complete analysis of these issues and recommendations were produced and are available on the project website. Other than completing the cluster research for the year, the project also expanded its network, bringing together the different actors in the safety and security arena to discuss issues that had surfaced in the cluster activities.

The five clusters for 2003 were:

1. Security Scenarios
2. Incident management and response
3. Intermodal responsibility
4. Data transmission and hosting
5. Container security

### **1. Security Scenarios:**

The main results of this cluster were:

- Development of a framework for security scenarios in intermodal supply chains
- Selection and description of three intermodal supply chains (chemicals, healthcare, electronics)
- Development of a framework for analysis of the safety and security issues involved.

The three intermodal supply chains were selected for having the following characteristics:

- Business activities with at some stage an exchange of freight between US and EU
- Major role for intermodal transport throughout the supply chain
- Products with a high security profile (related to the value of the products, the importance to society or the risks toward the general public)
- Recognition of the importance of transport security issues by the companies involved.

### **2. Incident Management and Response:**

The focus for the first year of the incident management and response cluster activities was on communication, legislation and documentation for two main areas: freight crime and dangerous goods. Special attention was also given to the transportation of toxic waste.

The main issue with freight crime is that, while there are no borders within the EU to stop criminals from crossing into another Member State, there are still legal and technological barriers restraining data exchange between countries and organisations that could, with timely information, stop or limit this type of criminal activity. A number of companies have begun implementing data exchange systems but these different systems are not compatible and data cannot be exchanged amongst Countries. These solutions are also very fragmented because they are not coordinated with the public authorities of all the different EU member states.

Electronic data exchange is also an issue for the transportation and incident management of dangerous goods. Incidents involving dangerous goods are not very frequent, but when they do occur, the consequences can be very grave. These consequences can be minimised by emergency services' prompt and effective intervention and the selection of optimum response and incident management measures. To do this, emergency services require timely and accurate information describing the incident in as much detail as possible as soon as is practical after the incident has occurred.



Lack of standardization between different public authority agencies and between different EU Member States also hampers incident management involving dangerous goods because it creates a series of communication and organisational issues that undermine the efficiency of law enforcement across the dangerous goods transportation supply chain. This is exacerbated when there are interfaces between different modes of transport that have conflicting priorities.

Effective control, supervision and enforcement of toxic waste transportation is also hampered by the lack of standardization of databases containing information on permits issued and the general lack of data exchange between the public authorities of different countries.

### 3. Intermodal Responsibility:

- In its latest regime, air transport of goods points the way to possible improvement in liability regimes for other modes
- The search for regime simplicity leads towards strict(er) liability
- Forensic difficulties make networked solutions and such apparently useful structures as INCO-term CIF inefficient as to liability attribution
- Efficient tracking and tracing of cargoes stand to alleviate many of the legal problems, particularly helping to focus on which of the network regimes apply
- Mandatory national and international regimes sit uncomfortably with freedom to contract; and different national courts and legal systems apply and interpret even globally-accepted Conventions in different ways
- The commercial instinct is all too often hesitant to alter the fundamentals of on-going commodity market and transport practices- even if they are illogical, unbalanced or anachronistic
- The EU focus towards the neutral "Freight integrator" has a bearing on many of the above topics

Coupled with the deficiencies in respect of first-instance responsibility is the continuing difficulty of pinning liability on a party other than the last carrier, because of the forensic problems of determining when, where, and through whose fault a loss, damage or delay in respect of the cargo occurred. As we point out in our paper, the rapid progress being made in tracking and tracing of cargo offers real hope of improvement in this regard.

The overriding hope of many whose research or commercial practice involves consideration of the responsibilities inherent in intermodal transport of goods, is for there to be replacement of the existing unimodal Conventions with a single transport Convention, covering all forms of transport and applicable irrespective of whether the cargo is covered by paper or electronic documentation. We have pointed out in our paper typical difficulties of overlap between Conventional application (centred, for example on lack of clarity at interchange between stages of the journey - such as a holding area on the dockside or in a depot - or where a cargo which has been carried by road is then loaded onto a ferry- whether or not still on its road trailer). There are also many impediments in the path of parties who wish to set in train an end-to-end contract of their own, in that one Convention or another may well be given mandatory effect and thus override their own contractual provisions despite their wishes to the contrary.



#### **4. Data Transmission and Hosting:**

In the first year of the SIT project, cluster work has concentrated on the development of an analysis methodology, aimed at future assessment of the risks and possible measures to reduce the risks related to data transmission and handling in intermodal transport.

The proposed methodology, i.e. RMT (risk measurement table), was presented to the consortium and subsequently approved. It enables identification and documentation of the risks and measures in a way which can be easily understood and communicated. The RMT will probably have benefits for the other clusters as well.

#### **5. Container Security:**

When the subject of container security is broached, container seals are invariably mentioned. For 2003, the Container Security Cluster focussed on the main issues that arise when using container seals and also what can be done to improve their effectiveness.

A comprehensive look at the transportation supply chain was undertaken to understand the main issues with the use of container seals. Seals increase security in many ways, but a seal will only work if the personnel involved are trained and informed. For any type of seal to work, whether it is a simple mechanical seal or a more complex electronic seal, certain basic rules have to be followed. Based on the issues highlighted in the supply chain analysis conducted, a few simple guidelines, both for seal manufacturers and seal users were developed to increase the effectiveness of seal use.

Seal replacement and empty containers can potentially pose risks to security. Companies are under no obligation to seal empty containers and do not do so because of the high cost entailed, leaving these containers vulnerable to tampering. Also, when containers are controlled and inspected, authorities many times remove a very high security seal and replace it with those of a lower calibre. This problem will be further aggravated when the use of electronic seals increases. What will authorities use to replace them?

Legislation regulating seals in the EU and the US differ widely and, even within the EU, some Member States have more stringent standards than others. This lack of international standard creates confusion and inefficiencies on several levels particularly because there is no central database that states what seals are approved by what country.

The events of September 11th have triggered further evolution in the field of container security and technology is now seen as a viable solution to make containers "smart" and, therefore, more secure. Recently, electronic seals have been developed which permit remote sensing of the seal status and automated identification. Changes in the field of container seals will continue at a rapid pace as companies structure their operations to ensure greater security and safety in the transportation of goods.



You can join the SIT Network and participate in one of the many activities planned for 2004. This includes:

- A number of round tables that will be held throughout the year to discuss with experts "hot topics" in the area of intermodal safety and security
- The SIT SEMINAR, taking place today and the seminar and conference scheduled for 2005
- The cluster work, that centers around specific topics
- The results of these discussions and other information will be diffused via the project Newsletter and the website

The SIT website has a major role in the project, since all activities are disseminated through it and all documents produced by the project can be found here. The information base available on the website is constantly updated and holds the latest information in the area of intermodal safety and security. Including:

- policy developments,
- related initiatives and projects,
- the latest technologies and
- a host of other information.

The website is currently being modified and will contain regularly updated news on all the aspects of transport security.

The SIT website is also where you can share information on current products and projects that you are working on and share your issues with others.

- issues that surfaced during the cluster work undertaken last year and based
- feedback received from experts via meetings, networking and the project website
- Current market needs

The safe and secure intermodal transport thematic network has determined that, for 2004, the project activities will centre around six main topics:

1. Crime Incidents in Transport
2. Certification of Transport Providers
3. Data Transmission and Hosting
4. Container Security
5. Risk Reduction in Supply Chains
6. Demonstration Projects

#### Crime Incidents in Transport

Main objectives:

- Assess the scale of the problem
- Gather information on incidents with greatest economic impact for Europe
- Identify main issues and best practices
- Identify relevant databases



Focus on the several issues related to certification of “secure” transport service providers:

- Identification of certification schemes
- Contribution to a secure supply chain
- Certification versus regulation
- Best practices

### Certification of Transport Providers

Main objectives:

- Identify main problems regarding data transmission and hosting (especially between various modes of transport)
- Identify main measures taken by service providers to minimise risks
- Identify best practices
- Complete Risk Measurement Table

### Container Security

- Focus on container security systems in place that make container seals more effective. Including:
  - o Personnel Training
  - o Processes to secure and monitor containers
- Identify measures regarding container security
- Gather information on practical problems companies face when dealing with these measures

### Risk Reduction in Supply Chains

This cluster will look for best practices regarding the application of safety and security systems in selected supply chains:

- Information will be gathered from several sources
- Problem areas will be identified
- Solutions will be presented

### Demonstration Projects

This cluster will bring together project leaders from relevant demonstration projects throughout Europe to share experiences and disseminate results

- public projects
- private projects

The SIT network has been created for all of those who are interested in the area of intermodal safety and security so please, become part of the SIT network:

The Thematic Network is open to all:

- Share information on projects and products
- Discuss your issues
- Participate in workshops and seminars
- Contact SIT at: [sit@mail.ertico.com](mailto:sit@mail.ertico.com) or through [www.sitglobal.org](http://www.sitglobal.org)



---

## Crime Incidents in Transport

*Ton Van Der Lee - Foundation for Tackling Vehicle Crime , Netherlands*

If we look at vehicle theft in the past three years, we can see that passenger car theft has declined by 20% in 2003 and has also declined for 2004, while there has been no change for vans, lorries and trailers. There are over 400 000 vehicles stolen in Europe per year, which adds up to a total cost of 15 billion euros per year.

Trucks can be stolen for many different reasons. There are different reasons to steal a truck:

- ringing
- parts
- the load

90% of theft is cargo theft however, stolen trucks are also used to transport stolen goods. Trucks are also, many times, stolen so that thieves can utilize the actual vehicles. Thieves can use gas and weapons against drivers or use fake police uniforms.

The theft of load in Netherlands causes 150 million Euros in damages per year to the transport supply chain.

In the Netherlands, an investigation of a criminal group revealed that one of its members was a driver who had worked in 20 different companies. He had extensive knowledge of the security policy of all these companies. This lead to the conclusion that there is a lack of screening of new drivers.

There is a very big market for stolen goods. Stolen loads can usually be sold within a few hours or days.

Prevention measures are very important. Companies and governments need to work together to ensure that when regulations are put in place, security for drivers is provided. For example, with the new legislation covering driver resting time, governments should ensure that drivers have safe parking spots where they can stop their vehicles.

All the different parties involved in the transport supply chain need to work together across borders to achieve the same objective - to catch the thief!

---



---

## Global Supply Chain Security Initiatives

*Susan Evans - Director of Business Development EMEA, Savi Technology*

The many different security initiatives currently in place are not just focussing on port to port legs or inbound legs but rather, the whole supply chain.

Initially led by US Customs and Border Protection right after September 11th, new legislation has been implemented to increase security in the transport supply chain. This includes:

- The 24 Hour Manifest rule. EU customs has also implemented measures similar to the US 24 hour manifest rule but the difference is that they require to have the manifest 24 hours before the vessels reach the ports.
- Smart Containers supporting C-TPAT and,
- the IMO's ISPS code.

There are a number of initiatives currently taking place around the globe. Some are led by government agencies and some by private companies. The US trade development agency, for example, has provided funding for developing countries for such projects as the STAR/Thailand BEST project and SST Africa Feasibility Study

Most projects address the use of technologies and process definition to provide better visibility, control and documentation of shipments. These new initiatives do not set out to create new technology but rather, use existing technology to make more information available to the different players in the supply chain, automate processes and make supply chains more efficient. We should leverage existing learnings and best practices and look at the applicability of these projects in Europe.

### Operation Safe Commerce (OSC)

The US government, under the Department of Homeland Security, has provided 58 million dollars for a project with 18 tradelane pilots. This initiative is called Operation Safe Commerce (OSC) and will be completed by the end of 2004.

The tradelanes comprise corridors from Asia to the US and from Europe and South America to the US. These projects look beyond the use of electronic seals because it is easy to take the doors off a container without breaking a seal. It looks at multiple components:

- tracking
  - non-intrusive inspection
  - intrusion detection
  - threat sensors
  - information systems
  - and other technologies
-



These technologies also help diminish the amount of intrusive inspection necessary (physically opening containers for inspection), thus decreasing supply chain duration and costs for shippers.

The concept of Security Layering is also very important. Depending on the level of security threat, different security layers are applied, such as; shipper verification, container tracking, scanning, intrusive inspection, etc.

### **Smart and Secure Tradelanes**

The SST project, on the other hand, is industry led and was initiated by P&O Ports, Hutchinson Port Holdings and the Port of Singapore Authority. Phase I of SST is completed and for Phase II the focus is network expansion, growing volume of containers on the network and additional technology where needed.

Three tradelanes are also being tested in Africa under SST Africa. This is sponsored by the USTDA and the project includes advisory roles from World Customs Organization and local customs participation as well as a global Insurer. .

### **Safe and Secure Intermodal Transport Across the Globe**

The SIMTAG project is a European Commission project that aims at improving safety, security and efficiency. It has created an Internet portal that stores information that can be shared by different players in the transportation supply chain.



---

## Security from a Shipper's Perspective

### *Andrew Traill - Head of rail freight, maritime and air cargo policy*

The European Shippers' Council is a pan-European body whose members include organisations such as the FTA and whose purpose is to provide its members with a European voice and to provide information and networking on issues of common concern.

As with any pan European organisation, its views can be mixed. On security this is not different. There are those who are concerned or sceptical about the need for more security in the supply chain and fear that it will become a barrier to trade and especially tear down the principles of SEM if applied to intra-EU trade.

Others (including the FTA) have more easily accepted the inevitable drive for security from our participants and governments and accept the fact that industry must take some responsibility for helping protect society and the economy from terrorists.

This is the starting point we have chosen because when all is said and done, we have to minimise the impact of potential barriers to trade and find benefits.

The FTA has long believed that the best way to minimize negative impacts of heightened security is through the Known Shipper System. The ESC has supported this in the absence of any other solution.

But the known shipper system needs to be clearly defined as there is often confusion. The term Known Shipper is misleading because it involves shippers, carriers, agents and whomever else is in the supply chain.

It is all about securing cargo from unauthorised access and making this known to the authorities. You can make cargo known at any point in the chain, it doesn't need to start with the shipper. But, of course, if the shipper leaves it up to someone else to secure the cargo and make it known, there will be costs attached and it may not be an easy thing to do.

So in our known shipper system, you could have a known shipper, a known operator and a registered (or known) agent. What do they all do?

**Known Shipper** - Secures cargo from point of origin (this ensures that those in the chain maintain security of cargo when it is in their hands) to either the port of export (assuming ISPS port and carrier or airline) or through to the end customer.

**Known Operator** - can include road carriers, rail, inland waterways. They are the ones that maintain security of the cargo.

**Registered Agent** - contracted by the shipper who either maintains security or makes it secure and ensures it is secure through the supply chain.

---



What qualifies one as a known shipper?

The security plan checklist, distributed to seminar attendees, can be used as a guide to explain what it is they might be expected to do to qualify as a known shipper. It is a mixture of elements found in the practices of C-TPAT, TAPA, ISPS and UK Airfreight.

Risk Assessment:

There is no guarantee that just because you are a known shipper that authorities will look at your cargo as low risk. What can make cargo low risk or high risk? You could be from a high-risk area or carrying dangerous cargo. There are different factors that will increase your chances of being checked or delayed but one would expect the chances of this being greatly reduced.

But risk assessment could appear subjective:

Decisions will vary according to:

- National threat level
- Perception of threats elsewhere
- Specific intelligence
- Trust in other states' policing. EU member states will not trust other member states to police according to their levels. The standards applied may well vary and because of this potential for variance the known shipper system is voluntary. The member states will make their own minds up as to what is a threat or not and how they will react. It is not the job of the industry to do this.

But industry, or rather individual companies, will need to second guess and decide

- a) What security measures and standards will reduce the risk of delay?
- b) What measures can it afford?
- c) What measures are worth the cost?

Member States will need to ask themselves:

- Does this apply to international, EU or domestic transport?
  - o What are the terrorist threats
  - o What are the economic consequences?
- How can it be policed?
  - o Resources
  - o Costs
- How effective will it be?

And what if a few companies determine the benefits of the known shipper, known operator and registered agent are not worth the costs?

- Will it make it harder to secure national interests?
- Would making it mandatory score an economic own goal for the terrorists?
- It's for governments to decide - and for us to explain - the consequences for trade and industry



---

What are the commercial incentives for the industry?

- There are commercial and supply chain benefits but they are not always easy to quantify. If Member States want industry to volunteer in greater numbers, they need to provide incentives:
  - o Insurance - they need to cap the liability on the consequences of a security incident

It is a pragmatic approach, accepting the inevitable and we can be challenged on this.

We are happy to look at any alternatives but until something else appears, we think the known shipper system, as I have explained, will minimise the impacts of tighter security. What assets are we trying to protect? Our business from the impacts of security regulation, business people from prosecution. And our brands. No one wants their brand associated with a terrorist attack. Quick start-up of business. If there is an event, industry needs to start moving again swiftly or else their own survival will be in doubt.

There should also be benefits for companies that choose to sign up. This will be in the form of:

- Control of the supply chain
- Efficiency
- Lower costs
- Reliability
- Lower theft.