EUROPEAN COMMISSION
DG TREN

SIXTH FRAMEWORK PROGRAMME

THEMATIC PRIORITY 1.6

SUSTAINABLE DEVELOPMENT, GLOBAL CHANGE & ECOSYSTEMS

INTEGRATED PROJECT – CONTRACT N. TREN-06-FP6TR-SO7-69821

Retrack

REorganization of Transport networks by advanced RAil freight Concepts

Deliverable no.	D2.4
Title	Safety and security: State of the Art: Summary
Dissemination level	Public
Work Package	WP2
Author(s)	Jean Claude Dellinger
Co-author(s)	George Kotsikos
Status (F: final, D: draft)	F-01022008
File Name	D2.4-Public-Safety and Security State of the Art: Summary-Final v3-Dellinger-01022008.doc
Project Start Date and Duration	01 May 2007 - April 2011

SIXTH FRAMEWORK PROGRAMME

SAFETY and SECURITY State of the Art: SUMMARY

Rail transport security faces new threats from international terrorism which are not well defined. Nevertheless **new rail freight service** launching makes mandatory, via an integrated approach, to **address current security threats** and to assess social as well as **economic consequences**. While providing reliable, cost-effective tools in assessing, preventing and combating the novel threats of international terrorism different framework conditions and **regional disparities** have to be regarded.

The objective is to identify terrorist threats and consequences to new rail freight service with the potential to support the industries and transport operators' **competitiveness, identifying and promoting threat-cost-benefit optimised solutions**.

The security is dependent on **efficient cooperation and coordination** among Public Authorities (in charge of threat identification) of the States concerned by the new service, the EU Institutions and the relevant stakeholders. The threat posed by the criminal use of dangerous substances and the **level of risk involved** is also dependent on this cooperation and coordination.

Customs and border protection **requirements are constantly evolving**. Traditional fiscal roles continue (such as the collection of excise duties), but there is now additional emphasis on the identification of threats to **local** and **national** security – a first line of defence against possible insurgent attacks.

The priorities have moved from monitoring cross-border cargo and reducing international shipments of contraband, to **screening** for explosives, arms, dirty bombs and weapons of mass destruction.

Identifying such threats is increasingly more difficult, hidden inside a vehicle or concealed in the middle of the shipment. The **challenge is rapid detection without disrupting the daily flow of goods**.

A lot has already been achieved concerning the security of dangerous substances (HCDG like explosives, radioactive products, etc) both in the Member States and at EU level. It is clear however that more can be done in such areas as enhancing the exchange of information, disseminating best practices, **establishing coordination mechanism and taking joint actions** on particular issues.

The issues of cargo tampering, people and contraband smuggling and terrorism need to be assessed and solutions evaluated based on a **realistic freight "Risk" assessment associated to « transport mode » and local threat scenarios**. Tracking of cargoes, sensors to notify the operators of intrusion and performance of cargo control and protection must be evaluated to ensure security **without harming transport chain activities fluidity, productivity and cost-effectiveness.**

TABLE OF CONTENTS

TABLES

FIGURES

1 DELIMITATIONS

1.1 LIMITED SCOPE

The scope of the present study covers mainly the safety & security issues related to transported goods. The focus of this study will therefore be on the freight/cargo and its environment without developing the security aspect related to the rail system (i.e. rail infrastructure, signalling, power supply). Nevertheless, the impact on the rail system will be mentioned to highlight the problems that may need to be addressed

In relation to the transportation of dangerous goods, the focus will be on security aspects, assuming that the safety measures defined in the existing regulations are fully applied and well known by the stakeholders. Safety is just a word/concept in headlines and crucial challenges in this area are not handled. This is not in contradiction to the purposes outlined in the proposal for RETRACK where security questions are stressed and focused.

1.2 SAFETY VS SECURITY

In this document Safety and Security are linked to some keywords that are used to precisely define the application domain and consequently the measures than will need to be considered to solve specific problems. It is important to note that the need for "**identification**" is mandatory for both, but not in the same way (see the example for Nuclear material).

SAFETY	SECURITY
PROTECTION	**PREVENTION**
detection of "RISK"	"SEARCH" devices
"post-accident"	"sensitivity"
"emergency response"	source localisers

Need for IDENTIFICATION, via adapted technologies

Example for Nuclear materials (via spectrometry)	
Identify what is happening!	Differentiate between NORM, Medical & Artificial sources
What is the activity & related dose?	Reduction of "false alarms"
What is the real RISK ?	Prevent "masking" of sources
Personal / Mobile / Fixed equipment	**Fixed / Mobile / Personal equipment**
Irradiation Gamma (& neutron) Dosimeters (µSv) Dose rate monitors (µSv/h)	Radiation sources Gamma (& Brehmstralung) Scintillator (cps)
Contamination Alpha & Beta Surface monitors (cps)	Special Nuclear Material Neutron He-3 or BF3 counters (cps)

1.3 DEFENCE VS SECURITY

Defence technologies/devices are not necessarily adapted to the “security” requirements, since the threat environment is very different as is briefly presented in the table below.

Table 1 DEFENCE vs SECURITY, a changing threat environment.

DEFENCE		SECURITY
International conflicts		**Civil wars**
State actors		**Non-state actors**
Identified aggressor		**Covert ops**
High-tech		**Low-tech**
Military casualties		**Civilian casualties**
Mission oriented defence		**Civilian crisis management**

2 INTRODUCTION AND GENERAL APPROACH

2.1 GLOBAL SECURITY

Freedom and justice and to ensure the security of individuals and goods within the European space are the aims of the security strategy adopted by the European Council following recent attacks.

Global security can be defined as the ability to ensure the collective safety of a given group of individuals, with sufficient levels of **prevention** and **protection** against risks, threats of all types and their impact, wherever they come from, and under conditions that favour an unhindered development of collective and individual activities (INHES definition - Institut National des Hautes Etudes en Sécurité).

This definition covers the following components: economic security, health security, IT and digital security (data, networks), territorial security, airspace security, maritime security, civil security and the fight against terrorism, organised crime and fraud.

This general approach, characterised by dealing simultaneously with systemic and transversal security, cause and effect, has been retained by the European Commission. Via think tanks bringing together public and private players, four major security assignments have been defined:

- The fight against terrorism and organised crime
- Infrastructure, sites and networks security
- Border security (land and maritime)
- Crisis management, rapid intervention and reparation

It is in this framework that the RETRACK project falls, adopting this approach to freight transport in general and rail transport in particular.

2.2 FREIGHT TRANSPORT CONTEXT AND GLOBAL SECURITY

As major drivers for the world economy and industry, transport networks are particularly well developed with the exception maybe of the most remote regions of the globe. Every citizen and organization is concerned by transport security. Characterized by an extreme efficiency and flexibility, each network provides a virtual infinite range of opportunities for users, considering all transport modes and the complex infrastructure network. Like any complex system, this tremendous capacity of the transport system introduces some vulnerabilities and malfunctions. Transport vulnerabilities come from the sector's characteristics such as, logistic chain complexity, volumes, range of products (with vague origin / description / owners), the number and the multiple nationalities of actors and the possibility for product's owners to hide their identity behind networks of complex international structures. If control and management of such a system is a major economic stake, it is quite difficult to ensure. These malfunctions and vulnerabilities provide opportunities for criminal and terrorist organizations.

It is quite clear that freight transport lends itself easily to illegal trafficking of all types of products, such as explosives, drugs and radioactive sources. In addition, there is a "human" traffic aspect in the form of illegal immigrants (sometimes potential terrorists or criminals). Directly (vector for terrorist acts) or indirectly (financing through various types of trafficking) these activities often contribute to providing support for organised crime and terrorist networks. The trafficking of dangerous and/or toxic substances and other illegal networks (immigration, refugees, prostitution, etc.) are a major concern for governments and citizens. Moreover, in the short and medium term, they could have a direct impact on the population safety and daily lives (health, violence, terrorism, etc.). In this context, it seems vital to discuss about freight transport, taking into account the security requirements with regard to people and property in general, and the fight against activities connected with crime and terrorism in particular. This is all the more true in the current context of trade globalization and cross-border crime and terrorism development. Moreover, security requirements are an integral component of the discussions taking place in parallel about the internal and external EU policies and values implementation. Indeed increased threats, which can be illustrated by recent terrorist actions against transport, and the vital role of people and goods movement in European and international societies, place transport security as a priority. Some catastrophic scenarios have to be considered. For example, when some illegal substances (and/or individuals) are conveyed by a mode of transport (aeroplane, train, ship, truck, etc.), can transform it into a formidable weapon, discreet and inoffensive in appearance, but easily brought to strategic locations carefully chosen to cause the maximum amount of damage and to be used as obstacles or projectiles.

With the evolution of trans-national terrorism, no country is safe from threats or serious terrorist acts affecting it directly or affecting foreign interests on its territory. The impact in terms of destabilising the population and creating disorder in the country may well be the same or very similar in both of these instances.

The response to this threat therefore must be coherent between interdependent countries and notably between European Union Member States participating in a common vision and a common future. Failing this, the weakest link may well be the first to be attacked, but the repercussions will also be felt by the others.

Each Member State must be able to foresee and be continuously prepared to respond within the framework of its national administrative organisation; likewise, within each transport company, be it urban, regional, national or international transport, etc., each will have to play its role fully because transport is a terrorist target, as history has reminded us unfortunately too often.

3 SECURITY REQUIREMENTS AND CONTROL ACTIVITIES RELATED NEEDS

Ensuring security requirements in the goods transportation field necessitates transparent, reliable and productive control procedures and harmonised norms, standards and equipments throughout the supply chain and notably in nodes (inland waterways and maritime ports, logistics platforms, railway shunting yards, airports etc.). These requirements have direct and indirect impacts on transport operations (longer delays, lower fluidity and productivity) and cost-effectiveness, but also on the administrations in charge of the control.

It is frequently stated that the responsibilities of each and everyone must be defined clearly and the information channels between them must be improved continuously in order to provide the most suitable response in this context. Analysis of threats is the specific work of public authorities and their specialised units whereas analysis of weak spots in transport systems must constantly be carried out by operators in order to reduce them as far as possible.

It is vital for the authorities and companies to work together on this subject so that these two approaches can be compared in order to reinforce protection of citizens. This joint analysis work upstream and coordinated intervention on the field calls for a minimum of common culture and mutual understanding supported by the proper training for the staff concerned.

In addition, detection is linked with identification and must lead to an adopted “treatment” procedure of the inspected loading unit. The data required for decision making must permit a fast and safe intervention, either by putting in quarantine the concerned loading unit or by launching a specific tracking and tracing procedure to follow the illicit substance in mind to know its destination or its final consignee.

3.1 REGULATION IN SECURITY SCREENING

The main actors involved in freight transport regulations and more generally in transport security are the United States Administration, the European Commission and the World Customs Organisation.

Various initiatives on transport security are in progress, starting with air transportation which was the first mode concerned (and which is a reference).

Legislation was applied to **airports**, with common basic standards and inspections on a regular basis. The Chicago convention was interpreted on common bases.

In December 2002, through **regulation (EC) No 2320/2002**, the Commission established common rules in the field of civil aviation security across all Member States. The main objectives of the regulation were to establish and implement appropriate Community measures, in order to prevent acts of unlawful interference against civil aviation and provide a basis for a common interpretation of the related provisions of the Chicago Convention in particular its Annex 17. These objectives were achieved by the setting up of common basic

standards for aviation security measures and appropriate compliance monitoring mechanisms. Introduction of the regulation caused the Member States to review their National Aviation Security Programmes (NASP) to reflect any new requirements within the regulation. The majority of States have supplementary national aviation security legislation, some of which extending the requirements set in the regulation. The key areas impacted include passenger and baggage, airline operations, aircraft, performance and **freight** (screening and trans-shipment handling). The regulation (EC) No 1217/2003 sets out detailed requirements on how the National Quality control Programmes shall be carried out and reporting of undertaken activities shall be reported to the Commission.

Since 11 September 2001, aviation security in the US has undergone dramatic changes. With the enactment of Air Transportation Security Act (ATSA) in November 2001, a single body, the Transportation Security Administration (TSA) assumed overall responsibility for aviation security within the US.

Work on **maritime** security began within the International Maritime Organization (IMO) in February 2002, culminating on 12 December 2002 at the IMO Diplomatic Conference with the adoption of an amendment to the International Convention for the Safety of Life at Sea (SOLAS Convention) and an International Ship and Port Facility Security Code (ISPS). The latter:

- enables the detection and deterrence of security threats within an international framework,
- establishes roles and responsibilities,
- enables collection and exchange of security information,
- provides a methodology for assessing security,
- ensures that adequate security measures are in place.

Thus ISPS code guarantees sound management techniques and in addition the ship itself could be identified (AIS), tracked and has the ability to give alerts.

The Commission has proposed a regulation aimed at incorporating these measures into binding community law (COM(2003)229). The legislative process is currently on-going.

In June 2002, the World Customs Organisation (WCO) adopted a resolution on security and facilitation of the **international trade supply chain**. A task force was set up within its Secretariat-General in order to:

- Define implementing measures
- Protect international trade against terrorist attacks
- Protect the international logistics chain against being used for the illegal transport of weapons of mass destruction for terrorist purposes.

The Kananaskis Summit (June 2002) addressed the subject both in terms of maritime security in general and of the particular case of **containers**.

In parallel with the adoption of the Maritime Security Act (2002) and the creation of a Department of Homeland Security (2003) by the US Congress, three types of recent measures concerning the maritime sector should be mentioned:

- The container security initiative,
- The 24-hour rule,

- The proposed rule making for the elimination of crew list visas.

Agreement with the United States of America on intensified customs co-operation on container security are also in hand.

The European agreement concerning the international carriage of **dangerous goods** by road (ADR), that took place at Geneva on 30 September 1957 under the auspices of the United Nations economic commission for Europe, was entered into force on 29 January 1968. To be more consistent with that of United Nations recommendations on the transport of dangerous goods, models regulations, the international maritime dangerous goods code (of the international maritime organization), the technical instructions for the safe transport of dangerous goods by air (of the international aviation organization), the regulations concerning the international carriage of dangerous goods by rail [RID] (of the intergovernmental organization of international carriage by rail – OTIF/COTIF) and the Leaflet UIC – 471-3 “Inspection of dangerous good consignments in international traffic”, edition 2 from 08/2003 (it is in balance with COTIF and is continuously updated), the ADR has been regularly amended and updated.

The EU Directives 94/55/EC regarding the transport of dangerous goods by road (ADR) and 96/49/EC regarding the transport of dangerous goods by rail (RID) already address the carriage of dangerous goods. In 2005 new security rules were introduced into ADR and RID, which require a wide range of measures to be taken to minimise the theft or misuse of dangerous goods that may endanger persons, property or the environment.

Today thirteen classes and 3,300 categories of hazardous materials have been listed (the list and quantity of hazardous materials are updated every 2 years). Regulations concerning **transport of hazardous (or dangerous) materials** are certainly voluminous, complex and restrictive, but at present they are deemed insufficient.

It should be noted that major disasters have not involved hazardous materials. Nevertheless, they may pose a threat given the fact that they can induce accidents (e.g. fires, explosions) or can possibly be used in terrorist attacks (improvised explosives devices). The products concerned certainly are liquid (or become liquid very easily, for example animal fats, margarine) have a high calorific capacity, or mixed with chemical compounds and elements can be converted to an explosive compound (through a chemical reaction or series of reactions), but does this mean they should be classified as hazardous materials? If this was the case it would be impossible to transport anything, but it should be borne in mind that transport of such materials are potentially hazardous and new concepts must therefore be developed, such as the creation of a new class of hazardous products corresponding to specific transport conditions.

To be effective, this initiative (measures or directives) must be validated by the relevant European and international bodies.

Additional specific “Directives” concerning some specific products have been produced, like for example the EU Council Directive on 93/15/EEC of 5 April 1993 on the harmonisation of the provisions relating to the placing on the market and supervision of explosives for civil uses, as well as the Commission Decision 2004/388/EC addressing, to a certain extent, the notion of traceability making the production of certain documents, in accordance with a standard template for intra-community transfers, compulsory.

In particular, the new measures identify high consequence dangerous goods (HCDG), those dangerous goods which have the potential for misuse in a terrorist incident and which may as a result, produce serious consequences such as mass casualties or mass destruction. For HCDG additional security measures are required. For example each participant involved in the carriage of these goods must adopt, implement or comply with a security plan and have devices or arrangements in place to prevent the theft or misuse of the cargo or vehicle. These Security Plans/Security Management Systems must be risk based and result in adequate security measures being operational.

We can also mention the following EC projects related to the subject:

- The project INTERFACE (**I**mprovement of i**N**termodal **TER**minal **F**reight oper**A**tions at Border **C**rossing t**E**rminal - FP5), targeting improvement in quality of data exchange in the freight transport including data concerning RID
- The project EMBARC (European Maritime study for Baseline and Advanced Regional and Coastal traffic management – FP5)
- The project SECCONDD (SECure CONtainer Data Device) will initiate the international standardisation of the technical interface between a secure container or vehicle, and a data reader at a port or border crossing. The primary purpose of the container interface is to enable law enforcement officials to determine where a container or vehicle has been, whether items such as explosive devices, drugs etc. or people may have been inserted en route, and whether there may be hazardous items within it. Secondary purposes are to interface to a cargo tracking system and to provide data for automated cargo handling systems.
- The "Roadrunner" operation, a trans-European joint operation with the WCO and the ZollkriminalAmt Institute (German Customs) to detect in "real time" drug trafficking along the Balkan road,
- The Interpol Balkan route programme called "Probalkan", aiming to stimulate the **exchange of intelligence and the inter-agency cooperation** in order to fight drug trafficking along the Balkan Road more efficiently,

Concerning specifically the containers:

- **ISO Standardization** (TC 104/ SC 4 / WG 2): Technical Committee 104 is working on the standardisation of Freight Containers. Sub Committee 4 is responsible for Identification and Communication. Working group 2 is working on automatic identification equipment for containers and related equipment. The Working Group is presently in the process of setting a number of different standards to accommodate the container transport industry.
  - ISO 18185 Freight Containers – Electronic Seals

    Describing the capabilities of the RFID based electronic High Security Seal based on the High Security Seal defined in ISO 17712. The current definition of the electronic High Security Seal is based on read-only active RFID (battery assisted operation)
  - ISO 10374 Freight Containers – Electronic License Plate Tag

    Describing the Electronic License Plate Tag affixed to a container and its ability to identify information about that specific container using RFID communication technology.

- **ICSO Standardization**: The International Container Security Organisation is dedicated to increasing the security and efficiency of international commerce by creating and implementing standards for container security devices and systems. ICSO focuses on:

- Information systems that notify Customs and other government officials or authorised business personnel when shipments and containers are compromised during transit.
- Cost effective container security devices that detect and report in-transit container intrusions and other irregularities.
- Additional capabilities as they are developed that can be incorporated into the systems such as radiation detectors or sensors that detect changes in temperature and humidity.
- Information technologies to securely store data, to securely transfer data between authorised parties, and to ensure business data privacy.

WCO Concept of Authorized Economic Operator

The World Customs Organization (WCO) has designed standards to secure and to facilitate the ever-growing flow of goods in international commerce. These standards are set forth in the SAFE Framework of Standards (SAFE Framework.), which was adopted by the WCO Council at its 2005 Sessions. A vast majority of WCO Member administrations have expressed the intention to begin the process of implementing the SAFE Framework provisions. In recognition of the urgency of launching this new program without undue delay, the Council adopted the basic SAFE Framework document which provides the broad overarching principles concerning security and facilitation of the global supply chain. The SAFE Framework incorporates the concept of the Authorized Economic Operator (AEO), and the Council directed the WCO to develop more detailed implementing provisions for the AEO concept.

The Community Customs Code brings together in a single and coherent body of law the general rules and procedures applicable to goods trades between the Community and non-Community countries. The proposal for a regulation (EEC) No 2913/92 establishing the Community Customs Code (COM(2003)452 OJ C 96 of 21.04.2004) explores ways of strengthening security requirements for international movements of goods. Aiming to this, the proposal introduces an obligation for economic operators to provide the customs administration with information on the goods before they are exported from or imported into the European Union. The proposal provides for the introduction of common criteria at Community level for the concepts of "risk", "risk management" and "authorised operator" in order to avoid distortions in the internal market and security loopholes. It also proposes that Member States be required to use risk analysis techniques. To do so, the Commission must establish a common risk management framework. European Commission is actually working on a modernised customs code where a number of measures to tighten security around goods crossing international borders are proposed. These measures will result in faster and better targeted checks which will reconcile the demands for trade facilitation and improved security.

3.2 SECURITY SCREENING APPROACH IN THE RAIL SYSTEM

The various means of transport – road, rail, air, water – and their network can be considered the “lifeblood” in a modern society. Their use has now become so finely balanced and interconnected, that even minor disruptions could have a far-reaching impact. A terrorist attack could provoke disaster and destabilise society and business, but other crimes and fraud are to be considered as significant causes of damages and loss of property and lives.

The UIC reports that in the EU 25 more than 500 million tons of freight are transported per annum over a local, national and international rail network covering almost 100 000 km of track. With the enlargement process, EU has now direct borders with less stable regions. The Railway system will have to ensure that a consistently high level of security is established across its new, more diverse territory. The importance and the impact of the Railway system on the economy, the citizen life and the environment in Europe are quite obvious. Measures to increase security in mass transportation systems are becoming a growing “market requirement” as well as prerequisites for operators and services. They will be so in years to come. A strong competition in the coming years is foreseen in European market.

The nodes in the rail based transport system, (railway stations, freight terminals), the infrastructures (bridges, tunnels), railway lines as a whole, are particularly vulnerable to external and internal attacks, as well as control and command systems. It is absolutely vital to protect these neuralgic points.

Furthermore, in an industrial society, large quantities of potentially hazardous raw materials and smaller quantities of chemicals and toxic substances are actually available and transported.

Innovative but realistic and viable solutions to secure transport infrastructures are a particularly important objective.

The focus must be on prevention, early identification, increasing redundancy (functionality in all possible crisis situations) and increasing the performance of the emergency services in a crisis. Moreover, the general political intent in nearly all EU countries and the EU aims to make railway traffic faster, more comfortable and more international, due to the general amount of traffic and to environmental reasons.

An important implication thereof is that especially the security concepts and practices have to become much more integrated and much more interoperable between the railway operators.

Contributing to the development of an integrated system to improve the security of rail transportation through better protection of railways and trains and to reduce disparity in security between European railway systems makes necessary to embrace the following phases:

3.2.1 Threats characterisation, Constraints & Clearing House on Security identification

Rail transport security faces new threats from international terrorism which are not well defined. Therefore, it’s important, via an integrated approach, to address current security threats and to assess social as well as economic consequences. While providing reliable, cost-effective tools in assessing, preventing and combating the novel threats of international terrorism different framework conditions and regional disparities have to be regarded.

The objective is to identify terrorist threats and consequences to the European railway system with the potential to support the industries and transport operators' competitiveness, identifying and promoting threat-cost-benefit optimised solutions. This threat/cost/benefit analysis should enable infrastructure managers and Railway Undertakings to make use of

the regularly updated state-of–the-art knowledge on security threats and counter measures with regard to the rail system.

Attacks against the infrastructure (stations, depots, tracks, signalling systems, energy supply, communication), rolling stock, freight and persons has to be considered and include potential primary and secondary damages in order to assess the potential impact of threats. Based on "the relevance, feasibility and likelihood of attacks" (delivered from threat scenarios), counter measures have to be generated for the most relevant security threats. The analysis of the costs and benefits of each counter measure will then lead to a list of priorities for implementing effective terrorism counter measures. Together with the assessment of regional disparities in the European railway system, which also considers different regulations and human rights, this will give advice to **what is feasible and possible**.

3.2.2 Means of Railway Terrorism / Crime identification

The objective is a complete and comprehensive frame of possible terrorism/crime means of attack to Railway and how the attack could be carried out **("short-list" of the most likely modes of attack)**.

The security threats can be integrated within 6 different categories: robbery, assaults, trafficking illegal substances, vandalism, fraud and terrorism. Each of these types of risk obeys to different purposes and use of different tactics to accomplish their aim. Though all these crimes can be found within the transportation environment, the focus will be placed on measures and solutions to prevent, deter and quickly retrieve forensic information (if the preventive measures failed), which are linked to the transported goods. Thus, solutions will be evaluated, which will counter four of these types of crime: **robbery, assaults, trafficking illegal substances and terrorism**.

A 1999 survey by COLPOFER (collaboration of railway police services) showed that 279,241 crimes were reported, of which 8,978 were attributed to theft of goods and 28,136 to assaults, (the other being vandalism and fraud). Although terrorism acts numbers are low, their impact in terms of economical incidence for the cities is huge.

The characteristics of substance and its effect, the way to prepare a "weapon", or new ways of attack by electromagnetic "bombs" must be analysed in terms of feasibility and likelihood of consequences (from blanking communication to destroying equipments). Sabotage or physical alteration of critical part of the system is also considered. The events related to security issue are not limited to Terrorism. Crime and violence are a part of analysis and description as well as natural catastrophic events.

The main part of technologies and systems conceived and used to monitoring significant deviation from normal states of critical components of railway, as a result of a terrorist or criminal action and to manage a crisis situation, could be useful as an early warning of natural events that could affect the system. A specific analysis will be devoted to the definition and analysis of combined threats.

The following substances and ways of attack can be considered:

- **CBRN** (Chemical, Biological, Radiological, Nuclear) Substances & Devices
- **Bombing & Explosive Devices**

- Electromagnetic Terrorism – out of scope
- System Alteration (sabotage or disruption) & Train/Control Post Hijacking – out of scope
- **Combined Threats**

3.2.3 Railway System Assets Target identification

The objective is to clearly identify, by an appropriate "taxonomy", the railway assets, sub assets and critical components, in order to define and to scrutinize the possible related threats, both in terms of attack means and kind of perpetrators.

The word "asset" here includes the "physical" ones (like stations, tunnels, rail network, trains, bridges etc.) as well as the "logical" ones (like information and management systems used for the service). Furthermore, all the persons who have "contacts", continuous or random, with the above mentioned assets are included (i.e. rail men, passengers, simple visitors), as well the transported freight.

Starting from the data base of possible threats (the "short-list" of the most likely modes of attack) and legal, economical or political aspects, a list of threat scenarios and the condition of each main subsystem asset of railway has to be produced. For each significant physical part of railway, the critical component must be identified and analysed in terms of credible risks, via an additional damage and likelihood analysis.

The result will be a comprehensive set of requirements for specific solutions and protection "main phases": Prevention, Mitigation, Crisis management.

This relevant issue will allow for a decision to be made "where" to place priority in the efforts to be made: a big threat with possible big consequences but with a small likelihood will probably be considered less worthy of immediate attention (and actions) than a small threat with minimum consequences that can be easily realized (i.e. atomic bomb versus a hacker)

The following assets can be considered:

- Station & Buildings (Command Centres) – out of scope
- Tracks and Structures (Yards, Tunnels, Bridges) –out of scope
- Rolling Stocks – out of scope
- Fixed installations (Signalling, Power Supply, Communication & Information) – out of scope
- **Persons** (Passenger & Luggage - **Staff**)
- **Transported Freight & Dangerous Goods** (including transhipment)

3.2.4 Actual and Future Risk - Reactions & Countermeasures identification:

Society in general and railway organisations in particular, have to deal with new threats to the railway environment. Consequently they must exhibit increased preparedness for such threatening events. Protection systems have to be developed to prevent loss of human life, valuable assets, property, public utilities, installations etc. These integrated protective systems for improvement of the security of rail transportation can be characterized as comprising of a mix of mission critical technology, applications and operational procedures to

be followed. They also include the human factors involved in the use and management of advanced technology, tools and procedures.

In this approach three “main phases” of protection will be distinguished:

- Prevention,
- Mitigation,
- Crisis Management.

Based on the described protection requirements for each of the identified vulnerable “Railway subsystem assets targets”, the objective is to produce an overview of protective systems or mission critical solutions for the most relevant threat scenarios in the specific railway environment, taking into account the three defined phases of protection.

The “short-list” of the most likely modes of attack, will lead to a selection of the most relevant threat scenarios and the identification of vulnerabilities in the railway environment. As a result of a thorough risk analysis, related to actual and future risks as well as immediate operational consequences, a comprehensive set of protection requirements has to be defined. These requirements for the protection of both physical and transported assets of the Railway System will be the starting point for the description of protective systems for each of the identified vulnerabilities.

This activity will focus on the three different phases of protection:

- Prevention and preparedness (how to prevent an attack?)
- Mitigation and recovery (how to minimize the effects and consequences of an attack?)
- Crisis Management and disaster recovery (how to recover from an attack?)

For each relevant threat scenario (or each identified vulnerability) a protective system (or “mission critical solution”) for the aforementioned “phases of protection” will be outlined.

Preventive measures, suppression activities, reactions and countermeasures have to be described in terms of:

- mission critical technology to be used, procedures to be followed as well as
- human factors involved in the use and management of technology, tools and procedures.

3.2.5 Integration of “protection solutions” (for transported assets):

The objective will be on integration of “protection solutions” for the transported assets (i.e., persons and luggage, **freight**). The integration has to consider that passengers, freight and luggage could be both targets of potential threats and means to attack the railway system, by infiltration of terrorists or criminals.

Many physical assets of the railway (station, trains, depots, terminals and yards) are involved. Interfaces with other transportation systems must be taken into account in the process. The Architecture has to be designed in order to integrate (also in different time scale) the necessary protection solutions and handle different technologies coming out from legacy system as well as existing or new generation technologies.

Moreover, the architecture has to be designed to get through adequate processing data and information fusion in order to increase the capability of situation awareness and identification of threat scenarios.

This will embrace both - Peoples (staff) Clearance Control – and – Freight Clearance Control.

3.3 APPROPRIATE TRAINING

As mentioned previously, training aspects are crucial for the staff of transport organisations faced with this challenge that is commensurate with the needs for exchanges of information to prevent the threat and similarly to ensure a coordinated response in the event of an attack. This training should target primarily 3 categories of staff:

- **Drivers/pilots of transport modes** (trains, road, air, maritime and river networks, etc.) and **operators of terminals**, stations, etc, each of having a specific role to play of vigilance and alertness, and subsequently of behaviour in the field, to facilitate the work of customs, police and rescue services.
- **Managers** not directly involved in the event, but have to manage crisis situations, handle communication aspects and relations with the media, analyse the conditions for resumption of services after an attack, consider the needs of victims and their families, etc.

In crisis situations such as those created when an attack occurs, the disruption and stress are such that if the process needed is not a reflex action, it may well never be adopted in time. Hence it must be repeated in advance under conditions as close to reality as possible and it is in this respect that exercises, full-scale simulation and scenarios take on their full importance. It is not a matter of teaching transport staff to conduct themselves like police officers or members of rescue units nor to teach the latter the specifics of the tasks performed by transport staff. The aim is instead to enable each person to act in the best manner depending on his/her job and to be able to grasp the needs and reasoning of others.

Situations will never be identical because terrorism itself evolves and the environment changes. Reactions will never be the same in the case of an isolated attack against an airplane in broad daylight and an attack or multiple attacks simultaneously against a heavy transport mode inside a tunnel as it has been seen in the attacks in Europe which targeted mainly rail transport.

Nonetheless, use of exercises, full-scale simulation based on “threat scenarios” can yield better reflexes in emergency situations and also in normal conditions; they can foster sufficient vigilance without it becoming an obsession or paranoia.

4 EXISTING SITUATION IN RAIL SYSTEMS: CONTROL PROCEDURES AND AVAILABLE DETECTION & IDENTIFICATION SYSTEMS

The actual state of the art in railway security and protection systems and technologies, is really not exciting, at least concerning integration and coherence of technologies (best practices).

Despite worries, significant improvements in rail-related security are slow to emerge due to:

- Low levels of transit authority investment
- Complexity of the challenge
- High cost – dubious efficiency of technologies
- Unclear responsibility share between the different stakeholders

Different priorities, different research approaches and very different threat perceptions and awareness (beyond the objective differences in national circumstances) are today present, that are of concern to big and small railway operators alike in EU countries.

Existing solutions or technologies commercially available and mainly imported from other sectors (e.g. air transport, maritime or military) are only in very few cases viable for railways and realistic in term of cost (investment and operational costs), performance and impact on the service.

There are of course many examples of international co-operation of railway operators, manufacturers etc., however they mostly intend to directly improve the service for the customers and the operation (e.g. establish new trains, new lines etc.), and few of them had a European wide or a security focus.

The same is true for the security research sector. Beyond small scale activities between some interested railways operators, there have never been research activities along a longer time frame. The first EU driven research activity for railway security was the TRIPS project (2005 – 2007) within the PASR project suite. Though TRIPS intends to produce very important results (e.g. the threat analysis will probably be very useful) its main focus is sensor technology in railway environment and system architecture and performance.

The development of efficient and accurate **detection tools** is an absolute necessity. Where prevention activities have failed or have been circumvented, it is up to detection tools and practices to limit the risk of criminal activities.

A comprehensive approach to detection is necessary. The detection can be achieved with various techniques including X-ray systems, sniffer dogs, vapour detection systems (e.g. for explosives) etc. Practice has shown however that the use of a single detection technique may not lead to satisfactory results when it comes to the detection of certain type of substances. Consequently, a combination of methods may be necessary.

As most of the information related to the detection of dangerous substances (HCDG) may be sensitive and/or classified, any follow-up activities in this area will have to take this into consideration.

This should be done while always taking due consideration of the applicable security rules.

4.1 EXISTING PROCEDURES/TECHNOLOGIES

Over the years, a number of international agreements have been concluded to establish appropriate control standards on specific categories of goods to ensure security and safety for our societies, economies, environment and wild life.

A list of illustrative control agreements and programmes are listed here:

- The Wassenaar arrangement on export controls for conventional arms and dual-use goods and technologies
- Nuclear export controls
- Nuclear non-proliferation treaty
- Comprehensive nuclear test-ban treaty
- Chemical weapon convention
- Biological weapon convention
- Drugs, prevention of crime, money laundering
- Control of endangered species
- Control of intellectual property rights

The application and implementation on site of these control agreements and programmes requires adapted monitoring tools.

The effectiveness of customs services can be enhanced through modern technologies. Customs administrations, especially those in developing countries, face operational, financial, structural and human challenges when equipping themselves with modern technology. The objective consists of examining what technology can offer in terms of protecting society and trade, a real priority for the WCO's Members. The world customs exhibition, in September 2003, was an opportunity to present a variety of equipment, such as:

- The latest inspection devices (relocatable, pallet, portal) using technologies like X-ray and Gamma-ray systems, metal detector, penetrating radars, gas (CO2) detectors, high resolution visual, infra red and thermal imagery, acoustics systems
- Information and communication technology solutions
- Electronic and manual seals
- Radiation detectors
- Systems for identifying and detecting persons

A new class of multi-application detectors using biotechnology is also coming on the market for drug detection, explosives detection, mine detection, biological and chemical agents to protect against chemical and biological weapons, environmental monitoring - dioxins, mold, fungi, etc. Detection of chemicals e.g. explosives and drugs, and of bacteria is an important part of security, environmental, industrial and military activities.

Related to environmentally prompted detection, the objective is to expand the range of detectable explosives. Good results have been shown in the detection of TNT and Tetryl; Also for PETN results are promising, while detection of RDX needs further development. In addition, there is a need to develop portable versions with similar performance capabilities as stationary facilities.

Cutting-edge technology gives access to imaging and chemical analysis of a variety of objects, including human tissue. Security screening is also possible because materials such as plastics, clothing, cardboard, and semiconductors are transparent to terahertz. This

property opens up a vast number of potential applications like the rapid characterisation of drugs.

A forum highlighted the crucial situation for customs authorities and terminal operators to intend to facilitate understanding of the concept of security and facilitation of the international trade supply chain. Detection equipment and systems need to be fast, accurate and easy to handle and should be able to operate in severe environments. High probability of detection and low false alarm rates are also mandatory. The system not only needs to alarm for a substance, but it has also to identify the substance.

In a practical way we are finally facing two global threat scenarios:

1. Introducing prohibited materials or persons inside the railcars/containers. This can be done either from the departure point (concealment in a container) or at anytime during the journey (stopover in a yard).

2. Theft, diversion or direct attack of valuable/dangerous assets.

Scenario 1: "Trojan horse"

a) This requires scanning the containers before loading, or before crossing a border.

Processes and technologies employed are mostly dependant on the quantity/proportion of containers to be checked. For detecting nuclear/radiological smuggling, a small amount of containers may go through high resolution portals (Germanium type); this type of technology avoids false positive (NORM and masking of special nuclear material) and false negative (shielding of SNM) alarms, but constraints on sensitivity limit the throughputs. Therefore they are recommended as Secondary Screening (ie after a first filter, which can be intelligence data or a primary screening).

Primary Screening portals (low resolution) can be used at a much higher throughput; however, they are not sufficient alone because the amount of false alarms (up to 20%), and require to be combined with an efficient Secondary Screening process.

Some of key development to promote a speedy and efficient scanning process:

1. Taking into account the existing logistics flow and embedding detection technologies in locations where containers are already stopped.
2. Combining multiple technologies in order to speed up the process (e.g. X-Ray and Gamma portals in one step for the operator) and in order to improve detection performances ('systems of systems' where the result of a previous scan is used to perform a targeted inspection through another technology).
3. Integrating the results of inspections into one single platform or database and disseminating the data to multiple users. Firstly, this would enhance cooperation between the parties ; secondly, an centralized independent authority could overview the full process.

b) This requires guaranteeing the integrity of the load.

Electronic seals can be used in combination of other technologies (GPS tracking, video triggered when the seal is opened) so that the container status can be recorded and tracked

by all parties. In the case of an opening, it is important that other data facilitate the understanding of the event (where, when, by whom).

<u>Scenario 2</u>: "External threats"

a) Tracking the containers

As mentioned before, electronic seals should be tied within a system that reports railcars positions, and that possibly triggers an alarm when abnormal itinerary is detected.

b) Securing regular stopover and transhipments areas

People accessing the areas where trains are stopped and containers handled should be controlled through regular access control (although difficult in open areas such as marshalling yards) or through a combination of RFID badge and video cameras (people walking in the sector without carrying a RFID badge would trigger an alarm and be video recorded).

If CBRN threats are also considered against stations, a network of sensors may also be proposed.

c) Monitoring and deterring threats against sensitive containers

Trains are most vulnerable when stopped outside regular stations. For the most sensitive or valuable assets, a on-board video monitoring system may be installed to monitor stopovers, triggering an alarm when individuals are detected in the immediate vicinity of the railcar.

General remarks:

- Any on-board monitoring systems should be adaptable to the level of surveillance required (dependant on the threat level and on the load); ideal would be a kit of "plug and play" devices such as seals, GPS, cameras, or any sensors, that can be used separately (for a minimal tracking) or combined together (for the most valuable assets) without changing the core of the system.
- Key issues to solve for most on-board system is power consumption (as it may most likely be stand-alone) and compliance with all national rail safety regulations.

4.2 IDENTIFICATION OF TECHNOLOGIES TO BE USED, ADAPTED, COMBINED OR DEVELOPED

4.2.1 Security mission areas considered:

- Border security
  - Detection/ identification functions
  - CBRNE detection capabilities
  - Sensor & detection technology
- Protection against terrorism and organised crime
  - Functions for detection, risk assessment, position localisation

  - Capabilities for detection, threat assessment models
  - Sensor and detection technologies
- Critical infrastructure protection
  - Detection/identification functions
  - CBRNE detection capabilities
  - CBRNE detection technology
- Restoring security in case of crisis

CBRNE = *Chemical, Biological, Radiological, Nuclear, Explosive*

To do so a panel of detection and identification tools and devices (technologies) have been developed and are available on the market. These are not always well adapted to the specific need of the freight railway transport and the real level of risk. The following "solutions" can be mentioned:

- The latest inspection devices (relocatable, pallet, portal) using technologies like X-ray and Gamma-ray systems, metal detector, penetrating radars, gas (CO_2) detectors, high resolution visual, infra red and thermal imagery, acoustics systems
- Information and communication technology solutions
- Radiation detectors
- Systems for identifying and detecting persons
- Cargo integrity - Electronic and manual seals
- Tracking & Tracing and video surveillance

For these control operation and in addition to Technologies / Devices, the use of animals like Dogs, Bees, etc. will also have to be mentioned.

We will develop here after a selection of:

- the main missions applicable in the case of rail transportation and
- main solutions to fight against potential threats (risks) on the concerned corridor

4.2.2 Container supply chain security

The events of 9-11 were a catalyst for an increase in vehement pressure placed on global supply chains, illustrated by new organisations, regulations and initiatives:

- Establishment of Department of Homeland Security **DHS** and Customs
- Border Protection **CBP**
- Container Security Initiative **CSI**
- Customs-Trade Partnership against Terrorism **C-TPAT**
- Advanced Manifest Role **24 hour rule**
- International Ship and Port Facility Security Code **ISPS**
- Operation Safe Commerce **OSC**

The approach for supply chain monitoring is the following:

- Monitoring must incorporate the whole end-to-end supply chain and all transport modes from shipper to consignee
  - RFID based electronic door seals (eSeals & smart seals)
  - Onboard units mounted inside the container (smart units)
- Automatically autonomous monitoring
  - Identification and data capture at fixed check points (key supply chain nodes) like border crossing, terminal gates, hubs etc, or on demand with mobile data reader or hand holds
- System of separate internal securities
  - Each actor in the supply chain have to maintain the ”clean“ state of the container only for his area of responsibility
- Separation of security and content information
  - To ensure security, no information on the content is required but only information on the **integrity**
- Common software platform to enable stakeholders to aggregate data and collaborate in a secured environment
  - Open architecture allowing interoperability with legacy or emerging technologies
  - Basis for value added and third party applications
- Capture potential efficiency gains for all involved supply chain participants
  - Development of an overall economic model of costs and benefits
- ISO Standards * for e-Seals & and container licence plates
  - E-Seals : ISO 18185, active RFID tag, read only, single use, 433 MHz, 2,4 GHz
  - Licence plate : ISO 10374, passive RFID tag, read only, 860 – 960 MHz
  - Shippers tag : ISO 16363, active RFID, read / write, multiple use
  - Smart unit : no standard specified

    * FDIS Final Draft Industrial Standard

Examples of technical systems (selection) of e-Seals, Data Reader & Communication, Smart Seal (RFID e-Seals; Mobile & fixed Reader; Communicator; Smart Seal including Sensors, GPS and Quad-band GPRS) are listed below

- HiGTek Container Security: **e-Seals and Data Reader**
  - Applications: Tanker Truck Monitoring, Locking Systems, Container & Cargo Security, Asset & Supply Chain Managemnet

- Savi Technology Container Security: **e-Seals and Data Reader**
  - Applications: Savi ® Transportation Security System, Savi SmartChain ® Enterprise Platform, The Savi SmartChain ® Asset Management Application

- GE, Fairfield, Mitsubishi, Siemens (CommerceGuard): **Smart Container Solution**
  - Applications: Container Security Device CSD, Wireless Reader, CommerceGard Network

- IBM, Maersk (TREC): **Smart Container Solution**

- Applications: the GMM-Framework (GMM – Global Movement Management)
- Focus on: People, Goods, Conveyances, Money and Information

- OHB Teledata : **Cargo Tracking and Tracing Solution**
  - Including: Sensor network (Temp., Pressure, Humidity, etc.); Door Lock; Trailer ID; Short range active RFID; Satellite / terrestrial Communication network.
  - Applications: Existing system will be applied to security issues

- Canberra: **Smart tags and Seals developed for the IAEA**
  - Main characteristics:
    - Logs tamper events, open/close events, inspection data, and seal status
    - Tamper proof enclosure
    - Encrypted data storage
    - Essential For Maintaining Room / Container Security and Content Accountability
    - Electronic seals ensure integrity of containers
    - Application: Nuclear and radiological materials

Data Seal System characteristics:

- Portable electronic seal used for remote seal verification
- Provide instant real-time tamper verification
- Capable of integrating with radiation portal monitors (i.e., date/time stamp)
- Tamperproof closure, vibration proof, wide temperature range, battery life of up to 5 years, operation without batteries of up to 30 years

Cargo detection and screening system – data seals

- Step 1: A data seal is applied by placing it on a truck or cargo unit (container)
- Step 2: A reader can transfer seal data to appropriate authorities/operators
- The data seal and its pertinent information (e.g., opened, tampered with) can be tracked to any location.
- Data can be transferred via satellite link.
- Appropriate authorities/ operators monitor all seals on the web-based application.

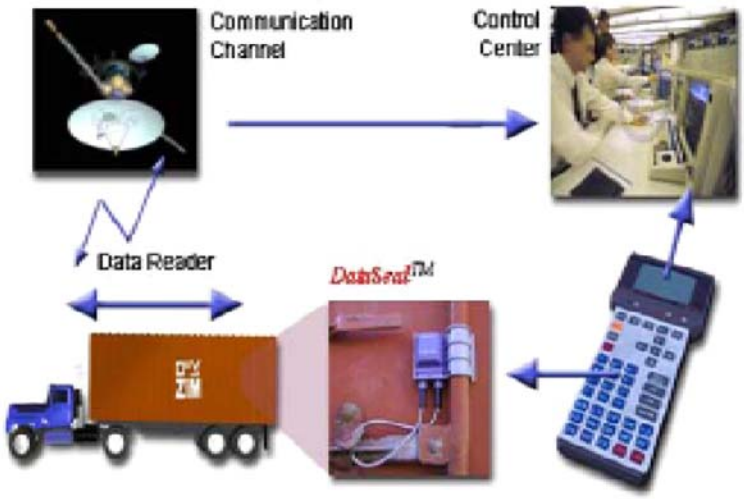

Figure 1 Operating principle of DataSeal™ system

Facts & recommendation

- The container supply chain security has been demonstrated successfully, all functionalities specified for the field test procedure have been verified
- Weakness and missing issues:
  - A worldwide approach covering the complete supply chain is still missing
  - The draft supply chain security directive has been refused from the European Parliament
  - Networking & collaboration
  - Awareness creation
  - Education, training and motivation
  - Interoperability and transparency of processes, interfaces and data
  - Harmonized infrastructures
  - Implementation strategies

The future ? GE/ Fairfield/ Mitsubishi/ Siemens? - SAVI/ Hutchinson? - Port Holding? - OHB/ HEC/ ISL? - IBM/ Maersk Logistic? – EADS?

"System of Systems" concept should be promoted with the following objectives:

- Need for regulation compliance for improved supply chain security and efficiency is evident
- Decentralized systems & data bases
- Open and standardized interfaces
- Compatibility
- Secure communication between servers

Active video surveillance

Gemini-N Surveillance:

- Records visual data and generates text information based on the triggering setup
- Can watch any external trigger
- Tamper resistant sealed case

Homeland Defence Camera:

- Industrial grade high-speed camera
- Records JPEG format
- Can be triggered by radiation detection device alarm
- Allows for digital review of recorded images

GARS Review Software:

- Stores data from surveillance and associated systems
- Records event log (state of health files)
- Can monitor multiple cameras and record alarm annunciation

Other

- Smart video with motion detection
- Remote and local review software
- Data authentication and encryption
- Modular architecture
- Remote and autonomous operation

4.2.3 Terminals & Borders control (detection & identification technologies)

Customs and border protection requirements are constantly evolving. Traditional fiscal roles continue, such as the collection of excise duties, but there is now additional emphasis on the identification of threats to local and national security – a first line of defence against possible insurgent attacks.

The priorities have moved from monitoring cross-border cargo and reducing international shipments of contraband, to screening for explosives, arms, dirty bombs and weapons of mass destruction.

Identifying such threats hidden inside a vehicle or concealed in the middle of the shipment, is increasingly more difficult. The challenge is rapid detection without disrupting the daily flow of goods.

4.2.3.1 X-ray screening

X-ray screening systems have set the industry standard in cargo inspection for more than 15 years. They are available in various forms, from mobile units ready for use on all terrains in less than 30 minutes, up to fixed high-volume installations.

The market offers advanced integrated security solutions based on **trace detection equipment, X-ray screening systems**. These systems safeguard those in the front line and the public at large; protecting buildings and transport systems; screening everything from a ticket to a truck.

Such detection equipment is used by military forces and public service workers who need to be equipped for **chemical agent detection** and **biological warfare agent identification**; by staff responsible for airport security, transportation security and critical infrastructure security; by customs officers responsible for **contraband detection and cargo security** (based on x-ray screening), and by the emergency services.

Protecting transit systems from acts of terror presents unique security challenges. Good detection can act as a deterrent.

The aim is to support the security professionals by giving them the best tools for the job. These should be available not only at the security checkpoint but throughout all areas of the airport or transport terminal, plus intelligent video and networked systems for maximum efficiency.

The first civil market in transportation security is airport x-ray used in the **search for illegal and dangerous items** in checked baggage, hand-baggage or on passengers themselves. The combination of two principal technologies, trace detection and x-ray screening, and the addition of new technologies such as millimetre wave, results in systems to detect **explosives and weapons in baggage**.

The second market is at the centre of the port security process for the inspection of all import & export containers. Cargo screening systems at the port entrance allow rapid throughput for all export containers. Images of scanned containers are created to enable ‘green lane’ routing.

Below a selection of primary and secondary screening systems, plus permanent installations for high volume terminals and border crossings are given:

- Mobile X-ray inspection system for large consignments inside trucks and sealed containers.
- Mobile X-ray inspection system to detect illegal consignments inside trucks and sealed containers for customs applications. Powerful penetration.
- Dual View version for more effective inspections and shorter inspection times.
- Universal X-ray system for cars, vans, large size pallets and containers for items up to 3000mm height.
- Powerful high energy mobile X-ray system to inspect loaded trucks and containers. Ready to operate in just 30 minutes.
- Powerful high energy X-ray scanner to inspect loaded trucks and containers at ports, airports, and border points. Easy to install and re-locate. Stand-alone unit requires no additional external infrastructure.
- Stationary powerful high energy X-ray system for fully loaded trucks and containers. Requires permanent installation on a dedicated site at ports, border crossings and airports dealing with heavy traffic.
- Stationary powerful high energy X-ray system for railroad vehicles passing through a scanning tunnel. With specially designed fast-sampling and speed self-adaptation

technology, the system is an ideal solution for non-intrusive and rapid inspection of railway vehicles at a fixed railway station or border crossing. The system can penetrate railcars while generating, processing, and storing the image data taken from a rolling freight train with speeds of up to 30 km/h without any image distortion. (High energy implies radiation safety areas which are not acceptable depending local environmental protection regulation!)

For fast search at security checkpoints for staff checks and to equip police and first response teams, the following hand-held equipment for explosives, weapon, illegal items or chemical agent detection are available:

- High sensitivity hand-held metal detector.
- Table top system for simultaneous detection of explosives and narcotics on baggage.
- Document Scanner - Table top system for detection of explosives or narcotics on travel documents.
- Hand held product for detection of explosives or narcotics, either vapour or trace particles. Detects also chemical warfare agents & toxic industrial chemicals.
- Raman Chemical Identifier to verify the identity of unknown solids or liquids.
- Walk-through portal for detection of explosives or narcotics on people.
- X-ray inspection system suitable for small items in areas with increasing security demands.

4.2.3.2 X-ray & Gamma-ray combination

Application example: Integrated Container Inspection System (ICIS)

A layered security approach integrating non-intrusive inspection and identification technologies such as:

- Radiographic imaging
- Radiation screening
- Automatic container identification

Is designed to scan high volumes of containers with minimal impact on traffic flow

Why ICIS?

- ICIS aids in the detection of WMDs and RDDs:
- Data can be collected on every container with minimal impact on operations and productivity (Equipped with fast-shutter for non-stop operation, able to scan vehicles moving at speeds up to 16 km/hr, capable of scanning more than 300 vehicles per hour).
- RPM alarms on radioactive cargo
- Alarms focus attention on potentially high-risk containers
- VACIS can help mitigate RPM alarms caused by NORM
- VACIS can reveal anomalous high density material
- ICIS data can support **CSI, ISPS** and the **Megaports** scanning requirements

Radiation profile + radiographic image + container ID + manifest = What's in the box

4.2.3.3 X-ray & Neutron inspection (Under development: EURITRACK EC project)

A new concept is highlighted in this project for the detection system: it relies on the combination of two complementary non-destructive assay techniques based on pulsed fast neutron analysis and X-ray Computed Tomography. This is the core of the project with contributions and integration of numerous recent R&D results. A large part of tasks for the development of dedicated software for data treatment and decision making are planned to be performed.

The targets are **explosives** (**drugs** as a bonus thanks to similar techniques of detection) and other concealed illegal materials with a great potential of impacts. Radioactive materials are of particular importance in that context with the threat of radiological dispersion devices also known as "**dirty bombs**".

At this moment only the feasibility of the technique has been demonstrated, Its performance must be highly improved (detection time too long: 15 min per identified suspected point)

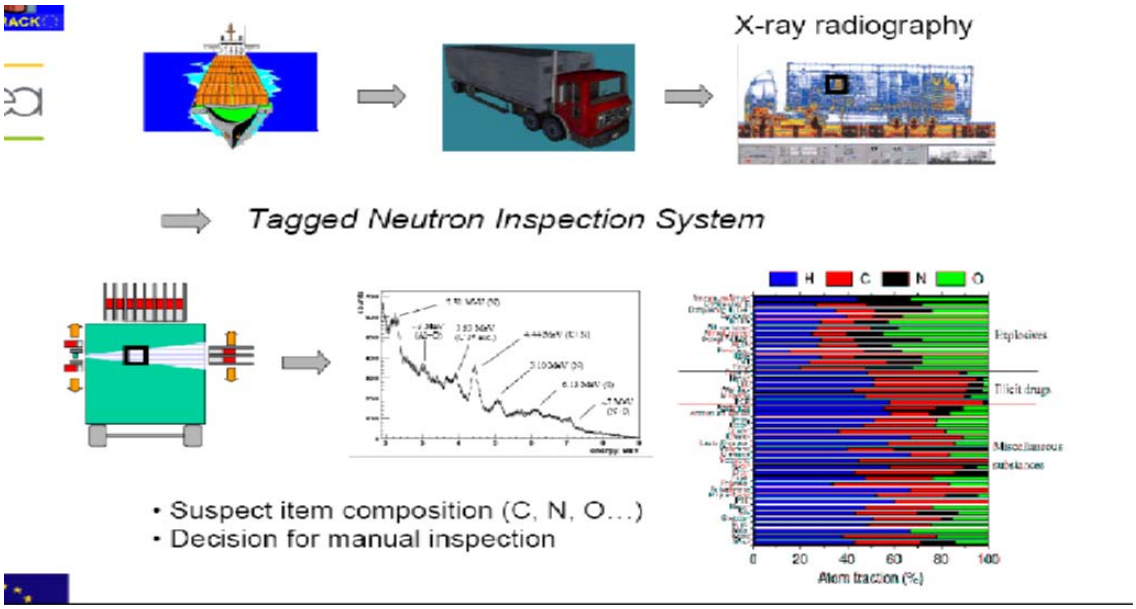

Figure 2 Applications and operating principle of X-ray detection systems

4.2.4 Radiological & Nuclear material

4.2.4.1 Context

The U.S & European Governments emphasize the dangers of nuclear and radiological terrorism

Ingredients for a nuclear weapon are vulnerable:

- There is a risk of terrorist theft of nuclear materials in 40 countries; nuclear materials are especially vulnerable in the former Soviet Union.
- According to the International Atomic Energy Agency (IAEA) Database on nuclear smuggling, 662 cases of radiological smuggling have occurred.

Example of specific threat scenario:

- Terrorists would obtain special nuclear material from a former Soviet Union state;
- Assemble a simple thermonuclear device;
- Smuggle it across central Europe;
- Ship it through international ports to the US in a cargo container;
- Detonate it in or near a major target

4.2.4.2 Radiological & Nuclear Detection and Response Strategy

Incident prevention:

- Generate real-time characterization data to determine if a detection involves radiological or nuclear materials
- Utilization of spectroscopic capabilities to reduce “nuisssance alams”, enhance ability to detect “masked” RDD and nuclear weapons materials
- Transmit to appropriate authorities specific video images triggered by an external detection event and radiological detection.

Emergency response:

- Detection equipment for protecting the health and safety for first responders
- Detection equipment for area scanning and population screening
- Transmit system data to operation centre

4.2.4.3 Safety and Security Measurement Solutions

Challenges:

- Many Smuggling Routes–Materials can enter the country by sea, land or air through many global routes
- Impact on Commerce–Technology solutions can not result in slowing commerce
- False Alarms–Too many false alarms slow commerce and result in system operators turning off systems or reducing sensitivity requiring a shift to spectroscopy
- System Integration–Detection elements must be part of a single cohesive system (global architecture) with data collection to a central location
- Human Factors–Systems must require only limited training for security personnel to use
- System Operations-CBRN security systems may not be operational
- Many Potential Targets–Terrorists have thousands of targets, thus requiring mobile systems that can be rapidly deployed based on intelligence information

Responses:

- Systems at Transit Points–Radiation detection and surveillance systems installed at international airports and borders including mobile systems
- Spectroscopy–Specialization in spectroscopy systems that minimize false alarms
- Data Collection–Utilization of technology to collect data on system operations and operational procedures
- System Integration–Integration of various CBRN security, detection, and monitoring components (e.g., detection equipment, seals, x-ray machines)
- Verification–Application of review systems provide verification of system operations, operational procedures, and protection of CBRN materials
- Visual Imagery–Deployment of surveillance systems that provide recording, digital storage and remote operations of all system components

4.2.4.4 Developing security elements to meet the threats of tomorrow

Solution providers actively work with key agencies that face the extremes in future security threats:

- Department of Defence –U.S. Army
- Department of Homeland Security (DHS)
- Department of Domestic Nuclear Detection Office (DNDO)
- Department of Energy (DOE)
- International Atomic Energy Agency (IAEA)
- Etc ….

The Security Application

- Intended to detect smuggled/contraband nuclear material
- Radiological Dispersion Devices (RDD) or the sources to make them
- Nuclear Weapons, based on Special Nuclear Material (SNM)

Deployed at

- border crossings, terminals, cargo entry points, traffic choke points, possible target facilities, etc.
- typical pedestrian, vehicle, cargo monitoring

What is the problem on security?

- Need : ability to detect any activity above “natural background”
- Problem : also detect radiation from NORM or patients
    - Naturally Occurring Radioactive Materials (NORM) will give problems in shipments of goods : YOU HAVE TO CHECK & IDENTIFY but source can be “hidden” or “masked”
    - Medical Sources in patients will give problems when scanning people/staff (terminal, yards, and trains): YOU HAVE TO CHECK & IDENTIFY but is the person really a patient?

Advanced Spectroscopy Portal (ASP) program to resolve significant problems with current inspection approach:

- Large volumes of traffic at border crossings and other locations
- Excessive “nuisance” alarms – innocent commerce, NORM, medical isotopes
- Low sensitivity secondary inspection devices (hand-held)

A family of high, medium and low resolution portal monitors to prevent covert nuclear attack from smuggled nuclear weapons”(DHS RFP)

- High Resolution – HPGe (Germanium)
- Medium Resolution –NaI
- Low Resolution –Plastic Scintillator

High and medium resolution to be deployed as primary and/or secondary devices

ASP (Advanced Spectroscopy Portals) Goals

- Discriminate between Naturally Occurring Radioactive Materials, Special Nuclear Materials, and medical and industrial sources of radiation.
- Prove that illicit radionuclide is not present in important quantities, even in the presence of other “masking” radionuclide.
- Provide a tool with more sensitivity than the primary screening monitors, to allow for targeted special examinations of suspicious vehicles even if they didn’t trigger the primary portal.
- Provide source location information
- Ensure and improve the legal defensibility of any data that is collected.

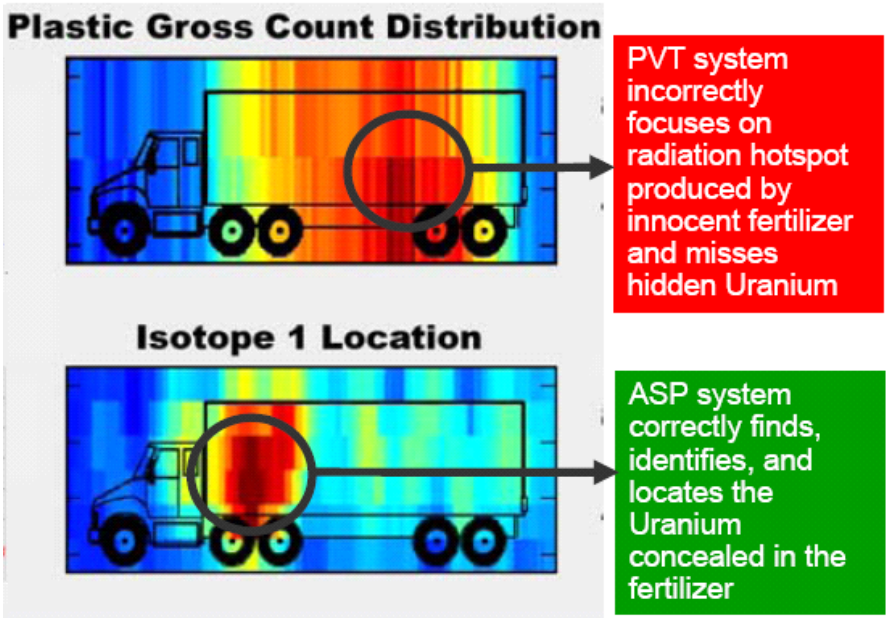

Figure 3 PVT and ASP system applied to road haulage inspection

Advanced Spectrometry Portals (ASP): HPGe detector based systems advantages:

- Less “nuisance” alarms due to innocent NORM natural radiation (=6-9% of all container shipments)

- Less mistakes
- Less human intervention
- Better accuracy & positioning
- Enhanced detection of hidden or masked sources

4.3 IMPACTS OF CURRENT CONTROL ACTIVITIES ON THE TRANSPORT CHAIN FLUIDITY AND COST-EFFECTIVENESS

Recent terrorist events, organised crime and fraud have had the effect of intensifying the fight against clandestine immigrants and trafficking of illegal substances .Specific checking measures have been imposed by public authorities, particularly focused on the transport systems.

In relation to freight transport, such measures have a far from negligible impact on efficiency and cost, and this is only the beginning. Terrorism scenarios are developed by Homeland Security departments in various countries in the world and will lead to ever greater constraints for the transport chain.

Air transport has been the first to be subject to new regulations and standards in the fight against terrorism and the trafficking of illegal substances (narcotics, explosives, dirty bombs) as well as clandestine immigrants. Everyone is also aware of the disruptions at check points in airports (border security) and particularly the time taken by security inspections.

Maritime transport is equally concerned by border security and is now beginning to incorporate a certain number of demands made by authorities for the security monitoring and checking of containers. The immediate impact of setting up such measures has been a deterioration in the quality of service in ports (dwell-time, efficiency, costs, etc.), and this is due to the lack of integration of security checks and controls into transportation and/or handling operations.

As highlighted before, Rail is just starting the “process”, but has the opportunity to take advantage from the experience of other modes.

In fact, the crucial point, not as yet dealt with in a context of global security, is the matching of security check performances (detection, identification and monitoring of illicit products and clandestine immigrants) and the efficiency of the transportation system (quality of service, cost, profitability).

In relation to security control and inspection equipment, we attach particular importance to identifying the failings of existing systems, in relation to risks and threats of all types (to be identified and defined by the authorities concerned). This must permit the recommending, depending on the diagnostic, of sociological and organisational guidelines for improvements, as well as concepts for prevention, protection and crisis management when actually faced with such threats. The major problem today remains that of “false alarms”. This concerns absolutely all systems (detection and identification) on the market. A global and systemic approach shall permit the putting forward of innovative solutions.

To this must be added another major factor that deeply perturbs the transportation chain. This is the ever growing involvement of politics in the marketplace, namely investment decisions are no longer solely linked to a return on investment but are linked, as a priority, to political requirements mainly as regards the fight against security weaknesses. New drivers are emerging for the logistic (CO2 emission, security, human factors) which will not necessarily imply the cheapest solution.

The measures that result from this will become ever greater constraints for the transportation system. Faced with this phenomenon there are two possibilities:

1. To add to the existing chain more equipment that complies with the new security requirements. This is what is being done presently in accordance with elaboration of the “formal notices” as regards the checking demands, and which requires retroactive integration and an adaptation of the transportation chain.

2. A complete re-engineering of the transport chain that allows the integration and anticipation of security requirements (direct and/or anticipated political decisions and taking into consideration threat evolutions), while taking into account during its design, the environmental problems (pollution, ecosystem, quality of life) and the economic considerations, as well as town and country planning, in order to develop reliable and profitable industrial solutions (Security by design).

Related to security screening: At present and in order to provide a simplified view of the situation, the screening and inspection equipment mainly concerns threats.

In fact, the detection equipment, the identification of illicit products (and clandestine immigrants) is specified by those organisations in charge of such controls, mainly customs and the police, and exclusively in order to provide measures against terrorism, organised crime and fraud. Thus an abstraction is made of the actual operating conditions and constraints (particularly in relation to the imperatives of goods transport).

Moreover, technologies differ in relation to the particular substances requiring detection, the detection equipment and procedures multiply when faced with goods in containers.

Such successive operations, added haphazardly to existing operations, without integration into the process of the transport chain, inevitably lead to delays due to the excessive time taken by detection and the processing procedures required to establish a diagnosis. In order to avoid congestion in the transport chain, screening is often carried out in parallel, outside the terminal, and this leads to the low number of containers actually being checked (by random sampling).

A certain number of tests are actually underway, or have been carried out in different ports across the world and in the US. At present, for containers on trucks, a maximum speed of 16 to 20 km/h is feasible for certain types of checks (X-ray and gamma ray), as well as for container identification (number) and the truck identification (registration plate and driver photo).

These achievements are interesting and exceed the present state of the art, but their performance still remains insufficient, on one hand due to the threats (sensitivity of detection of other products using other technologies such as neutron beams), and on the other, in

relation to the flow of containers, particularly with the requirement for 100% screening which is highly likely to become obligatory.

Moreover, budgetary restrictions affect investment and operating costs and tend to nibble away at detection / identification performance, by leading to the use of bottom of the range or mid range systems. In experiments, this was linked to an increase in the flow of containers to be screened (speed through checks) and resulted to an important increase in the number of false alarms and this then led to the complete blocking of the transport chain since an alarm requires crisis management. Experiments were quickly suspended due to the disastrous financial cost of such false alarms and has led the DHS to completely rethink its high level security policy.

The goal now is to put in place a level of checks **matching the real risks** of the situation. This requires, based on a study of the risks, the definition of the security check type, the sensitivity of the sensors, the processing procedures and the emplacements of the sensors in the line carrying out the screening. Thus with adequate equipment it is possible to carry out just sufficient checks to limit the number of false alarms. It follows from this that equipment is developed for specific screening and risks and incorporates the possibility of carrying out low level checks when risks are judged low or acceptable, avoiding costly investigations.

This selection must enable an overall acceleration of diagnostics and reduce the overall costs. This approach is underway in the domain of the detection of radionuclide and we propose extending it to the whole range of illicit products to be detected and identified.

Thus, we shall clearly define the content of the 100% screening recommendations and shall demonstrate the ability to carry out 100% regulatory screening.

The R&D and budgetary programmes shall therefore be allocated and spent only where the risk justifies it. This interests both users and industries designing the measurement equipment.

The aim of the research can therefore be clearly described as follows:

1. To establish the performance requirements of checks in relation to the real level of risks (layered security concept)
2. To establish the limits of existing technologies in relation to such performance (identify the technologies most suited to answer needs or having a development potential able to satisfy such needs).
3. To validate the technologies in order to implement them in the transport chain and to identify the associated constraints (radiation levels, necessary protection, energy requirements, volumes, operating conditions).

The integration of security checking systems into the container handling chain without disturbing it and taking into account the associated constraints, is a factor that must be taken into consideration during development of the service and design of the platforms.

The following fundamental principles have to be applied in the approach to the subject:

- The approach does not separate the risk from the threat and the training focuses on the long term and not on the instant itself.

- A special effort will be required regarding provision of information, be it from the transport "sector" to public authorities, or vice versa. A multidisciplinary approach (human factors, human and cognitive sciences (reasoning)) is essential as well as consistency of means (importance of cultural aspects).
- The knowledge of risks/threats calls for a study of the chain of events and of impacts (particularly identification of the residual risks involved).
- The response to the problem of an alert is reliant on assistance in preventive surveillance because the systems in place are ill-adapted to the speed/brutality of the crisis event.
- The objective is to practice dealing with the unforeseeable.
- Before assessing scenarios, backbone scenarios must be identified first. Indeed, having too many scenarios is tantamount to none at all, hence a rigorous selection has to be made with contributions from all the players concerned.

4.4 EVALUATION OF THE SITUATION AT SHORT, MID AND LONG TERM ("IF NOTHING CHANGES"), NOTABLY REGARDING RISKS AND THREATS

The establishment of scenarios and requirements for civil security (where is the detection of dangerous substances (HCDG) needed? what and how much of it should be detected?) is essential for future work. Such scenarios are necessary in order to be able to focus resources and research; concentrate the debate on specific and concrete issues and problems; enhance the understanding of the problems of relevant actors across the EU including the challenge of the time of detection and false/positive alarm rates. Moreover, a discussion and exchange of views concerning the development of scenarios may allow the Member States to learn about the priorities of other Member States.

The scenarios could be developed on the basis of sectors/security missions (e.g. aviation, mass transit, major events, etc.). When relevant, each scenario/mission could consider two dimensions:

- Vectors of threat (e.g., a person, vehicle, container).
- Quantity and type of illicit substance to cause damage/harm.

The discussion on the development of scenarios would have to be conducted in a secure environment with individuals possessing appropriate levels of security clearances.

A matrix of what is desired and of what is possible today should be developed for each scenario. Such matrices could also help to target R&D. Furthermore, public authorities across the EU could benefit from knowledge of what is possible and what the threats are. The matrix could also be used as a basis for setting up standards, if deemed necessary.

Key framework for establishment of a matrix:

1. **Sector/mission and scenario** - specific consideration of requirement to detect dangerous substances (HCDG like explosives, drugs, radioactive products, chemicals, etc)
2. **Proportionality** (How much of security is required + against what levels of which dangerous substances (HCDG) we need to protect specific sector/scenario?)
3. **Reliability** (Are the detection solutions applicable and effective? What can the detection solutions achieve today?)
4. **Sustainability** (Can the measures last and for how long?)
5. **Affordability** (How much does it cost?)

6. **Future possibilities** (What can be done in the future? – technological foresight and how scenarios could look like?)

The matrix should also consider what level of security is realistically possible to impose on a scenario, what the consequences are and what should be a priority.

The private sector and research community should be engaged in the scenario development process. Manufacturers of detection solutions and the research community need to know what to detect in what scenarios in order to know what to aim for, if public authorities want to get the best tools available. The above-mentioned government group considering scenarios and requirements could adjust the sensitive information in a way that it could be shared with companies, researchers and other relevant individuals and organisations with adequate security clearances. The next step would be to adjust the information in a way that could be made publicly available. On the other hand, the private sector should be kept continuously involved in order not to wait only for the final results of the public sector work.

In the context of private sector engagement, the public sector should attempt to explain to the private sector that security may be in its interest (e.g., trust of customers in delivery of services, safe and secure services) and does not only bring costs.

5 CONCLUSIONS & RECOMMENDATIONS (NEW CONTROL AND INTERVENTION PROCEDURES DEFINITION AND INTEGRATION)

The security of the EU and its citizens is dependent on efficient cooperation and coordination among the Member States, the EU Institutions and all other relevant stakeholders. The threat posed by the criminal use of dangerous substances (HCDG) and the level of risk involved is also dependent on this cooperation and coordination.

As mentioned before, Customs and border protection requirements are constantly evolving. Traditional fiscal roles continue, such as the collection of excise duties, but there is now additional emphasis on the identification of threats to local and national security – a first line of defence against possible insurgent attacks.

The priorities have moved from monitoring cross-border cargo and reducing international shipments of contraband, to screening for explosives, arms, dirty bombs and weapons of mass destruction.

Identifying such threats is increasingly more difficult, hidden inside a vehicle or concealed in the middle of the shipment. The challenge is rapid detection without disrupting the daily flow of goods.

A lot has already been achieved concerning the security of dangerous substances (HCDG like explosives, radioactive products, etc) both in the Member States and at EU level. It is clear however that more can be done in such areas, such as enhancing the exchange of information, disseminating best practices, establishing coordination mechanisms and taking joint actions on particular issues.

The challenges faced by cargo industry are:

- Enhancement of cargo security level without significant impact on daily work or even better productivity for the processes (alarms)
- Reduce the staff to operate the sites security and integrating new and existing systems
- Secure efficient coordination with the Public Safety forces (Border/Police, Customs, Fire Brigades, Rescue, Health & Sanitary) all in charge of (National) Security

Introduction to Cargo security:

- **Risk managed vs. 100% screening** (due to limited technology and infrastructure, « flow of commerce » issues and finite resources). After approval of the US Congress (july 2007), president Bush has officially signed the new law "H.R.1 – Implementing Recommendations of the 9/11 Commission Act of 2007". The main measure concerns the 100% screening of containers to the US. This makes freight "Risk" assessment associated to «transport mode» of high importance.
- Known/ Unknown Shipper rules (security regulations) will also be mandatory.

The following specific objectives must be reached:

- Increase knowledge and develop technologies (and intervention schemes) for illegal substances (and undesirable person) detection and identification throughout the supply chain.
- Conciliate security requirements, controls reliability and transport chain fluidity.

The benefits will be on two levels:

- Enhancement of capacities to ensure security in the European freight transport chain (in particular at the European borders level), by control capabilities and performances improvement, without harming transport chain activities fluidity, productivity and cost-effectiveness;
- Providing tools to counter criminal and terrorist threat.

Rail transport security faces new threats from international terrorism which are not well defined.

Therefore, it's important, via an integrated approach, to address current security threats and to assess social as well as economic consequences. While providing reliable, cost-effective tools in assessing, preventing and combating the novel threats of international terrorism different framework conditions and regional disparities have to be regarded.

The objective is to identify terrorist threats and consequences to the European railway system with the potential to support the industries and transport operators' competitiveness, identifying and promoting threat-cost-benefit optimised solutions.

5.1 INTEGRATION OF NEW PROCEDURES (AND RELATED TECHNOLOGIES) IN THE TRANSPORT CHAIN (INTERCONNECT AND INTEROPERATE CONTROL ACTIVITIES BETWEEN THEM AND INTEGRATE THEM IN THE FREIGHT TRANSPORT CHAIN)

The aim is to conciliate security requirements, controls reliability and transport chain fluidity. We have to evaluate the appropriateness and acceptability, but also the actual limits, of monitoring devices (static or mobile multiple sensors) and systems used or useable (advanced technologies) to improve the capability to detect and identify (and follow) illicit goods and persons.

The approach should be the following:

- Identification and characterisation of risks and threats for transports related to illicit products (and dangerous goods)
- Identification of transport chain vulnerabilities along the route, threats being identified for each country (public authorities in charge of security issues)
- Identification and characterisation of singular points and routes throughout the supply chain
- Definition of the functional, operational and environmental conditions that the detection and identification systems must fulfil
- Determination of the associated procedures, the required reactions and modes of intervention

It will allow characterizing security requirements and needs in terms of control activities at short, mid and long terms.

5.2 IMPACT ASSOCIATED TO THEIR INTEGRATION AT SHORT, MID AND LONG TERM REGARDING CONTROL OPERATIONS PRODUCTIVITY AND SUCCESS RATE, TRANSPORT FLUIDITY, COST EFFECTIVENESS, …

Beyond the integrative and interoperability approach the security solutions to develop and integrate should take account of efficiency, user and customer-friendliness, the involvement of individual and group behaviours and legal aspects.

Inside the objectives are to be underlined:

- Identify and “repair” the weakest links in systems and infrastructures, reducing vulnerability of rail transport systems
- Build flexibility into systems so that they can be modified to address more and unforeseen threats.
- Use tools and technologies as “circuit breakers”, in order to isolate and stabilize failing system elements.
- Search for technologies that reduce costs or provide ancillary benefits
- Build security into basic system designs where possible.
- **Identify illegal dangerous transported substances**.

The ultimate objective is to improve the competitiveness and usage of the railways transportation modes.

The main topics to be addressed by the railway system are:

- to develop an integrated system to improve the security of rail transportation through better protection of railways and trains, including:

- the immunity of signal and power distribution systems against electromagnetic terrorism,
- the detection of abnormal objects on or under ballast,
- clearance of trains before daily use,
- **control of access to driver's cabin, detection of unauthorised driver**,
- **new methods/tools to isolate and secure goods**;

- . to reduce disparity in security between European railway systems, including:
  - to reduce disparity of European railway systems' security,
  - demonstration of the potential of the European rail transportation systems for improved protection and homogeneity.