European best practices in safe transport of dangerous material supported by GNSS

Authors:
Gianmarco Baldini
(Joint Research Centre – European Commission)
(E-mail: gianmarco.baldini@jrc.ec.europa.eu.)
Antonella Di Fazio
Technological Innovation Department of Telespazio
Telespazio
(E-mail: antonella.difazio@telespazio.com.)

Transportation of dangerous goods is one of the main security applications in the transportation sector. Transportation of dangerous goods by road is the most common mode. It is also one of the most critical from the safety point of view, because roads are present in urban areas where the high density of population can increase the risk of civilian casualties in case of an accident. Like many other critical infrastructures, the transportation sector has been increasingly dependent on ICT components and services to improve the exchange of information. Because mobility is an important aspect of this sector, the services of positioning and navigation, like the one provided by GNSS, are particularly important. The paper presents the results of the FP6 MENTORE project in the area of transportation of dangerous goods by road. The paper identifies the main vulnerabilities of systems of transportation of dangerous goods and describes the related mitigation solutions or best practices, which can be adopted to minimize the risk for the population.

1 Introduction

The transportation sector is one of the most relevant elements in the economy of a nation. It is responsible for moving millions of passengers and millions of tons of goods through infrastructures deployed for thousands of kilometres both inside and across nations. The way of life of the citizens and their safety is highly dependent on transportation and the growth of a nation may be limited in the absence of an adequate transportation infrastructure.

The transportation sector includes many different modes of transport (maritime, road, railway, aviation and pipeline) and a wide range of applications. Some of these applications are quite relevant to the security and safety of the society and the general public. For example, in case of natural disasters, transportation is essential to bring, in time, essential material for the resolution of the crisis.

Transportation is dependent on a number of technologies and other infrastructures (e.g. energy) to provide its services with efficiency. In particular the transportation

1 Disclaimer: the views expressed are those of the author and cannot be regarded as stating an official position of the European Commission
sector has been increasingly dependent on ICT components and services to improve the exchange of information, implement more sophisticated applications for the transportation users and increase the synergy among the various elements of the transportation chain.

Location services like the ones provided by GNSS are particularly important in the transportation sector because of the mobility of its components. The knowledge of the position of the transportation vectors is an essential functionality to increase the overall security of the transportation chain.

The role of GNSS in the transportation sector has grown considerably in the recent years. From maritime transport, the use of GNSS has expanded to road transport and aviation. GNSS is used to control the position of the maritime vessels in the sea, the position of trucks in fleet-management applications and it will have an important role in aviation, once the future generations of GNSS will be deployed.

In this paper, we will focus on the use of GNSS for the application of safe road transport of dangerous materials. GNSS (GPS) technology is presently used for tracking & tracing functions and remote control of the dangerous material shipment. Dangerous goods are substances or articles that, because of their physical, chemical (physicochemical) or acute toxicity properties, present an immediate hazard to people, property or the environment. Types of substances classified as dangerous goods include explosives, flammable liquids and gases, nuclear or radioactive material, corrosives, chemically reactive or acutely (highly) toxic substances.

Specifically on nuclear transport, about 20 million packages of all sizes containing radioactive materials (which may be either a single package or a number of packages sent from one location to another at the same time) are routinely transported worldwide annually on public roads, railways and ships (source [14]). These use robust and secure containers, and generally carried in purpose-built trucks, wagons and ships (as the nuclear industry generally chooses to undertake shipments of nuclear material using dedicated, purpose-built transport vehicles or vessels). Radioactive material is not unique to the nuclear fuel cycle and most transports of such material are not fuel cycle related. Radioactive materials are used extensively in medicine, agriculture, research, manufacturing, non-destructive testing and minerals' exploration. The regulatory control of shipments of radioactive material is independent of its intended application and the same safety procedures are employed, whatever the intended end-use.

The transportation of dangerous goods is regulated by a number of policies at national, European and global level and the paper provides an overview of the current status of the regulatory framework in Europe. Regulations have the purpose to minimize the risk of incidents and guarantee an effective response. They establish rules for the shipment of dangerous goods, and fix constraints for their storage and transit in sensitive areas.

The authors have participated to the MENTORE (iMplemENtation of GNSS tracking & tracing Technologies fOR Eu regulated domains) project managed by the European GNSS Supervisory Authority (GSA) through the 6th Framework programme funds.
In the pilot projects, GNSS (GPS/EGNOS enabled) devices are mounted on the vehicle, carrying dangerous goods to collect information on position, date and time. The information is then transmitted through a commercial communication system (GSM/GPRS and satellite) to a control centre, where these data are compared against a predefined path. Any deviation generated an automatic alarm to notify law-enforcement agencies and the fleet managers. The system can be integrated by a risk analysis of the territory, where are identified the most vulnerable areas in relation to the type of transported dangerous goods.

Security aspects should also be taken in consideration. GPS or GSM/GPRS signals could be jammed to cause Denial of Service (DoS) or spoofed to provide a false position.

The paper will identify the vulnerabilities of the system of transportation of dangerous goods and will describe some of the mitigation solutions like authentication of the GNSS signal or backup communication systems.

The paper has the following structure:

- An overview of the current regulatory framework for the transportation on road and specifically of the dangerous goods in Europe.
- A description on the application of GNSS for the transportation of dangerous goods.
- A description of the MENTORE project.
- An overview of the vulnerabilities of GNSS for the transportation of dangerous goods
- A description of the potential mitigation techniques and best practices.

2 The regulatory framework for the transportation of dangerous goods in Europe

The regulatory framework for the road transportation is quite wide and it covers a number of different applications.

Even if the focus of this paper is limited to the European context, a description of the regulatory framework cannot be limited to the EU directives and the laws of the member states.

The European framework is part of a more global regulatory framework for a number of reasons including:

- Member states of Europe conduct trading outside the boundary of the European Union.
- The EU directives are based or they are dependent on international regulations. See for example the European agreement concerning the International Carriage of Dangerous Goods by Road (reference [3]).
- Member states may participate independently to regulatory bodies on road transportation.

An overview of the main road applications and correspondent regulations for nuclear transport and dangerous goods is presented in the following table both at international and European level.
### Table 1 Regulation for Transportation of Dangerous goods by road.

<table>
<thead>
<tr>
<th>Nuclear transport</th>
<th>UN Recommendations on the Transport of Dangerous Goods.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>International Regulation</strong></td>
<td><strong>European Regulation</strong></td>
</tr>
<tr>
<td><strong>European Regulation</strong></td>
<td><strong>European Regulation</strong></td>
</tr>
<tr>
<td></td>
<td>DIR. 2001/7/EC and DIR. 2003/28/EC; Commission Decision 2002/886/EC; DIR. 1995/50/EC (on uniform procedures for checks on the transport of dangerous goods by road), emended by DIR. 2001/26/EC.</td>
</tr>
</tbody>
</table>

At European level, we have different types of legislative acts:

- Regulations are legislative acts, which define compulsory rules to be applied to all member states in Europe.
- Directives are legislatives acts, which must be translated to European laws.
- Recommendations are not compulsory but they can evolve into proposals for regulation or directives.

Even if they are not strictly legislatives acts, the following documents can affect the regulation process:

- Best practices are related to policies and/or to voluntary regulations (self-regulations) aimed at the collective benefits (normally for social and welfare interest).
- White Papers and Green Papers describe a new strategy or approach and they are the EU instruments to start a regulation process.
In the context of dangerous goods, the main legislation act is the ADR (Accord européen relatif au transport international des marchandises Dangereuses par Route) or “European Agreement concerning the International Carriage of Dangerous Goods by Road”, which governs the transnational transport of dangerous material. This history of ADR goes back to 1957, under the aegis of the United Nations' Economic Commission for Europe and it started to be applied from 1968. Recently, a new set of amendments were approved and entered in force from 1st January 2009 (see reference [3]) as ECE/TRANS/202, Vol. I and II or ADR 2009. Chapter 1.10 in Annex 2, is specifically focused on the security aspects for the transportation of dangerous goods and specifies the security requirements. In the section of provision for high consequence dangerous goods (paragraph 1.10.3.3) the use of tracking devices is recommended to monitor the movement of high consequence dangerous goods.

Recently in occasion of the MENTORE workshop held in Brussels on June 2009, the EC announced that one of the present priorities of the EU agenda is to draft a proposal for an EC directive for real-time tracking of dangerous materials (see reference [13]).

3 Transportation of dangerous goods based on GNSS.

Dangerous goods for transport on the road include substances and articles that have explosive, flammable, toxic, infectious or corrosive properties. A classification of the dangerous goods is presented in table A of the ADR (see reference [3]).

Generally the transportation of goods by road always presents the risk of traffic accidents. If the goods are present in the list defined in the ADR, the risk for the safety of the citizen may increase dramatically. Hazards like fire, explosion, chemical burn or environmental damage can be a direct consequence of a road accident involving a truck carrying a dangerous good. A road accident of this type can become a serious emergency crisis if it happens in a densely populated area like a city.

The knowledge of the position of the transportation vector can be an essential element in preventing or resolving, in an efficient way, an emergency crisis of this kind. This is the functionally commonly called “Vehicle Tracking” or “Tracking and Tracing” where the position of a vehicle can be monitored through a location devices and other equipment.

Tracking and Tracing can be passive or active:
- Passive Tracking where the tracking device stores the vehicles location, through a positioning device (i.e. GNSS terminal), and other data (i.e. vehicle condition or container status) and stores this information in a data storage systems. At the end of the trip, the data can be collected and examined.
- Active Tracking, where the tracking device stores and the vehicle location, through a positioning device (i.e. GNSS terminal), and send it through a wireless communication system to a control room for real-time update and monitoring.

The passive tracking may store a large number of information on the condition of the truck or the goods during the trip, but it does not provide real-time monitoring to the control centre. Because of this reason, it may be of limited help to improve the security and safety of the transportation of dangerous goods even if the collected data may be used to help the identification of the possible causes of the accident.

Active tracking can be used both to prevent an accident and to improve the response and resolution of the emergency crisis, which follows an accident. In case of road an accident, fleet managers can intervene and notify public safety responders in a more efficient and faster way by providing the last position of the truck. GNSS-based systems can also help to prevent a road accident by cross-checking the position of the truck with the conditions of the road, weather conditions or traffic jams, which could increase the risk of a road accident. The driver could be notified by the control centre through commercial communication systems like GSM/UMTS.

In active tracking, the position of a truck is frequently transmitted to a control centre to inform the fleet managers of the position of the various trucks on the road. The position of the truck is determined through a GNSS receiver mounted on the vehicle. Until now, GPS receivers have been used, which have limited accuracy and availability especially in urban areas. Future systems could take advantage of the improved availability and integrity of navigation systems like EGNOS or Galileo. The position of the track is transmitted to the control centre through various wireless communication systems like cellular networks (GSM/GPRS/UMTS), satellite networks or even WLAN networks in urban areas based on WiFi or WiMax. The evolution of the Intelligent Transportation System (ITS) paradigm may provide additional types of communication systems. The information to be transmitted to the centre is usually limited in size, so there is no need of high data rate communication links. On the other side, the use of commercial systems may become an issue to validate reliability requirements for the whole system.

One challenge is also to guarantee when the GPS signal is reliable. Currently GPS is not able to provide such information to the terminal, but this is essential to provide the adequate level of service to a fleet manager responsible to transport dangerous goods.

A number of tracking & tracing systems for dangerous goods have been implemented in Europe in recent years. One of the pioneer projects is SIMAGE (see reference [10] for details) whose main aim was to implement a pilot information system for the near real-time monitoring of vehicles carrying hazardous freight and provide early alert warnings to the competent authorities in the case of emergency associated with the dangerous goods transport.
Other examples of this type of projects is PROMIT financed as part of the Framework Program 6, whose objective is to “contribute to a faster improvement and implementation of intermodal transport technologies and procedures and to help promoting intermodal logistics and mode shift by creating awareness on innovations, best practices and intermodal transport opportunities for potential users as well as for politicians and for the research community” (from reference [5]).

Another example is described in [6], where is described a remote identification system for dangerous goods safe transportation in Lithuania.

The described projects have identified a number of issues to be resolved including:

- Monitoring the transport of dangerous substances is not only a technological challenge, but also and, perhaps more importantly, a participatory challenge.
- In absence of legislation, has to be adopted on a voluntary basis.
- Different competing technologies and architectures are available. Standardization is needed to converge on a single and efficient solution. An objective should be the standardization of messaging structures for data exchange between interested and authorized parties
- Needs a “sustainable business model”, featuring: collaboration between all interested public and private stakeholders, adoption of existing standards, service-oriented approach, interoperability and possibly integration with fleet management, new business opportunities and spin-off business services (e.g. customer services, anti-fraud, environmental management).

4 MENTORE project

MENTORE is a two-year project promoted by the European GNSS Supervisory Authority (GSA) through funds from the 6th Framework Programme.

MENTORE targets the use of the EU GNSS, EGNOS (European Geostationary Navigation Overlay Service) and Galileo, for “Regulated tracking and tracing” services.

“Tracking & Tracing” targets a class of services for land applications, requiring the knowledge of the position of assets or persons, as provided by satellite navigation technologies.

The added value of EGNOS in comparison to GPS relies in the capability to provide “guaranteed positioning”, thanks the exploitation of its integrity function. Thus, the present availability of EGNOS over Europe, in view of Galileo over the world, enables tracking & tracing services based on guaranteed positioning. These services can support the implementation of regulations and policies requiring precise and reliable localisation: the so-called “Regulated tracking & tracing” services.
Regulated Tracking & Tracing services address a wide range of applications in the transport and personal mobility markets. The most relevant benefits of these services are public and social; however they also imply commercial interests.

Specifically concerning the transport of dangerous material, a number of best practices adopted at National or European levels are presently operational using GPS positioning.

MENTORE has implemented and operated EGNOS tracking & tracing services in two real-life cases involving Italian industry and authorities (Italian Ministry of Transport): carriage of nuclear material (Mit Nucleare) and hydrocarbons (ENI).

In particular, MENTORE has proven through a technical/real-life demonstrative implementation and a resulting validation that the transport of dangerous goods can benefit of EGNOS. In both above mentioned cases, MENTORE has verified that EGNOS provides additional value with respect to the GPS, thanks to more reliable and accurate positioning and surveillance. The result is an increase of safety, of which drivers, goods owners, transport operators and authorities can benefit.

An overview of the architecture is provided in the following picture. The main elements are:

- The EGNOS On-Board Unit (OBU), CS-NAV enabled and with a dual mode communication (GPRS and Globalstar satellite communication)
- The LoCation Server (LCS) in the Service Centre providing CS-NAV services based on a Telespazio proprietary solution.
- The software platforms providing service access to the end users, via a simple web interface or a dedicated client application or through already existing application.

EDAS (EGNOS Data Access System [15]) is a server that gets the raw data directly from the EGNOS system and distributes it to Service Providers in real-time, within guaranteed delay, security and performance.
MENTORE results and conclusions are that EGNOS today (and Galileo in the future), can be a key tool for the regulated control of dangerous material transport, supporting the enhancement of public safety and transport efficiency:

- Today EGNOS-based services can satisfy the need for guaranteed positioning, as required by Authorities, goods owners/producers and transport operators.
- In the future, EGNOS/Galileo features (service guarantee, integrity, and possibly authentication) can be fundamental differentiators with respect to GPS, especially in supporting liability/responsibility chains.

Law enforcement agencies take advantages from guaranteed information related to position, travelling times and route, while commercial transport operators and users benefit from effective shipment and in compliance with regulations.

5 Vulnerabilities of transportation of dangerous goods based on GNSS

Transportation of dangerous goods is a critical application, which may have a severe impact on the safety of the citizens if there are vulnerabilities, which could be used by criminal attackers.
Application providers do usually employ procedures, which are designed to ensure the protection of the public and the environment. For example, shipments of irradiated nuclear and high-level radioactive material fall into the highest security class (category I), for which a large number of technical and administrative requirements have to be met.

Security during transport is achieved by a combination of:

- An armoured transport vehicle
- An armoured escort vehicle
- An armoured control centre
- Communication lines between vehicles, control centre and police,
- Vehicle tracking (present solutions are based on GPS plus with satellite communication, for reliability purposes).

For what the transport of dangerous material it is in general concerned, in Europe it is mostly performed by road and increasing steadily. In 2005 road transport of dangerous goods reached 78 billion tonne-kilometres (tKm) for the EU-25 and Norway, with flammable liquids accounting for 60% (see reference [7]).

As described, the vehicles themselves are usually well protected and the related security procedures are well know and established.

As described before, the application for the transportation of dangerous goods is based on a control room where the positions of the vehicles are displayed and monitored on digitised maps. The centre collects high frequency data reports, which are processed for:

- Continuous tracking and tracing
- Control of shipment in a specified route (according to the plan and authorised path)
- Incident prevention, thanks to the monitoring of status parameters
- Alarm raising in case of anomaly condition detection
- Recording and logging for regular roundup of reported incidents
- Informing the emergency response forces for the emergency management arrangements.

Vulnerabilities may be present in any point of the information workflow. In this paper we will focus on the vulnerabilities aspects of GNSS and the communication systems.

Analysis of the vulnerabilities of GNSS and specifically of GPS has been proposed by a number of research centres around the world. One of the most complete studies is [8] produced by John A. Volpe Transportation Systems Centre.

In the report, the vulnerabilities are classified on the basis of unintentional or intentional attacks.

In the first category (unintentional), are classified wireless interferences from natural phenomena like ionosphere interference due to solar flares or other causes. These phenomena may introduce errors on the satellite-terminal path as amplitude
or phase variations (or both). In this same category, we can also consider wireless interference from man-made systems, which may ‘jam’ the GNSS signal. GNSS signals (especially GPS) are characterized by very low power levels at the terminal and narrow spectrum band occupation. Both features make GPS signal very vulnerable to external wireless interferences. Radio Frequency spectrum regulators take great care that the spectrum occupation by communication services is divided in adjacent bands, which do not overlap. Unfortunately communication systems may not be designed or deployed with the proper care. Electronic components of the communication system may not be properly configured and they may generate spurious emissions or adjacent-band interferences in frequency bands, which were not allocated to them by regulators and which may overlap the GNSS frequency bands.

The effect is that the GPS signal mounted on the vehicles used to transport the dangerous goods may not be able to determine their position in the specific geographical area affected by the wireless interference.

The second category is represented by intentional attacks. In this case, an attacker can implement a simple jamming attack or spoofing attack. A jamming attack is simply a wireless signal transmitted in the frequency bands used by GNSS with a level of power and spectrum bandwidth, which effectively cause Denial of Service (DOS). The interference signal should be at least 40 dB above the GNSS signal level of with wide spectrum occupancy (in the order of MHz). The modulation of interference signal should resemble a GNSS signal or be complex enough to make its identification more difficult. Devices of this kind are very easy to implement and deploy and they are not necessarily expensive. An airborne low-power jammer can effectively disrupt a GPS signal over a large geographical area.

In a spoofing attack instead, the objective is to synchronize a GNSS terminal receiver to a fake GNSS signal to provide a false position to the end-user. Various types of spoofing attacks are possible but the most effective is to synthesize a GNSS signal, which overrides the real GNSS signal to “fool” the GNSS receiver. Spoofing is more complicated to implement than simple jamming. On other side, a jamming attack is easy to identify (there is no GNSS signal) while a spoofing attack, if well implemented, may not generate any alarm or notification.

In comparison to other GNSS applications in the air traffic or maritime domain, these types of vulnerabilities may be less critical. Transportation of dangerous goods does not require a high level of precision, unless the devices are in an urban environment. The position of a device is anyway constrained by the transportation infrastructure itself (i.e. roads). Unintentional interference from a badly configured communication system is usually limited to a geographical area, which can be easily identified. As a consequence, unintentional interferences may not be a critical issue.

On the other side, intentional interferences can be more serious. Attackers can “jam” or “spoof” the GNSS signal to create a weakness in the system in preparation to other attacks. If the control room of the fleet management systems does not know the position of the vehicle transporting the dangerous goods or if the transmitted position is wrong (because it has been spoofed), an attacker can physically attack the vehicle or cause a road accident.
Vulnerability is the communication system used to transmit the position of the vehicle to the control room.

The communication systems should be reliable, secure and with adequate coverage to provide connectivity to the vehicle for the entire journey. Today a number of communication systems can be used for this purpose:

- Cellular networks like GSM/GPRS and UMTS have usually good coverage and they can provide a reasonable level of security. Reliability may be an issue because their design is based on business considerations and not specifically on reliability. If a large number of users is present in the area (major event in an urban environment or congested highways), the connectivity to the vehicle, which transports dangerous goods, may not be guaranteed because the traffic usage has grown beyond the maximum network capacity.

  A solution based on cellular networks has the advantage of being quite economical as GSM/GPRS/UMTS card costs less than 100 Euro.

- Satellite communication systems have excellent coverage, high level of security and reliability. Installation of the communication terminal and traffic cost may be high in comparison to cellular networks. Because of the mobility of the vehicles, low-frequency satellite communication is recommended. They are usually used as back-up solution (see chapter 6).

- WiFi/WiMax has been recently deployed or they will be deployed in urban environment. Currently, they do not provide sufficient coverage. Only the most recent standards (i.e. Mobile WiMax 802.16e) provide support for mobility.

Communication system can also be “jammed” like the GNSS signal but the attacker requires significantly more power to implement the attack. As a consequence, even a very powerful jammer may create Denial of Service (DOS) to communication only in a limited area, which would not seriously affect the transportation chain.

Other vulnerabilities may be present at the level of the ICT infrastructure, which supports the application of dangerous goods. Most of the security considerations are not specific for this application and they will not be considered in this paper. The major issue is the protection of the data with the position and contents of the vehicles. This information, usually stored at the control centre, should be protected against criminal attackers, who can use it to implement a physical attack against the vehicle.

Shipments of dangerous goods are far too hazardous and there is great potential for endangering human life and damaging our environment through mishaps in the course of transportation. It is essential for all actors (manufactures, carriers, terminals, users, governments…) to continually work towards minimising the risk of mishaps in the transportation and the harm done by mishaps that do occur.

6 Mitigations techniques and best practices

Both the research and industry domain have presented solutions to reduce the risk of the vulnerabilities presented in the previous paragraph.
The large majority of the systems designed for the transportation of dangerous goods are currently based on GPS, but new GNSS systems are being designed and deployed like EGNOS and Galileo.

EGNOS provides Commercial Service (CS) enabling land applications for professional markets in Europe. The CS is based on the use of). For regulated tracking & tracing applications like the transportation of dangerous goods, the added value is the provision of guaranteed positioning.

For the regulated control of dangerous material transport, EGNOS/Galileo features can validate the requirements imposed by the regulatory framework described in paragraph 2, especially in supporting liability/responsibility chains:

- Law enforcement agencies take advantages from guaranteed information related to position, travelling times and route, which can be used, in case of accidents, for prompt response and emergency assistance and for liability/responsibility treatment.
- Commercial transport operators and users benefit from effective shipment and in compliance with regulations, while increasing the overall efficiency.

For the transport of dangerous goods, MENTORE successful experimented the advantages resulting from the use of both EGNOS OS and EGNOS CS (based on the EGNOS data disseminated by EDAS, as mentioned before).

In the case of transport of hydrocarbon (ENI), a comparison has been done between the positions measured with two on-board units: a GPS one and a second one enhanced to use EGNOS OS. The results of EGNOS versus GPS performances experimentation show an enhanced stability and accuracy that ENI has considered interesting feature for operational uses ([11]).

In the case of nuclear material transport (Mit Nucleare), EGNOS CS service architecture has been implemented and demonstrated. The added value as compared to GPS relying in the capability to provide “guaranteed positioning” has been considered an interest feature by both Mit Nucleare and the Ministry of Transport, enabling reliable tracking & tracing and safety increasing ([12]).

Thus, in relation to the vulnerabilities mentioned in paragraph 5 the following countermeasures can be provided through EGNOS/Galileo:

**Unintentional Ionosphere interference**: Integrity of signal can mitigate the impact of unintentional interference from ionosphere effects. In EGNOS and Galileo, integrity represents the level of confidence a user can have in the computed position and the estimated error. Tracking & tracing systems know the probability that the position of the vehicle, transporting dangerous goods, is correct.

**Jamming**: The availability of E5 signal and of the authentication feature will provide Galileo services with more robustness than the GPS ones against wireless jamming. As a consequence intentional jamming of Galileo signal will be more difficult to achieve and it will require jammers with higher power. An issue could be that related to the cost of dual-frequency receivers or the complexity of the device for managing the authentication. However, social and commercial the benefits achievable through a robust positioning services can justify the additional cost and complexity.
**Spoofing:** The Galileo authentication will enable the prevention of spoofing attacks.

Additionally Galileo will possibly provide the capabilities of the Public Regulated Service (PRS). An issue could be that PRS service will be mostly adopted by Public Safety and Military organizations, while commercial fleet managers may not adopt it.

A number of solutions can be adopted to improve the communication links used in the transportation of dangerous goods.

Commercial networks like GSM/GPRS/UMTS do not have prioritization capability to the users in their design like public safety communication systems like TETRA. As a consequence, a wireless provider cannot give priority to the traffic related to the transportation of dangerous goods in comparison to the normal traffic. The evolution of 3GPP and LTE may provide the prioritization capability requested by this critical application.

In the meantime, the most efficient solution is to use mobile satellite communication as a backup of GSM/GPRS/UMTS communications. A sensor can detect when the GSM/GPRS/UMTS communication is dropped or degraded. The mobile satellite communication can be then activated to transmit the information on the position and condition of the vehicle.

In the future the evolution of Intelligent Transportation System (ITS) can also provide the additional communication means with increased levels of robustness even if the coverage will be initially limited to urban areas.

Beyond the technical challenges related to navigation and communication, the transportation of dangerous goods would benefit by the adoption of best practices and common standards. The current scenario presents a fragmented use of technologies, services and data formats, which should be unified to increase the interoperability and reliability of the overall integrated system.

From the implementation viewpoint, today’s best practices at national level will most likely be the driver behind any introduction strategy at European level. National authorities should carry out the standardization process in combination with the legislative policy implementation.

Member States shall support large-scale implementation by stimulating the use of EGNOS in the presently operating solutions and platforms, to involve key players (stakeholders and relevant associations) and set up a clear regulatory process.

A complete best practice program at European level should:

- evaluate and validate the use of EGNOS in live operations and real commercial deployments.
- Promote harmonisation among national best practices.
- Promote technical standardization.
- Provide feedback to the regulatory process.
- Increase the synergy with the public sector on the basis of the consideration that the transportation of dangerous good may have a strong impact on the security and safety of the citizen.
7 Conclusions

Transportation of dangerous goods on the road is a key business sector that also implies citizens’ safety aspects. For this reason, it is important to identify the related vulnerabilities and countermeasures. EGNOS and Galileo can play an important role as a tool for enhancing transport efficiency while ensuring public safety. R&D projects such as MENTORE allow evaluating the proper use of these technologies in conformance to the existing regulation framework. One of the main issues in the integration of tracking and tracing systems is that the context is still highly fragmented. Thus, future developments need to address technical standardization, the identification and definition of best practices at European levels and feedback to the regulatory process.

References
