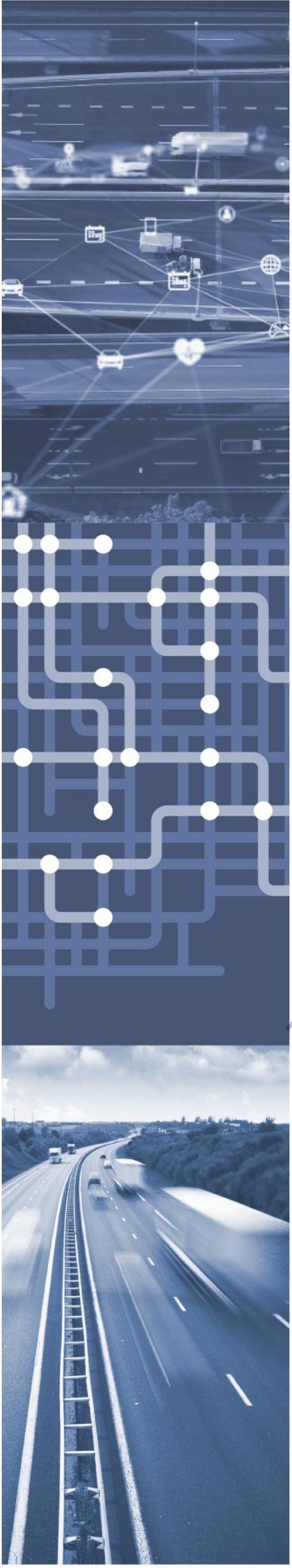


TAPA EMEA
Transported Asset Protection Association

TSR

Trucking Security Requirements Guidance Document for users of TAPA Standards

Telematics Systems Guidance V2

TAPA EMEA
Pastoor Ohllaan 39
3451 CB Vleuten
The Netherlands

www.tapaemea.org
info@tapaemea.org
Tel. +31 619 5734 61

TAPA does not represent nor warrant that the information contained in this document will prevent any loss, damage or injury to a person or property, because of burglary, theft, hold-up, fire or other cause, or that the information will in all cases provide the protection for which it is intended. If the reader chooses to use any information in this document, they assume all risk and liability for doing so.

Contents

TAPA Transported Asset Protection Association

Trucking Security Requirements

TSR 2023

APPENDIX A: HARD SIDED TRUCK
APPENDIX B: SOFT SIDED TRUCK
APPENDIX C: RIGID VANS/ FIXED BODY TRUCKS
APPENDIX D: SEA CONTAINER

1. Introduction

TAPA has produced this Telematics Systems Guidance (TSG) to provide helpful and supporting information on telematics systems for users of the TAPA Trucking Security Requirements (TSR) Standard.

The idea for producing a TAPA guide on telematics systems came from supply chain security professionals who are also members of TAPA. This guide covers how telematics systems can be used in supply chain security for road transportation and also provides examples of devices that are intended for such purposes.

TAPA has included images and information on products in the TSG. These products are available commercially and are considered examples of products that help protect vehicles and their cargo; other similar products are available. TAPA does not endorse any of the products included in this document. TAPA cannot specify which product is appropriate for a TAPA TSR security level.

The purpose of this document is to:

- Provide additional detailed information on telematics systems solutions not covered in the TSR;
- Provide an overview of the risk that usage of these systems can mitigate;
- Provide users with industry best practices on how to implement telematics systems;
- Provide users with telematics systems implementation examples that will help in the selection and identification of suitable products for the respective TSR level;
- Provide suppliers with examples of telematics systems and their intended use.

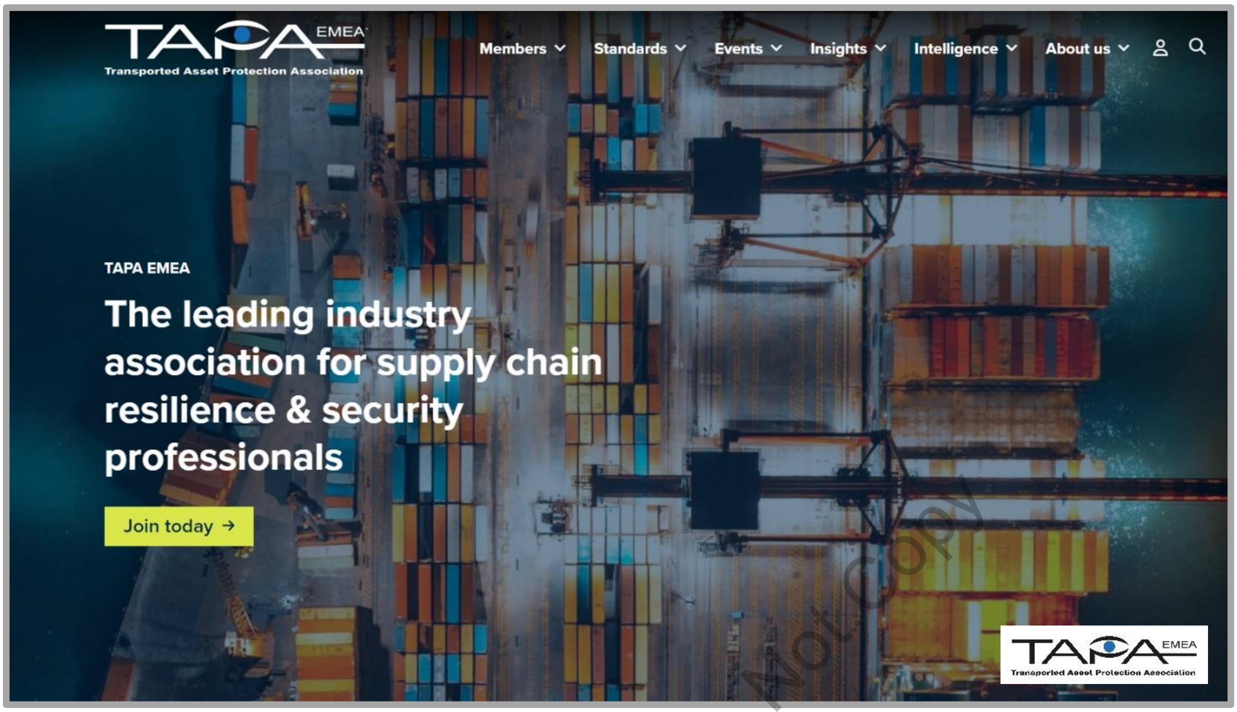
This document will be reviewed and updated as necessary, providing TSR users with up-to-date information on telematics systems. The latest version will be available to download from the Standards section of the TAPA website.

2. About TAPA

Cargo crime is one of the biggest supply chain challenges for manufacturers of valuable, high-risk products and their logistics service providers.

The threat is no longer only from opportunist criminals. Today, organized crime rings are operating globally and using increasingly sophisticated attacks on vehicles, premises, and personnel to achieve their aims.

TAPA is a unique forum that unites global manufacturers, logistics providers, freight carriers, law enforcement agencies, and other stakeholders with the common aim of reducing losses from international supply chains. TAPA's primary focus is theft prevention through the use of real-time intelligence and the latest preventative measures.


TAPA EMEA
Transported Asset Protection Association
Members
Standards
Events
Insights
Intelligence
About us
Join today →
TAPA EMEA
Transported Asset Protection Association

TAPA EMEA

The leading industry association for supply chain resilience & security professionals

TAPA's Mission

TAPA's mission is to help protect members' assets by minimizing cargo losses from the supply chain. TAPA achieves this through the development and application of global security standards, recognized industry practices, technology, education, benchmarking, regulatory collaboration, and the proactive identification of crime trends and supply chain security threats.

3.What is Telematics

Telematics is an interdisciplinary field that encompasses telecommunications, vehicular technology (road transport, road safety, etc.), electrical engineering (sensors, instruments, wireless communications, etc.), and computer science (multimedia, Internet, etc.)

The term Telematics is a combination of the words telecommunications and informatics and is used to broadly describe the integrated use of communication and information technology to transmit, receive, and store information from telecommunications devices to remote destinations over a network.

One of the most common applications of telematics is the tracking of cars, trucks, equipment, and other assets by using GPS technology and a type of communication, the GSM network being the most common.

Telematics systems in commercial vehicles were initially used as a fleet management solution and generally consist of a telematics device, other connected hardware, sensors, and software platforms. These systems can process and analyze data, such as position, vehicle speed, trip distance/time, idle times, harsh braking and driving, fuel consumption, vehicle faults, battery voltage, and other engine data.

Telematics is shaped in several different ways for different applications or needs, being widely spread in the modern automotive world.

Vehicle tracking means having information about the location, status, and behavior of a vehicle or fleet of vehicles. This is achieved through a combination of a GPS (GNSS) receiver and an electronic component (usually containing a GSM GPRS modem, SMS sender, 3G/4G modems) installed in each vehicle that is communicating with the user (dispatching, emergency, or coordinating unit) through a PC-based or web-based software. The data is turned into information by management reporting tools in conjunction with a visual display on computerized mapping software.

Several types of vehicle-tracking devices exist. Typically, they are classified as passive and active.

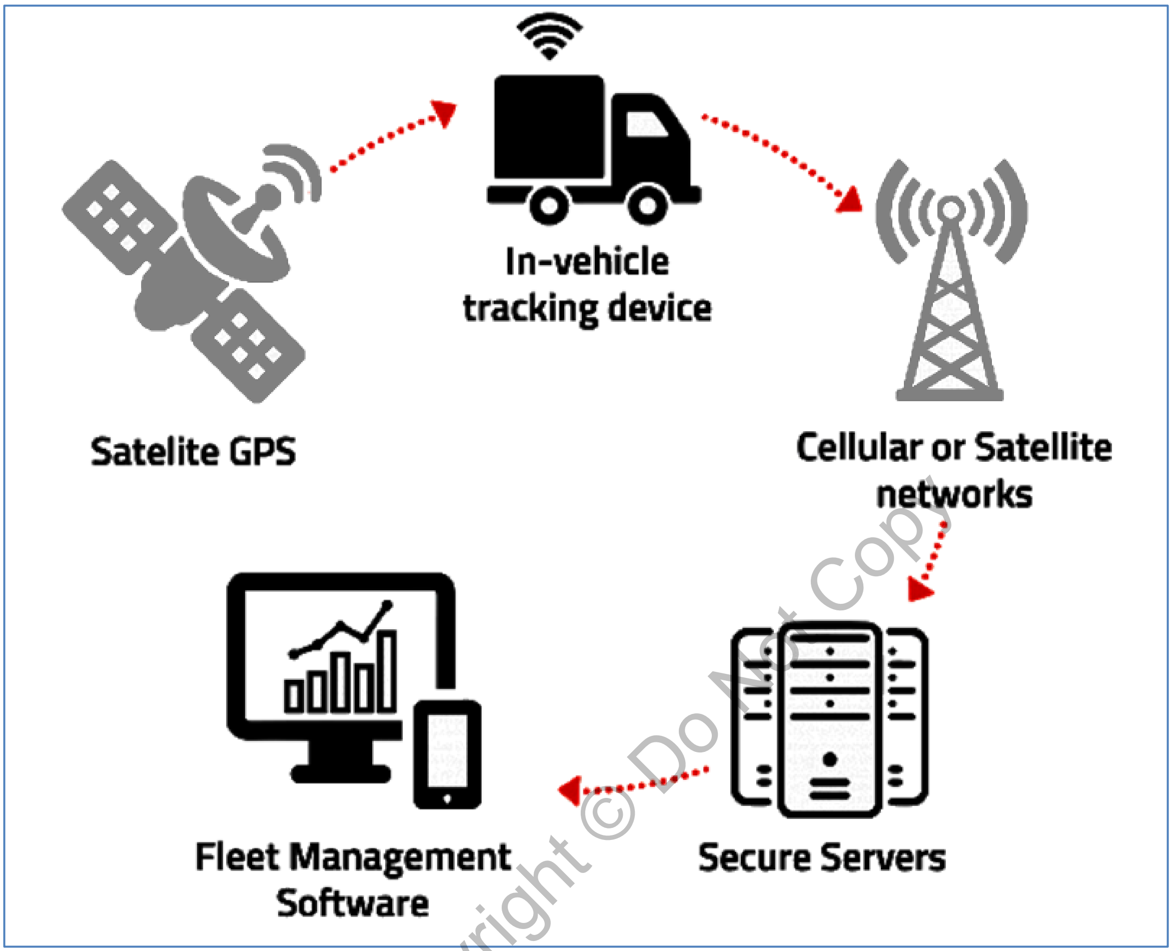
Passive devices store GPS location, speed, heading, and sometimes a trigger event such as key on/off, door open/closed, etc. Once the vehicle returns to a predetermined point, the device is removed and the data is downloaded to a computer for evaluation. Passive systems can include auto-download type devices that transfer data wirelessly once in a predefined area.

Active devices also collect the same information but usually transmit the data in near-real-time via cellular or satellite networks to a computer or data center for evaluation.

Modern vehicle tracking devices combine both active and passive tracking abilities: when a cellular network is available, and a tracking device is connected it transmits data to a server; when a network is not available the device stores data in internal memory and will transmit stored data to the server later when the network becomes available again.

For detailed vehicle locating and monitoring, the tracking can be accomplished by installing a box into the vehicle, either self-powered with a battery or wired into the vehicle's power system.

Especially for monitoring, additional sensors should be connected to the tracking box, so operational information (i.e. door opening, panic button, or intrusion alarm activation) is transmitted along with the location.


In-vehicle tracking device
Satelite GPS
Cellular or Satellite networks
Fleet Management Software
Secure Servers

Major components of the GPS-based tracking are:

1. **Tracking unit:** The device is fitted onto the vehicle and captures the location information, possibly including other vehicle information, and sends it at regular intervals to a central server via the integrated modem;
2. **Tracking server:** The tracking server has three responsibilities: receiving data from the tracking unit, securely storing it, and sending this information on demand to the user;
3. **User interface:** The UI enables the users/operators to: access the vehicle tracking data such as vehicle location and different signals recorded locally; it enables information access management; it shows the vehicle data; it highlights important details or it allows different formatting and reports for specific needs or KPI analysis.

4. Requirements and Associated Risks

In this chapter we will focus on the requirements of TAPA TSR 2023 related to telematics, providing insight on what is the intention of the Standard and some of the associated risks that the required measures are trying to mitigate.

The topics that are reviewed are listed below:

- Documented tracking protocols
- Tracking and tracing devices
- Basic tracking
- Tracking system reporting rate
- Events reported by the telematics system
- Backup battery – tractor
- Backup battery – trailer
- Controlling the reporting rate of the tracking device
- Duress alarm for driver
- Alarm response and maintenance procedures
- Audible alarm for cargo compartment doors
- Tracking device failure
- Routing system
- Route changes
- Locking Systems Enhanced Option - Cargo compartment door lock
- Rail Transfer Enhanced Option – Use of tracking systems
- Escort Enhanced Option – Tracking and duress alarm
- Cargo Compartment Alarm Devices Enhanced Option – Alarm loops and integrated netting/tracking device to be able to send/transmit breach alarms

Documented tracking protocols

Why?

Detailed and documented protocols are a very good method to ensure effectiveness (that the response protocols address the issue) and consistency (that all involved personnel will behave exactly in the same way in all incidents) of the entire process.

Associated Risk(s):

If the response protocols are not effective, it means that the incident will not be handled correctly. If the response protocols are not somehow documented (not necessarily printed) there is always the risk that the involved personnel will not follow exactly the protocol (usually because they are under stress) and usually, this has a consequence on the effectiveness of the protocols. It is also strongly recommended to test the response protocols before putting them into effect, otherwise during their application, in case of an incident, one might find that certain items were not very effectively organized.

Tracking and tracing devices

Why?

Tracking devices are the components that collect and transmit all signals from the vehicle to the monitoring center (and vice versa), offering the capability to monitor the routes. Tracking means to know what the location and the status of the vehicle are. Monitoring means to compare the actual location and status of the vehicle with the ones planned.

Keep in mind that you cannot monitor something that is not planned!

Associated Risk(s):

If the criminals manage to locate the device when they enter the cabin, they shall destroy it, so you shall not be able to track the vehicle.

If there is only one method of communication, there is the risk of this method not being available during the complete route. Having an alternative communication method increases the effectiveness of the tracking device.

If the device antenna is installed at a place that can be easily seen (e.g., the roof of the tractor or truck), then it is probable that the attackers shall destroy it, so that even if the device is installed in a covert location and is not found, it shall not be able to receive GPS signals or transmit GSM signals, if the antenna is broken.

Basic tracking

Why?

This requirement is actually in place to give the LSP the capability to check offline (usually after the conclusion of the complete route or a route's leg) that the route was executed as planned and that there were no violations of the agreed activities (e.g., planned stops, parking areas, etc.).

Associated Risk(s):

This is the least demanding tracking requirement in the Standard, addressing mostly the basic level of certifiable security, to provide the fundamental control after the route. Its absence gives the drivers the capability to execute the routes as desired with extremely minimum overall control.

Tracking system reporting rate

Why?

A standard reporting interval should be defined for the receiving software to be able to identify any communication disruptions or device malfunctions. Furthermore, the higher the value of the transported goods and the associated risks, the shorter the reporting interval should be for the monitoring function to be able to confirm proper execution of the route or get an associated alarm (e.g., route deviation) as early as possible and be able to initiate the respective response protocol. This requirement related to the trailer/container mitigates the risk of criminals being able to interfere with the onboard system/telematics (e.g.: tamper with the device, jam the GPS/GSM signal, etc.) and the monitoring center losing contact and not being able to track and monitor the cargo.

Associated Risk(s):

Usually, the route details are not embedded into the tracking device but in the receiving software, it is very important to identify as early as possible any potential deviation from the planned route. Additionally, the loss of 2 or 3 consecutive signals from the tracking device might be proven to be the initiation of a criminal attack, due either to the identification and damage of the tracking device/antenna or executing a jamming attack.

Events reported by the telematics system

Why?

These requirements are in place because, in most security incidents, these events can identify the initiation of an attack or an undesired situation. Attackers very often try to identify the telematics devices and interfere in any way possible with them to stop/avoid the tracking capability of the vehicle. Additionally, any unplanned stop of the vehicle or unauthorized opening of the cargo compartment door might indicate the initiation of a security incident.

Finally, the battery of the telematics device is extremely important for its operation (especially in case of attacks where the perpetrators might disconnect the main power source of the device) and the status of the battery charge should be known to the monitoring center, usually in percentages.

Additionally, the unhooking event is extremely important in case criminals decide to leave the tractor and steal the complete trailer with the use of another tractor.

Associated Risk(s):

Two major risk categories are associated with road cargo transportation: personal injury or loss of human life during a violent attack and loss of vehicle/cargo during an incident (e.g., hijacking, robbery, deceptive stop by disguised criminals, theft while the vehicle is parked, an internal attempt by company personnel, etc.).

Backup battery - tractor

Why?

This requirement addresses the risk of the attackers disconnecting the main power source of the tractor's telematics device, so the device stops reporting the location and status.

Associated Risk(s):

The associated risk is that, in case of disconnection of the main power source, without a backup battery, the telematics device shall not be able to operate, therefore the monitoring center will have no information related to the location and the status of the vehicle.

Backup battery - trailer

Why?

This requirement addresses the risk of the attackers disconnecting the main power source of the tractor's telematics device so that the device cannot report location and status.

Associated Risk(s):

The backup battery capacity needs to ensure communication every 5 minutes for at least 24 hours, giving the monitoring center and the relative authorities the time window necessary to deploy the recovery operation of the stolen trailer.

Controlling the reporting rate of the tracking device

Why?

This requirement supports the capability of the AMC to change the reporting rate of the tracking device remotely to increase the effectiveness of recovery operations. Also, the AMC should be able to send a remote command to increase the reporting interval to preserve the battery, so the recovery team has more time to locate the stolen vehicle or when the recovery team and the LEAs are very close to locating the stolen vehicle, the AMC should be able to decrease the reporting interval (e.g., to 1 minute) so that the authorities can follow the vehicle in real-time.

Associated Risk(s):

The absence of this requirement might increase the risk of complete drainage of the telematics device battery, prior to the conclusion of the recovery operations.

Duress alarm for driver

Why?

The driver should be able to inform the monitoring center related to the recognition of an undesired situation or the development of an attack without the attackers being able to identify this activity (e.g., without triggering a siren or other identifiable signal).

Associated Risk(s):

The duress alarm should be silent to ensure the driver's safety and to notify the AMC that a situation is under development while the attackers are unable to hear the alarm signal.

Alarm response and maintenance procedures

Why?

To ensure systems shall work as expected in case of an incident.

Associated Risk(s):

For example, if the opening of the cargo compartment doors is not monitored due to a malfunction or lack of a clear process, then there is always the risk that the attackers would open them without either the driver, the LSP, or the AMC being able to identify the incident.

Audible alarm for cargo compartment doors

Why?

Audible alarms are usually a very effective deterrent to make intruders run away after they recognize that they have been detected.

Associated Risk(s):

If, on opening, the cargo compartment doors do not produce an audible alarm, and they are opened without authorization, then there is always the risk of the attackers continuing their intrusion without any disruption after they open the doors.

Tracking device failure

Why?

The AMC must know when the tracking system does not function or if the GPS signal is lost. Usually, the device failure is identified by the loss of communication with the receiving software, so it is a software-generated alarm. The GPS signal quality (at least 3 satellites) is very important for the monitoring center to validate the location reported by the device.

Associated Risk(s):

If the AMC is not aware of these situations (device failure or GPS signal lost/wrong), then there is no capability to initiate any onsite response because the location is unknown.

Routing system

Why?

Very often there is a requirement for the driver to deviate from their planned route due to traffic jams, road works, etc.

Associated Risk(s):

If the latest software version (maps) is not installed, there is always a risk that the system will not guide the driver to the best alternative route.

Route changes

Why?

All deviations from planned routes should be confirmed by the monitoring center, following a pre-defined procedure to ensure the validity of this change due to navigation system guidance.

Associated Risk(s):

If these deviations are not confirmed based on a predefined protocol, there is always the risk that a fraudulent or criminal action causes these deviations.

Locking Systems Enhanced Option - Cargo compartment door lock

Why?

This requirement enhances the security of the cargo compartment as the rear door lock-down system is operated remotely, usually from the carrier's premises or the AMC.

Associated Risk(s):

Remote operation of the rear door, without the intervention of the driver, decreases significantly the risk of unauthorized rear door opening.

Rail Transfer Enhanced Option – Use of tracking systems

Why?

Tracking is considered effective in rail transport as well.

Associated Risk(s):

Tracking with monitoring always enhances the security of the transported cargo, in the rail terminals where a lot of criminal activity takes place, but also during planned and unplanned stops during transportation.

Escort Enhanced Option – Tracking and duress alarm

Why?

When escort vehicles are used, they should be tracked/monitored and equipped with a panic button.

Associated Risk(s):

The tracking/monitoring of the escort vehicle, combined with the installation of a push and/or voice-activated duress alarm, enhances the AMC notification process in case of a security incident, even if the escorted truck is not equipped with security devices.

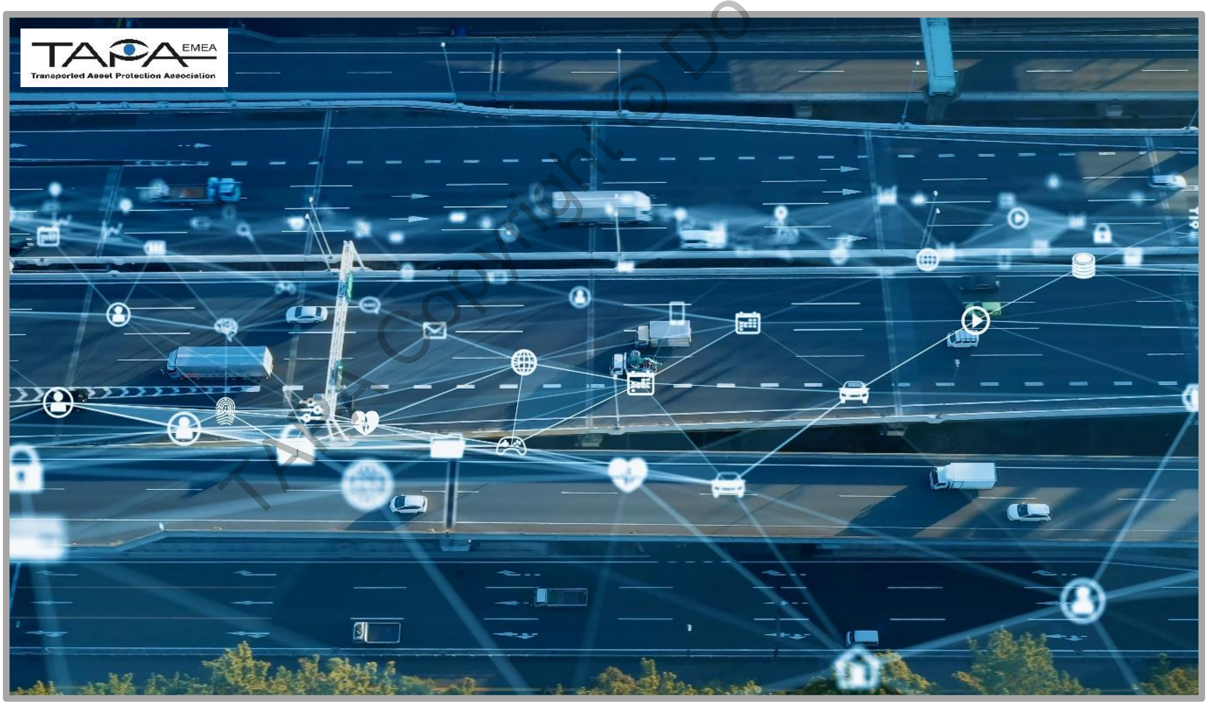
Cargo Compartment Alarm Devices Enhanced Option – Alarm loops and integrated netting/tracking device to be able to send/transmit breach alarms

Why?

This additional enhanced option introduced in the 2023 TSR standard intends to mitigate the risk of one frequent modus operandi for penetrating the trailers usually in parking areas. Criminals used to cut holes in the side, the roof of the trailers, or the rear doors and steal cargo. Alarm loops and/or integrated net alarms must be connected to the trailers' tracking device (usually), so the generated alarms are transmitted to the monitoring center and the carrier's home base.

Associated Risk(s):

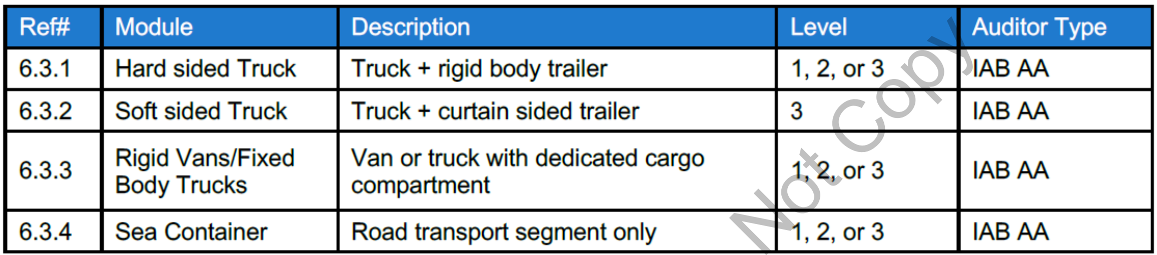
Without these improved alarm detection devices, penetration from the side walls or roof might not be detectable via traditional door intrusion sensors. Penetration through holes without actually opening the rear doors might go undetectable without these systems as well.



5.TSR Overview related to Telematics

Implementation of TAPA TSR 2023 can be achieved through a variety of setups, depending on the level that the LSP intends to certify. The correct security level, as well as any additional security measures, should be chosen depending on the value of the cargo and the risk indicators identified during the risk assessment.

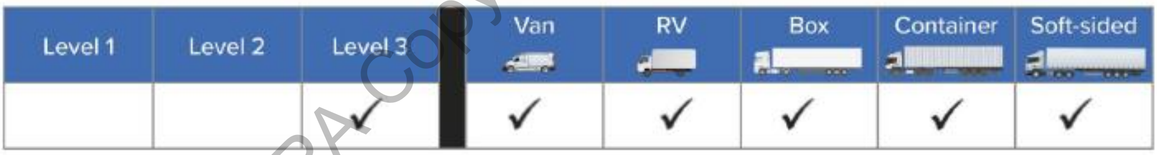
Throughout this section, we will provide a high-level overview example of the setups needed for each of the three TSR 2023 levels.



Ref#	Module	Description	Level	Auditor Type
6.3.1	Hard sided Truck	Truck + rigid body trailer	1, 2, or 3	IAB AA
6.3.2	Soft sided Truck	Truck + curtain sided trailer	3	IAB AA
6.3.3	Rigid Vans/Fixed Body Trucks	Van or truck with dedicated cargo compartment	1, 2, or 3	IAB AA
6.3.4	Sea Container	Road transport segment only	1, 2, or 3	IAB AA

TSR 2023 level 3

This level is the only certifiable option for curtain siders and it provides the basic level of security protection.



Level 1	Level 2	Level 3	Van	RV	Box	Container	Soft-sided
		✓	✓	✓	✓	✓	✓

To comply with the requirements, the vehicle must be equipped with:

a. A tracking device must be installed in a covert location in the truck/van tractor.;

b. Standard “reporting interval” for tracking unit in the truck/van tractor must be not less than one report every sixty (60) minutes.

The tracking device must be installed in the vehicle (in the case of an articulated vehicle, either in the tractor or the trailer) in a covert location that is not visible or easy to reach (e.g., not under the seat of the vehicle or in the glove compartment). Therefore, standalone tablet-like systems are not an option, as they cannot be installed covertly and can be easily removed during an attack. The same installation rules apply to the antenna(s) of the device to provide the necessary positioning and communication to locate the vehicle.

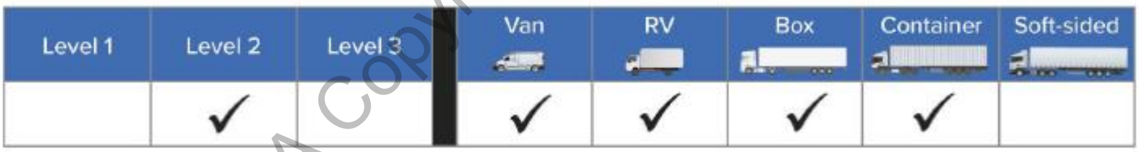
The reporting rate of the system must not be less than one report every sixty minutes. The most common implementation for this is to use a GSM data connection (e.g., 3G, 4G, 5G, CDMA).

c. Satellite navigation system installed (route planner) recognizing detours, traffic jams, etc. to avoid unnecessary stops or delays.

The dedicated route planner must be installed in the vehicle to assist the driver to follow a pre-planned route or to plan an alternative route due to unforeseen circumstances. The system must have the latest available software version installed and in use so that it provides accurate data to the driver.

TSR 2023 level 2

This level provides moderate security protection and is intended for hard-sided cargo transport vehicles.



Level 1	Level 2	Level 3	Van	RV	Box	Container	Soft-sided
	✓		✓	✓	✓	✓	

A certifiable system for level 2 must have the following components:

a. A tracking device must be installed in a covert location in the truck/van tractor and, where available, must be capable of utilizing at least two methods of signaling such as 3G, or SMS/GPRS using GSM or CDMA and must be equipped with at least one covert antenna.

The tracking device must be installed in the vehicle (in the case of an articulated vehicle, either in the tractor or the trailer) in a covert location that is not visible or easy to reach (e.g., not under the seat of the vehicle or in the glove compartment). Therefore, standalone tablet-like systems are not an option for level 2, as they cannot be installed covertly and can be easily removed during an attack. The same installation rules apply for the antenna(s) of the device, out of which at least one GPS & GSM antenna combination must be installed covertly (e.g., not on the roof of the vehicle) to provide the necessary positioning and communication to locate the vehicle.

The reporting rate of the system must not be less than one report every thirty minutes and the device must have at least two methods of signaling so that the position of the vehicle is communicated to the server even if one of the methods is unavailable (e.g., low network signal, jamming attack, etc.). The most common implementation for this is to use a GSM data connection (e.g., 3G, 4G, 5G, CDMA) as the main data connection and have the device fall back on SMS/GPRS transmission in case the main link is down.

The telematics system must be able to geofence routes and parking locations so that, if geofencing is used, an automatic alert is raised if the agreed route is not followed or any unauthorized stops occur.

These functionalities require a capable device and additional development on the server end, so the complexity of the entire system increases. The carrier should check if the respective system complies with the requirements before implementation.

b. A manually activated silent alarm (duress alarm) present in reach of the driver that must send a signal to the LSP's/Applicant's home base and third-party AMC. A mobile silent device option needs to be available if the driver has pre-approved criteria to leave the cab (sickness, accident, emergency incident etc.).

The system must be fitted with a duress alarm (panic button). Usually, this is located near the steering wheel so that the driver can push it in the event of an attack. The system should raise an alarm to the LSP but not signal in any way locally, as any indication to the attackers that an alarm was generated could expose a risk to the driver`s safety.

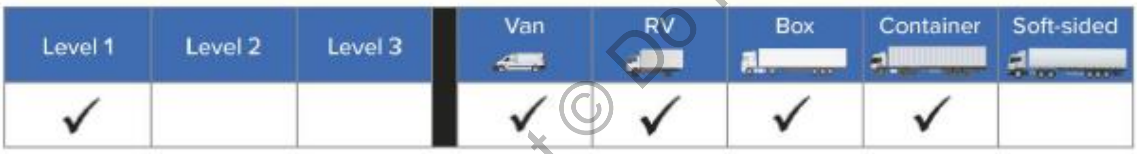
If, during the planning of the trip and after the risk assessment, a possibility of the driver leaving the cabin is identified, there is a need for the duress alarm to be mobile. This can be achieved either by an independent mobile device (e.g., personal tracker, security app on a mobile phone) or by having a device that communicates wirelessly with the telematics system in the vehicle (e.g., via RF, Bluetooth, etc.). Depending on the operation, the LSP must choose an option that ensures that the device has the necessary range for the driver to use in case of an emergency.

c. Satellite navigation system installed (route planner) recognizing detours, traffic jams, etc. to avoid unnecessary stops or delays.

   Similar to level 3, an up-to-date dedicated route planner must be installed to assist the driver.

TSR 2023 level 1

This is the level with the most requirements within TSR and provides elevated security protection.



Level 1	Level 2	Level 3		Van	RV	Box	Container	Soft-sided
✓				✓	✓	✓	✓	

A level 1 system must have the following components:

a. A tracking device must be installed in a covert location in the vehicle and, where available, must be capable of utilizing at least two methods of signaling such as 3G or 4G or 5G, SMS/GPRS using GSM, CDMA or satellite tracking device and must be equipped with at least one covert antenna.

   This requirement is similar to the one for level 2, with the difference that the standard minimum reporting interval is one report every five minutes. Additionally, the monitoring center must be able to change the reporting rate of the device as needed to assist in case of a security incident (e.g., decrease it to save battery or increase it for live monitoring).

   Also, if an articulated vehicle combination is used, each vehicle must be fitted with an individual tracker, one for the tractor and one for the trailer. While the vehicles are tethered, the reporting rate interval must be fulfilled by only one of the devices.

The tracking device must report at least the following events:

1. Device tampering of any of the installed security systems – the device should sense if an active attempt to compromise the device integrity or the data associated with the device is in progress and report the alert to the AMC;
2. Truck stoppage – the vehicle is not moving for a defined amount of time (as determined by the operation, routing, and associated risks) or the engine shut down;
3. Tracker battery status – level of the battery charge, usually reported in percentage;
4. Cargo area door opening – this can be achieved via a variety of sensors and contacts. If the vehicle has multiple doors, it is important to monitor all of them or have an implementation that restricts the opening of any unmonitored door(s) unless the door with the sensor is opened first.

When a trailer or container is used, the tracking device must report at least the following events:

1. Untethering (unhooking) of the trailer/chassis – the uncoupling of a trailer/chassis during transportation must raise an alarm;
2. Device tampering of any of the installed security systems – same as above;
3. Truck/trailer/container stoppage – same as above;
4. Tracker battery status – same as above.

In case of an alarm, this should be sent automatically at the moment of occurrence, and not at the next reporting interval. This is needed for the AMC to detect a threat as soon as possible and react accordingly.

The system needs to raise an alarm if it detects that there is a communication problem with the tracker (usually two consecutive messages are not received from the vehicle) or the GPS signal used for positioning is lost. Any of these could indicate that an attack is in progress (e.g., tampering with the device or attached antennas, jamming, etc.). The generated alert must be sent to the AMC.

b. The vehicle tracking devices must be equipped with a battery backup capable of maintaining the signaling capacity of the tracker for no less than 24 hours at a ”reporting” rate of no less than one ”report” every five minutes while the trailer is untethered.

The tracking device (in the case of an articulated vehicle both in the tractor and the trailer) needs to be connected to a dedicated battery that provides enough power for the entire telematics system (e.g., tracking device, panic button, door sensor, etc.) for at least 24h while maintaining the reporting rate of at least one report every five minutes. The battery system can be either integrated into the tracking device or in an external power pack. However, the installation (equipment and wiring) should be covert in order to prevent tampering with the power supply in case of an attack.

c. Unauthorized opening of cargo compartment doors activates an audible (acoustic) high-decibel alarm.

This can be achieved by installing a siren that is linked to the cargo door(s) sensor(s). A high sound intensity level is considered one above 100 dB. The LSP should always check for compliance with the local regulations regarding noise pollution.

d. A manually activated silent alarm (duress alarm) present in reach of the driver that must send a signal to the LSP’s/Applicant’s home base and third-party AMC. A mobile silent device option needs to be available if the driver has pre-approved criteria to leave the cab (sickness, accident, emergency incident etc.).

Same requirement and implementation as TSR level 2.

e. Local audible alarm if unauthorized entry to driver’s cab occurs.

This requirement can be achieved by installing a burglar alarm vehicle security system. Usually, this type of system monitors door opening, broken windows, movement within the cab, and excessive shocks, and has an integrated siren. Some vehicle manufacturers offer this as an option when buying the vehicle, but there are a lot of aftermarket solutions that can be used successfully too.

f. Satellite navigation system installed (route planner) recognizing detours, traffic jams, etc. to avoid unnecessary stops or delays.

Similar to levels 2 and 3, an up-to-date dedicated route planner must be installed to assist the driver.

6. Telematics Systems for Security Use

When we refer to telematics systems in this document, we are not focused on fleet management systems. We are focused on how these systems could be utilized to enhance the security of the trucks and trailers that are transporting high-value goods, and on how we can monitor security violations. Security violations are related to both event-triggered violations (i.e., the driver pushes the panic button) or activity-related violations (i.e., the crew opens the cargo door in a location that is not classified as a delivery/customer's location – or the vehicle has deviated from its scheduled path).

Fit for purpose

Telematics for security use is required to enable real-time tracking of the transport by knowing the location and the status of different sensors connected to the tracking unit that are installed and configured to provide a good indication of the status of the vehicle and the load.

Modern tracking devices are best suited to be used for security. The devices should be capable of combining active and passive tracking, to ensure continuous reporting of the vehicle status without interruption or information loss.

To ensure continuous data sending (updating with real-time data and status to the tracking server and also in the user interface), the tracking devices used should be capable of detecting main communication signal loss and switch automatically on to another communication method to keep sending real-time information to the tracking server. For example, if the main internet connection used by the tracker is 4G technology, if the 4G signal is lost then the device should automatically start sending the data through a different method, such as SMS.

The tracking devices installed on vehicles used for HVTT cargo transport collect and send specific information and events together with the location to the tracking server. The information reported should enable the users and system operators to know in real time the vehicle location, the status of the integrity of the tracking device and connected sensors, and the status of specific *security signals* that contribute to ensuring driver and cargo protection.

Usually, for updating all the necessary information used for security protection, the tracking device installed on the truck and/or trailer is wired to the power system and to specific sensors already available on the vehicle, or specially mounted to enable required event monitoring (i.e. panic button, door contact, etc.).

An important feature of telematics designed for security is to enable two-way communication between the users and the systems installed on the vehicles. This means that the tracking device is sending data from the vehicle to the platform and the platform can send data to the tracking device on user demand. This feature enables users to send out, from the user interface to the tracking device, different commands (e.g., lock operation, remote changes to the reporting interval, activate secure mode, etc.). If the system has an integrated display, this function can extend to communication with the driver via messages, sharing the planned route and secure stop areas, etc.

A short synthesis of the main components of the security telematics are:

- **Tracking kit:** devices fitted onto the vehicle that captures the positioning information, including other data acquired from special/dedicated sensors or electrical components (part of the GPS kit), and that send the information at regular intervals or instantly in case of security alarm to a central server;
- **Tracking server:** receiving data from the GPS tracking unit and its sensors, securely storing it, processing the information to detect any deviation, and serving this information on demand to the user;
- **User interface:** The UI enables the users/operators to access the vehicle tracking data such as vehicle location and different signals recorded locally, as well as interacting with the system on the vehicle if the capability is implemented.

All the above enables real-time tracking and reporting of all security signals that are required for the monitoring bodies/entities/operators (i.e. alarms monitoring and intervention teams/organizations) that one could take action based on specific procedures, in case the driver or the cargo are being threatened/attacked.

Quality and conformance tests

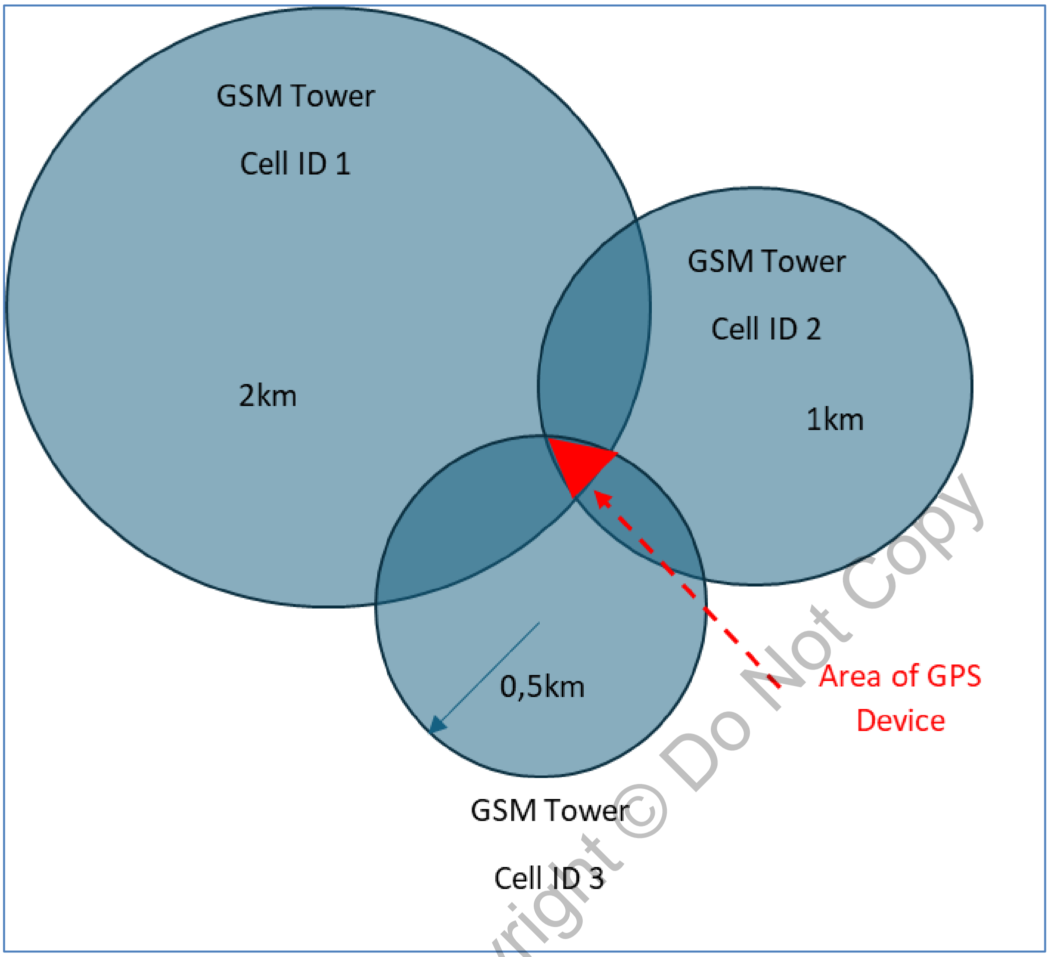
Telematics systems, being information technology equipment installed in vehicles, require a series of certifications. These quality tests are related to GSM technology and GPS technology such as Electromagnetic Compatibility (EMC) and CE marking for use in the EU.

Network Coverage

All telematics devices include a communication module to broadcast the information collected. The technology used varies from the newly established (e.g., ZigBee, LoRa, NBIoT, WiFi) to more traditional (Bluetooth, RF, Satellite) and GSM, which is the dominant form of communication in transportation.

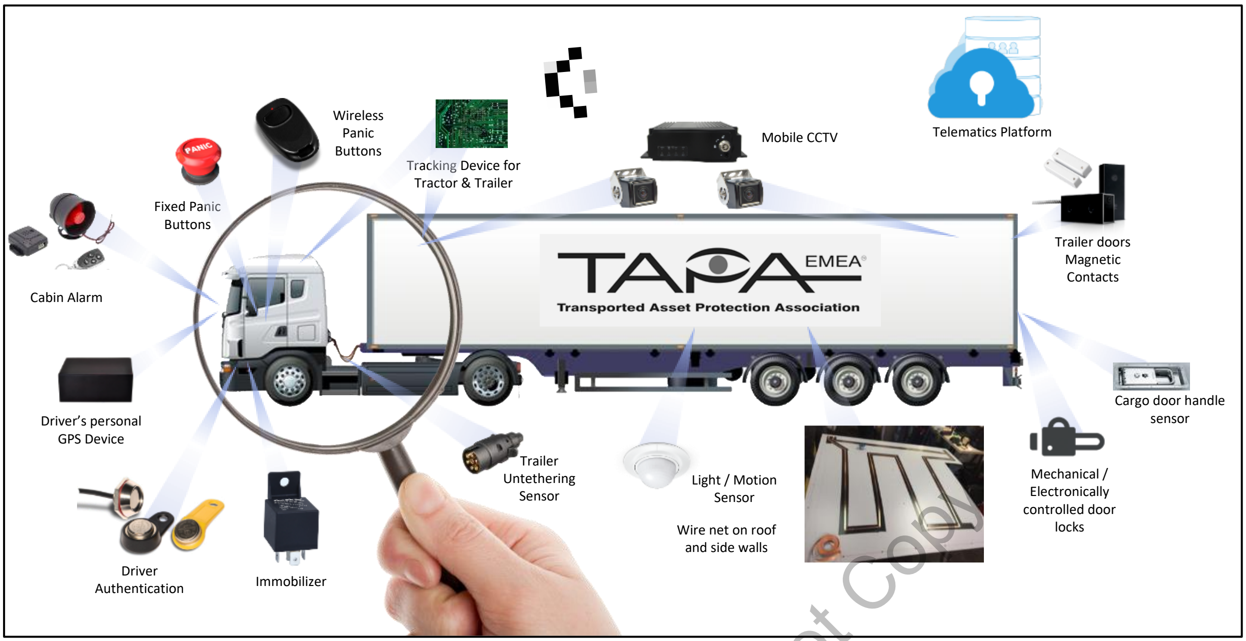
Connectivity is crucial when we combine technology and security both for communication but also for localization. Thus, every route risk assessment includes the identification of areas of low GSM coverage or lack of coverage (black holes) and the deployment of specific response protocols.

Furthermore, the GSM network is being used as a method of localization when the telematics devices fail to fix a GPS position (e.g., placing a device in a pallet inside a hard-sided trailer reduces GPS signal significantly). In such cases the device will broadcast the GSM Tower Cell ID that it is connected to and the telematics software can predict the area where the device is located. If the information available is a single Cell ID then the prediction would result in an area of many square kilometres. But if the device is capable of reporting all GSM Tower Cell IDs that it can scan in the area that it operates in, then the telematics software can use triangulation to make a very precise prediction, resulting in an area of a few meters (e.g., the area highlighted in red in the following picture).



Integration with different sensors

Telematics systems for security include hardware such as multiple telematics devices, sensors for trailer doors (e.g., magnetic contacts), panic buttons, sensors related to truck and trailer untethering, and others. Moreover, all this hardware is connected to a telematics platform, capable of decoding all data collected, presenting it to a digital map layer, and setting specific rules that generate critical events. In addition to the hardware-generated events, there are also software-generated events such as geofence violation, loss of communication, and others.


Wireless Panic Buttons
Fixed Panic Buttons
Cabin Alarm
Tracking Device for Tractor & Trailer
Mobile CCTV
Telematics Platform
Trailer doors Magnetic Contacts
TAPA EMEA
Transported Asset Protection Association
Driver's personal GPS Device
Cargo door handle sensor
Trailer Untethering Sensor
Light / Motion Sensor
Wire net on roof and side walls
Mechanical / Electronically controlled door locks
Driver Authentication
Immobilizer

(Example of a telematics security system for a tractor and a trailer)

Component	Short description
Telematics Device/tracking unit	GMS / GPS device providing real-time position of the track and trailer. Available options: Capability to recognize jamming attacks, Driving Behaviour analysis.
Fixed Panic Button	A wired button is installed permanently in the driver's cabin or next to the trailer's door, connected to the telematics device input.
Wireless Panic Button	RF button of short-range connected to the telematics device input.
Driver's Personal GPS device	GMS / GPS device providing real-time position of the driver. Includes a panic button and could also allow man down© events.
Driver Authentication	System designed to recognize/authenticate the driver (e.g., reader and tag, code entered via keypad). Could be installed in combination with an immobilizer to prevent ignition-on by unauthorized drivers.

Component	Short description
Immobilizer	Relay that will deactivate the vehicle ignition by non-authorized drivers or upon panic button activation. Could also be activated remotely via the telematics device.
Tractor alarm	The cabin alarm is connected to the telematics device input to send an event when there is an intrusion attempt.
Trailer untethering sensor	Sensor connected to the telematics device input that will recognize the tethering/untethering of the truck and trailer.
Electronically controlled Trailer Lock	Permanently installed lock that is connected to the telematics device and can report the status of the lock (locked/ unlocked) but that also can be controlled remotely.
Magnetic contact	Magnetic contact connected to the telematics device input to identify when the trailer door is open/closed. Advanced option available: security-paired magnetic contacts that cannot be manipulated by a magnet.
RF proximity sensors	RF sensors are connected to the telematics device input to identify when the trailer door is open / closed. Very secure, as they cannot be manipulated, but have a bigger power consumption than magnetic contacts.
Wire-net	Installation of a wire net on the sides, the roof of the trailer, and the doors, connected to the telematics device input, is meant to trigger an event when an attempt is made to cut an area of a hard-sided trailer to access the cargo area.
Light / Motion sensor	Connected to the telematics device input to trigger an event if an attempt is made to cut an area of a hard-sided trailer to access the cargo area.
Mobile CCTV	CCTV that records video locally but can also stream video upon request or after an event is triggered i.e., door open.
Cargo door handle sensor	Sensor for the trailer door handle connected to the telematics device input that will recognize the attempt to open the trailer’s door.

Component	Short description
Telematics Platform	Tracking platform decoding all telematics messages.

Best practices

TAPA TSR is the industry Standard regarding secure transport of cargo by road and it has been widely implemented by different companies throughout the logistics sector.

The feedback from the different stakeholders is the force that drives the evolution of the Standard, as new threats appear and the industry needs to adapt to mitigate the developing risks.

From the experience of the companies that have adopted TSR and implemented it successfully, a series of best practices have been identified, regardless of the TSR level or type of implementation.

Devices designed for security

As telematics is commonly deployed in most activities where a commercial vehicle is used, the offer for such systems is very varied. However, for security purposes, it is recommended to use a system that has been designed for this particular use case as the supplier has the expertise required to provide a reliable solution.

When multiple tracking devices are installed, it is recommended to place them as far from each other as possible to reduce the chance that both are silenced by a jamming attack.

Covert installation

One of the first things that an organized crime group will do during an attack is to try to disable the tracking device(s) installed on the vehicle(s). The best way to counter this action is to install the tracking units in areas that are not easy to reach and identify (e.g., behind the dashboard of the vehicle, inside the trailer). The same should be done with any external antenna and power lines connected to the tracking units.

Nothing visible from the outside

When transporting vulnerable cargo, it is important to not attract unnecessary attention. As such, the components of the security telematics system should be installed in a way that they are not visible from the outside. If external parts are required for the operation of the system, these can be masked by different methods to be as inconspicuous as possible. In this way, the vehicle does not attract the attention of an opportunistic attack and the criminals cannot easily tamper with the system by removing the external components (e.g., an external GPS or GSM antenna).

Devices resistant to variation in temperature, humidity

Considering that the security systems are installed on commercial vehicles, the entire system should be designed to work under the various environmental conditions that the vehicle could encounter (e.g., high variation in humidity and/or temperature, vibrations, dust and dirt, etc.). Special attention should be given to the connections that are exposed to the elements, as these are vulnerable points throughout the installation. To ensure reliability, the entire system should be tested under real-life conditions before normal operation.

Integration between all components should be tested throughout

As security systems have a great variety of sensors and components, all the parts must be compatible and work together under all the possible conditions that the vehicle might encounter.

Driver personal tracker

To enhance the safety of the driver and increase the response time in the event of a security incident, there is the option of using a personal security tracker. These types of devices come in a variety of setups but are mostly split into two categories: standalone (a device with its own communication modem and internal battery, used solely for security) and mobile software application (installed on a smartphone).

Regardless of the device type, the main functions of the devices are to be used as a mobile panic button for the driver in case of a security threat, and to give the AMC the possibility to precisely locate the driver to assist.

When a mobile software application is used, or installed on a smartphone, the activation of the alarm must be possible without having to deactivate the screensaver of the smartphone and without having to open special apps. The driver must be able to activate the alarm right away, in a simple way easy to perform even when under stress.

Several additional options can be used, such as a man down© alarm (often referred to as an incapacitation alarm), which triggers an alert if the device senses that the user has suffered a slip, trip, fall, attack, health issue, or has become immobile for any other reason, and silent call function, which allows the AMC to activate the microphone of the device and listen to what is happening so that they can gather additional live data, which is extremely important during a security incident.

As these types of devices have their own battery, there is a need to implement a process to make sure the battery is charged, and maintenance is performed regularly.

Remote engine immobiliser

An extra security measure is the installation of an engine immobilizer that can be controlled remotely through the telematics system. Usually, this works by blocking the start of the engine and cannot be activated while the engine is running. This function can be activated when the vehicle is not moved for an extended period (e.g., driver long break).

Another option that can be linked with the engine immobilizer is driver identification (e.g., via ID tag, pin code, etc.), which prevents vehicle operation by unauthorized persons.

Backup batteries

The need for additional backup batteries is covered by TSR level 1, as the security system must have the necessary power to function even if the vehicle is stopped for long periods. The challenge of using batteries is that the charging capacity decreases over time. Therefore, regular maintenance and testing of the batteries within the system is very important.

A good practice is to install batteries that have a bigger capacity than the calculated consumption. In this way, the system will have a greater chance of working even if there is a decrease in battery capacity caused by wear over time.

Installation of the batteries should follow the same guidelines as for the tracking device and have a covert position, as disconnection of the battery in case of an attack would fail the tracking device.

Using one integrated monitoring solution

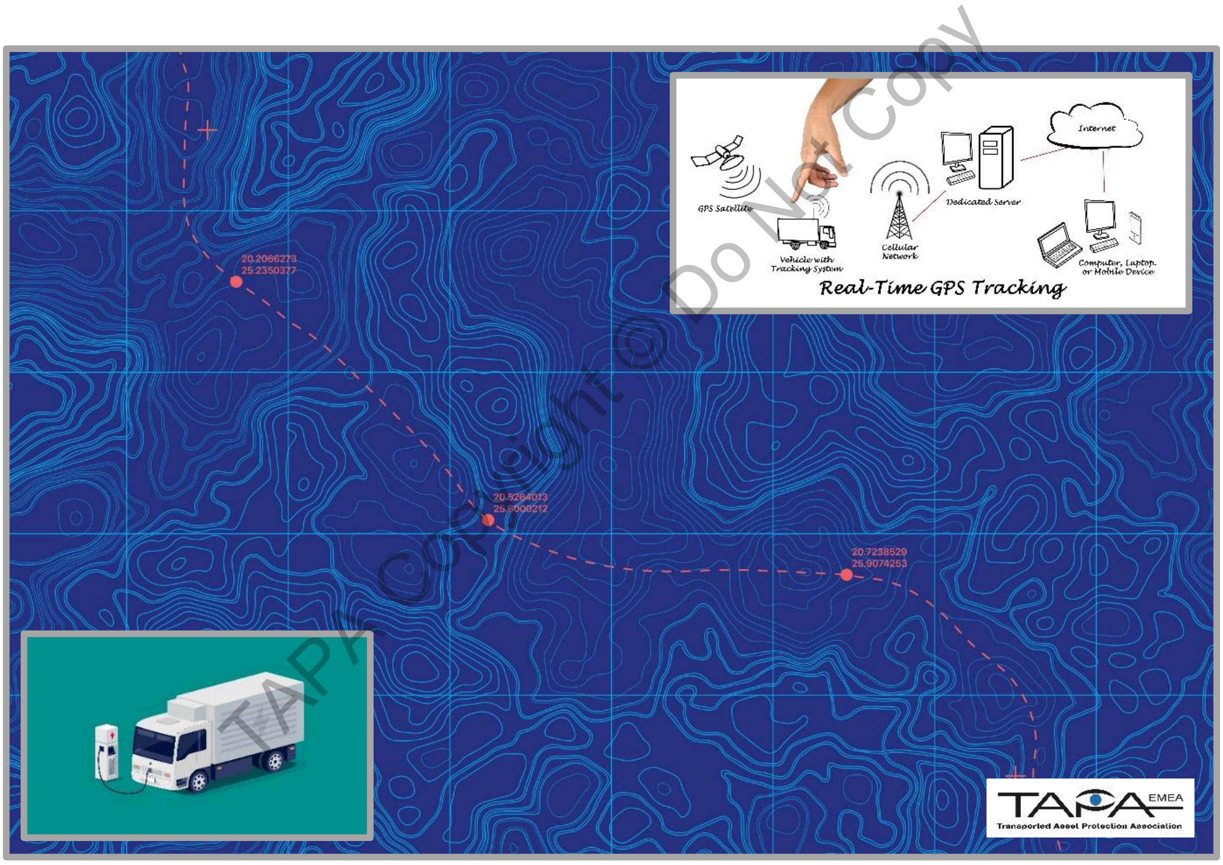
As the security system on a vehicle can have a high level of complexity, with various components and subsystems, there is a need to have a centralized solution where the monitoring center can have a clear overview of the status of the vehicles, receive the alarms and interact with/control the telematics security systems. Having all this under one solution provides the AMC operator with the best reaction time in case of an incident, when every delay is critical, and can further jeopardize the security of the driver and/or of the cargo.

Note that tracking and monitoring are two different operations: Tracking means that you know the status (i.e. location) of one of your assets (in this case a truck or a trailer), whereas Monitoring means that you know what the status of your asset should be, for example, its location, and you can compare it with the actual location provided by the tracking system (in our case), so you can be assured that your asset is where it was planned to be. Any deviation between the actual and the scheduled location/status of the monitored vehicle should raise an alarm.

Factory-ready TSR Certifiable vehicles (trucks, tractors, and trailers)

Lately, it has become very usual that truck and trailer manufacturers prepare their vehicles for certification directly from the factory. This way the retrofit installation works are avoided, facilitating both the warranty validity of the vehicles as well as damages that might occur both to the structure as well as to the vehicles' computer.

This latest trend takes place in both conventional trucks and tractors as well as electric-powered or hydrogen-powered trucks.



7.Special Topics

What is jamming - how “anti-jamming” tracking devices work

The telematics devices used commonly for vehicles’ tracking and monitoring use GPS and GSM to operate. The devices receive signals from GPS satellites to calculate their location on Earth (this is only reception) and then they use the GPS network to transmit these locations and other data to the related geolocation server (the tracking software). They can also receive signals from the tracking software, so the device–software communication is dual path, both reception and transmission.

The official definition of jamming in communications is that jamming in wireless networks is the disruption of existing wireless communications by decreasing the signal-to-noise ratio at the receiver sides through the transmission of interfering wireless signals. Since this definition does not mean anything to most of us, we could say that jamming is the intentional prevention of communication signals transmission and reception.

The technical concept that this is executed is that the jammer increases the electromagnetic noise at frequencies where the transmitted and received signals exist, therefore the actual communication signals are covered by this man-made noise and cannot make it through.

As happens with all wireless networks, both the GPS and GSM networks are vulnerable to interferences, a fact that is well known to and is being taken advantage of by criminals targeting supply chain operations worldwide. These man-made interferences can be performed by dedicated devices that are easily accessible on the market, also known as jammers, and which can typically operate in one (or more) of the three following modes:

- GSM Jamming: A GSM jammer is a device that blocks all transmission or reception signals, usually by creating interference at the same frequency ranges used by telecommunication providers. As a result, any SIM card (either in a phone or any other device) will either lose signal entirely or experience a significant and sometimes impairing loss of signal quality, therefore communication with the tracking software/server shall be impossible.

- GPS Jamming: In general, signal jamming occurs when there is an obstruction between the signal's transmitter and receiver. Particularly in the GPS network, jamming refers to masking satellite transmissions before any GPS receiver can locate and lock on them. The process is simple; the receiver's module that monitors the airwaves for satellite signals fails to receive any, even though the broadcasting from the source continues, resulting in its inability to determine a location.
- GPS Spoofing: Spoofing features an entirely different mentality compared to jamming. A device featuring GPS spoofing will attempt to deceive any GPS receiver by broadcasting counterfeit GPS signals, structured to resemble a set of normal ones, or by re-broadcasting genuine signals captured at a different location or at a different time.

Having described in short, the jamming principles and process, it looks like the tracking software/server is practically not able to identify whether a device stopped communicating with it due to device malfunction, loss of GSM network, or jamming. This is a task that modern tracking devices can accomplish, and it is a good point to clarify that there are no commercial GPS/GSM devices that are immune to jamming. What is available in the market are tracking devices with "jamming detection".

So, devices having "jamming detection" capabilities can recognize the characteristics of a jamming attack and even though they cannot communicate with the tracking software/server to report this attack, there are several actions that can be taken on the device side. For example, when a device identifies a jamming attack, it can activate one of its digital outputs and lock permanently the doors of the vehicle or start blinking a led inside the cabin to inform the driver that his truck is under jamming attack, and he must activate the related response protocol.

Another very important question about jammers is what is their effective range? Typically, a small, low-power GPS jammer might have a range of about 10 meters, while a more powerful jammer could disrupt GPS signals within a radius of several hundred meters. As far as GSM jammers are concerned their range depends on their power source and location. A jammer of different forms and sizes starting with the portable one can jam signals of about 10 to 15m range. It can go up to 1.5 km for the larger devices. Portable jammers can be carried in passenger vehicles, but as their range is not sufficient to block a long truck's devices (especially if there are two installed devices, for example, one in the cabin and one at the rear of the trailer), the attackers often use two or more passenger cars to attack the targeted truck. Strong jammers need adequate power 230Vdc to operate therefore they are usually stationary or in case they are carried on large tracks they should be professionally installed to get all the power they need to operate. Finally, keep in mind that jammers can block all mobile communications networks, including 3G, 4G, and 5G.

Just for completion of the information, for a device to be able to overpass GSM jamming, there should be an alternative communication channel (i.e. satellite communications[1]) which is quite rare in the COTS (commercial-of-the-shelf) tracking devices market.

What are the expected changes for telematics with the increased commissioning of electric trucks?

Based on recently published research studies (statista.com[2]) in 2022, electric trucks larger than six tons in the EU-27, Norway, Switzerland, and the UK numbered around four thousand units or 0.1 percent of the total trucking fleet in Europe. However, by 2030 the number of electric trucks larger than six tons is due to increase to approximately 562,000 units and 9.2 percent of total trucks in Europe. This marks an increase of 86 percent in the number of electric trucks over six tons in weight between 2022 and 2030. Only for reference, in 2021, Switzerland recorded the largest heavy-duty electric truck market in Europe, with around 77 vehicles. It was followed by Norway, at 56 heavy electric commercial vehicles.

Additionally, only 1.75% of German commercial vehicles currently have alternative drive systems. There are 68,312 battery-electric vehicles, 92 hydrogen fuel cell vehicles, and 517 plug-in hybrids.

[1] https://www.iridium.com/markets/autonomous-vehicles/
[2] https://www.statista.com/statistics/1313051/europe-heavy-electric-truck-market-volume-by-country/

The German government is aiming for one-third of commercial vehicle mileage to be electric or based on electricity-based fuels by 2030. The CO_2-based truck toll, which has been in force since December 2023, sends a price signal to promote alternative drive systems. The "KsNI-Richtlinie" supports this change with around 1 billion euros in funding. (The facts and figures are taken from the German DVZ article "The proportion of trucks with alternative drives is only 1.75 percent")[3].

As fleets transition to electric vehicles, the data captured by telematics is becoming more and more important. Information about driving and distance requirements can be used to determine which conventional vehicles are best suited for replacement with EVs.

After the transition to EVs has taken place, telematics systems are still important. They enable real-time monitoring of the state of charge, helping prevent potential issues like charger downtime or vehicles running out of charge. They also provide insights into energy usage patterns, helping to cut costs. Telematics data helps fleet managers to:

- Improve operations by:
  - optimize charging schedules,
  - ensure vehicle readiness,
  - maintain hardware uptime,
  - facilitate maintenance.
- Ensure the safety of drivers in case of hijacking or violent attacks and the security of the cargo/vehicle:
  - when in transit, and
  - during short and long breaks.

[3] https://www.dvz.de/politik/detail.html?tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Bnews_preview%5D=154245&cHash=cc10aeb42fff5715ed5149192aad71f4

Related to drivers' safety and cargo security, TAPA standards mandate the following equipment to be installed at a higher level of certification, including enhanced options:

- Tracking device(s) with a main and backup power source (battery)
- Fixed and/or portable panic button(s)
- Intrusion alarm systems in cabin and trailer
- Cargo compartment door sensors
- Electronic/electromechanical or manual rear door locks
- Cargo compartment lock-down system
- Cargo compartment alarm loops or integrated netting

Typical power consumptions of the above equipment are listed below:

- Any GPS tracker in working mode that is connected to a cellular network, computing live incoming GPS data and transmitting the data over a cellular network is going to be consuming between 60mA and 120mA of battery power depending on the tasks being performed by the CPU at the time. With no ignition on, engine running, or movement detected the device will go into a low power 'sleep mode' state of usually below 6mA (0.006Amps) of current consumption for a device that is hard-wired into a power supply and ready to enter live working mode at an instant. We need always to take into account when we program the operational mode of a tracking device that most of the time the GSM module must be kept always ON, for the device to be able to receive transmitted commands from the tracking software/server, otherwise we run the risk the device not to receive a command in real-time (i.e. change transmission frequency, or lockdown the rear doors, etc.), in case the GSM module is in sleep mode, and receives. It is only when it wakes up.

- Panic buttons are devices connected to the tracking devices, waiting to be used, therefore they do not consume any considerable power.

- Intrusion alarm consumption: vehicles' alarms are designed to consume very low power from the vehicle's battery. They typically draw less than 50 milliamps of current. Cabin alarms are usually armed when the driver is out of the vehicle (engine off) whereas the cargo compartment's alarm might be ON throughout the route.

- Electromechanical locks: power consumption varies from 10 to 70 milliamps, depending on the size, strength, and complexity.

- Alarm Loops and integrated netting: most of these devices are passive, therefore the power consumption is negligible.

- Cargo compartment door sensors: most of these sensors are passive magnetic contacts, therefore the power consumption is negligible.

The transition from conventional trucks to electric ones is not expected to create any disruption in the telematics technology for security purposes, as power shall be available to support all these devices both during transit as well as during parking since there is a trend that secure parking locations to be equipped also with chargers for these vehicles, therefore enough power shall be available also during rest times for the security systems to operate according to requirements.

8. Frequently Asked Questions (FAQs)

As TSR is a global Standard, the different network coverage and cost of telecommunication from one area to another has been taken into consideration while setting the requirements.

As telematics systems are fundamentally technology-driven, with today`s fast development of telecommunication standards and hardware, as well as more capable software solutions, there is a wide variety of solutions that can be used concerning the TSR.

This section seeks to provide comments on some of the questions TAPA receives on telematics systems.

Is 2G accepted as a communication method about TSR?

No, as of TSR 2020 - 2G is no longer a certifiable option. TAPA has excluded this method as it has been shut down or is in the process of being deprecated by network operators so that they can reclaim those radio bands and re-purpose them for newer technologies (e.g., 4G, 5G). Only 3G and above cellular networks are certifiable.

What exactly is meant by geofencing about TSR?

Using Global Positioning System (GPS) technology, tracking systems can accurately track a vehicle's position. Geofencing is an option that can be incorporated as a feature of the vehicle tracking system and can be created by the tracking system software program. The "geofence" is set up by an administrator who defines a geographical virtual perimeter or corridor for the vehicle and/or trailer. Geofencing allows the administrator to set up automatic alerts for a vehicle. The alerts could include route deviation outside of the geofence, unscheduled stops in or outside the geofence or reverse movement inside the geofence. Geofenced areas may also include the delivery/collection point/parking locations, trailer lock/unlock.

Why aren't mobile tracking devices allowed to be used on TSR 1 trucks?

TAPA does not exclude the use of mobile tracking devices, but the preference is for fixed installations because they provide the most confidence in the tracking system to meet the requirements during normal operations and in the event of an emergency.

The fixed or mobile tracking devices must be fit for purpose. Other associated requirements such as backup battery, fitting in a covert location (not under the seat), anti-tampering, reporting rate changes, related procedures, etc., all need to be compliant with the relevant sections of the Standard and cannot be waived or judged as not applicable due to the limitations of a mobile tracking solution.

For TSR1, can the battery of the vehicle be used as a backup battery for the tracking unit?

TSR 2023 does not forbid connecting the telematics system to the battery of the vehicle, but this does not comply with the requirements of the Standard. The battery of the tractor or trailer (e.g., in the case of a temperature-controlled trailer) is not a dedicated backup battery for the security system and can easily be disconnected in case of an attack. To comply with the Standard, the system must be equipped with a backup battery capable of maintaining the signaling capacity of the tracker for no less than 24 hours at a reporting rate of not less than one report every five minutes. The battery can be integrated in the tracking device or it can be installed additionally, but it must be dedicated to the tracking device.

Are mobile panic buttons mandatory for TSR1 and TSR2 and, if yes, do they need to be independent from the system on the vehicle?

The need of the mobile duress alarm and the device type is determined by the type of logistics operation the LSP is implementing. The requirement is there so that the driver can notify the LSP or the AMC in case he is faced with a threat while being out of the cab (e.g., comfort break, accident, emergency situation, etc.).

During the audit, the LSP must prove that the implemented process covers this type of risk by providing the driver with a mobile device or by having additional measures (e.g., using two drivers and only one driver being allowed to leave the cab at any given time).

To enhance the security of the driver, it is better to have multiple fixed panic devices present within the driver's reach, which are installed as inconspicuously as possible.

9. Useful Links

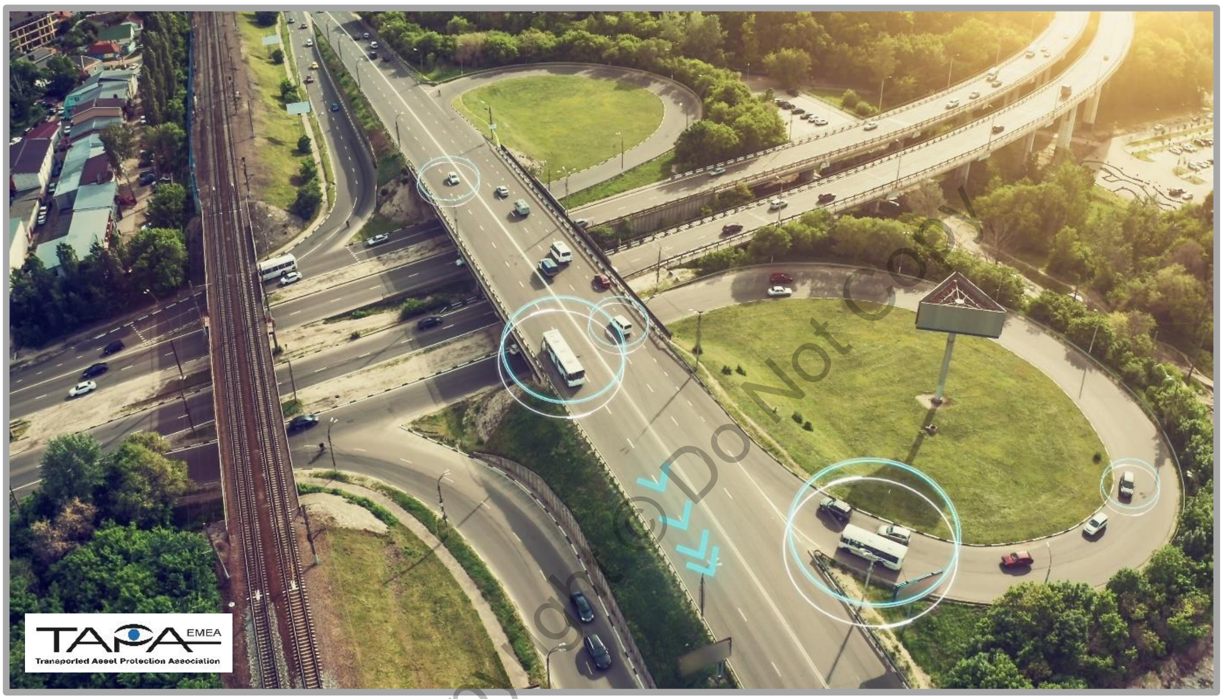
TAPA Members - Security Service Providers (telematics systems)

- http://www.autida.com
- https://en.g4stelematix.com/secure-supply-chain
- https://www.imbema.com/
- http://www.multiprotexion.com
- https://sensos.io/
- http://www.people-t.com/
- http://www.zf.com
- https://e-dentic.fr/

Information & background knowledge of the TSG

- BEIDOU http://en.beidou.gov.cn/
- GALILEO https://www.gsc-europa.eu/
- GLONASS www.glonass-iac.ru
- GPS www.navcen.uscg.gov
- QZSS www.qzs.jp/en/services/
- GPS World magazine https://www.gpsworld.com/
- EE|Times How does a GPS tracking system work? https://www.eetimes.com/how-does-a-gps-tracking-system-work/#
- R. Knippers Satellite-based positioning https://unstats.un.org/unsd/geoinfo/ungegn/docs/_data_ICAcourses/_HtmlModules/_Documents/D06/documents/D06-04_KnippersPPTeaching.pdf
- Comparison of wireless data standards https://en.wikipedia.org/wiki/Comparison_of_wireless_data_standards

- PCMag CDMA vs. GSM: What's the Difference? https://www.pcmag.com/news/cdma-vs-gsm-whats-the-difference
- ISO/TS 15143-3:2020 Telematics data https://www.iso.org/standard/76394.html



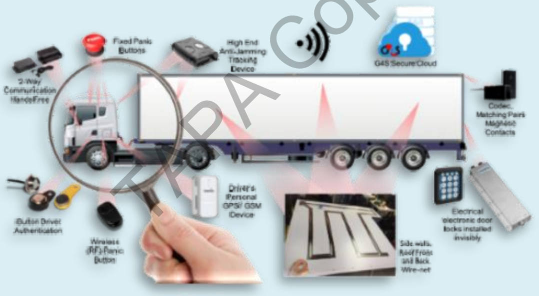
The following products, solutions, and mentioned Security Service Providers are only suggestions to assist in compliance with our TAPA TSR standards. It is important to note that TAPA assumes no responsibility for the incorrect selection, faulty installation, non-conformity, or non-fulfillment of the chosen telematics solution concerning the TSR levels. Additionally, TAPA does not guide which telematics solution would be preferable for each TSR security level. The following data and information are based on descriptions and visual material provided by TAPA Security Service Providers. The appropriate telematics solution, associated installation, and respective vehicle type are to be agreed upon between the user and the supplier. TAPA acts solely as a supporter and facilitator in the selection of the designated telematics solution.

10. Appendix A: Telematics Systems Examples

10.1. Vehicle Tracking Systems

Ref VTS	Product	Description
VTS-01	SCALAR EVO Touch	ZF's truck connectivity device for security and high-value cargo provides track & trace, navigation, routing, and integrated anti-start function. Product number 551 010 0xx 0.
		ZF http://www.zf.com/
VTS-02	SBS Telematic System, powered by Tcomm	The trailer tracking software which combines all relevant trailer tracking data like location, EBS data, temperature, TPMS, etc. With this software, you also can set alarms, block the lock remotely, change the method of unlocking, or set up geofencing.
		imbema http://www.imbema.com
VTS-03	SBS Universal telematic solution	Rugged European-produced tracking device with real-time onboard geofencing and multiple digital and analogue inputs and 24-hour backup battery.

		imbema http://www.imbema.com
VTS-04	ALTAIR AJ EVO	MAXIMUM SECURITY - TELEMATIC ESCORTS.
		MULTIPROTEXION http://www.multiprotexion.com
VTS-05	SIRIO TST	HIGH SECURITY - SECURITY TRIP / CORRIDORING.
		MULTIPROTEXION http://www.multiprotexion.com
VTS-06	ANTARES TSR 1 ALL IN ONE	HIGH SECURITY - SECURITY TRIP / CORRIDORING.
		MULTIPROTEXION http://www.multiprotexion.com

VTS-07	Double L 4.1	Portable or Permanent Multi-use real-time monitoring device.
		http://www.people-t.com/
VTS-08	Double L 5.0	Portable or Permanent Multi-use real-time monitoring device.
		http://www.people-t.com/
VTS-09	G4S TLMX - VTS TSR1	Installed tracking device and tracking platform with alert functionalities.
	 Fixed Panic Buttons High End Anti-Jamming Tracking Device G4S Secure Cloud 2-Way Communication HandsFree Codec Matching Pairs Magnetic Contacts iButton Driver Authentication Wireless (RF) Panic Button Driver's Personal GPS/ GSM Device Electrical electronic door locks installed invisibly Side walls, Roof Front and Back Wire-net	G4S Telematix https://en.g4stelematix.com/secure-supply-chain
VTS-10	G4S TLMX - VTS TSR1+	Top-of-the-line installed tracking device and tracking platform with alert functionalities.
		G4S Telematix https://en.g4stelematix.com/secure-fleet

10.2. Cargo / Asset Tracking System

Ref CATS	Product	Description
CATS-01	SCALAR EVO Guard	ZF's trailer connectivity device for security and high-value cargo, reefer connectivity, and EBS. Product number 554 090 0x1 0.
		http://www.zf.com/
CATS-02	SBS E-Container lock	The mobile e-container lock secures the doors of your container against burglary and monitors the cargo in real time.
		http://www.imbema.com
CATS-03	SBS Asset tracking system	Trace all your material such as trailer, container, or pallet truck. The hardened device continues to work under the toughest conditions.
		http://www.imbema.com

CATS-04	SBS Advanced asset tracking system	Trace all your material such as trailer, container, or pallet truck. The hardened device continues to work under the toughest conditions.
		imbema http://www.imbema.com000
CATS-05	SBS Live track & trace system	Low maintenance, no battery but supercapacitors, tracking system with which you can follow equipment such as trailers.
		imbema http://www.imbema.com
CATS-06	SPY BOX	Self-powered GPS unit, rechargeable battery. Ready to be installed on any type of vehicle (specialized technician not required).
		MULTIPROTEXION http://www.multiprotexion.com
CATS-07	SIM-LESS SPY BOX	Self-powered GPS unit, long-life battery replaceable. Ready to be installed on any type of vehicle using supplied magnets or screws.
		MULTIPROTEXION http://www.multiprotexion.com

CATS-08	Flex 4.1	Portable Multi or Single-use real-time monitoring device, for cargo and assets.
		http://www.people-t.com/
CATS-09	Flex 5.0	Portable Multi or Single-use real-time monitoring device, for cargo and asset.
		http://www.people-t.com/
CATS-10	Sensos Cellular Label	The first disposable, globally connected cellular label that provides accurate, real-time location tracking and conditioning monitoring.
		SENSOS https://sensos.io/

CATS-11	Epyo	Track every parcel, pallet, goods, and process: reduce by 80% losses and claims. Scan every label with cameras automatically. Our Milestone open platform solution allows to use of any CCTV hardware, we do can retrofit.
	EXPLORE MILESTONE MARKETPLACE Technology Browse by technology START BROWSING XProtect Add functionality, add value	e-dentic https://e-dentic.fr/
CATS-12	Cooler-Guard	Cyber-secured, keyless lock system and platform, manual locking/automatic locking. No batteries, -power supply or -cables in doors. Integrated sensors, indication in truck cockpit. Integration to other systems enabled and supported. The operating temperature is -30 degrees to +65 degrees. Audit trail, lock status with GPS.
		AUTIDA http://www.autida.com/

10.3. Personal Tracking Systems

Ref PTS	Product	Description
PTS-01	SOS MATIX	SOS Matix, the portable panic button that keeps drivers safe.
	KEEP SAFE SOS MATIX WITH A BUTTON FleetUp App Store Google Play Download the App and see the localization The new safety button and locator for drivers TAPA PREMIER PARTNERS MULTIPROTEXION	MULTIPROTEXION http://www.multiprotexion.com

PTS-02	**G4S TLMX - VTS TSR1+**	**Personal tracking device and platform with live tracking and several alert scenarios.**
	Panic Button Routing to the scene of the incident Fall Detection 5 speed dial contacts	G4S Telematix https://en.g4stelematix.com/g4s-withu-pro
PTS-03	**G4S TLMX - VTS TSR1+**	**Mobile app and platform for the protection of lone workers.**
		G4S Telematix https://en.g4stelematix.com/g4s-withu-pro

Publishing and copyright information

The TAPA EMEA copyright notice displayed in this document indicates when the document was last issued.

Publication history

First published in April 2022.

The first (present) edition was published in March 2024.