TAPA TSR

Telematics Systems Guidance V1

A TAPA Trucking Security Requirements Guidance Document for users of TAPA Standards

TAPA EMEA COPYRIGHT© DO NOT COPY

www.tapaemea.org

TAPA EMEA
Pastoor Ohllaan 39
3451 CB Vleuten
The Netherlands

info@tapaemea.org
Tel. +31 19573461

TAPA does not represent nor warrants that the information contained in this document will prevent any loss, damage or injury to a person or property, by reason 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.

© TAPA EMEA 2022

CONTENTS

1.	Introduction	3
2.	About TAPA.....	4
3.	What is Telematics	6
4.	Requirements and Associated Risks	9
5.	TSR overview related to telematics	14
6.	Telematics systems for security use	21
7.	Frequently Asked Questions (FAQ)	30
8.	Useful links.....	32
9.	Appendix A	33

TAPA EMEA COPYRIGHT© DO NOT COPY

© TAPA EMEA 2022

1. Introduction

TAPA has produced this Telematics Systems Guidance (TSG) to provide helpfully 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 cargoes; 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.

TAPA EMEA COPYRIGHT © DO NOT COPY

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.

© TAPA EMEA 2022

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 EMEA COPYRIGHT PROTECTED DOCUMENT COPY

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 2022

TAPA EMEA COPYRIGHT© DO NOT COPY

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.

© TAPA EMEA 2022

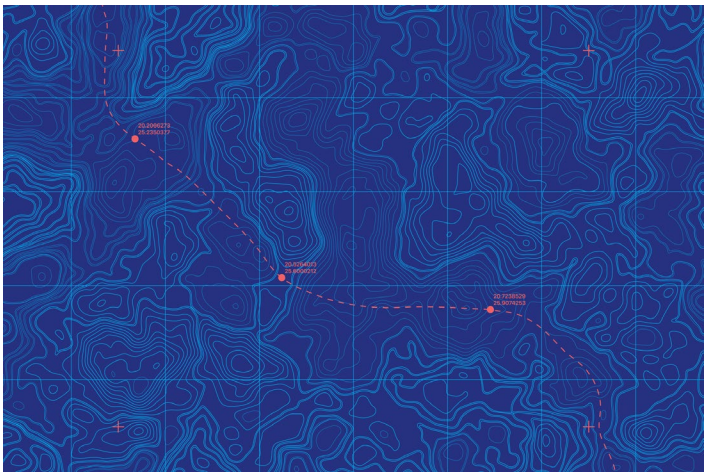
3. What is Telematics

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 between 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, 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 analyse 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.

TAPA EMEA COPYRIGHT© DO NOT COPY



© TAPA EMEA 2022

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

Vehicle tracking means to have the information about the location, status and behaviour 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*.

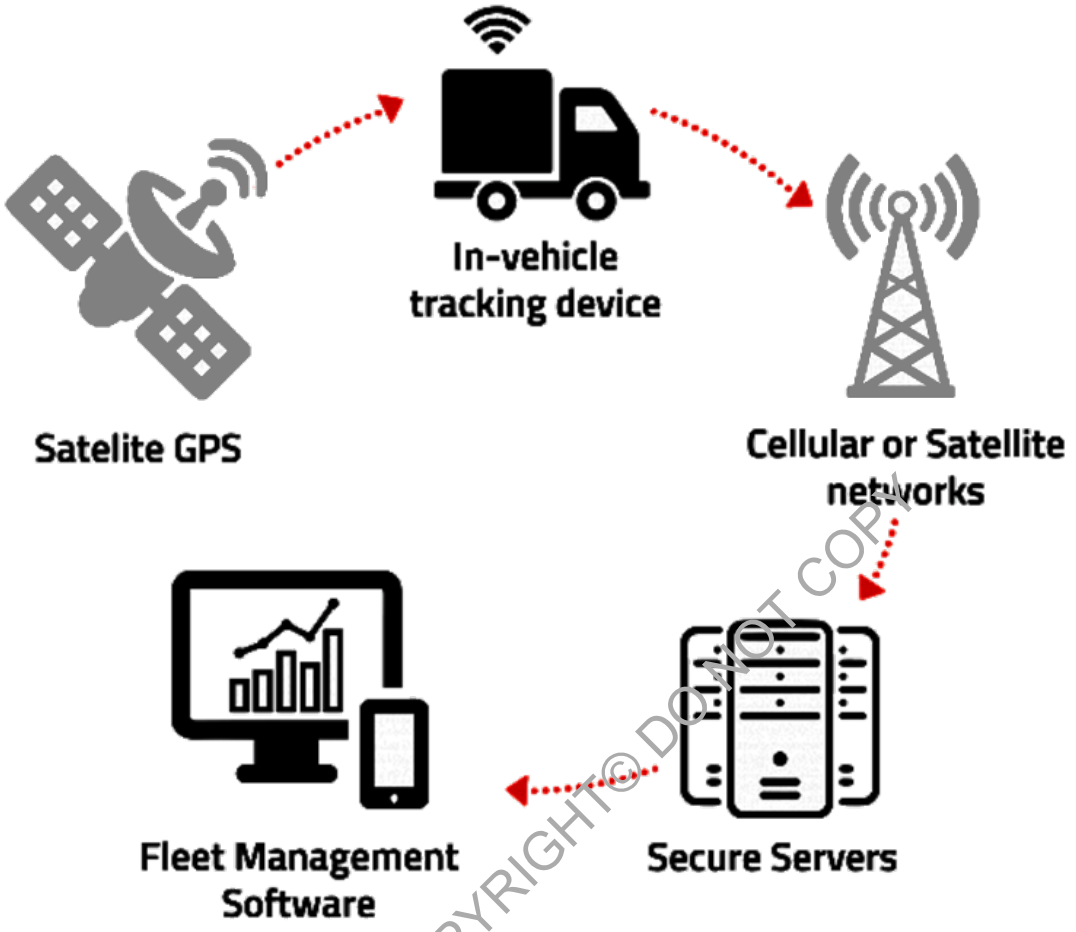
Passive devices store GPS location, speed, heading and sometimes a trigger event such as key on/off, door open/closed, etc. Once the vehicle returns to a predetermined point, the device is removed and the data is downloaded to a computer for evaluation. Passive systems can include auto-download type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

TAPA EMEA COPYRIGHT© DO NOT COPY

© TAPA EMEA 2022



(Typical fleet telematics setup)

TAPA EMEA COPYRIGHT© DO NOT COPY

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.

© TAPA EMEA 2022

4. Requirements and Associated Risks

In this chapter we will focus on the requirements of TAPA TSR 2020 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.

Documented tracking protocols

Why?

Detailed and documented protocols are a very good method to ensure effectiveness (that the response protocols actually 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 shall 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.

TAPA EMEA COPYRIGHT© DO NOT COPY

Tracking and tracing devices

Why?

Tracking devices are the components that collect and transmit all signals from the vehicle to the monitoring centre (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 in order 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 in order 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 centre losing contact and not being able to track and monitor the cargo.

Associated Risk(s):

As 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 criminals' attack, due either to identification and damage of the tracking device/antenna or executing a jamming attack.

TAPA EMEA COPYRIGHT© DO NOT COPY

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 unauthorised opening of the cargo compartment door might indicate the initiation of a security incident.

© TAPA EMEA 2022

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 centre, 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.).

TAPA EMEA COPYRIGHT© DO NOT COPY

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 centre 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 centre 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 presethe rve battery, so the recovery team has more time to locate the stolen vehicle or, alternatively, 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 are able to follow the vehicle in real-time.

© TAPA EMEA 2022

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 centre 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):
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?
It is very important that the AMC knows 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.

TAPA EMEA COPYRIGHT© DO NOT COPY

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 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 caused these deviations.

TAPA EMEA COPYRIGHT© DO NOT COPY

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 transports as well.
Associated Risk(s):
Tracking with monitoring always enhances the security of the transported cargo, especially in the rail terminals where a lot of criminal activity takes place.

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.

5. TSR overview related to telematics

TAPA EMEA COPYRIGHT© DO NOT COPY

Implementation of TAPA TSR 2020 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 2020 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

© TAPA EMEA 2022

TSR 2020 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
		✓	✓	✓	✓	✓	✓

In order to comply with the requirements, the vehicle must be equipped with:

a) An installed tracking device providing remotely stored archival information relating to the position of all FTL Supplier/Buyer dedicated trucks. Location and time stamp when vehicle stops and moves;

Usually, the tracking device does not communicate the position of the truck and the data is downloaded after the transport has finished. For articulated vehicles, the tracker can be installed either in the tractor or the trailer. The data collected helps the shipper and the LSP to check whether the planned route and stops have been respected. Most fleet telematics systems provide more functionalities than the ones listed above and can be successfully used for certification.

b) 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 in order to provide assistance to 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.

TAPA EMEA COPYRIGHT© DO NOT COPY

TSR 2020 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 signalling 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 case of 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) in order to provide the necessary positioning and communication to locate the vehicle.

TAPA EMEA COPYRIGHT© DO NOT COPY

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 signalling 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.

© TAPA EMEA 2022

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 in close proximity to 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 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 which ensures that the device has the necessary range for the driver to use in case of an emergency.

TAPA EMEA COPYRIGHT© DO NOT COPY

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.

© TAPA EMEA 2022

TSR 2020 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 signalling 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 in order to assist in case of a security incident (e.g., decrease it to save battery or increase it for live monitoring).

Also, in the event that 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.

TAPA EMEA COPYRIGHT© DO NOT COPY

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 – vehicle is not moving for a defined amount of time (as determined by the operation, routing and associated risks) or engine shut down;
3. Tracker battery status – level of the battery charge, usually reported in percentage;

© TAPA EMEA 2022

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 in order 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 device or attached antennas, jamming, etc.). The generated alert must be sent to the AMC.

TAPA EMEA COPYRIGHT© DO NOT COPY

b) The vehicle tracking devices must be equipped with a battery back-up capable of maintaining the signalling 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 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 in the tracking device or in an external power pack. However, the installation (equipment and wiring) should be covert in order to prevert tampering with the power supply in case of an attack.

 © TAPA EMEA 2022

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

TAPA EMEA COPYRIGHT© DO NOT COPY

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 for enabling 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 about the status of the vehicle and the load.

TAPA EMEA COPYRIGHT© DO NOT COPY

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

In order 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, status of the integrity of the tracking device and connected sensors, and the status of specific *security signals* that contribute to ensure driver and cargo protection.

© TAPA EMEA 2022

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.

TAPA EMEA COPYRIGHT© DO NOT COPY

A short synthesis of the main components of the security telematics are:
Tracking kit: devices fitted onto the vehicle that capture the positioning information, including other data acquired from special/dedicated sensors or electrical components (part of the GPS kit), and that sends 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 in order 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 enable 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.

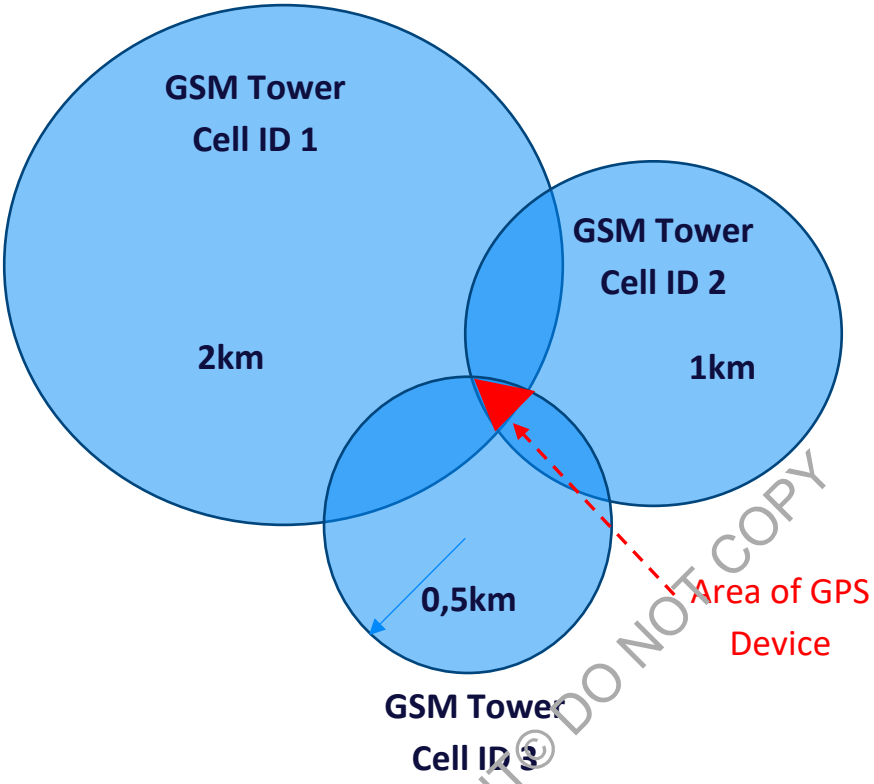
Network Coverage

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 localisation. 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 localisation 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).

TAPA EMEA COPYRIGHT© DO NOT COPY



TAPA EMEA COPYRIGHT© DO NOT COPY

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 which 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.

© TAPA EMEA 2022

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

TAPA EMEA COPYRIGHT© DO NOT COPY

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 attack, Driving Behaviour analysis.
Fixed Panic Button	Wired button 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.

© TAPA EMEA 2022

Component	Short description
Driver Authentication	System designed to recognize / authenticate the driver (e.g., reader and tag, code entered via keypad). Could be installed in combination with immobilizer to prevent ignition-on by unauthorized drivers.
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	Cabin alarm 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 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, 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.
Telematics Platform	Tracking platform decoding all telematics messages.

TAPA EMEA COPYRIGHT© DO NOT COPY

© TAPA EMEA 2022

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 in order 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 in order to reduce the chance that both are silenced by a jamming attack.

TAPA EMEA COPYRIGHT © DO NOT COPY

Covert installation

One of the first things that an organised 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 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 in order 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).

© TAPA EMEA 2022

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, it is important that all the parts are compatible and work together under all the possible conditions that the vehicle might encounter.

Driver personal tracker

In order 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 (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 in order to provide assistance.

There are a number of additional options that 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.

TAPA EMEA COPYRIGHT© DO NOT COPY

Remote engine immobiliser

An extra security measure is the installation of an engine immobiliser 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 immobiliser is driver identification (e.g., via ID tag, pin code, etc.), which prevents vehicle operation by unauthorised 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 result in a failure of the tracking device.

TAPA EMEA COPYRIGHT© DO NOT COPY

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 centralised 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 jeopardise the security of the driver and/or of the cargo.

© TAPA EMEA 2022

7. Frequently Asked Questions (FAQ)

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 in relation to the TSR.

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

TAPA EMEA COPYRIGHT© DO NOT COPY

Is 2G accepted as a communication method in relation to 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 in relation to 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 setup 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.

© TAPA EMEA 2022

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 to 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 2020 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 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. In order to comply with the Standard, the system must be equipped with a backup battery capable of maintaining the signalling 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.

TAPA EMEA COPYRIGHT© DO NOT COPY

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).

© TAPA EMEA 2022

In order 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.

8. Useful links

TAPA Members - Security Service Providers (telematics systems)

- http://www.autida.com
- https://www.g4stelematix.com/
- https://www.imbema.com/
- http://www.multiprotexion.com
- http://www.tecnicasdeingenieria.com
- http://www.viasatsystems.ro
- http://ww.waynet.it
- http://www.zf.com

TAPA EMEA COPYRIGHT© DO NOT COPY

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

© TAPA EMEA 2022

9. Appendix A

Telematics System Examples

9.1. Vehicle Tracking Systems

Ref VTS	Product	Description
VTS -01	ANTARES TSR 1 ALL IN ONE	HIGH SECURITY - SECURITY TRIP / CORRIDORING
		Multiprotexion Srl http://www.multiprotexion.com
VTS -02	SIRIO TST	HIGH SECURITY - SECURITY TRIP / CORRIDORING
		Multiprotexion Srl http://www.multiprotexion.com
VTS -03	ALTAIR AJ EVO	MAXIMUM SECURITY - TELEMATIC ESCORTS
		Multiprotexion Srl http://www.multiprotexion.com

TAPA EMEA COPYRIGHT© DO NOT COPY

© TAPA EMEA 2022

VTS -04	HEAVY WAY Security	Fleet Management Solution with focus on High Level Security
		W.A.Y. S.r.l. http://www.waynet.it/
VTS -05	G4S TLMX - VTS TSR1	Installed tracking device and tracking platform with alert functionalities
		G4S Telematix S.A. https://www.g4stelematix.com/
VTS -06	G4S TLMX - VTS TSR1+	Top of the line installed tracking device and tracking platform with alert functionalities
		G4S Telematix S.A. https://www.g4stelematix.com/
VTS -07	TX-TRAILERPULSE	TX-TRAILERPULSE helps you make smart decisions to manage and improve the daily utilization of your trailers.
		ZF Group – CVCS http://www.zf.com

TAPA EMEA COPYRIGHT© DO NOT COPY

© TAPA EMEA 2022

VTS -08	**TX-TRAILERGUARD**	**TX-TRAILERGUARD helps you optimize the security for your cargo & trailers and improve safety standards on the road.**
		ZF Group – CVCS http://www.zf.com
VTS -09	**TX-GO**	**Truck-independent on-board computer without a display, TX GO is designed for installation behind the dashboard enabling real-time fleet follow-up.**
		ZF Group – CVCS http://www.zf.com
VTS -10	**TX-SKY**	**Fixed mounted on-board computer with touchscreen, TX-SKY registers all driver and truck information and data from other sources.**
		ZF Group – CVCS http://www.zf.com
VTS -11	**Runtracker 6.x**	**Runtracker 6.x records coordinates instantly as well as other data from the vehicle. All the information transmitted is accessible through the web application.**
		VIASAT SYSTEMS http://www.viasatsystems.ro

TAPA EMEA COPYRIGHT© DO NOT COPY

VTS -12	Gesinflot	Telematic Solution for Trucks and Semitrailers.
	TDI Técnicas de Ingeniería SL http://www.tecnicasdeingenieria.com 	
VTS -13	SBS Universal telematic solution	Rugged European produced tracking device with real-time onboard geofencing and multiple digital and analogue inputs and 24 hours backup battery.
	SBS Security & Safety Products BV http://www.imbema.com 	

TAPA EMEA COPYRIGHT© DO NOT COPY

9.2. Cargo / Asset Tracking Systems

Ref CATS	Product	Description
CATS - 01	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. Operating temperature is -30 degrees to +65 degrees. Audit trail, lock status with GPS.
	Autida AB, Stockholm, Sweden http://www.autida.com 	

© TAPA EMEA 2022

CATS - 02	SBS Asset tracking system	Trace all your assets such as trailer, container or pallet truck. The hardened device continues to work under the toughest conditions.
		SBS Security & Safety Products BV https://www.imbema.com/
CATS - 03	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.
		SBS Security & Safety Products BV https://www.imbema.com/
CATS - 04	SBS Live track & trace system	Low maintenance, no battery but supercapacitors, tracking system with which you can follow equipment such as trailers.
		SBS Security & Safety Products BV https://www.imbema.com/

TAPA ONLY COPYRIGHT© DO NOT COPY

9.3. Personal Tracking Systems

Ref PTS	Product	Description
PTS -01	SOS MATIX	SOS Matix, the portable panic button that keeps drivers safe.
		Multiprotexion Srl http://www.multiprotexion.com

© TAPA EMEA 2022

PTS -02	**Smartphone app**	**A personal tracking system, with panic button and silent call features. All information transmitted is accessible through the web application.**
	Viasat Systems http://www.viasatsystems.ro	
PTS -03	**Watch**	**A personal tracking system, with panic button and silent call features. All information transmitted is accessible through the web application.**
	Viasat Systems http://www.viasatsystems.ro	
PTS -04	**G4S TLMX - PERSONAL**	**Personal tracking device and platform with live tracking and a number of alert scenarios.**
	G4S Telematix S.A. https://www.g4stelematix.com/ 	
PTS -05	**G4S TLMX - MOBILE**	**Mobile app and platform for the protection of lone workers.**
	G4S Telematix S.A. https://www.g4stelematix.com/ 	

TAPA EMEA COPYRIGHT© DO NOT COPY