SECUR-ED

SECured URban transportation - European Demonstration

D21.1 Public transport security terminology & definitions

Document identification	
Related SP / WP	SP 2 / WP 21
Related Deliverable	
Lead Participant	Joint Research Centre (JRC)
Contributors	MTRS3

Reference	SCR-WP21-D-JRC-006
Dissemination Level	PU
Lead Author	Fivos Andritsos - JRC Gilad Rafaeli, Paul Abbott
Reviewers	RAILPOL THALES

This document is issued in the frame and for the purpose of SECUR-ED project. This project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261605.

History

NB: a **status** is associated to each step of the document lifecycle:
- Draft: this version is under development by one or several partner(s);
- **Under review:** this version has been sent for review;
- **Issued**: this version of the document has been submitted to EC.

Version	Status	Date	Author	Main Changes
0.1	Draft	06.09.2011	JRC	Update consistent with SECUR-ED document template (visual identity) Add of the full explanation of the use of the word "interoperability"
1.0	Draft	08.09.2011	JRC	Update of definitions following the WP 21 meeting of September 01 2011 in Brussels
2.0	Draft	08.09.2011	JRC	Draft Updated
3.0	Draft	12.09.2011	JRC	Draft Updated
4.0	Under review	04.10.2011	JRC	Version sent to peer reviewer 1&2
5.0	Under review	13.10.2011	JRC	Reviewed version
6.0	Under review	11.11.2011	JRC	Update with additional definitions
7.0	Under review	11.11.2011	JRC	Version sent to Thales for final validation
8.0	Issued	14.11.2011	THA	Version submitted to EC

TABLE OF CONTENTS

1 Abstract & Purpose

1.1 Abstract

This document has been prepared following a systemic overview of public mass transport security sources to identify and document a common set of security terminology, definitions and acronyms for use throughout the SECUR-ED project.

This document is intended to be a *living* document, i.e. be continuously updated according the needs and circumstances throughout the project's life.

1.2 Purpose of the document

This document provides a common set of terms and definitions for use in the execution of the tasks comprising the SECUR-ED project.

It is divided into three sections, according to the expected classes of readers / users of the document:

- Security and safety risk management definitions
- Information & communication technologies definitions
- Public transport definitions

2 References

2.1 List of acronyms

APTA	American Public Transportation Association
COUNTERACT	Cluster Of User Networks in Transport and Energy Relating to Antiterrorist ACTivities
DG	Directorate General (European Commission)
DIN	Deutsches Institut für Normung
EC	European Commission
ETSI	European Telecommunications Standards Institute
EU	European Union
FP	Framework Programme (EC research)
FTA	Federal Transit Administration
ICT	Information & Communication Technologies
IPR	Intellectual Property Rights
ISECOM	Institute for Security and Open Methodologies
ISO	International Standards Organisation
JRC	Joint Research Centre
LAN	Local Area Network
MODSafe	Modular Urban Transport Safety and Security Analysis
QA	Quality Assurance
QC	Quality Control
R&D	Research and Development
RFID	Radio Frequency Identification
RTD	Research & Technological Development
SECUR-ED	Secured Urban Transportation – European Demonstration
SoA	State of the Art
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WP	Work Package

2.2 Referenced documents

The following documents are referenced:

R[1] COUNTERACT / PT5 - Public transport security planning - organisation, countermeasures & operations guidance. Available at http://www.uitp.org/knowledge/projects-details.cfm?id=433

R[2] TETRA Association, www.tetra-association.com

R[3] Transit agency security and emergency management protective measures, Federal Transit Administration (FTA), November 2006

R[4] Transit Security Design Considerations, Federal Transit Administration (FTA), November 2004

R[5] Technical Recommended Practice for the Selection of Cameras, Digital Recording Systems, Digital High-Speed Networks and Train-lines for Use in New Transit-Related CCTV Systems, APTA Technical Standards document, August 2008

R[6] MODSafe Modular Urban Transport Safety and Security Analysis, Deliverable No. D 9.1 - Hazard scenarios related to security aspects

R[7] Institute for Security & Open Methodologies www.isecom.org

R[8] Physical Security Information Management www.psimtrends.com

R[9] Institute of Electrical and Electronics Engineers. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY: 1990

R[10] An introduction to video content analysis industry guide, British Security Industry Association, June 2009

R[11] Railway industry website www.railway-technology.com

R[12] US 49 CFR Parts 1500, 1520, 1540, 1552, 1572

R[13] ISO 31000, Risk Management Standard

3 Security and Safety Management Terms and Definitions

Access Control	A system of technical means, personnel and procedures, which enables an organisation to control access to areas and resources in a given physical facility or computer-based information system. It has 3 essential functions: entitlement check, identification and documentation of the persons entering a certain controlled access area.
Accident	A specific, unpredictable, unusual and unintended incident, which occurs in a particular time and place with no immediately apparent and deliberate cause but with marked effects and, generally, negative outcome. See also *Incident*.
Actor	Any person or group of persons who interacts with a system / procedure, in the particular case of a public transport system.
Asset	Any person, part or feature of a system that has a value such as physical assets, human assets, soft assets (i.e., knowledge, experience) and information assets.
Best Practice	Any method or technique that has consistently shown results superior than when using other means, and which can be used as a benchmark to strive for.
CBRN devices	Devices of Chemical, Biological, Radiological, Nuclear nature, which may require special response like post-incident decontamination of people and/or assets. In particular: • **Chemical:** dispersion of toxic chemical agents or toxic industrial materials (TIM) by non-military means, many with little or no clearly evident characteristics. Symptoms (e.g., passengers collapsing) may the first indication of an attack. • **Biological:** dispersion of disease-causing living organisms or replicating entities (viruses) that reproduce or replicate within their host victims and used to kill or incapacitate humans, animals or plants • **Radiological:** radioactive and/or radio-toxic material spread, usually through the detonation of conventional explosives, in the form of an IED or VBIED – as a 'dirty bomb'. • **Nuclear:** device aiming at a nuclear explosion and the consequent thermal and radiation effects; a weapon of mass destruction potentially requiring a national or multinational level response.
Chief Security Officer (CSO) / Security Officer / Corporate Security Manager	An individual responsible for the overall security management and preparedness of a public transport operator / infrastructure manager (PTO/IM) whose functions are usually identified in a security plan.

Communication Protocol	A defined communication format and set of rules containing the control procedures required for data transfer across the link interfaces and to / from the user's application programs, also including the timing, sequencing and error control of the exchanged data.
Crime	Any act or commission of an act that is forbidden, or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment.
Crime Prevention Through Environmental Design	A multi-disciplinary approach to limit the opportunities for crime by focusing on design and the creation of an environment not tolerating crime.
Crisis	A situation, derived from natural or man-made causes, which has the potential to compromise the safety (physical, economic, environmental etc.) of an individual, a group, a community or the whole society. A crisis usually triggers particular modes of governance, typically described with the terms crisis (or emergency) management (or response).
Crisis Management Group	A group convened when a crisis occurs to provide strategic decision making and co-ordination both within the organisation and with relevant external organisations e.g. police and government agencies.
Critical Asset	An asset (human or material) the loss, denial or damage of which would substantially compromise the main functions of the system / organisation.
Cyber Attack	Damage, unauthorized use, exploitation or destruction of electronic information by means such as viruses, worms, Trojan horses, phishing, denial of service (DoS) attacks, unauthorized access and control system attacks**.**
Cyber Security	All means for protection against cyber-attacks, e.g. firewalls, anti-virus SW, intrusion detection and prevention systems, encryption etc.
Deflagration	The act of triggering/igniting substances that result to processes slower than an explosion, i.e. they do not result to shock waves.
Design Basis Threat (DBT)	A set of assumptions regarding threats (number of adversaries, their modus operandi, the type of tools and weapons etc.), against which security systems / measures should be planned, designed and implemented.
Detonation	The act of setting up (triggering) and explosion; very rapid ignition of explosives resulting to explosion (shock waves).
Emergency	An unforeseen or unplanned situation that has implications for the safety of persons and for assets and requires immediate attention.
Emergency Operating Procedure (EOP)	A pre-planned documented arrangement for managing or executing a set of actions in an emergency situation to ensure the safety of the people and a pre-identified level of operations and/or services.

Emergency Services / First Responders	The fire, police or ambulance services where an incident occurs. In the context of SECUR-ED, this excludes any PTO/IM's internal security forces.
Entitlement	Evidence of the right to benefit a service or access an area, typically a ticket, a travel or access card or an entrance permit.
Explosive Ordnance Disposal (EOD)	Actions performed by specialists to neutralise devices such as IEDs, IIDs or VBIEDs (see below).
Explosion	A sudden release of energy in an extreme manner, usually resulting in the generation of high temperatures and release of gases leading to rapid increase in volume and shock (i.e. supersonic) waves. Explosions can involve reaction with oxygen (combustion) or not (decomposition). See also: detonation and deflagration.
Explosive	Material which, when ignited, produces an explosion. Materials capable of producing shock (supersonic) waves are usually called high explosives.
Explosive component	Non-explosive material that, if combined/mixed to another material can produce an explosive material.
Explosive device	Device, comprising explosive (or explosive components) and a detonator, designed to cause an explosion. Explosive devices include military ordnance, civil and industrial devices as well as improvised devices (IED) meant to be used for terrorist or criminal acts.
Forensics	The application of scientific knowledge to legal problems; scientific analysis of physical evidence (as from a crime scene).
Formal Safety Assessment (FSA)	A systematic process for assessing the risks associated with a system, procedure activity and for evaluating the costs and benefits of various possible options for reducing these risks.
Functional Requirements	A set of functionalities needed and / or expected from a product or a service under development or procurement. Alternatively referred to as 'user requirements'.
Functional Specification	The breakdown, quantification and association of the system's functional requirements to the main system's functional components.
Functionality	The ability to perform a certain function; function is an action or use for which something is suited or designed.
Guideline	A non-specific rule or principle that provides direction to action or behaviour; a plan or explanation in setting standards or determining a course of action; any document that aims to streamline particular processes according to certain rules and/or aims to achieve set objectives. Guidelines are adhered to voluntarily and are never mandatory.

Hazard	A situation that can be a source / cause of harm to life, health, property, or environment; hazards are normally dormant, i.e. they represent a potential harm; a hazard can materialise through an incident (active hazard) that actually causes harm.
Hazardous Materials (HAZMAT)	Solids, liquids, or gases that can harm people, other living organisms, property, or the environment, including materials that are radioactive, flammable, explosive, corrosive, oxidizing, asphyxiating, bio-hazardous, toxic, pathogenic, or allergenic. They are grouped by class, e.g., Class 1 Explosives, and identified by a United Nations number, e.g., 1005 Anhydrous Ammonia.
HAZMAT Team	Personnel specially trained to handle hazardous materials.
Hijack	The act of taking control of a vehicle (at land, sea or air) for terrorist or criminal purposes. The use of the term hijack has been extended to the virtual world (hijack a computer system, hijack someone's identity etc.)
Identification	Evidence of identity.
Immediate Actions (IA)s	Pre-planned actions taken immediately by the operational staff concerned in an emergency or when an incident occurs and before, if notified, the arrival of emergency services or other responding organisations.
Impact	The consequences of an incident – harm to persons, physical damages, direct and indirect costs like damage of reputation or perception of security.
Improvised Explosive Device (IED)	An explosive device produced using available materials, e.g., timing devices, means of detonation, explosives (commercially available or improvised, i.e., 'home made') and articles, such as nails for additional impact. IEDs may use components of military explosive articles and also contain incendiary materials. Initiation may involve a remote controlled device or timer mechanism.
Improvised Incendiary Device (IID)	A device produced from available flammable materials, intended to set fire to the target and cause serious damage from the heat and the dense and toxic fumes produced, An IID may be initiated manually on site, e.g., a Molotov cocktail, by a timer mechanism or a remote controlled device,. An IID may be combined with an IED.
Improvised Radiological Device (IRD)	A device intended to spread radioactive material, most commonly the spent fuel from nuclear power plants or radioactive medical waste, usually by conventional explosives, with the intention to harm, kill and/or cause major disruption. Also known as a dirty bomb. It is not a nuclear weapon as it does not involve a nuclear explosion.
Incident	Something that has happened and is likely to lead to some consequences. It includes events of both internal and external causes, deliberate or accidental and not necessarily of negative consequences. In that sense, it is a more general term than *accident*.

Incident level	Ranking of incidents in terms of potential severity for command, control and response purposes typically as follows: • **Level 1** - Incidents that do not affect the safety of people, system assets and operational capability. • **Level 2** - Incidents affecting assets and operations in one or more stations, other facilities or line of route but not constituting a serious threat to people. • **Level 3** - Incidents that result in casualties and/or significant traffic disruption or damage to the system's assets. • **Level 4** - Crises involving multiple casualties and destruction/denial of critical assets (human, vehicles, facilities and other infrastructure) hence compromising the main functions and operations of the system.
Incident response plan	A plan detailing the response to an incident or an emergency situation.
Information Capture	Recording information, through a sensor-based device (camera, microphone, etc.), on a permanent or temporary storage medium, in a manner allowing accessibility by humans.
Intrusion detection systems	Sensor based (optical, microwave, vibration etc.) systems designed for the detection (and consequent alarm) of intruders crossing a perimeter or entering a protected area; they can be classified in perimeter protection systems (along fences, open spaces, etc.) or built spaces (home or industrial burglar alarm systems).
K9	K9 or K-9 is an abbreviation and homophone of 'canine', and refers to the use of police dogs such as those used for bomb or drug sniffing.
Lead person (LP)	An identified qualified person appointed in an organisation with responsibility for the overall on-site incident command and control of their response (may also be referred to as "Emergency Management Coordinator").
Minimum Standard	A formal document that establishes uniform engineering or technical criteria, methods, processes and practices that set the lowest acceptable level of quality or attainment. Standards can be technical, functional or goal-based.
Operations Concept (CONOP)	A written document describing an overall picture of an operation or series of operations frequently embodying operational strategies, methods, principles, plans, policies also organisation and command structures. It identifies connected or separate operations to be carried out simultaneously or in succession, by the entire organisation or by one or more of its operational bodies.
Performance criteria	The parameters that quantify how the system / component fulfils its functionality.

Perimeter security	A system of technical means, personnel and procedures aiming in ensuring that nobody enters (or exits) a defined area except through the controlled access points. It has three essential functions: Deter, Delay (or deny) and Detect (& document) any intrusion, sometimes referred as 3D.
Personal Data	Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (EC Directive 95/46 article 2.a).
Personal Data Protection	All regulations, technical systems and procedures that aim at the protection of such personal data throughout the acquisition / transmission / use / storage and disposal cycle.
Personal Protective Equipment (PPE)	Protective clothing, helmets, goggles, other garments or equipment designed to protect the wearer's body from injury due to blunt impact, electrical hazards, heat, chemicals, and infection.
Poisonous by Inhalation (PIH)	A gas that is (or is presumed to be) toxic to humans to a degree posing a hazard to their health if inhaled even in minute concentrations.
Privacy	The quality or state of being secluded from company or observation.
Probability of Attack / Probability of Occurrence	The probability of a threat materialising. The probability of a certain incident occurring.
PTZ cameras	Cameras that have the capacity to pan, tilt and zoom, usually in remote control but sometimes also in automatic mode.
Public area	Areas that are meant to be accessible to the general public; these can be of free or limited access; in the later case access control is generally limited to entitlement (i.e. control for a ticket or a access/travel card but not identity control)
Public entity	Entity / body / organisation not necessarily of public (state) ownership but of public character (i.e. serving the public or ensuring a public function).
Public infrastructure	All infrastructures (i.e. equipment, constructions and areas) that are meant to be at the service of the general public rather than the various specific actors or professionals
Risk	The potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome); the effect of uncertainty on objectives (ISO 31000)
Risk (Security)	The degree of exposure to a threat. The risk increases with the potential impact and the probability of a threat materialising. Risk is measured in escalating categories.

Risk assessment / analysis	A step in a risk management procedure: the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (or hazard). Quantitative risk assessment requires calculations of two components of risk: R, the magnitude of the potential loss L and the probability P that the loss will occur. Qualitative risk assessment is usually performed where statistical data for a quantitative assessment are missing. It usually involves the use of score matrices.
Risk Based Approach	A security risk management approach, based on categorisation of the risk level following a risk assessment, selection of risk mitigation safeguards based on cost-benefit considerations, operational and technical feasibility, and accepted risk management strategies.
Risk Management	The identification, assessment, and prioritization of risks followed by coordinated and efficient application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.
Sabotage	Tampering intended to undermine the integrity of systems with the objective of causing damage to assets, and/or harm to humans, and disrupting routine operations; e.g. causing derailment, interfering with signalling, power supply or communications systems.
Safeguards	Any measure (action, procedure or technique) that mitigates risk by reducing the vulnerability of a system, the potential impact from a threat or the probability that a threat materialises.
Safety	The state of being free of risk or danger (natural or accidental); being in control of recognised hazards and reducing risk of harm or damage as low as reasonably practicable. The term 'safety', when used as an attribute, encompasses all measures, actions or systems aiming at ensuring the state of safety.
Safety incident	An accidental event, of internal or external causes, that is likely to lead to some negative consequences and compromise safety.
Safety Management System (SMS)	Documented arrangements/process identifying an organisation's safety policy, the means of achieving and maintaining defined safety targets, the distribution of roles and responsibilities and the response to incidents and investigation. For main line railways Directive 2004/49/EC (Safety Directive) a SMS is a fundamental operational requirement.
Security	The set of means / actions through which safety is ensured, in particular against intentional threats. Thus, the term 'security' encompasses all measures, actions or systems aiming at preventing intentional threats from compromising safety.
Security Incident	Deliberate act intended to harm and injure, damage equipment and infrastructure, disrupt operations and compromise safety**.**
Security Master Plan	A document defining the overall roles, responsibilities and management arrangements of a security organisation.

Security officer	Person responsible for security within an organisation or facility. The functions of the security officer are usually prescribed within a security plan; sometimes referred to as chief security officer.
Security Plan	A document, usually the outcome of a security risk assessment, defining the management chain and responsibilities in relation to security and detailing the measures (protective and reactive) such as procedures, systems, methods and staff, implemented at a particular facility or organisation for its protection against security threats and in response to security incidents.
Security Regulator (Security Regulating Body)	A public entity, governmental or recognised by government, responsible for defining statutory security requirements and for ensuring their application.
Security Risk Assessment	A process used to systematically analyse potential threats to a specific target. The process includes identifying and classifying assets by their criticality; the analysis of a range of potential threats and their probability of being realised, and their potential impact. A vulnerability assessment may be performed as part of a risk assessment.
Security Risk Management	The process of identifying security risks and selecting and implementing mitigating safeguards based on risk management strategies.
Security Staff	Members of PTO staff, whose role is primarily concerned with the security of PTO operations and assets.
Security Threat	The expression of intention (or perception of a possible intention) to provoke a security incident, i.e. to harm or injure, damage equipment and infrastructure, disrupt operations etc. Security threats may materialize into security incidents that are a concern for safety.
Sensitive Security Information (SSI)	Information relating to security activities that is sensitive yet unclassified, the public disclosure of which may harm public transport system security, cause invasion of privacy or reveal trade secrets, privileged or confidential information.
Site (of an incident)	The area within which the response to an incident is managed.
Standard Operating Procedure (SOP)	A pre-planned documented arrangement for safe and effective management of a task.
Surveillance	Observation from a distance, usually by means of electronic equipment (such as CCTV cameras) or, sometimes, by no- or low-technology methods such as human agents
Terrorism	The intentional and unlawful use of force / violence, deliberately targeting or disregarding the safety of civilians with the intention of inflicting significant harm to persons and/or damage to property; causing panic and fear; intimidating or coercing a government or a civilian population to further a religious, political or ideological goal.

Threat (Specific)	A threat, which may give a time, directed at a specific target, e.g., a train, station or other asset and which may relate to the use of any type of IED, IID, VBIED, CBRN devices or the use of firearms. Specific threats may or may not result in an actual incident, but can involve serious operational disruption, safety and cost issues.
Threat Level / Advised Threat Level	The 'advised threat level' or 'background' threat level, defined by a government agency.
Threat, Vulnerability and Risk Assessment (TVRA)	The process of risk assessment, disassembled into its independent or dependent processes.
Toxic Industrial Materials (TIM)	A general description of any substance that is poisonous or harmful to humans, animals, plant life or the environment.
User Requirements	A set of needs and / or expectations of the user(s) from the product, system or service under development. The term 'users' encompasses any citizens, businesses or public authorities that might use the final product, system or service.
Vehicle Borne Improvised Explosive Device (VBIED)	An IED carried by a vehicle – usually containing a large amount of explosives, intended to cause maximum casualties and damage.
Vulnerability	A weakness, e.g. in physical structures, personnel protection systems, process or other areas that may be exploited by perpetrators
Vulnerability assessment	Any review, audit, or other examination of the security of a public transport infrastructure asset to determine its vulnerability to unlawful interference, whether during conception, planning, design, construction, operation, or decommissioning.

4 Information and Communication Technology Terms and Definitions

Access Control (ACS)	A system enabling an organisation to control access to areas and resources in a given physical facility or computer-based information system. The access control's functionality answers one or more of the following questions: • Something I have (for example: a card, entry authorization); • Something I know (PIN code); • Something I am (individual biometric identification).
aGPS	Assisted GPS - a system, which can, under certain conditions, improve the start-up performance of a GPS satellite-based positioning system and used extensively with GPS - capable cellular phones.
Automatic Number Plate Recognition (ANPR)	An image-processing technology used to identify road vehicles by their license plates. Often referred also as LPR (Licence Plate Recognition).
Area of Interest (AOI)	A general or specific area in the video frame or stream, concerning which rules have been defined via a video analytics application.
Backbone Transmission Network (BTN)	A central communication network serving mission critical systems.
Closed Circuit Television (CCTV)	A system using video cameras to capture / transmit / record a signal to a specific place, on a limited set of monitors, though a point to point (P2P), point to multipoint, or mesh wireless links. According to ISO/DIS 22300: Television system in which signals are not publicly distributed.
Contactless smart card	RFID based (proximity read/write) smart card used for entitlement (ticket) and/or electronic means of payment
Digital Video Recorder (DVR)	An electronic device including application software that records video in a digital format to a disk drive, USB flash drive, SD memory cards and other local or networked mass storage device.
Dome Camera	Surveillance cameras, usually with PTZ capacity, that are mounted into a dome-like enclosure either for protection or for being less invasive (not to look like a camera).
Early Warning System	System that permits the warning and, possibly, the communication on an imminent threat or incident very early in the incident response cycle. The recipient of the warning can be the concerned public or appropriate emergency response staff.

Field of View (FOV)	The part of the scene that is visible through the camera at a particular position and orientation in space; objects outside the FOV are not recorded. It is most often expressed as the angular size of the view cone, as an angle of view or a ratio of lengths.
Frames per Second (FPS)	The frequency (rate) at which an imaging device produces unique consecutive images expressed in frames per second (FPS).
Geographic Information System (GIS)	A system designed to capture, manage, analyse, store, manipulate and display all types of geographically referenced information.
Global Positioning System (GPS)	A satellite navigation system based on a large number of designated satellites (the US Department of Defense, Galileo, Glonass, Baidu), which transmit time signals that are received by a receiver on the ground. Transmissions received from four or more satellites calculate the position through triangulation.
Human Machine Interface (HMI) / Graphical User Interface (GUI)	Graphics - based visualisation of a control and monitoring system.
Incident Management System	Software developed specifically to support incidents. The software collects, analyses, displays and investigates data through one or more control stations. Most applications are capable of managing processes, tasks and inputs; defining process escalation; classifying incidents based on risk levels, and controlling security, safety, operational, communication and information systems, via physical or logical interfaces.
Information Capture	The recording, through a sensor-based device (camera, microphone etc.), on a permanent or temporary storage medium of information in a way such as it can be accessed by humans.
Integrated security systems	An integrated security system, application or solution, tightly coupled together as a functional unified system
Interoperability	The capability to communicate, execute programs or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units (ISO/IEC 2382-1:1993). The property of a product or a system enabling it to work with other products or systems, present or future, without any particular restrictions or additional implementation. In SECUR-ED, minimum requirements for interoperability guarantee that the solutions demonstrated will be modular, open and scalable.
Intrusion Detection System (IDS) / Burglar Alarm System (BAS)	Electronic alarms alerting the user to a specific danger, classified into home or industrial burglar alarms and perimeter intrusion detection.
License Plate Recognition (LPR)	An image-processing technology used to identify road vehicles by their license plates. Often referred also as ANPR Automatic Number Plate Recognition.

Local Positioning System (LPS)	A system using wireless communication – a transmitter and a receiver to calculate the location via triangulation and displays it using a software application.
Location Based Services (LBS)	Information or entertainment services, accessible with mobile devices through the mobile network and utilizing the ability to make use of the geographical position of the mobile device
Network Video Recorder (NVR)	A system receiving video input over a network and recording it in a digital format to a disk drive, USB flash drive, SD memory card or other mass storage device and allowing for selective restitution of the collected videos.
Perimeter Intrusion Detection System (PIDS)	A generic name for electronic perimeter security systems, including vibration detection, optic fibers, seismic detectors, volumetric systems, transmitter-receiver technologies, video analytics, scanning observation systems, radar systems and more.
Physical Security Information Management (PSIM)	A category of products that integrate an organisation's disparate security devices and systems into a single unified operating picture.
Public Address (PA)	An electronic amplification system with a mixer, amplifier and loudspeakers, used to reinforce a sound source.
Security Control Centre (SCC) / Security Operations Centre (SOC)	A physical location at which command & control and communication systems are installed to enable security operation management.
Systems Interoperability	The ability of two or more systems or components to exchange and make use of information.
Terrestrial Trunked Radio (TETRA)	A digital trunked mobile radio interoperability standard, used by Private Mobile Radio users such as Public Safety, Transportation, Utilities, Government, Commercial & Industrial, Oil & Gas and Military etc., which allows equipment from multiple vendors to interoperate with each other.
User Requirements	A set of needs and / or expectations of the user(s) from the product, system or service under development. The term 'users' encompasses any citizens, businesses or public authorities that might use the final product, system or service.
Video Analytics (VA) / Video Content Analysis (VCA) / Intelligent Video Analytics (IVA	The automated analysis of images or video streams, usually acquired through CCTV systems, in order to create useful information about the content.
Video Recording System	A DVR or NVR
Video Surveillance	Remote observation and/or recording of one or more persons or a certain area by means of connected video cameras (CCTV or other system).

VMS (Video Management Software) / VMX (Video Matrix)	Software operating on a computer or a server, which is used to manage monitoring, analysis and recording functions of monitoring / surveillance systems.

5 Public Transport Terms and Definitions

ATVM / ATIM / TVM (Automatic Tickets Vending Machine)	A machine, which automatically dispenses travel tickets or loads a smart card with a specific sum of money after the customer inserts cash or a credit card into its slot.
Automatic Fare Collection System (AFC)	Transport payment system based on the use of information and communications technologies. Also referred to as electronic ticketing.
Automatic Vehicle Location System (AVLS)	Position determination via an automatic technology or combination of technologies, such as global positioning system (triangulation of satellite signals), signposts (beacons at known locations transmit signals picked up by a vehicle) or ground-based radio (triangulation of radio tower signals). It typically includes real-time reporting of that location to a dispatcher with the aim of assisting operations control.
Bus	A rubber-tyred road public transport passenger vehicle powered by diesel, gasoline, battery, hybrid or alternative fuels, or a combination of fuel engines contained within the vehicle.
Bus Rapid Transit (BRT)	A type of limited-stop service operated on exclusive lanes that are physically separated from the rest of the road traffic except at junctions. A BRT line combines intelligent transportation systems technology, priority at junctions, rapid and convenient fare collection and is integrated with land use policy in order to substantially upgrade the bus system performance.
Commuter Rail	Regional rail or suburban rail operation for local short distance travel between an urban area and adjacent suburbs (e.g. RER, S-Bahn, Stadtbahn).
Contactless ticketing	An automatic fare collection system where payment is validated without any physical contact between the user's ticketing device (contactless smartcard) and the in-vehicle or platform payment device.
Control Facility / Operations Control Centre (OCC)	A PTO or IM central command post, responsible for operations and incident response in a specific geographic area.
Diesel Multiple Unit (DMU) **Electric Multiple Unit (EMU)**	A train set consisting of self-propelled carriages capable of being coupled with other units of the same or similar type and still being controlled from one driving cab either diesel powered (DMU) or electric (EMU).
Emergency Call System (ECS)	A communication system installed in passenger facilities or onboard trains, which allows audio communication between a person and the control center or the rolling stock driver. The system may include a fish-eye lens camera enabling real time display of the caller.
External organisations	Non-public transport organisations, including specialists / consultants, contractors, tenants and neighbours, but excluding emergency services.

Fleet Management System	An integrated ICT system for the management of a fleet of vehicles for operational and data analysis reasons.
Franchise	A privilege or exceptional right granted by the state to a person or company. In urban bus transport, franchise can also mean the granting of monopoly rights to a person or company for a given price or remuneration (called **franchise fee**).
Frontline Employees	Members of PTO staff, usually at stations or on trains or buses, who interface directly with passengers in the frame of tasks related to operational arrangements.
Heating, Ventilation, Air Conditioning (HVAC)	The technology for indoor or rolling stock environmental comfort.
Infrastructure Manager (IM)	The organisation responsible for providing, maintaining and controlling the use of the infrastructure serving public transport operators. This responsibility may be combined with that of a PTO.
Inter-modal transport facilities / interchange	A passenger facility where several transport systems operate in a coordinated, synchronized manner.
Interoperability	In SECUR-ED project, *interoperability* has an additional meaning: the "interoperability concept" forms the basis of the development of an interoperable framework, where security solutions for mass transport systems are designed within a common architectural approach, so that systems and solutions are "transferable", i.e. sharing a generic approach although specific applications shall depend on the local conditions. The word "Interoperability" in SECUR-ED is not related to the "Interoperability" of rail systems within the European Railway system as defined by the Interoperability Directive 2008/57/EC. The "interoperability concept" in SECUR-ED does not imply for different mass transport security systems to be "interoperable" and connected to each other.
Light Rail Transit (LRT) / Light Rail Vehicle (LRV)	An Urban Guided Transport (UGT) system operated in parts of the network not segregated from general road and pedestrian traffic while in other parts with segregated right-of-way. The segregation may include some sections of line where inadvertent access is not possible.
Local authorities	Any level of local, public, municipal or regional government.
Member State (MS)	Any Member State of the European Union.

Metro	An Urban Guided Transport (UGT) system operated on its own right of way and segregated from general road and pedestrian traffic. A metro is consequently designed for operations in tunnels, viaducts or at surface level but with physical separation in such a way that inadvertent access is not possible. Metro systems are also referred as *underground*, *subway*, *tube or U-Bahn*. Rail systems with specific construction issues operating on a segregated guideway (e.g. monorail, rack railway) are also treated as Metros as long as they are designed as part of the urban public transport network.
Mission Critical	Any element of a system (equipment, process, procedure, software, etc.) whose failure will result in the stoppage of business operations, i.e., critical to the organisation's 'mission'.
Neighbours	Property and premises immediately adjacent to those of a PTO or IM, or sufficiently close to potentially be affected by an incident occurring on the other's premises.
Operations	A PTO or IM activities, including bus, train and station operations and other activities for which they are responsible.
Other responding organisations	Any PTO or IM (other than the incident response plan owner), or external organisation (other than emergency services/first responders) that may be involved in the response to an incident. This includes specialist security responders such as EOD teams.
Public area	A location at which transport services are supplied to the public, such as a bus or train station. Some stations may be private property with access for the public, but for the purpose of SECUR-ED they are considered as public areas.
Public entity	Entity / body / organisation not necessarily of public (state) ownership but of public character (i.e. serving the public or ensuring a public function).
Public Information System (PIS) / Transport Information Systems (TIS)	A system providing passengers with real-time information concerning their journey, such as arrival and departure times using e.g. television screens and LCD displays. In case of emergency, such systems can be used also for Public Address reasons.
Public infrastructure	All infrastructures (i.e. equipment, constructions and areas) that are meant to be at the service of the general public rather than the various specific actors or professionals
Public Transport Authority (PTA) / Organising Authority	Government entity at state, regional or municipal level that is responsible for the policies on public transport services and market on a given territory. Depending on the case, it may be supported by a separate entity (e.g. PTE – Public Transport Executive) in charge of putting into practice the decisions adopted at the political level.

Public Transport Operator (PTO)	An organisation, public or private, that manages the operations of public transport services concerned with the mass mobility of citizens. This includes main line railway undertakings, metro, tram and bus operators including their support facilities, such as rolling stock and maintenance facilities, and involves international, national, suburban or urban networks. Main line rail PTOs are also known as railway undertakings. A PTO may also be an infrastructure manager.
Railway Undertaking	Main line rail PTO may be identified as railway undertaking.
Rolling Stock (RS)	Rail and road vehicles, such as passenger carriages, trams, locomotives and buses.
Safety Integrity Level (SIL)	A relative level of risk reduction provided by a safety function, or to specify a target level of risk reduction.
Station Operator	An organisation with overall responsibility for managing the operation of a station. May be a PTO or IM.
Traffic Management System	A system that regulates or helps regulating traffic, based on real-time information
Train Operating Company (TOC)	A PTO, particularly with main line railways, may also be identified as a train operating company.
Train / Railway Signalling	A mechanical or electrical device installed on or beside a railway line to transmit information relating to the state of the line ahead to train drivers.
Transport Authorities	Organisations of public character that regulate transport at local, regional, national or EU level.
Urban Guided Transport (UGT) systems	Public transport systems permanently guided by at least one rail, intended for the operation of local, urban and suburban passenger services with self-propelled vehicles and operated either segregated or not from general road and pedestrian traffic.

- End of Document -