WHITE PAPER FOR
PUBLIC TRANSPORT STAKEHOLDERS

Based on the lessons learned in SECUR-ED

This White Paper benefits from the conclusions of FP7 PROTECTRAIL
(www.protectrail.eu)
Content

1. Introduction and context.........................................................................................................................3
2. Security Organization, Procedures & Training.........................................................................................4
3. Information Management and Architectures..............................................................................................8
4. Video-Surveillance and Intrusion Sensors.................................................................................................12
5. CBRN-E Response ....................................................................................................................................17
6. Telecommunications & Impact of the Mobile Applications ......................................................................19
7. Cyber-Resilience .......................................................................................................................................23
8. Methodologies and Ethical Conduct .........................................................................................................28
9. Way Forward............................................................................................................................................30
1. Introduction and context

Security is a cornerstone of any sustainable mobility policy and mobility system. Making public transport secure is a complex task, as the system must be open, accessible, affordable, and must enable an efficient free flow of passengers. At the same time, transport systems face a broad spectrum of threats, ranging from low-probability-high-impact events (e.g. terrorist attack) to the daily threats (e.g. vandalism).

SECUR-ED with its 41 partners, its ten field demonstrations conducted over Europe, the support of its wide-spectrum Advisory Groups and the multiple studies conducted, has produced a wealth of results encompassed in over fifty documents. Most of these results are discussed in the specific frame of the Project and, as such, difficult to implement directly in a different context. This is why the present White Paper has the ambition of concentrating on the results and recommendations which bring an added-value to the public transport security stakeholders in their respective activities.

The focus of SECUR-ED has been put on urban public transport, but almost simultaneously and with many partners in common, PROTECTRAIL has addressed the security issues associated to the mainline rail system. The two projects managed to avoid duplication of efforts through joint experts Working Groups and common solutions, whenever applicable and relevant. Many of the conclusions and recommendations carried by this White Paper are the results of this joint activity.

If mainline rail is characterized by trans-border activities with multiple operators, complex convoy compositions and long distance (sometimes in remote and scarcely populated areas), urban systems are more isolated from each other, serve high concentrations of population and involve more varied types of vehicles and stakeholders. However, numerous security concerns are similar and, especially in the very populated areas, the distinction between suburban rail lines and mainline rail is not always possible to do, implying therefore in some cases for operational reasons a commonality of security solutions.

The security solutions, procedural or technical, are strongly influenced by the growing role taken by Information and Communication Technologies (ICT) in the transportation systems, but this does not change the fact that most of the assets have a life expectancy of several decades. This is why the prescriptions listed hereafter generally consider their interactions with the legacy systems, as well as a future-proof vision within this same scale of time.

In public transport, where the passenger is at the same time the main beneficiary of the security measures and - together with the staff - the potential victim of resulting privacy breaches, the long-term vision of the security approach can only be based on an ethical dynamic balance between societal benefits and prevention of unnecessary intrusive methods, this balance changing rapidly with the local context, the international (security) situation or the evolution of the general use of technology.

This White Paper has been prepared as a guideline for the security organizations in charge of the public transport, and especially the operators. It considers the daily operations, optimized procedures, as well as the vision of the future security systems. In response, the industrial and research communities will also find clear directions for their future relevant activities. To make this overall picture future-proof, whenever a general consensus is possible, the White Paper strongly suggests that the parties formalize the most beneficial minimum provisions into international standards.
2. Security Organization, Procedures & Training

Security is the set of means and/or actions through which the integrity of the public transport customers, staff and assets is ensured against intentional threats. The threats faced by Public Transport Operators (PTOs) range from daily crime and anti-social behaviour, such as group violence, vandalism and graffiti, to serious crime using arms and firearms, and terrorist activities involving explosives or toxic materials. If realised, these threats can lead to harming people, to cause physical damage of the PT assets, disruption of services or system shutdown.

Public transport systems differ in many ways from airports, seaports and critical facilities in their physical structure, geographical distribution, their regulations, operation and more. However as with these other systems the public transport security concept is comprised of three interlinked elements:

- Security organisation setup, which includes interfaces with internal and external bodies;
- Risk based strategy, implemented through a structured security risk management process; and
- Risk mitigation safeguards and policies, which include operational arrangements, procedures, technological, communication and information management systems, physical protection means, incident response and business continuity planning.

Security Organization

Security organization remains driven by common sense; as applicable and relevant, it is recommended that PTOs appoint a specific individual who will be responsible for security, and will have defined areas of authority. This function is usually called “Head of Security” and must report to a level high enough in the organization to get the appropriate decisions taken and implemented. Security activities are split into: risk management and preparedness, operational duties and the efficient use of the available security technologies.

Risk management and preparedness are primary drivers and SECUR-ED confirmed the key role played by the PT security staff, despite the growing importance of technology in the domain. Further to risk assessment and training detailed here below,

- PTOs generally have established some prescribed interfacing and training with the external security organizations, so that all relevant actors become familiar with each other’s working environment and security methods and requirements; SECUR-ED has shown that an enhanced cooperation between PTOs and prevention, security & first responder authorities (police, intelligence services, fire departments, ambulance, etc.) proves to be very beneficial for all of the involved parties. They can for instance take advantage of the risk assessment sessions to pull-back from the routine procedures and drills and look into the newly-discovered threats and try to find the right solutions. The work in SECUR-ED has also shown that it is crucial to refresh regularly with the relevant partners the risks common understanding and priorities.
- During project duration, it became growingly clear that cyber threats apply to all the facets of the PTOs assets and system with an obvious potential security impact; in practice, this means that the need for cyber threat experts is no more reserved to information management tools. Accordingly, cyber threats should determine PT organizations to provide an appropriate response and to evolve towards a single unified security structure.
Risk Assessment Doctrine (nature, methods and tools)

Risk assessment is one of the major practices recommended in SECUR-ED; its relevance has been validated in very diverse situations over Europe.

The reference document is ISO31000, which fully describes the risk management process, as summarized in Figure 1 below; it is applied when a new asset is put in service and with the appropriate granularity to draw the most relevant and cost effective response, and regularly refreshed as environment, interconnections, events, etc. change; this process can be supported by dedicated software tools, like the RiskAs developed in SECUR-ED.

Figure 1: Risk Management process according to ISO31000

A key finding is that PTOs are of course familiar with the layout and structure of their systems, but given that most European PT networks are old and have developed over time, relevant expertise has disappeared and not all changes may be properly recorded or communicated to other departments. This leads to some difficulties to have a relevant risk analysis, done as per the above standard. Few know the global picture in all its details, it is therefore of utmost importance to include all relevant PTO departments in a risk analysis work.

This is especially true in order to integrate cyber threats into the overall risk assessment method, and many legacy systems incorporate hidden processing capabilities.

To conclude, Risk Assessment is both a first step and an on-going process; it is the driving factor for all security solutions including definition of the necessary procedures and trainings.
Training Concepts & Implementation

The basic objective of a training plan is to enhance staff preparedness in view of preventing and managing threats. Training dedicated to daily threats and conflicts management is accordingly a must, while selection of other courses will follow risk assessment recommendations.

Some general principles apply:
- All staff should have at least a training providing a basic notion and awareness of security;
- A prerequisite is to assess what staff already knows before implementing the lessons – lessons which, in turn, have to consider the security knowledge of each staff category;
- Security trainings should encompass the “refresher” method – repetitive short trainings, drills, etc., in order to strengthen the preparedness of the PT security staff.
- It is necessary to link training with technologies, including future developments, and procedures.

The aim of the project had been to develop numerous security trainings that are both comprehensive enough to cover a wide array of jobs and situations, but also generic enough so that the numerous operators can pick them up and easily adapt them to local conditions. In fact, some of them may target a larger scope (these lessons are neither limited to security nor to public transport).

Varied implementations during the SECUR-ED demonstrations proved their good adaptability to each specific security type of organization. In practice, this successful approach is a blend of generic trainings and adaptations made directly by the operators to the local context, like legacy infrastructure and procedures, national regulations, etc.

The lessons learned from the development of the SECUR-ED training are the following:
- Before implementation, all training lessons should be properly adapted to the relevant local conditions: language, country/regional regulations, transportation modes, specific to company processes, etc.
- Both the text and the images (or other support tools used) of training lessons should be adapted to the local context of the trainees, in order to better understand the lessons and also to familiarize themselves with the PT environment.
- The “train-the-trainer” lessons (and kit) are highly appreciated because they help enable an operator to do the training himself. However, qualified people that could give this course are hard to find, therefore it remains a significant challenge in this field.
- In the lessons, try to strengthen the links with LEFR (Law Enforcement and First Responders) in order to familiarize with each other’s protocols and increase efficiency.
- Training should not only aim at better training staff, but also at identifying gaps within the general PTO architecture.
- It is sometimes necessary that security training be complemented with other related subjects in order to tap the entire potential of the lessons – e.g. training with (enhanced) psychological components.

For many of the SECUR-ED lessons, Computer-Based Trainings (CBT) complementary to classroom trainings have been produced; they are easily adaptable and user friendly, and prove to be optimum for refresh cycles, but sometimes even a training basis.

Interested operators may consult UITP for details and availability conditions.
Simulation

Simulation is a well-known and cost-effective approach to address design of complex systems; mature tools developed for construction and air conditioning are obviously also applicable to assess resilience of infrastructures to security threats. Provided all physical measures are available (or accessible), simulation is the approach of choice to emulate, and accordingly control, the dispersion of dangerous substances in underground or 3D structures, as real experimentation with the substance of interest are generally impossible.

Relevance of simulation, linked to operators’ knowledge, was also demonstrated with flows of humans. Complementary to real drills, or for the design of new infrastructures, it is possible through smart agents to model the flow of persons, evacuation, etc., and test an infrastructure to adjust corresponding procedures. It must be noted that, contrary to drills where participants are aware of the absence of real threat, it is possible to better recreate and evaluate the impact of various panic situations through simulation.

Figure 2: Simulation and evacuation drill in Milan
3. Information Management and Architectures

SECUR-ED (consistently with PROTECTRAIL) based its vision of a future-proof interoperability framework on design patterns which are successfully used in other industries. These include the following elements:

- A reusable Service-Oriented Architecture (SOA);
- An Event-Based Architecture for data exchange between various security components and decoupling the components from each other;
- Reuse of well-established and proven standards which reduce the non-recurring cost of software integration;
- Building modular components with web services;
- Supporting discoverable components to reduce the configuration effort and improve the reusability;
- Building on an IP network (cabled or wireless) which is dimensioned to support consistently the video surveillance streams necessary to assess, confirm and investigate security incidents.

The ultimate objective of enabling solution providers to adapt their solutions with minimal non-recurring costs, must be confronted to the reality of on-board systems with limited processing capability, of interfacing with legacy systems, of ensuring a guaranteed configuration control in all situations, etc.; implementations will accordingly borrow as much as possible from this overall picture to be future-proof, but may not adopt the full possible openness.

In other words, the ideal scheme needs to be adapted to interface legacy and ensure dependability; typically all aspects relative to discovery and flexibility in configurations apply only at the design level; in day-to-day operations, systems must obviously remain untouched.

The foundation remains the Event Driven Architecture (EDA) consisting of numerous event producers and event consumers from various locations and various stakeholders of Public Transport operations. Devices from on-board and wayside (i.e. sensors and devices like CBRNE detectors, intrusion detection, laser scanners and devices like video cameras and recorders, video analytics, etc.) send events ranging from basic alerts with limited environmental information to more complicated alerts with various information and resource fields which are vital for a better understanding of the situation on the ground. These sensors and devices are called event producers.

This calls for a common Event Format which includes location (and in all probability the affected area), absolute occurrence time (in UTC), a unique event identifier and type, attached resources as well as source and contact information. After extensive analysis, the Common Alerting Protocol (CAP) of OASIS appeared as the best existing standard for the public transport sector. Today, CAP is used extensively for weather and earthquake warnings in public and commercial Emergency Alert Systems like Google Public Alerts; it is however not yet endorsed by an internationally recognized security standard.

The OASIS specifications define a data model for a wide range of applications like safety, security, health, weather and environmental threats, telecommunication and cybersecurity. The recommended approach is an XML Schema representation of CAP to implement the event providers and consumers based on that standard. The proposed event format inherited the following CAP standard features:

- Multi-operational and multilingual messages;
- Three dimensional and flexible geographic description;
- Message update and cancellation;
- Links through web service endpoints (URL’s) to further information such as images, reports and videos.
Interoperability relies on both a common data model and shared representation. Shared representation is important for all stakeholders to collaborate based on the same information assets. It starts with the same wording, shared facility information and ends in common geographical maps.

For surface infrastructures, the GPS coordinates (WGS-84) is the natural response; for underground or 3D infrastructures, there is today no standard and no effective localization method if dedicated infrastructures are put out of order by a security incident. In practice, one can rely on drawings or textual descriptions based on one surface GPS point, keeping in mind that infrastructure shared by several owners needs specific interfacing.

SECUR-ED demonstrated that a global pragmatic Geographical Information system (GIS) as per the above can be shared by several stakeholders and that general consistency between the various stakeholders and fixed or mobile assets can be reliably achieved. Geo-location in 3D and underground structures remains nevertheless clearly a research and a standardization domain to explore (as already noted in EC Mandate M487 on Security Standardization).

When several systems, typically from different vendors, need to cohabit, a reliable message exchange can be achieved through the implementation of an Event Broker. This can rely on the Eventing Framework specification WS-Notification, which can contain any type of XML data format. A Message Server manages all incoming and outgoing messages and can deliver and handle high performance, clustering, transactions and a wide range of cross-language clients and protocols. If an event consumer is not available the message server can store undelivered messages and retry delivery out of a message queue.

The consumers of these messages are diverse and more and more belong to different owners, such as the different levels of Security Operation and Control Centres (SOCC) or Crisis Management Systems (CMS). The flow of information follows accordingly the process depicted in Figure 3.

Figure 3: Participants in a global security context
The role of a **Security Operation and Control Centre (SCCC)** is to ingest and correlate various event sources into a single platform and thus improve the situational awareness among those persons that need to work with the information, for instance security operators or first responders. Several SOCC’s can share a situation and cooperate. Typically such a system visualises the events in a GIS map and shows related video cameras, recorded videos and it provides operational and security related procedures. Simple events can be correlated to a major incident which means that the event contains additional information on for instance a responsible person, severity, certainty, and urgency. The SOCC system helps the operator in his daily work to suppress nuisance alarms, to group similar alarms, and to relate the event with other information and sensors. The SOCC may guide the operator in stressful situations through electronic Standard Operational Procedures (eSOP). These procedures are programmed today but could be executed as a graphical business process in the future. To allow for a continuous improvement of the eSOPs during operation, the decisions and actions of the operator can be recorded consistently with the videos. With such a system the operator can be trained with simulated operational situations.

Standard tools exist to support such process automation or orchestration; typically, **BPMN** (an OMG specification) helps to identify responsibilities, to define a common operational process for all stakeholders and to embed this process into a modern SOA infrastructure (Figure 4).

![Figure 4: Model and execute flexible Business Processes based on SOA infrastructure](image)

A **Crisis Management System (CMS)** is a solution to manage a crisis with various responders and any class of requested stakeholders. A CMS has to handle multiple operators, transportation modes and locations. A crisis manager has to act and make decisions based on all available real time information. This information can come from external experts and external media types like news feeds, live and recorded, as well as fixed and mobile video that need to be integrated. As situations evolve, hand-over from one CMS to another CMS may prove to be necessary.

As all security systems become digital over-IP and telecommunications develop, information is more and more shared between independent security systems. Their consistency is accordingly crucial for a timely response and post event investigations.
SECUR-ED has demonstrated that following the above principles, supervision systems from different vendors can work together, monitoring all sorts of sources, while specialized details can be obtained through resource links; to do so, the common mapping and time reference are prerequisites, even if sometimes difficult to implement in the public transport environment. This applies, for example, to vehicle to wayside interactions, typically to consistently locate an event shared between a train or a metro and position on the platform, generally requiring combined position of head of train and of the mapping inside the train.

Such required consistency applies to the video-surveillance feeds; this supports the decisions of the operators and allows ISO22311 standard export of CCTV evidence, assisting fast and efficient forensics investigations by authorities. Similarly, proper interactions between video analytics and supervision (like for tracking) provide for shorter operator’s reaction time.

Therefore, interfacing between digital over IP and legacy systems can only be encouraged, as it is generally easy to implement and the basis for the future, keeping in mind the emerging demand for a take-over of the assets (video, evacuation, etc.) by the authorities for crisis management, with the support and the cooperation of the operators.

Finally, organizations intending to procure or operate the above described systems, in full or in part, must keep in mind that they are potentially vulnerable to cyber threats; they are accordingly invited to visit section 7 of this document dedicated to cyber resilience, as early as possible in their acquisition process.

→ **Mobile Applications and Security Events**

Mobile applications used by staff, but also increasing by the public, with the extensive use of multimedia, create a new paradigm in the management of security events, isolated or massive. They may generate an enhanced incident management responsiveness (and cooperation) when combined to Supervision and crisis management systems, as well as create confusion, if multiple contradictory messages are received.

Each first responding organization must prepare itself, as part of the Future Emergency Call systems (112, etc.). A doctrine and then procedures must consider how to take timely proper decisions with multiple contradictory messages and more generally to perform classification with a proliferation of multimedia-rich messages for an incident. Even more fundamentally, the scalability of “Human as a sensor” concept needs to be studied in depth, pending availability of commercial applications.

Generalization of mobile terminals in an environment of social networks has an obvious impact on crisis management and on information to passengers during such crisis; correct information must be provided to the relevant person and not to everyone! In other words, during a crisis, passengers will access social networks through their mobile terminal and information may arrive before official communication by the operator, leading to unpredictable behaviour. This emerging matter clearly requires research and doctrines.
4. Video-Surveillance and Intrusion Sensors

To support the general requirement for future-proof interoperability and modularity of the public transport systems, SECUR-ED, as PROTECTRAIL, demonstrations confirmed that the sole implementation of the video-surveillance (also called CCTV) industry standards (IEC 62676-1&2 and even ONVIF profiles) is not enough. Implementation of such generic standards is further complicated by the regulatory need for stability and trustworthiness as well as privacy protection imposed on security video systems.

➔ Basic Infrastructure

The first level recommendations are accordingly for:

- A generalised use of RTP/RTSP streams carrying video, H264 compressed, with metadata, time stamped at the frame level, consistently with the security events described above; this profile may evolve over the time to accommodate higher density or new compression schemes, but without structure changes.
- Full modularity of the basic services associated to video, independently of their physical implementation (see block diagram of Figure 5).
- Video-surveillance systems are networks of distributed PC’s; as such they are potential targets of cyber-attacks, against which they must be protected (physically, by training the staff and/or with software).
- Digital video, especially when live information with low latency is required, has stringent needs for communications channels (no buffering is allowed); this implies a good quality of service for the communication but also an optimised set-up in the network architecture to minimise throughput at any point of the network in all circumstances (typically a case by case trade-off between UNICAST and MULTICAST).
- The system must preserve full consistency between time and metadata associated with the streams, the events produced by the analytics (see below) and the supervision tools.

These recommendations most often apply to incremental systems, while legacy solutions of diverse generations are already in place, and especially in that case the cost of infrastructure upgrading (wiring and power) is generally one order of magnitude higher than of the new video components. The objective is then to create an “ONVIF-like” video over IP behaviour at the interface to be future-proof. Different off-the-shelves solutions are available, like A/D encoders to interface analogue video streams or IP-over-Coax to reuse existing “analogue” cables, eventually
allowing installation of IP cameras while keeping the legacy coaxial cables. The main recommendation is to interface legacy for conversion to “standard” video over IP as near as possible to the source, rather than adding proprietary interfaces to legacy for each application.

→ Video Analytics

Several video analytics solutions have reached intrinsically a reasonable level of maturity, such as:

- **Intrusion detection**: to detect objects existing in restricted areas, it is necessary to extract objects in video frames. Object extraction consists of background generation, configuration of region of interest (ROI), extraction of object candidates based on background subtraction and contour labelling, noise elimination, and calculation of object information such as size and position. Algorithms of intrusion detection can help in:
  - Detection of persons in areas that are supposed to be empty and especially vehicles not in service;
  - Perimeter anti-intrusion (including in-service tracks);
  - Graffiti prevention.

- **Video tracking**: video tracking is the process of locating an object (or more than one) that moves in time, using a camera. An algorithm analyses the video frame and gives as output the position of the targeted objects. The main difficulty in video tracking is to capture the correct position of targets in consecutive frames, especially when objects see their aspect change over the time and move at a higher frequency than the frame rate. Semi-automatic tracking is a tool provided to video-surveillance operators (normally police for legal reasons) to support them in doing more efficiently a task performed today manually, after appropriate training. This function can be activated locally for benign events, but can also be run at the security control centre in real-time in case of more complex situations, which may imply several different systems active in a given area. As security staff is generally called just after the event, the tracking function is expected to cover reverse replay and faster than real time to catch up with live situation. Experimentations are promising, but developments are still under way to achieve such full capabilities.

- **Crowd assessment**: crowd density assessment provides information that may be relevant for both security and safety. It is also a key parameter for making the right decisions in several security-related crisis situations. It must be noted however, that in many large cities crowds, as such, are not considered a situation critical to detect for security reasons. Similarly, and often with the same tools, multiple individuals collapsing in a station can be detected confirming, for example, a chemical attack in a given area.

- **Face recognition**: a face recognition system is a biometric technology; it is close to a human recognition process and can be compliant with privacy regulations, as long as it is not associated to any personal data and produced results are not recorded. This technology is extensively used in controlled environments, but may be difficult to implement as it is sensitive to video quality and to many variations (facial expression, lighting, face orientation, etc.).

Implementing such analytics tool in a real public transport environment proves to be more complex than in controlled environments. The main difficulty is to define precisely for each camera what to detect and what not to detect; to be very concrete, a system supposed to detect suspicious left objects will be quickly rejected by the operators if there is an alarm each time an empty paper bag is left in on the floor.

Systems monitoring areas that should be empty or designed to provide qualitative results (crowd density, massive fall, etc.) generally give good results. This assumes that the video quality (with regard to the item to detect) is good.
and that all the environmental and context variations (like shadows or light reflections associated to movements of vehicles) are properly taken into account. More generally, it is wise to consider video analytics as operator supported tools (like for semi-automatic tracking).

More generally, it must be kept in mind that analytics tools have two main interfaces (the streams, i.e. video and metadata as per ONVIF and export of the results, as standard geo-localized events, consistent with those of the other types of sensors) and obviously an interface for human confirmation. As illustrated in Figure 5, this logical behaviour must remain independent of the physical implementation, like embedded in the camera, stand-alone or centralized and in any case the reference must remain the capture time and location of the source video. As indicated in section 3 above, it is recommended as well to stick to the minimum standard format for events derived from OASIS CAP and rely on associated URLs for details.

On a qualitative point of view, fixed cameras, with a performance adapted to the lighting and environmental conditions are usually a prerequisite for analytics performance and good quality of the streams (especially no lost packets) is anticipated, a characteristic which may be difficult to achieve if the communication network has not been dimensioned for wideband streams.

A calibration performed camera per camera is required for most analytics algorithms (e.g. to determine its 3D location and orientation or to adjust to internal lighting conditions). For large setups (50+ cameras), it is recommended to either automate these calibration procedures or make them simple and possible remotely. It is worth noting that some attempts are under evaluation of self-learning systems, which would take their decision based on a change with reference to past statistics.

![Figure 6: Semi-automatic tracking in Bilbao](image)

**Video and Non-Video Intrusion Detection**

The main objective of intrusion detection systems is to assess remotely the reality of the threat consisting in an unwanted presence in an area expected to be closed to the public. Detection rate must be high, but with a very limited false alarms rate; in most cases, to avoid undue overreactions, the system must allow remote visual confirmation.

Intrusion detection is closely linked with the video-surveillance capabilities, as there is generally no unique response, but a combination of detection sensors (video algorithms, laser barrier, smart fence, radar, etc.) and confirmation with some form of video (visible and/or IR as per environment requirements); in that respect, promising results have been obtained with new generation of IR CCTV cameras in all weather conditions and with an imaging range...
exceeding 500 meters. In all cases, consistency with the Information management prescriptions of section 0 is required.

Interfacing with the Authorities

In urban environment in general, and with the development of public transport of all kinds, there is a growing expectation from the authorities for being able to use the assets put in place by the different infrastructure owners to manage their security, for a consolidated situation management in case of a major crisis. This applies to all sources of data, as explained in section 0, but has special implications for videos, as they rely on time sensitive data streams.

In practice, this implies being able to go back to the origin of the incident and then navigate with agility (faster than real time, backwards, etc.) to understand the sequence of events or to perform special tasks, like tracking an individual over the full extent of a city. Tools do not exist today to achieve this level of interoperability between heterogeneous systems and the only option is to extend the scope of existing standards; roadmaps have in fact been put in place to build on IEC 62676 and ISO 22311.

In addition to the real-time (or near real-time) solutions described above, videos are collected to be usable for forensic analysis. This implies minimum video quality (sometimes mandated by law), proper and unambiguous identification of the scenes, time of occurrence and the ability to be decoded by police systems. The above mentioned ISO 22311, recently promulgated, addresses these requirements consistently with the general prescriptions of this White paper.

Mirroring these considerations, it must be recognized that if video-surveillance can be extremely useful for security management and crime investigation, it might result in an unnecessary intrusion into citizen privacy (this concern is addressed in section 8).

Cyber Threats and Trustworthiness

General considerations regarding the response to possible cyber threats are given in section 7. Only a few video-surveillance specific recommendations are discussed here, based on the fact that CCTV systems are de facto a set of multiple security-sensitive PCs connected to operators systems and left unattended in areas open to the public.

A basic precaution is to control access to rooms and network, then, even if an attacker has gained access to the video-surveillance network, the impact can be limited by:

- A strict management of passwords and authorizations;
- A configuration hardening of the clients and servers workstations (like USB ports);
- An increased resilience of the IP cameras configuration;
- The use of secured protocols for video streams transport (Secure RTP).

As allowed or mandated by local regulations, an integrity check may be put in place in the recording process of video streams to detect any corruption or manipulation on the collected data potentially used as an evidence.
Standardization Roadmap

Standards are developed by consensus to provide an interoperability environment in response to a common need addressed following a common doctrine. They generate a virtuous circle, when they are required through the calls for tenders with, in response, the solution providers developing their new solutions to comply.

Standards are not focused today specifically on public transport needs; as many different stakeholders with different systems may share a same environment and interact, it may be worth including restrictions in IEC 62676 and develop a dedicated profile; this may in fact be the role of IEC 62580-2 still in development for rail on-board CCTV.

Similarly, amendments to ISO 22311 based on the lessons learned in the first implementations must be introduced, like consideration given to the standard events model. ISO 22311 will most probably be as well the base of a standard for minimum requirements allowing hand-over from operators to authorities in crisis situations (sponsored by the newly created ISO TC292).

Figure 7: Video transmission from on-board in Bucharest

Figure 8: ISO 22311 player playing consistently Paris RATP & SNCF videos
5. CBRN-E Response

Chemical, Biological, Radiological, Nuclear, and Explosive (CBRN-E) threats may inflict damage to the physical infrastructure of the public transport operators and harm human beings. The public transport environment generally has a highly congested infrastructure (e.g. metro line carriages, platforms, station buildings). Blast wave reflection and focusing, and the build-up of an internal overpressure in confined spaces due to the expanding detonation products, intensify the impact as compared to more open environments.

Addressing such threats is generally more in the duties of the authorities than a responsibility of Public Transport Operators, but Project experts noted that simple precaution measures like transparent waste bins, small opening and regular servicing are measures that can be taken by the PTO itself. Their functionality clearly depends on factual disposal of the explosive device inside the waste bin by the terrorist. An open top chamber shields the public in an all-round horizontal plane as it directs the blast and fragmentation upwards. Blast mitigation is expected to be limited to the immediate vicinity of the bin only. For charges with a mass of several hundred grams up to approximately one kilogram, this may be sufficient to prevent lethality for people standing next to the bin.

Based on appropriate risk assessment, it is also essential good practice that all relevant stakeholders have already learned how to work together to provide the optimum response to incidents, even if they are low probability, and have prepared and tested decontamination and restoration plans for the identified potential threats. An example process is depicted in Figure 5 below.

Figure 9: CBRN Preparedness process
The SECUR-ED project showed that a number of technologies, provided they are cleared for use in the public, are efficient (although still improvable) and already available to the public authorities and eventually to PTOs to increase the security of urban transportation against CRN-E threats (Biological threats have not been addressed in SECUR-ED).

Due to the high potential impact of a CBRN-E incident, the possibility to detect the threat and implement an immediate response is essential to mitigate the adverse effects. Application of CRN-E sensors may accordingly prevent or reduce the consequences of an incident, while sensor selection and positioning should be based on threat analysis conducted by the CRN-E experts and the security stakeholders.

Current generation CRN-E sensors can be successfully adapted in PT infrastructure. The operational results are good with a low number of false alarms and a high detection rate of the simulant that were used for the tests on site. It confirms that the current technology is already usable, although still improvable. Sensitivity to dust and other environmental conditions may need to be enhanced to ensure durable performance of the sensors in the challenging environment of urban transportation. The capability to detect a very low concentration of substances or vapours (sensitivity) remains limited, but the sensors can already act as a first barrier against CRN-E threats.

Sensor outputs must comply with the format defined in section 3, but as associated information must be displayed to the operator in a way understandable by a non-specialist, a two-level approach is recommended i.e. an alarm and the link to an URL for providing the experts with detailed information.

As the surface to cover in an urban transportation network is huge and the range of the sensors is limited, grids of sensors have to be deployed, therefore multiplying the deployment cost. The cost remains accordingly an issue, which makes this matter more relevant for the Authorities, than for the PTOs; PTOs may nevertheless be called to cooperate at different levels, as per the local regulations.

Figure 10: A TNT detection in Lisbon
6. Telecommunications & Impact of the Mobile Applications

The telecommunication infrastructure and the different information exchange functions it provides nowadays plays a crucial role in the efficiency and resilience of a public transport network. Either to provide real-time traffic management, equipment command and control or to exchange safety signalling information, the telecommunication systems are an intrinsic part of the global public transport reality. Each stakeholder is impacted and the different facets are presented hereafter, taking into account both urban transports and main line rail.

→ Telecommunications in Public Transport Operations

Public Transport Operators, whether they have to design, install, maintain or simply make use of a telecommunication infrastructure, require the technical knowledge of such systems in addition to their primary role as transport operators.

When choosing the telecommunication technology that their transport network will need to support, public transport operators have to combine a large number of different requirements such as national and local regulations, technology availability, reliability, maintainability and overall data transmission performance figures.

The current evolutions in railway telecommunications are now allowing data packets from very different railway systems to use the same data channels. Bandwidth hungry real time surveillance high definition video feeds and safety relevant signalling information will put stringent requirements on the required communication means. The implementation of specific protocols or solutions for quality of service management now allows safety and non-safety relevant data to share the same communication infrastructure.

Whereas bandwidth limitations traditionally limited the use of certain on-board security solutions, telecommunication solutions now have to support the requested information flow. As an example, several tens of megabits of bandwidth could be required to support real time video transmission between one train and the wayside security control centre.

Public Transport Operators should carefully evaluate the following considerations when selecting an appropriate telecommunication technology or request its implementation:

- Coverage: certain telecommunication technologies being better adapted to specific transport network environments (long distance, underground tunnels, bridges and overpasses, etc.);
- Frequency limitations: national or local regulations sometimes limiting the availability of certain frequency ranges (commercial telephony, military exclusive bands, etc.);
- Performance: technological performance figures such as data rate and latency proving to be critical for certain systems or functions;
- Maturity: standardized, enduring and mature technologies providing better long term investments;
- Availability: the proportion of time the telecommunication system remains in a functioning condition dictating its potential use for specific operational functions;
- Reliability: reliable communication equipment simplifying the life cycle management;
- Maintainability: maximizing the telecommunication products’ useful life;
- Total cost of ownership: including the life cycle cost over many years of operation.
Although telecommunication standards, specifications and technologies such as GSM-R, TETRA and Wi-Fi have been broadly adopted in European railway environments, there is a strong possibility that new standards such as LTE will appear in the near future to cope with the need of ever increasing demand for higher data transmission rates.

Regardless of the adoption of dedicated frequency allocations for railway use or dedicated railway radio infrastructures, PTOs will have to maintain their expertise in telecommunication technologies for the upcoming years.

**Telecom Operators**

While LTE has had tremendous success in its expansion across Europe, supported by competitive pricing and infrastructure improvements, the application of LTE in security applications has remained a challenge. Security operators today have higher demands; namely with accessibility of real-time surveillance videos at high (HD) quality. Despite much improved infrastructure over the years, the available upload bandwidth is still commonly limited. Technologies that adapt generated bitrates to the available bandwidth would support this challenge; but these technologies are still in their infancy stage.

Another challenge is the lack of business offers / options from telecom operators that are geared towards the needs of industrial users. While consumers’ needs are focused, the industry typically has greater needs per machine-to-machine (M2M) communications. Beside a competitive price, M2M offers should include:

- Services to handle large subscriptions; including SIM card management and flexible payment options,
- Offerings for fixed IP addresses,
- Security features such as the limitation for access due to IP address filters,
- Services for the encryption of data traffic,
- Quality of Service in LTE.

Based on such services, other vendors could add more services for the management of the equipment on-board public transport vehicles.

**Rail Manufacturers / Civil Suppliers / Technology Suppliers**

The next-generation of railway communication system should support the high availability of the network, and its reliability for vehicle operations at high speeds. In addition, this system is required to efficiently transmit a large amount of data to support various railway services / applications. Traditionally, 802.11 based Wi-Fi solutions were used for Train to Wayside Communication. Due to the lack of high mobility support, Wi-Fi based solutions may not be the best option for certain real-time high throughput demanding security applications. Therefore, it is necessary to investigate alternative technologies which could fulfil the shortcomings of Wi-Fi solution.

The prevalence of wireless infrastructure with multiple Access Points (APs), combined with the use of latency sensitivity application have driven the need for fast handoff when switching from one node to another. The IEEE 802.11 standard introduces large latency during the ‘break-before-make’ handoff process. During this time, the regular Transmission Control Protocol (TCP) assumes packet loss which triggers congestion avoidance mechanism (called Slow-Start), which greatly affects the performance of real-time applications. This performance degradation will be severe when the wireless link is overloaded with many high throughput demanding applications like video...
streaming. Therefore, depending on the needs of an application, it may be necessary to implement some TCP performance improvement techniques like Performance Enhanced Proxy (PEP). Commercial off-the-shelf products using PEP enhancement have proven seamless performance during network handovers in various PROTECTRAIL and SECUR-ED deployments.

Wi-Fi operates in unlicensed ISM band therefore enabling PTOs to operate without needing to request for any approval, but the downside is that this spectrum is also shared by many other users and as a result the system has to be resilient to interference. From this point of view, 5 GHz spectrum has an advantage over 2.4 GHz, by having less congestion. Depending on the country where the system is deployed, only a portion of the 5GHz is available for outdoor use (5.470 – 5.725 GHz in most European countries).

Contrary to Wi-Fi, LTE is designed to support high mobility (around 350 km/h) with very little to no impact on user experience during ‘make-before-break’ handoff. LTE does however require frequency license to operate, and in most cases the license is very expensive; which makes it impractical for PTOs to own and operate the infrastructure independently. Also, the infrastructure cost of setting up a private LTE network is much higher than a Wi-Fi based deployment. This was apparent in PROTECTRAIL, where not only getting a temporary license for LTE was cumbersome, but the infrastructure cost was much higher than a Wi-Fi based deployment.

Even though commercial LTE can satisfy the needs of many security applications, the availability of a consistent wireless coverage is still questionable. This is particularly true for indoor environments, like station platforms or depots. LTE can be reinforced with Wi-Fi infrastructure on weak sections of the alignment to enhance reliability in supporting security application. This deployment approach was used successfully in a number of PROTECTRAIL and SECUR-ED demonstrations.

To be able to meet future traffic demand, 3GPP (the standard governing body for LTE) is considering introducing unlicensed spectrum into LTE (known as LTE-U). The initial focus will likely be on unlicensed 5 GHz spectrum, which co-exists with 5 GHz Wi-Fi spectrum. LTE-U will enable carrier aggregation operation to aggregate a primary cell using licensed spectrum, and secondary cell using unlicensed spectrum. In addition to 5 GHz spectrum, TV white space is also being considered for LTE-U.

UIC has launched the “Future Railway Mobile Telecommunication System (FRTMS)” project, focusing mainly on identifying suitable candidate technologies like LTE for railways to use after the obsolescence of GSM-R. This group has closely worked with 3GPP on bringing some of the key voice features from GSM-R into next LTE release 13. In addition to this, there are some commercial deployments where LTE is tapped into existing TETRA band (400 MHz). All these initiatives show that in the near future main line PTOs can combine both voice and other data into a single wireless infrastructure and therefore reducing the infrastructure and operational cost. Urban rail has developed a specific approach and initiative (Spectrum User Group), through which its specific needs have been identified and shared by the relevant PTOs and manufacturers.

LTE will spur the development of more advanced vital and non-vital application developments in the near future as it is already doing with Wi-Fi solutions.
Investment Roadmap to address Eminent Needs

The landscape of security technologies in the public transportation domain has evolved over the last years and continually grows. Main characteristics of changes pertain to a paradigm shift in technology development being much more driven by consumer demand leading to a digital convergence – previously separate technologies such as voice, data, and video now share resources; and interact with each other synergistically.

Hence it is essential to implement a new mind-set for the planning, the operation and the maintenance of security systems. First of all, the communications backbone needs to accommodate many different services and this can only be done on the basis of an IP-based system. While in the past dedicated networks existed for telephony, CCTV, passenger information, and public address systems; in modern mainline rail systems, all these services will be taking advantage of more common infrastructures. That means that it is necessary to take a holistic approach on the communications infrastructure when it is time to update the system. It is of utmost importance to first define an overall goal that suits future communications needs and then plan the transition from legacy to IP-based communications systems based on a thorough analysis of the existing infrastructure. For instance, it is often possible to re-use existing cabling to reduce installation costs when updating the system. So while some legacy infrastructure may be kept, it is crucial to have a clear transition path to modern infrastructure because when legacy infrastructure does not support new technologies, it can lead to much higher costs for maintenance and for a later phase out.

It is also very important to understand that it is cheaper and more efficient to update the communications network regularly. Many advantages in applying IT lifecycle management techniques can be reaped. Keeping the network infrastructure up-to-date enables high compatibility with modern technologies. Costs are also distributed more evenly over time and the risk of getting stuck with outdated equipment that is difficult and expensive to maintain is reduced.

The technical specifications of communications network for the rolling stock and wayside infrastructures of public transport systems require much greater consideration; especially from having much of the technologies of today and tomorrow requiring a (greater) level of interconnectivity. Major considerations should not only be placed on the required bandwidth of today, but to build-in a level of future-proofing. It might not be necessary to accommodate for all the required bandwidth for the foreseeable future but measures should be taken to allow for scalability and flexibility.

To support modern technologies in public transportation systems, legacy systems must plan migrations to an IP-based common infrastructure and also apply greater consideration into how the IT infrastructure shall be set up and maintained. Such considerations will support greater system longevity with a communications backbone that is scalable, flexible and less expensive.
7. Cyber-Resilience

Urban public transportation systems usually require embedded systems and several form of control systems to manage dynamic physical processes. In the past these systems were highly isolated with no outside connections (air gapped networks), and were implemented with proprietary control and communication technologies. Although in recent past the emergence of highly sophisticated attacks has repeatedly demonstrated the possibility to circumvent air gapped systems, some PTOs still rely on isolation as the main way to protect themselves.

With the development and dissemination of new concepts and modern ICT technology, new systems and technologies are being introduced into PTOs infrastructure, and often connected with legacy systems, to increase PTOs efficiency and effectiveness in transporting passengers in an increasingly competitive environment. This results in an increase of the dependency on information systems and technology to assist and optimize operations, and consequently in an increasing need to urgently address the issue of protection of PTOs cyber infrastructure.

SECUR-ED found that the strategy commonly used by PTOs to handle cybersecurity (as it is commonplace in many organizations) tends to set apart the physical/infrastructural security from the information/cybersecurity. While this might not have been critical in the past, it will have a significant impact in PTOs in the future, in particular if one considers a cybersecurity incident that crosses safety or security (of passengers and assets) domains.

To address the topic SECUR-ED (Figure 11) started by analysing existent standards, frameworks, policies and technologies to establish the state of the art. A set of indispensable PTO specific procedures and best practices were developed, together with a risk assessment model. Applicable Cyber defence technologies were identified and a PTO-specific Intrusion Detection System (BPIDS) was developed and demonstrated.

SECUR-ED cyber-capacities were demonstrated in Paris and Lisbon in a live PTO environment where cyber-attacks were part of a set of broader security threats.
Finally the Cybersecurity roadmap for PTOs (public document ref. SCR-WP35-T-THA-031) was produced to guide PTOs in implementing a cybersecurity program as well as to share lessons learned from SECUR-ED.

The roadmap starts by clarifying the connection between safety, security and cybersecurity and identifying disruptive concepts/technologies (such as Industry 4.0, predictive maintenance & big data, Automated Train Control systems, etc.) that are already present and will impact PTOs in the future and thus may affect PTOs security.

-risk management-
While cyber risks have been traditionally managed separately from other security risks, given the increasing importance of the cyber component in PTOs operations, as previously stated, SECUR-ED concludes there is an urgent need to shift into an integrated and holistic cyber risk management approach.

The roadmap addresses how cyber security fits in the overall risk management strategy of a PTO, how does it relate with Urban Transport Risk Management, namely addressing the interaction between safety, security and cyber risks (Figure 12) and references possible risk management approaches that may be suitable for different size/type PTOs.

-reference frameworks, standards and regulation-
Taking into account the increased exposure to cyber threats due to IT proliferation and new technologies, it is recommended to establish an architecture framework to outline the technologies used in transport infrastructure, as well as their integration and interdependencies.

The roadmap describes a comprehensive framework of assets, architectures and technologies used by a PTO taking into account the different types of transport operated by PTOs as well as the cases where the mainline transport operator is not the infrastructure owner/operator (as defined in the 4th Railway Package from the EU commission).
For the rail/metro domain it addresses on-board, wayside, station and OCC systems and networks. Energy distribution automation systems, train control and automatic operation systems and computer-based train control are also analysed.

Specific architecture frameworks for bus transportation including on-board (e.g. on-vehicle controllers, automated vehicle management system, etc.) and back-office systems are also reviewed in the roadmap.

Finally, generic frameworks for systems common to most of PTOs such as Passenger Information Systems, Ticketing and Surveillance (including video, intrusion detection and access control) are analysed.

To provide a systematic way to address information security, sector associations and standardization bodies have developed a set of standards. These systematic views have the advantage of providing a common language between different market operators, as well as providing standardized strategies to validate the efforts of each entity towards information security.

It is thus of significant importance for PTOs to be familiar with the security-related standards, best practices and industry-accepted recommendations existing in each of the technological domains they work with, given that these references may be of significant importance when considering the definition, implementation and improvement of their cybersecurity programmes.

The analysis of the existing standards, best-practices and recommendations builds upon the architectural framework, posing as a reference to improve the security of those systems, by pinpointing the standards that might be used to address the specificities of each system domain. The roadmap standards and recommendations analysis is divided in three classes:

- Energy distribution and automation control (EDAC) systems – systems that handle the distribution, automation and control of the energy throughout the transport network;
- Industrial automation and control systems (IACS) – systems that handle the control and automation of the transport infrastructure, namely the automated control and interaction with the station, wayside and on-board systems;
- Information technology (IT) systems – general IT systems.

Besides ISO, IEEE and IEC standards, national and international agencies recommendations are addressed, as well as European level regulation in the field of privacy and protection against cyber-attacks.

Organizational Impact and Procurement

For many PTO organisations, cybersecurity requirements are not yet addressed in requests for proposals for new projects or legacy systems even though urban public transportation is experiencing a big transformation due essentially to new regulations at the European level and massive use of IP-based technologies. The lack of cybersecurity knowledge (competencies) and awareness, as well as cost reductions in particular for infrastructures, have not allowed for the transformation of organisations in order to cope with cybersecurity requirements, implementation and operations. The roadmap addresses cybersecurity organizational impact and its relation with organizational maturity level.

To introduce security into new systems from early design stages, and to enable its maintenance throughout the system’s lifecycle, PTO organizations must establish security requirements in the procurement processes of new
systems, ensure these requirements are fulfilled in the systems acquired, and manage the risks associated with the system’s supply chain. Guidelines for addressing cybersecurity in systems/services procurement, including outsourcing and cloud, are identified in the roadmap.

Implementation Approach

Either if we consider PTO organizations that already have well established security practices, or PTO organizations which have not reached such security development level, there is a set of security recommendations, in the form of security strategies, measures and controls, which might be considered absolutely essential to adequately increase the security of the PTOs IT environment.

The implementation of those recommendations should take into consideration the size and nature of the PTO organization, to better suit them to the specific environment. Taking into consideration the information security management system (ISMS) functions and process stages that must be implemented to operationalize an ISMS, and also the industry standards, best-practices and recommendations presented, it is possible to define a preliminary approach to the implementation of such a program, as depicted in Figure 13. This should thus be used as a discussion starting point towards an implementation of that perfectly suits the environment and operational constraints of each particular PTO.

Besides this first implementation steps, the roadmap provides recommendations on measures and controls for gradually addressing the assessed risks.
Future Directions

The cyber security threat landscape is evolving faster than ever, making it difficult for PTOs to keep their infrastructure, procedures and policies up-to-date to face the arising threats.

Awareness about the current cyber threats in public transportation systems is not sufficiently widespread, making awareness programmes for PTOs an urgent necessity. Awareness is needed at Management, Operations and Suppliers levels.

The particular nature of potential threats combining security, safety and cyber security very specific to a PTO is still an impediment for cooperation between departments.

Development of a holistic risk assessment/management view for each PTO is required to drive radical changes and provide foundations to bring new skills needed to overcome cybersecurity threats.

Due to the highly heterogeneous nature of technologies in use within a PTO, there are several security frameworks, standards and guidelines that may be applicable to different parts of the PTO infrastructure, allowing the PTO to give the first steps on implementing a cybersecurity program. Nevertheless, those standards often overlap, contradict or leave gaps and were not designed in a holistic way having the public transportation business and its unique combination of threats in mind. Based on the new nature of the systems, the development of a PTO specific security/safety framework cannot avoid considering the cyber security component, including:

- Certification processes for human resources;
- Consolidated risk assessment and management strategies;
- Advice on the design and implementation of cybersecurity solutions;
- Certification processes for products/systems to resist particular threats or combination of threats and to provide levels of assurance for dedicated cybersecurity functions.

Several national authorities consider that regulation is of utmost importance to guarantee the security of European public transportation. EU experts (DG CNECT) already recommend that regulations address mandatory cybersecurity standards, certifications and guidelines for critical infrastructures including public transports, with mandatory periodic auditing and security testing, as well as incorporation of cybersecurity supervision capacities in existing local supervision bodies.

To assess, monitor and compare the implementation of measures by PTOs and member states, a common generic measurement tool (i.e. a cybersecurity capability maturity model that covers technology, regulatory, educational and operational dimensions) will need to be developed.

To support PTOs, further development of new technologies affiliated to cyber resilience is required to face the continuous increase of attacks and the specific nature of pre-defined data flows in many instances of industrial and, transport and energy automation systems.
8. Methodologies and Ethical Conduct

Being a Demonstration Project, with a number of experimentations embedded in the operational urban transport system of ten different cities in Europe, SECUR-ED, although setting-up experimental solutions, has also some attributes of an operational project. As such, some of the lessons learned may be used by PTOs as means of conducting their security activities and future operational security projects.

**Lessons of SECUR-ED Governance**

Without any order of priority, the following recommendations must be considered:

- Plan programs to keep staff at all levels in the organization aware and trained (including refreshment training) on basic security threats and responses.
- In the technical domain, organize knowledge preservation or transfer to ensure that there is an intimate knowledge in the organization of all legacy systems, which may contain some data processing function, as they may be the entry point for a cyber-intrusion.
- And for a consistent future, develop a medium/long-term data management plan, with core architectures, in which the security solutions will find their place.
- Base any new security management decision on a comprehensive (i.e. including the emerging threats like cyber or impact of mobile applications) risk assessment and review regularly the previous ones.
- Take advantage of such risk assessment sessions to exchange with the local security stakeholders beyond the routine procedures.
- Establish an internal (or dedicated external, if more appropriate) ethics and privacy referent, knowledgeable of the main principles as well as of both the local/national and EU regulations, accessible even for minor advice.

**Ethics and Privacy**

Any future research or operational project must rely on the core values, developed and clarified throughout the lifetime of the project, summarizing in:

- Respect the legal provisions, including those concerning privacy and personal data protection,
- Maintain respect for the autonomy and dignity of persons,
- Ensure that any value for and/or any threat to society is identified,
- Guarantee socially responsible activity, and
- Demonstrate the maximized benefits while minimizing any potential for harm to society in general and to the travelling public in particular.

As mentioned above, to ensure practically the implementation of these values, the first key step is the presence in the PT organization of a privacy referent, possessing and being able to deliver comprehensive and up-to-date knowledge of regulations. In the case of very complex projects, especially if covering several countries, the set-up of an independent group of privacy & ethics experts needs to be taken into account. Last but not least, the relevant National/regional Data Protection Authorities need to be informed (and their subsequent decision respected) whenever such projects are being implemented.
This aspect has been underlined time and again in SECUR-ED, where partners have noted the differences between ‘best practices’, socially acceptable actions/measures, the ‘unwritten rules’ and the existing legal requirements. Addressing all these and finding the right balance was and still remains a challenge for such activities. These all need expert interpretation, particularly in the case of complex projects, running in several EU states and drawing upon partners in a range of different industries and in public and private bodies.

It must be taken into account the fact that the societal impact of security measures is very broad and does not fall under the prescriptions of any law, thus finding accurate ‘social indicators’ makes it difficult to quickly ‘measure’ (especially *ex-ante*) the outcomes.

Passengers need to be secure and feel secure. However, there is also the market and image aspect to such changes. If the public agrees with the project and the potential outcomes in real-life, public transport will still be attractive to them. But in case there is a backlash of such activities – e.g. people not agreeing to more intrusive security measures, or people feeling less secure precisely because of enhanced security measures – the result will be that the PT usage will decrease, leading to bad publicity and less revenue for both operators and industrial partners. The assessment of societal impact remains a complex task within any project. Professional expertise in societal impact assessment is a field that still requires development and is linked to evidence-based policy making.

Following the experience of the SECUR-ED project experts have come up with a useful tool designed to check the legal and ethical issues and boundaries of such exercises – an ethical checklist that enables the operator to steer the security-related developments based on an ethical approach. Furthermore, the SECUR-ED experts suggested that a set of ethical best practices (a voluntary code of conduct) in the field of public transport should be created. Such “codes” have been proposed and established in other fields of endeavour (nanotechnology, genetics, sustainability, etc.). Public transport is as vital to the future of society as any of these fields. Consequently, the public, the industry and PTOs alike have a great deal to gain from the establishment and promotion of an ethically informed philosophy of “good practice”.

---

**Figure 14:** Security staff in Bilbao
9. Way Forward

While the SECUR-ED project comes to a close, the spirit of innovation and growth in the public transportation sector carries on. The community of experts that this project has graciously gathered will be extending discussions and carrying over activities to continue building on accomplishments of SECUR-ED. Some of the results and conclusions drawn from SECUR-ED have already supported developments and further considerations with standards bodies (e.g. IEC, ISO).

Contributions to Standardization Activities

The following standardization activities have been identified as crucial to support accelerated growth and innovation in the Transportation sector:

- A minimum format standard for security events is to be initiated in CEN TC391 within the EC mandate M487.
- Standard mapping format of underground and 3D infrastructures to be initiated through ISO Geographical groups.
- Discussions on CCTV standards will continue on IEC 62676 (TC79) and ISO 22311 (TC292), with a special focus on a dedicated public transport profile, metadata and interoperability with operators for crisis management.
- Contributions to the rail on-board standards (IEC TC9) will continue, with contributions to IEC 62580-1 and IEC 62580-2 (on-board CCTV).

Future Research Topics

The following items have been identified for future research:

- Optimized management of unattended objects.
- Crisis passenger information doctrine (in an environment of mobile-equipped communities) and additional uses of (passenger) mobile applications to support security and operations.
- Response to multimedia reporting of security events.
- Geo-location tools for underground infrastructures.
- Pattern similarity detection in video.
- Integrated and scalable training approach using simulations & mobile applications to train staff in support of reducing the need of dedicated in-person training.
- “Safety and security together” (network shared, infrastructure shared, etc.).
- Cyber security and cyber resilience in PT
- Enhanced cooperation between PTOs and LEFRs in the case of prevention, security incidents, safety aspects, etc.

Continued Implementation & Dissemination

Exploitation of the results will rely on the community of partners involved in this project, as well as the readers to this White Paper.

As indicated above, one of the most future-proof methods of exploitation is through actively pursuing the standardization activities through the respective national bodies and as soon as standards are promulgated, it may...
be worth considering, pending consensus of all parties involved, their endorsement in regulations and in the procurements for future systems. Knowledge sharing is one of the most critical elements in supporting an evolution in mobility. The partners of this consortium shall serve as ambassadors of SECUR-ED, continuing to educate and share the valuable results out of this project to support the growth and prosperity of the Public Transport and Security domains.

Should you have any questions or would like to learn more on any particular subject matter, please post them on the community site of the PROTECTRAIL and SECUR-ED Alumni¹ and experts will come back to you.

Seeds sowed will germinate anyway!

¹ Pending final site set-up, instructions are to be found on the SECUR-ED website (www.secur-ed.eu)
Contact SECUR-ED:

Project Coordinator: THALES
yves.perreal@thalesgroup.com

Visit us:
www.secur-ed.eu

SECUR-ED Facts:

Full name: Secured Urban Transport – European Demonstration
Nature of the project: FP7 Security Project
Total budget: EUR 40 million
Number of partners: 41
Start date: March 2011
End Date: September 2014