Secure Public Transport in a Changeable World

Security and Safety
Security is a relatively new challenge in the context of public transport. Security addresses problems caused intentionally. This differs from safety which addresses problems caused accidentally. The UITP Security Commission is made up of public transport security practitioners and offers support to UITP members on security matters. Its role is to collect and disseminate knowledge, experience and best practices on urban public transport security. It proposes UITP’s positions and priorities on security vis-a-vis other stakeholders and partners.

Security Threats
Security problems, or threats, are caused by people whose actions aim to undermine or disrupt the public transport system and/or to harm passengers or staff. They range from daily operational security problems, such as disorder, vandalism and assault, to the terrorist threat.

Security is key to an attractive service
Any public transport operator has a responsibility for and a vested interest in protecting its customers, staff and assets, as well as the reputation of the network – passengers who feel insecure may choose not to use the system. It is well known that public transport is increasingly important for urban areas to prosper in the face of challenges such as reducing congestion and pollution, and coping with changing urban density and social inclusion. Security therefore plays an important role in helping public transport to become the mode of choice for today’s citizens. Reaching excellence in security is therefore a prerequisite for UITP’s ambitions of doubling public transport market share by 2025.

Investing in appropriate security measures can potentially bring economic benefits. On top of helping to increase ridership thanks to a more attractive service, money can be saved on costs such as repairs of vandalised assets. For example, the Hamburger Hochbahn invested in a surveillance system inside metro cars and noted nearly a 50% drop in graffiti and vandalism, which was costing millions every year in repairs. Reassurance measures can also help to re-establish service after a major incident, reducing the financial impact.

In such an event, the operator can demonstrate that serious efforts have been made to protect passengers and staff. A positive image is key for the attractiveness of the system. In some circumstances, passengers can feel insecure, and this is sometimes reinforced by intensive media coverage of single events. However, this perception is often inconsistent with reality. You are ten times more likely to be involved in a fatal incident travelling by car than by public transport, whatever the cause of the incident.

Public transport is open, easily accessible without reservation, and used by millions of people every day. These characteristics are central to the efficiency of public transport and in turn the efficiency of modern urban society.

2 CCTV: a tool to support public transport security, UITP 2010
3 Terrorism, Transit and Public Safety: Evaluating the Risks, Todd Litman, Victoria Transport Policy Institute, 2005
Any security measure which is put in place must respect these prerequisites and be proportionate to the risk.

CUSTOMER SERVICE

Security is a customer expectation and investing in the customer experience makes the system more attractive and gives passengers confidence to use it. Accurate and prompt information given on the network, together with staff presence, helps to fulfil this expectation and is key to maintaining confidence among staff and passengers. Keeping the network clean and well maintained with a proactive approach to reducing crime and vandalism also reassures passengers that the space is being managed and looked after. Safety and security are “taken for granted” attributes of any transport “lifestyle service”.

Good customer service makes for good security. It fosters awareness among staff to address security threats, and improves the perception of security among passengers. Such a customer service approach requires security to be embedded in the corporate structure and culture of the organisation. Security must be a priority from top management level down to front and back office workers.

THREE ‘PILLARS’ OF SECURITY

In order to respond to security threats, operators need a concise and integrated security concept based on risk assessment, adapted to the local situation and integrating a suitable set of security measures. A variety of possible security layers exists, which can be grouped into three interlinked ‘pillars’ (see Figure 1):

- the H(uman) factor;
- Procedures;
- Technology.

The H Factor

Staff engaging with the passenger creates a sense of reassurance which cannot fully be achieved by technology. Customers want interaction with real people, either directly or through technological devices. Similarly, only staff can provide direct help during incidents. For the H Factor to be most effective, staff must be qualified, trained, well-equipped and motivated: Train them, drill them, test them - there is no security without preparation!

Procedures

The organisation of security should be clear and consistent, including clear lines for alarm, command and control. A security risk assessment is the first step in understanding security needs and prioritising resources. Together with ongoing observation of incidents, the most appropriate security measures can be identified, with the flexibility to constantly adapt to changing situations. Security incidents, especially major ones, often happen without warning: emergency and contingency plans must be developed, communicated and drilled in advance in cooperation with all relevant partners.

Technology

Many technologies can be used to enhance security, for example surveillance systems. Proactive use of public address systems and help points demonstrate to customers that there is a human intervention which gives them more confidence. Security by design concepts such as good lighting and clear lines of sight have also been proven as effective.

The full potential for technology is huge but can only be realised with procedures and trained staff in place behind it. Machines can never fully replace humans and they will always be managed by staff, but they can help spread human resources more efficiently.

No one security measure is enough; it is the balance of security layers from these pillars which can have the best effects.

THREE PHASES OF SECURITY

Security can be considered in three distinct phases (see Figure 2):

Prevention

Measures which can prevent a security incident from taking place. By conducting a risk assessment and gathering intelligence, operators can identify which kinds of security incidents could be prevented. Prevention begins with the daily operational security problems: uncared for, dirty, damaged property is a breeding ground for more serious crime. Prevention also requires linkage with external partners.

---

5 Training courses and COUNTERACT Guidelines on conducting security risk assessment in public transport available from UITP: www.uitp.org/public-transport/security
Preparedness & Response

Even with preventive measures in place, 100% security is impossible. Therefore plans must be prepared to respond to incidents, mitigate the impact, train staff accordingly and carry out exercises. The results of the risk assessment give a basis for such plans. These procedures must swing into action immediately and have to be constantly adapted. They must be agreed and practiced with partners and authorities in advance. Staff training is essential.

Recovery

Procedures are essential for the quick recovery of normal service after an incident. Recovery is important for the financial health of the operation, but it also sends a clear message: it reassures passengers and gives them confidence to continue using the system. It also communicates to the perpetrators that their actions have a minimal disruptive effect.

Communication is key in the recovery phase and involves giving timely information to all relevant partners.

Recovery should also include an evaluation process for lessons learned, which feed back into the cycle of prevention, preparedness and response.

RESPONSIBILITIES AND PARTNERSHIPS

Security in public transport is a shared responsibility and requires clear governance. Responsibilities should be clearly defined and partnerships fostered for a holistic and consistent approach, including the financial aspect: who pays for what. Partners can include other public transport operators, law enforcement, various authorities, justice departments, political parties, neighbourhood and civil rights organisations, private security companies, the media, owners of shops and restaurants in and around the network, as well as passengers themselves. By taking a partnership approach, there is greater chance of success.

Implementing tailored public awareness campaigns and educating school children to behave correctly and respect the network are proven methods to reduce crime and anti-social behaviour. It also shares ownership of the problem with society.

A regular and ongoing exchange between relevant partners is necessary. Agreements or contracts describing the roles and responsibilities of each are helpful, and security measures should be discussed and agreed upon before implementation. All relevant partners should be involved when conducting a security risk assessment, and a two-way exchange on relevant intelligence with the authorities is vital.

A positive partnership with the media can help to reassure passengers and staff and increase confidence, especially during critical times.

Think outside the box - fostering relations with different partners takes creativity and effort, but the results can be substantial.

TECHNICAL NEEDS

As described above, technologies play an important role in public transport security and developments in this field are promising. A better dialogue should be established between the operators and the manufacturing industry to improve developments. Technological innovation should be based on the defined needs of operators, which are themselves based on risk assessment and experience. This will result in affordable technologies which are better suited to the open and accessible nature of the public transport environment.

Technologies are not stand-alone solutions and are more useful when they are multi-functional and integrated into existing solutions: operators need technologies for general operation, not just for security. Systems have long term lifecycles, and the cost of maintenance procedures must also be taken into account. These long-term investments must be planned very accurately by the operator with its suppliers.

The UITP Security Commission offers a dialogue to the manufacturing industry to improve technological innovation and development.

---

7 COUNTERACT guidelines for conducting public awareness campaigns available from UITP: www.uitp.org/public-transport/security
REGULATION

Any standardisation or regulation in public transport security should endeavour to support public transport achieve its core business and allow for local laws, culture and circumstances to be taken into account. Operators could envisage voluntary standards on technical applications in order for off-the-shelf technologies to become more suitable and affordable. However, operators could not accept standards which impose specific operational or procedural compliance, have the potential to be disproportionate to the risks, or result in an unreasonable economic burden.

There is increasing pressure to regulate security within public transport at the European level. UITP strongly believes that urban public transport is and should remain under the responsibility of the local authorities and favours the voluntary sharing of best practices through forums like the UITP Security Commission. There is no one-size-fits-all approach possible and the security threat level is not uniform throughout European member states.

CONCLUSIONS

There is no silver bullet to prevent security threats, but a lot can be done to mitigate the risks and impact of incidents. However, any measure put in place should be proportionate to the risk and should have a limited impact on the accessibility and efficiency of public transport, which are essential elements for its success.

Public transport remains one of the safest ways to travel and indeed has a central role in the well-being of society: a modal shift to public transport can reduce road-traffic accidents, and public transport is central to modern urban society, as described in the UITP Strategy. For public transport to be the mode of choice for citizens, citizens must feel safe and secure throughout their journey.

Security should therefore be seen as an investment to achieve this and an important element of customer service, balancing humans, technologies and procedures to reduce crime and the fear of crime on public transport.

RECOMMENDATIONS

- **Make security a corporate priority**
  Security must be embedded in the corporate structure and culture of the organisation.

- **Consider security as an investment, not a burden**
  Investing in security can strengthen the attractiveness of the service, helping to increase ridership, and potentially save money.

- **Conduct a security risk assessment**
  Guidelines for conducting a security risk assessment are available from UITP. It is the vital first step for a structured, clear and proportionate approach to security.

- **Be prepared!**
  No-one is immune to security threats, but good preparation can minimise the risk and the impact – and maximise the potential to respond.

- **Focus on the H Factor**
  Invest in the right staff for the right roles, and ensure a balanced approach between humans, procedures and technologies. Train them, drill them, test them!

- **Make security an integral part of customer service**
  Engaging with customers and providing information and a clean, well maintained environment gives customers confidence to use the system.

- **Foster relationships with partners**
  Security is a shared responsibility, and roles and relationships must be clearly defined. Partners should practice together regularly.

This Focus Paper has been prepared by the UITP Security Commission and approved by the UITP Policy Board.

Downloadable in EN, FR, DE, ES at www.uitp.org