2 Security Measures and Their Perception in Critical Infrastructure Context

Since the 9/11 terrorist attacks, public and political awareness of security has been a major concern. Providers of critical infrastructure have worked to fortify potential targets and protect critical gates, even in the area of public transportation. Attacks in Madrid (2004) and London (2005) emphasized this development and showed that there is still a certain level of vulnerability in public transportation systems.

According to Carnegie et al. (2010), the evolution of public safety and security concerns in the public transit industry over the last three decades can be traced in the literature. In fact, there is a thematic cut: while the literature during the 1980s and 1990s on transit security focused almost entirely on protecting transit passengers, personnel, and facilities from ordinary criminal activities, the primary focus has shifted to terrorism and similar threats since 2001. Many guidelines have been published by (governmental) organizations e.g., the U.S. Federal Transit Administration, the Association of German Transport Companies (Burkhard et al. 2008), and the German Federal Ministry of the Interior (Bundesministerium des Innern 2005). Academic publications are limited because of the scarcity of available information on security initiatives (Carnegie et al. 2010).

This section presents a review of the literature on the impact of terrorist attacks on public transportation systems as well as the challenge of preventing harmful attacks and the possibilities available to secure this critical infrastructure. Furthermore, it discusses the perception of security on customer levels and how effects of security measures are investigated in different disciplines.

2.1 Security and Its Research Players

Security can be defined as the product of human action and behavior—something that has to be produced and ensured. In general discussions about national security or internal security, all efforts come down to security measures (Nagenborg 2011). The main intention of these measures is to protect people, objects, and the

F. Brauner, *Securing Public Transportation Systems*,
DOI 10.1007/978-3-658-15306-9_2

environment from intentionally produced harm. Such discussions focus on the attackers, their reasons, the vulnerability of the company or critical structure, and potential damages that might occur because of an attack. In this context, decision-makers use countermeasures and preventive security measures to improve the level of security, but this is just one aspect of the effects of security measures. Decision-makers using risk management systems often neglect the subjective effects of hazards and countermeasures. The subjective side of security deals with human perception. Decision-makers often neglect this aspect when attempting to improve the security situation in their company because it is abstract and difficult to measure. Many scientists of different disciplines have discussed how people perceive security in daily life, the way threats work and how they affect individuals and societies, how individual security measures work, and what level of security is appropriate and not liberticidal (as George Orwell illustrated in his book "1984"). The importance of security perception is obvious. A satisfactory perception of security is a basic human need (Cömertpay et al. 2007) although the influencing mechanisms are almost incomprehensible. The balance between technical security solutions and perceived security by end-users often are mismatched because of different influencing factors (Köhn and Bornewasser 2012). This can cause inappropriate costs for decision-makers as well as a loss of customers.

Currently, security research programs such as the German Civil Security Research Programme of the Federal Ministry of Education and Research (BMBF) convey societal effects of research, specifically the increasing permeation of technology in society (2012). In particular, the effect of new technology on society is part of this research. New threats such as terrorism, natural disasters, pandemics, and increasing vulnerability of critical infrastructure require a high level of prevention and/or interoperability of actors connected with technology solutions. To obtain sustained comprehension, there must be a dialogue between all stakeholders such as the government, economy representatives, and community members to achieve a high level of security (BMBF 2013b). This *high-level security solution* shall protect the democratic values of society. Often, security measures by themselves cannot provide a high level of security (e.g., full-body scanners at airport security gates). *Acceptance* by society and its implications thus becomes an important aspect. The development of new security concepts requires a multi-dimensional approach, including different disciplines such as *engineering*, *natural sciences*, and *social sciences*.

One possible solution is the multi-directional approach taken by the BMBF. According to this approach, there are two directions—horizontal and vertical. The horizontal direction comprises engineering and natural sciences that are fused together with humanities and social sciences by dialogue. As a result, technical solutions are discussed from the point of view of social questions and social ef-

fects. The vertical direction consists of the economy, stakeholders, and users (e.g., operating companies or providers, critical infrastructure, and public authorities). This group discusses the impact of technical solutions on the behavior of the public and personal rights. Both directions convey the social aspect and the impact of research on the society as part of security improvement.

2.2 The Vulnerability of Public Transportation

"Public transport systems are even safer than air travel, yet the feeling of insecurity is often greater"
(Dunmore 2010:10).

Today, critical infrastructure can be defined as "[…] assets, systems, and networks, whether physical or virtual, so vital […] that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (Department of Homeland Security 2013).

Public transportation faces different security problems and threats. Since 9/11, threats have included arson, explosives, weapons of mass destruction, sabotage, network failure, cyber-attacks, disruption of power, use of a transit vehicle as a weapon or weapon delivery mechanism, and hostage-taking. Staes et al. (2006) examined terrorist attacks against transit and concluded that 32% occurred on busses, 26% occurred on subways and trains, 12% occurred in train stations, and 7% occurred in bus terminals (Carnegie et al. 2010). Public transportation is an ideal target for terrorist threats because numerous customers use it, many stations have open access, and its use is impersonal. While air travel is a closed system with defined security controls at the input and output stream, public transportation is an open system based on the mobility of a maximum number of passengers. An impersonalized ticket allows criminals to enter a complex network with many possibilities to hide and perform harmful actions (Rhode 2012). Providers have an overview of neither the total number of customers nor their names or their exact localization. These specific factors complicate a standardization of a certain security level.

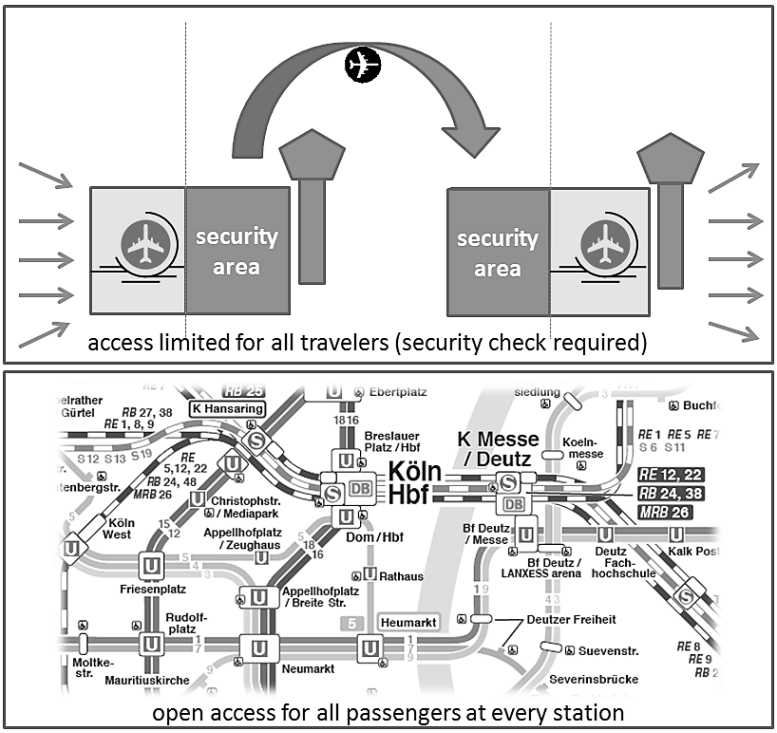

Figure 1: Closed system (airport on the upper side) and open system (KVB on the lower side) (Source: KVB 2015, adapted by author)

A second effect of this open system is the identification of passengers with the system itself. Normally, passengers use public transportation as a system with no control of public space, which causes a certain impersonality and lack of confidence (Dunmore 2010). In air travel, a pilot or a cabin steward is always in charge of taking care of passengers. They are specially trained to stay cool and calm and professionally handle difficult situations to ensure a secure feeling among the passengers. Thus, the value of identification and personification is much higher in air travel. Contrary to this, an impersonal system such as public transportation is much more prone to criminal intent than a closed and controlled system. Graffiti, vandalism, ticket fraud, sexual harassment, or other criminal intentions are problems of public transportation. For example, the cost of graffiti removal on Deutsche Bahn trains and BVG in Berlin amounted to 15.4 million Euros in 2008 (Berliner Morgenpost 2009).

The character of these critical infrastructure and the open system make it a lucrative target for terrorists. The word *terrorism* comes from the Latin origin *terror* and means *fear/scare.* It is an anthropogenic hazard with a high subjective threat component for citizens. An important consideration in the analysis of terrorist attacks is that this phenomenon follows no statistical patterns like natural disasters. "Most estimates of the probability of an event are based on some understanding of their past frequency. Simple applications of this frequency theory of probability can fail spectacularly when the possible event has occurred only rarely or never at all" (Falkenrath 2000:28). Initiated by human beings, it is an action of a decision process, including rational factors, subjective factors, and even reactions to, for example, policy decisions (Spencer 2013).

The following section chronologically discusses some major terrorist attacks on public transportation systems. These may show vulnerability when taking into account the intentional demolition, safety problems caused accidentally are not considered.

- Tokyo (Japan): On March 20, 1995, five members of the Aum-Shinrikyo sect released toxic gas in the subway/metro of Tokyo to avert a planned police raid on the sect's headquarters. During rush-hour traffic on Monday morning around 08:00 am, the five members of Aum-Shinrikyo each carried two plastic bags filled with liquid sarin and released it in different trains by punching the bags with the tip of an umbrella and then leaving the train. The liquid sarin vaporized and spread into the environment. As a result, 12 passengers died and 5,500 passengers were injured.
- Madrid (Spain): During rush hour (7-8 am) on March 11, 2004, 10 bombs exploded in four trains of the Madrid public transportation system. All four trains were travelling on the same route from Alcala de Henares to the Atocha station. The explosions occurred around 7:30 am as the trains were nearing Atocha station. A total of 191 people died and more than 1,800 passengers were wounded. Later, three additional bombs, which had not detonated, were found in the destroyed trains.
- London (United Kingdom): On July 7, 2005 at 08:50 and 09:47 am, four explosions occurred in central London. Three bombs exploded in underground trains around Liverpool Street and Edgware Road and between King's Cross and Russell Square. The last explosion took place an hour later in a double-decker bus in Tavistock Square. As a result, 56 people (including four suicide bombers) died and more than 700 were injured.
- Cologne (Germany): On July 31, 2006, two bombs, each composed of an 11-liter butane gas tank and a 4.5-liter tank of fuel, were hidden in suitcases and carried into two different trains of the Deutsche Bahn at the main station. The bombs had a timed detonator for 2:30 pm; fortunately, the bombs malfunctioned and did not explode. The suitcases were later found by staff

and brought to the lost-and-found office, where they were recognized and securely kept by the police. Using the Closed Circuit Television system (CCTV) of the Cologne main station, the police were able to identify the two assailants and arrested them in Kiel and Tripoli three weeks later.

- Mumbai (India): Several attacks have occurred in the city of Mumbai. In 2003, a bomb exploded in a train next to the Mulund station, killing 10 people and injuring 25. On July 11, 2006, a severe attack with seven bombs killed 209 people and injured over 700 in Bombay. On November 26, 2008, a fatal attack occurred at ten different locations in the city, including the train station at Chhatrapati Shivaji terminus. The group of attackers used explosive devices and guns and took hostages. In this attack, 164 people were killed and over 200 injured (CNN 2013).
- Volgograd (Russia): On December 29 and 30, 2013, two separate suicide attackers killed overall 34 people (including themselves) in two bomb attacks. The first attack took place in the entrance hall of Volgograd station next to a metal detector. The bomb with an equivalent to 10 kilograms of TNT killed 18 people and injured 44 people in the hall. One day later, a second bomb exploded in a trolleybus in Dzerzhinsky district, killing 16 people and injuring 41.
- Thalys-Train (France/Belgium): On August 21, 2015, an Islamic attacker tried to execute a terror attack in a high-speed Thalys-Train travelling from Amsterdam to Paris. Next to Brussels, the attacker pulled two hand weapons and started to shot. Several passengers overpowered the attacker, so that only two passengers were injured.
- Brussels (Belgium): On March 22, 2016, two suicide bombers have blown up in the departure hall at Brussels Airport. Shortly afterwards committed another attacker a suicide attack in the Maelbeek metro station. The attacks killed a total of 32 people.

Discussion about countermeasures that are effective against specific threats (response) focuses mainly on the reduction of probability of harm (prevention) and cost-effectiveness. The Federal Transit Administration (FTA) of the U.S. Department of Transportation recommended in a guideline called the “Public Transportation System Security and Emergency Preparedness Planning Guide” that all public transportation providers undertake a threat and vulnerability assessment based on a series of scenarios. According to the threat level, countermeasures can be specifically chosen.

2.3 Effects of Security Measures: Risk Management Systems

Carnegie et al. (2010) mentioned different ways to classify transit security measures, and the literature provides different classifications of security measures such as *prevention*, *response/mitigation*, and *monitoring* or *deterrence, and detection*, *mitigation*, and *response* (FTA 2003). They can also be classified according to threats against *components* of public transportation (e.g., stations, tunnels, vehicles, and railways). Staes et al. (2006) classified security measures in public transportation in accordance with *threat level* and *purpose* (see Figure 2).

Threat Level	Measures	Purpose
Minimum	- Simple physical barriers - Simple locks	Impede unauthorized external activity
Low	- Basic local alarm system - Simple security lighting - Basic security physical barriers - High security locks	Impede and detect unauthorized external activity
Medium	- Advanced remote alarm system - High security physical barriers - Watchmen - Basic communication	Impede, detect and assess unauthorized external activity
High	- CCTV - Perimeter alarm system - Highly trained armed guards - Access controls - High security lighting - Local law enforcement coordination - Formal contingency plans	Impede, detect and assess unauthorized external and internal activity
Maximum	- Sophisticated alarm system - Onsite armed response force	Impede, detect, assess and neutralize unauthorized external and internal activity

Figure 2: Transit security measures, their purpose and applicability under different threat levels (Source: Carnegie et al. 2010:9 according to Staes et al. 2006)

Depending on system boundaries, security can be measured with objective indicators. For example, statistics on crime, burglary, theft, and vandalism can show certain developments. Measurement of conditions before and after implementation of a security measure allows drawing conclusions about their effects. Several studies are available in the literature.

For example, Welsh et al. (2010) analyzed five studies on the effectiveness of using security guards for formal surveillance. In the first three studies, statistics of car theft in parking lots was used to measure before, during, and after security guard patrols. The studies of Laycock and Austin (1992) and Barclay et al. (1996) indicated numbers of thefts decreased when using security guards, and that the effect can be strengthened by also establishing a media campaign (Bar-

clay et al. 1996) or using additional security measures such as fences (Laycock and Austin 1992). Hesseling's study (1995) also observed a decrease of thefts but observed the same phenomenon in a control area without security guards. In the other two studies on "urban citizen patrols" in 1986 and 1989, the results were quite different. Kenney (1986) compared the crime statistics of 14 monitored subway stations with 14 unmonitored subway stations in New York. He measured a lower rate (2.7%) of criminal acts in monitored stations. Pennell et al. (1986, 1989) compared two urban districts over 30 months and found a burglary decrease of 25% in district A with patrols compared to 15% decrease in the control district B without patrols. In case of violent crime, they also captured decreases of 42% and 22%, but the control district experienced the larger reduction without urban citizen patrols. A later check showed that police officers were patrolling the control district. The results cannot be proven as correct (Welsh et al. 2010). These examples illustrate the difficulties of measuring the effects of security measures in the form of reliable statistical data. This makes it even difficult to transfer the results into risk management systems.

In the case of terrorism, probabilistic statistics are not available. Terror acts are rare events that cannot be statistically captured in reliable probability statements about certain scenarios and target objects. Therefore, research projects such as RiKoV, which measure the risks and costs of terrorist threats in public transportation, attempt to provide new approaches for holistic risk assessment, including analysis of the effects of security measures influencing the risk of terrorist acts (Lechleuthner et al. 2012).

The RiKoV project uses an adapted risk definition following Wilson et al. (2007) that consists of the three parts:

1. The threat (ability and motivation of terrorists)
2. The vulnerability of the system (based on the scenario and structural conditions)
3. The consequences of the attack (in terms of deaths, incidents, material damages, and short and long-term economic losses) (Wilson et al. 2007; Brauner et al. 2013b).

In this context, the different effects of security measures can be considered with a risk management formula. Figure 3 displays the modes of security measures effects. The preventive effect of security measures that attempt to prevent a specific threat is considered as part of the vulnerability. The author defines vulnerability as the strength or weakness of a potentially targeted asset and the protective systems for a specific threat (Brauner et al. 2014b, 2014e). In addition a second definition by Risk Analysis and Management for Critical Asset Protection

(RAMCAP) was used that describes a protective system as all existing capabilities and countermeasures at the asset or facility and their effectiveness (RAMCAP 2006). This includes analysis of preventive security measures, which Kersten and Klett (2008) called *"security measure type 2"*. The other effect (i.e., reducing the consequences of certain events), is called *"security measure type 1"*.

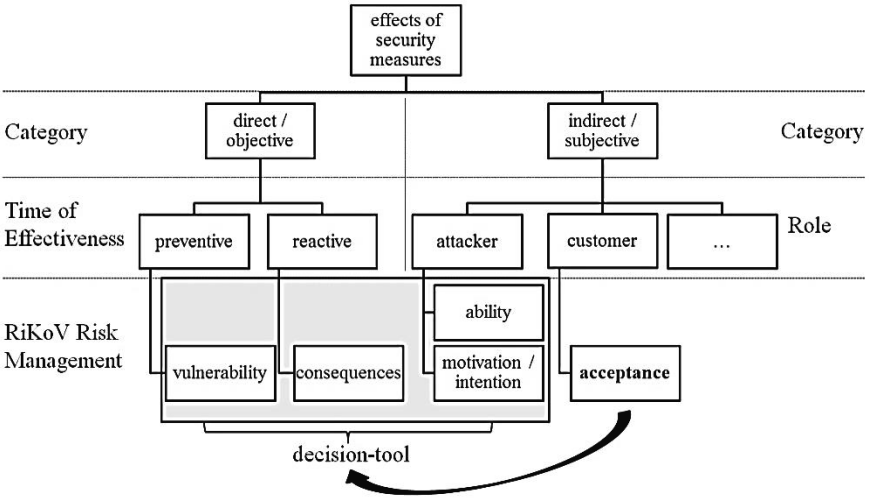

Figure 3: Effects of security measures according to RiKoV modified by author (Source: author according to Brauner et al. 2013a)

The management process does not consider the aspect of customer acceptance although this effect is already an essential part of the implementation decision. Kersten and Klett (2008) described in their book "IT-Security Manager" seven categories that should be considered in the validation process of security measures in IT systems. The categories can also be transferred to other sectors such as critical infrastructure (e.g., public transportation). The first step is testing suitability, which determines whether the security measure is appropriate, meaning it reduces the consequences (type 1) and/or prevents the threat (type 2). In this step, there is no discussion or assessment of the sufficiency of the security measure, but this is part of the second step, which is called an effectiveness check. The security measures should be sufficient according to the type in order to have an effect on the threat or consequence. The third step, which is interaction, assesses security measures regarding their effects on each other. Thus, security measures that influence other measures negatively can be identified. The practicability is the focus of the fourth step. In this step, the different security measures are ranked by their usability and possibility of error. Complex process-

es are more vulnerable, so the less complex a security measure in its context, the higher the practicability. Next, proof of acceptance is measured. The fifth step examines security measures regarding physical interference, unreasonable burden, and social discrimination from the users' point of view. The main part of this step is the assessment of perceived interference by the user rather than the assessment of actual physically interference. The last two steps determine economic efficiency and adequateness. Adequateness is more or less a corrective step that provides the possibility for a final evaluation of the security measure according to the protection demand. The adequateness analysis should avoid under- and overstatements (Kersten and Klett 2008).

According to Kersten and Klett 2008, acceptance analysis is an inherent part of a security measure implementation plan. It is often neglected, the author assumes this is caused by a lack of *easy-to-apply methodologies* as well as the difficulty of data acquisition, therefore this has to be considered in this study (marked in Figure 3).

2.4 Security as Part of Customers' Confidence and Satisfaction

Public transportation depends on customers' confidence and satisfaction. Customer satisfaction generally refers to maintaining customers' convenience and comfort. A lack of confidence leads to the feeling of insecurity and avoidance of public transit, which, in turn, leads to a negative impact on the economy. One approach to win customers' confidence is providing efficient customer services, increasing staff, security controls, and police patrols, or installing technical solutions such as camera systems. All these security measures act as deterrent factors and can prevent crime or harmful actions. However, from another point of view, a high amount of security measures—particularly the presence of police and security personnel—might arouse suspicion and the feeling of insecurity among passengers. In his 2010 article, "*Achieving the Right Balance*", Dunmore analyzed different arguments and claims for a number of measures. In his opinion, motivated, well-trained, and balanced customer service is the key to appropriate customer security perception.

The American Public Transit Association conducted a survey that included 120 public transit agencies to analyze the implementation of security measures post-9/11 (Carnegie et al. 2010). They determined the following: 88% of the agencies had adopted new or expanded existing security measures after 9/11, and 74% had already increased their security level before 9/11. In addition, the survey included an assessment of security needs as shown in Figure 4.

Needs and funding priorities	Very Important	Important
Operating Funding		
Funding Current Transit Agency/Local Law Enforcement Security Personnel	60.8%	17.5%
Funding Additional Transit Agency/Local Law Enforcement Security Personnel	52.9%	27.5%
Funding for Over-Time/Extra Personnel During Heightened Alert Levels	50.5%	29.7%
Creation of New Security Units, e.g., K-9 Teams	14.4%	24.4%
Training for Security Personnel	48.7%	38.1%
Security Training for Other Personnel	45.7%	39.7%
Security Planning Activities	42.6%	44.3%
Joint Transit/Law Enforcement Training	45.7%	36.2%
Customer Outreach	31.0%	40.5%
Access to Security Intelligence Information	34.5%	36.3%
Ongoing Technical Support for Security Plan Development	45.1%	40.7%
Capital Funding		
Automated Vehicle Locator Systems	67.9%	18.8%
Radio Communications Systems	85.7%	10.7%
Passenger-Operator Intercoms	21.6%	43.1%
Security Cameras On-Board Vehicles	72.6%	20.4%
Security Cameras in Stations	75.0%	16.3%
Public Address Systems On-Board Vehicles	42.2%	36.7%
Public Address Systems in Stations	42.4%	38.4%
Security Fencing Around Facilities	54.4%	32.5%
Chemical/Biological/Radiological Detection Devices	19.8%	34.0%
Intrusion Detection Devices	42.1%	33.3%
Controlled Access to Facilities and Secure Areas	71.1%	23.7%

Figure 4: Transit agencies' assessment of security needs (Source: Carnegie et al. 2010:11 according to American Public Transit Association 2004)

Convinced of the idea of a total quality management (continuous improvement process) and security needs, providers still face financial problems in implementing security measures. In Germany, many providers are municipal organizations. This leads to a rearrangement of the customers' role: On one side are passenger demands on the transit provider and on the other side is the municipality's demands on the transit provider. Taxes often supplement financing so that the books balance. In times of increasing costs and tight transit budgets, many transit providers have been forced to focus on the primary objective of maintaining system infrastructure in a state of good repair or managing growing ridership, neglecting security measures (Belyová and Schulze-Bramey 2009).

In 2002, the U.S. Government Accountability Office (GAO) listed insufficient funding as the most significant challenge to secure transit. The objective tricolon of effectiveness, efficiency, and customer satisfaction are linked and

thus decisions regarding implementation of security measures often require trade-offs between these three security-related objectives (Guerrero 2002, Carnegie et al. 2010).

2.5 Security Perception

The security allows two perspectives an *objective/structural* and a *subjective/perception* dimension. Both dimensions *objective* and *subjective security* can have diametrically opposed positions (Meng and Vollbracht 2014; Köhn and Bornewasser 2012). The assumption that a highly effective security measure is always accepted and raises customers' perception of security is false. Furthermore, the statement that the more security measures are implemented, the higher the security perception, is incorrect; there is no positive correlation (Wurtzbacher 2003).

The German research project "Subjektive Sicherheit im ÖPV Test und Evaluation Ausgewählter Maßnahmen" (SuSiTeam) defined *subjective security as a feeling of being secure*. Subjective insecurity is a continuum of feelings and situation assessment that is disturbed or even enhanced by a perceived threat of becoming a potential victim (Hempel et al. 2011).

The absence of fear or a feeling of safety is a basic need according to Maslow (1943), which is why security can be defined as a product or service, that has to be ensured like drinking water otherwise perception and emotions will become an additional threat. In Germany, in the last decade, the character of the dimensions has changed and merged. For example, the determination of threats is becoming more and more difficult due to their abstract character: Is a possibility or the feasibility of a terrorist attack a concrete threat?

However, the occurrence of a specific threat influences human security rather than the daily environment. Da Palma et al. (2012) described *human security* as a *construct of a different kind such as economic security, health security, and regional or local security*. According to their investigation, the regional or local community level affects citizens' quality of life and security. Regional developments (e.g., increasing urbanization, poverty, and increasing urban crime such as theft, burglary, and vandalism) and acts of physical or psychological injury (e.g., murder, infanticide, assault, rape, sexual abuse, and acts of intimidation and terror) influence the perception of security (Da Palma et al. 2012).

In case of terrorism, the behavior of the individual influences the group behavior. In microsociology sciences, this effect is called the *group with a common destiny* that handles situations in a *collective reflex* at an emotional level. As

a result, a lack of rational processing of information leads to possible uncontrolled behavior patterns (Schulze-Bramey 2012). These situations are difficult to handle, therefore, an understanding of influencing parameters helps to improve preventive action. Subjective security of customers is influenced by different parameters. Wagner and Lehnigk (2010) published already known parameters in public transportation systems such as individual parameters (e.g. gender, age, demography, state of health), proximity parameters (e.g. state of repair, dilapidation, security measures, amount of costumers), and other parameters (e.g. image, state of security, time of the day).

Köhn and Bornewasser (2012) examined parameters of security perception. They determined that, among all *unknown factors*, individual knowledge about the current security situation, individual attitude, and individual experience of protection/mitigation handling influence security perceptions.

Carnegie et al. (2010) examined a study of the Federal Transit Administration in 2001 that assessed the security perception of 25 transit agencies in the United States with 2,593 customer interviews and 634 vehicle operator interviews. He said the following:

- "The overall perception of security was generally very high among customers. More than 45% of customers perceived their transit systems to be very secure and another 30% perceived their systems to be secure. […]
- Consumer perception of security was lower for multi-modal systems and systems with more than 250 buses compared to smaller systems.
- Among security measures, security cameras and police patrols made customers feel the most secure (about 33% for each), followed by lighting (about 12%), intercom (about 9%) and other measures (about 13%).
- Customers felt most threatened by teenagers who they worried may harm them in some way. The crimes they worried about most were robbery and assault.
- Female passengers' perception of security was markedly lower than male passengers.
- Operators' perception of both in-vehicle and at-station security was distinctly lower than customers.
- About 35% of operators had observed security breaches, while only about 12% of customers observed such events." (Carnegie et al. 2010:12, according to FTA 2001).

In comparison, a 2011 analysis of the R+V Insurance that examined the German fear of terrorism in relation to the number of terror events that occurred, revealed that the average *level of terror fear* has been about 47.5% since 9/11 (prior it was 27.7%) (R+V Insurance 2011). Concerning societal risk aversion to extreme

events, Slovic et al. noted that the population seems to accept societal impact more easily from many small accidents than from accidents that are more serious but less frequent (Slovic et al. 1984).

2.6 Non-/Acceptance of Security Measures

The literature contains several definitions of acceptance. Most deal with the product/service and customer relationship and are similar to: "Acceptance is defined as gaining agreement from the customer that the deliverables produced […] meet the criteria defined by the customer" (Westland 2006:84). The origin of the word *acceptance* comes from the Latin word *accipere*, which means to receive and honor e.g. a recommendation. Webster's Dictionary defines acceptance as: "an agreeing either expressly or by conduct to the act or offer of another so that a contract is concluded and the parties become legally bound" (Webster 2014). In public transportation, this is the "transport agreement". The fact that acceptance is not bounded to a specific request between different people is important for the understanding of the concept. More often, acceptance is implicit by a certain act that can be misunderstood by incorrect assumptions or misinterpretation of reactions.

In the discussion of acceptance, the visibility of measures to customers plays a major role. Measures are divided into *covert* and *overt* measures. While physical barriers, security personnel, and television cameras are visible to customers, other measures such as emergency plans, remote sensors or detectors, and employee training are not visible (see Figure 5).

Transit Security Measure	Visibility to Passengers
Facility-specific Measures	
Physical barriers	High
Locking systems/Access control	Low
Public address systems and signage	Medium
Sweeps/inspections	High
Alteration of operations	Low
Local alarm system	Low
Perimeter alarm systems	Low
Advanced or sophisticated remote alarm system	Low
Simple or high security lighting	High
Watchmen	High
Highly trained armed guards	Very High
K-9 units	Very High
Remote sensors or detectors	Low
CCTV	Medium
Vehicle-specific Measures	
Panic button for operators	Low
Two-way radio	Medium
CAD/AVL technologies	Low
Onboard video camera	Medium
Onboard security personnel	Very High
Onboard sworn police	Very High
Protective structure for operator	Low
Specially trained operator	Low
Other Measures	
Designated "Shelter in place" locations	Low
Decontamination site	Low
Mitigation equipment	Medium
Fire suppression equipment	Medium
Employee awareness program	Low
Employee screening	Low
Basic communication	Low
Intelligence/Information sharing	Low
Formal contingency plans	Low
Evacuation and assembly lockdown	Low
Drills	High

Figure 5: Transit security measures and passengers' potential awareness (Source: Carnegie et al. 2010:8)

Public transportation providers often implement security measures and expect consensus from customers. While acceptance is difficult to measure, non-acceptance can be measured more easily by assessing customers' increasing replies in *feedback/complaint management*, *social media*, or, in the worst case, *decreased ridership*. As a result, (non-) acceptance is a social phenomenon, which can be described as a basic action feature and structure feature of the interpersonal life together (Lucke 1995), which fluctuates depending on the object, sub-

ject, and context. In the field of risk acceptance, Renn defined acceptance as a result of a decision process influenced by the subjective weighted consequences and probabilities (Renn 1980).

The construct of acceptance itself is very complex. Achieving the appropriate balance between positive, objective benefits and negative interference of customers (Dunmore 2010) is a major challenge.

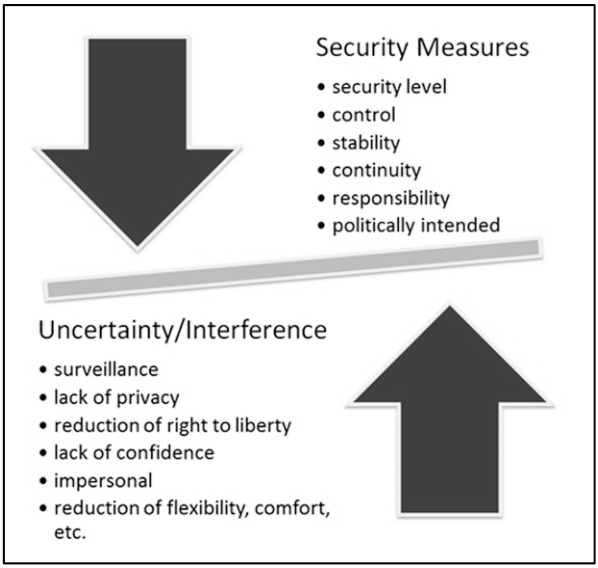

Figure 6: Achieving the appropriate balance (Source: Dunmore 2010, adapted by author)

Different approaches of different scientific fields can be applied to some degree to the topic of technology, security, and risk acceptance. The assignment is often not clear, but Renn (1980) worked out a summary of the different theories of technology and risk acceptance in general in context of nuclear energy (for details see Table 1).

Table 1: Explanation approaches of risk acceptance (Source: Renn 1980, adapted by author)

Area of Science	Theory	Brief Description	Authors
Economy	Theory of marginal utility	Estimation of marginal cost-benefits; comparison of individuals, groups, and society	Felix, Renn
	Economic theory of policy	Requirement maximization through resource mobilization and political Influence	Downs, Frey, Titz
Risk theory	Normative risk assessment	Best approach to estimate cost-benefits; risk minimization and alternative choices	Rowe, Lowrance, Kates, Fischoff, Sagan
	Normative decision-theory	Process optimization to help decision-makers to a 'fast' rational decision	Coombs, Orkent, Raiffa
	Descriptive decision theory	Determination of the determinants of the actual decision-making process	Janis/Mann, Pollatsek, Tversky, Vlek, Stallen, Coombs
	Revealed preference analysis	Historical risks as indicators for the assessment of future risks	Starr, Cohen
	Referred or expressed preference analysis	Empirical determination of risk elements through questionnaires	Fischoff, Slovic, Lichtenstein
Psychology	Psychoanalysis	Transfer of psychoanalytic terms and concepts	Schild, v. Erichsen, Wünschmann, Tubiana
	Psychology reduction theory	Transfer of psychological mechanism of perception	Pahner, Pelicier
Social psychology	Risk perception	Perception effects in risk estimation (attributive biases)	Maynard, Tversky, Fischoff, Slovic, Vlek, Kogn, Bierbrauer, Frantzen, Schmid-Jörg
	Risk socialization	Interpretative patterns for risk assessment	Gutmann, (Battelle), Cohen/Hansel
	Attitude concept	Attitude of subject cause acceptance	Otway, Niehaus, Davis, (v. Buiren), Fishbein
	Communication concept	Controversy is part of misdirected or distorted communication	Goerke, (Eisenbart, Crebsbach)
Sociology	Economic sociology	Results of scientific economy processes	Notwotny, Tschiedel, Prüß, Hülsmann
	Empirical conception	(Dis-)functional discussion of value orientation	Lübbe, Schoeck, Douglin, Tognacci, Melber, Turley & Stone, Gerhold
	System-analytical concept	Exchange of system and policy periphery	Schneckener, Daase
	Conflict theory concept	Discussion of interest conflicts and participation	Scharioth, Paschen, Andritzky
	Normative democracy	Discussion toward more democracy	Schumacher, Moßmann, Daase, Engert, Junk

This list is a brief overview of different approaches, and there is a great deal of social research work missing. However, it provides an impression of how many different points of views exist regarding determining acceptance in the context of technology and risk. Regardless of which approach is chosen, all the theories have their strengths and limitations (e.g., relying on assumptions) and are more or less comprehensive and accurate.

An approach that is easy to handle and applicable for decision-makers, is highly desirable but missing due to the complexity of this topic. Therefore, research institutes in different science disciplines and commercial organizations often execute acceptance studies on behalf of providers.

2.7 Summary of the Literature

The literature review shows the complexity of this research area. Different players are involved such as research (different disciplines), policies, authorities, industry, and society. A dialogue between all stakeholders is highly desirable and has to be supported (COM 2004).

Especially, critical infrastructure are vulnerable; their "[…] incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (Department of Homeland Security 2013) and have to be protected. Especially public transportation systems are highly vulnerable due to their open access and service to the public. Their operators have the dilemma to secure their systems on an acceptable level considering limited budgets, policy demands, and customer satisfaction.

Having a closer look on terrorism, an additional component is added to an already vulnerable system. Terrorism is an anthropogenic threat with low probability but high consequences. Normative risk approaches fail in assessing terror threats because the discrepancy can hardly be evaluated. New holistic risk management approaches are necessary to assess terrorist risks considering provider's needs (Pickl et al. 2011).

Security measure shall improve the security of public transportation system in context of terrorism. Various security measures in different categories are available, but their effectiveness on preventing terrorist attacks cannot be proven by statistics. Therefore, their objective effectiveness is mainly assessed by statistically data of crime act reduction, vandalism, etc.

Statistical data of crime act reduction (cp. Laycock and Austin 1992, Welsh et al. 2010, Barclay et al. 1996, Hesseling 1995, Kenney 1986, Pennell et al. 1986, 1989) cannot be transferred to terrorist events. Furthermore, in the field of sub-

jective (technology) acceptance of security measures, the variety of research possibilities and theories from different scientific disciplines leads to confusion and discouragement on the provider level. Recommendations (such as Commission communication COM 2004 or Burkhard et al. 2008) exist but in a very general manner and provide no definite framework. Although security measures have a positive effect, their operation causes more or less hindrances and restrictions for the customer. “Achieving the Right Balance” (Dunmore 2010) between objective security and customer satisfaction is a challenging task for public transportation provider. Hence, public acceptance of security measures is an important part of customer satisfaction and therefore of total quality management of the provider (Degenhart and Fiedrich 2004).

An explicit structural framework is missing, especially one that is capable of capturing the consequences of security measures at the customer level to compare them with the benefit expected by the provider. So how can the objective and subjective effects be measured and included in a risk management system? To answer this question and other arising questions, objectives are defined and a conceptual framework developed in Chapter 3.

http://www.springer.com/978-3-658-15305-2

Securing Public Transportation Systems
An Integrated Decision Analysis Framework for the Prevention of Terrorist Attacks as Example

Brauner, F.

2017, XXII, 213 p. 69 illus., 10 illus. in color., Softcover
ISBN: 978-3-658-15305-2