assert»
assessing security research:
tools and methodologies to
measure societal impact
assert-project.eu

*Criteria for Assessing and Mainstreaming
Societal Impacts of EU Security Research Activities.
Coordination and Support Action.*

A Case Study in applying Societal Impact Assessment in Public Transport Security

IRKS – Institut für Rechts- und Kriminalsoziologie /
HC - Hamburg-Consult GmbH

April 2014

The ASSERT-project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 313062.

Imprint

IRKS / HC

Authors:
Reinhard Kreissl
Matthias Mueth

Contact:
Reinhard Kreissl, reinhard.kreissl@irks.at
Matthias Mueth, m.mueth@hamburg-consult.de

ASSERT website

www.assert-project.eu

Version history

Version	Date	Change/Remark	Responsible (person, beneficiary/function)
0.1	17.02.2014	Structure	Matthias Mueth
0.2	26.02.2014	First Draft	Matthias Mueth
1.0	14.03.2014	Second Draft	Matthias Mueth and Reinhard Kreissl
2.0	08.04.2014	Final Version	Matthias Mueth and Reinhard Kreissl

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

The need for societal impact assessment (SIA) of security research has become a matter of course. However, the assessment of societal impacts of security research and security measures/practices should not be limited to analysing potential *negative* side effects only. Instead, besides avoiding negative outcomes, the potential of SIA to open up completely new solutions or even change paradigms should be harnessed by applying SIA pro-actively in a broader context, as will be exemplified in this paper. A precondition for doing so is mastering the complexity, multi-contextuality and changeability of the subject, including side- or even side-side-effects. While there is obviously no blueprint for this endeavour, a case study about the application of SIA in the field of Public Transport Security may serve as an example to illustrate aspects, effects and interrelations of as well as alternatives to security-measures.

So, why do we choose Public Transport (PT) to illustrate SIA of security measures and research? Well, because PT is *public*, and therefore everybody has a mental modal, i.e. a precise idea of what we are talking about. And at the same time, it is evident, that this seemingly simple and easy-to-navigate field is more complex than it might have been assumed.

This paper comprises two main parts: The first part gives an overview on the field of PT security (including stakeholders, their interests, potential security threats and measures). Furthermore, the ASSERT methodology and some exemplary questions compatible with the ASSERT guidance-paper for SIA-assessment will be applied to PT security.

The second part of this paper deals with the lessons learned by pro-actively including social-science and humanities in a PT security research project. This was conducted within the framework of Germany's National Security Research Programme.

This paper and case study certainly cannot be comprehensive. Nevertheless, it illustrates how the ASSERT-guidelines for SIA could be applied in practice with positive and negative examples[1].

[1] This paper has evolved within the ASSERT project, a support action for the European Commission. ASSERT is the acronym standing for "assessing security research: tools and methodologies to measure societal impact", and creates the basis for a tool as well as a strategy for the sustainable implementation of societal impacts in future EU research activities in the field of security. This case study is to be seen in the framework of other ASSERT-deliverables, namely the "Report on good practices of the exploration and assessment of the societal impact of research" by Lars Ostermeier/TUB and Barbara Prainsack/KCL, as well as the guidelines "State of the Art Societal Impact Assessment for Security Research by Kush Wadhwa, David Barnard-Wills and David Wright/Trilateral Research.

2 Exploring the field of Public Transport Security

Public Transport is a Critical Infrastructure and part of Security Research Programs not only on the European level (EU FP7; Horizon 2020), but also on national level, e.g. National Security Research Programmes in different Member States. On both levels, a number of projects have been focussing on Public Transport (PT). Unlike the European Commission, the German government with its National Security Research Programme has made it mandatory to include Social Science and Humanities. Some observers go beyond this by requesting that not only *research* on security in PT (and other fields) but also (long) established security technology and practices should undergo SIA.

Stakeholders in PT security

Exploring the field of Public Transport (PT) security, we start with identifying the stakeholders in PT

Some of the main stakeholders in security in PT are listed below:

- PT-Operators, i.e. public transportation companies,
- PT-Staff, especially drivers, field operatives and “security workers”,
- PT-Industry, for example suppliers of vehicles, electrical and mechanical equipment,
- Security-Industry, i.e. suppliers of security equipment and services,
- General public, including people living in the vicinity of PT-infrastructure,
- PT-passengers,
- Law enforcement entities, especially the police forces, and
- Others, including politicians and procuring authorities

This unfinished list of stakeholders suffices to reveal how manifold and different stakeholders are in the field of PT security. They are considerably diverse (thinking for example of the PT-industry vs PT-passengers) in terms of organisation (organised vs unorganised), in their ability to articulate their interests or even exercise power, etc.

Interests of stakeholders

It goes without saying that all these stakeholders do have their interests, often vested interests, legitimate or not, which do not necessarily match.

Here again, we will only incompletely depict a few (vested) interests of the mentioned stakeholders:

Public transport operators

- Increase of ridership and thus revenues
- Legal compliance (e.g. regarding new laws enforcing security, political decisions)
- Protection of assets and cost-cutting (due to damage/vandalism)

Field operatives and "security workers"

- Health and safety at work
- High level of objective and subjective (perceived) security

Public transport industry (e.g. suppliers of vehicles, electrical & mechanical equipment)

- Promotion and sale of products and services

Security industry (suppliers of security equipment and services)

- Promotion and sale of their products and services

General public and passengers

- Convenience
- High level of objective and subjective (perceived) security
- Enhancement of security while keeping moderate fares
- Secure neighbourhoods around PT stations

Law enforcement entities

- Low registered crime-rates / high level of objective security

It comes as no surprise that the diverse stakeholders in the field of PT-security have different interests, some are compatible, others conflicting (like cost-cutting by PT-operators vs increasing security for passengers and staff).

As we will see in the following examples, for some security measures in PT there will be "winners" and "losers". And, as stated above: The diverse stakeholders have better or worse abilities to articulate, lobby for, and enforce their interests, which is a matter of power[2].

Security-Threats

Turning now to the (potential) security-threats in PT:

Again, we potentially have a confusingly long list of thinkable security-threats in PT. For practical reasons we outline and structure the threats as follows, so that they are ranging from:

[2] "Power" as defined by Max Weber: "…the ability to control others, events, or resources; to make happen what one wants to happen in spite of obstacles, resistance, or opposition…"; see WEBER, Max (Nachdruck 1972): Wirtschaft und Gesellschaft. Tübingen.

- **Anti-social behaviour** (e.g. loud or aggressive misbehaviour of certain individuals or groups), to
- **Small-scale crime** (like pickpocketing, vandalism or verbal abuse) up to
- **Serious crime** (like physical abuses or even acts of terrorism)

This generic structure of threats suffices to show that security-threats in PT occur in many forms and with considerably different intensity.

Security measures

This leads to the measures improving security in PT.

As diverse as the threats, are the measures improving security in PT. There are many different ways to categorise the various safeguards. The following three categories (1) human factor, (2) technology, and (3) organisation and procedures allow subsuming all potential security measures, although only few examples are provided here:

- **Human Factor**, e.g. Awareness-Raising and Training of
  - Staff
  - Passengers
- **Technology**, e.g. Technical developments/equipment like
  - CCTV & pattern recognition
  - CBRNE-alarms
- **Organisation & Procedures**, e.g.
  - Emergency & Crisis Management
  - Research projects
  - Objective & Subjective (Perceived) Security
  - Service-Quality (like lightening, cleanliness or information available to passengers)

The last aspects listed here are "objective and *subjective* security" as well as "*service quality*". This may come as a surprise to some, when talking about measures improving *security* in PT. In the last two decades the conception of "*security*" has noticeably evolved: Nowadays it is not sufficient, that passengers in PT *are* objectively safe (after all, PT is among the safest modes of travelling), but that they also *feel* safe (i.e. subjective or perceived security). And this aspect of subjective security strongly correlates with quality of service, as has repeatedly been shown in research projects, e.g. SuSiPLUS[3], as well as in commissioned works (e.g. Munich[4]). Thinking this line of ar-

[3] SUSI-PLUS (Subjektive Sicherheit im Personennahverkehr mit Linienbussen, U-Bahnen und Straßenbahnen): Perceived security in public transport. Research project of the Hamburger HOCHBAHN AG for the Federal Ministry of Education and Research, Germany (2003-2005)

gument through to the end will at times influence the selection of security measures, and may even impact the agenda-setting, if not change paradigms.

This means…

To sum up this brief introduction to security in PT, we need to stress that there are many different measures for improving security in PT, and all these measures come with their distinct positive and negative (side-) effects. Furthermore, not only security-measures in a strict sense may be effective (and adequate) for improving security in PT, but also aspects like quality of service impact on objective as well as subjective security. For this reason, a holistic approach including SIA and "*thinking out of the box*" is required. Therefore, the role of SIA may far exceed merely identifying any potential *negative* outcome of a (technical) security-measure, but open up alternatives and identify additional options.

Examples for questions exploring potential Societal Impacts of security measures or research in PT

In accordance with the ASSERT-guidelines "State of the Art Societal Impact Assessment for Security Research" by Kush Wadhwa, David Barnard-Wills and David Wright/ Trilateral Research, the following section will exemplify a SIA-application in PT, providing examples for questions and exploring potential societal impacts with regard to security measures or research in PT. As stated already, this example of operationalising SIA in PT is a robust, hands-on approach for SIA-application, starting with simply formulating relevant questions. As there is no one-size-fits-all approach for SIA, these questions shall not be understood as a blueprint. Instead, they do serve as an illustration and exemplify SIA-questions, exploring a field and discovering relevant dimensions with positive and negative examples. In order to better achieve this goal, the questions will not be limited to one single security-measure or research-project but refer to diverse undertakings.

Possible queries to be raised in three rounds of questions

The ASSERT-methodology recommends three "rounds" of questions for exploring potential societal impacts of security measures in PT in the relevant dimensions:

[4] Herbert König (2009): "Gewalt in der U-Bahn – Haben Fahrgäste der MVG Angst? Untersuchung zum Sicherheitsempfinden in der Münchner U-Bahn", in: Der Nahverkehr, Heft 6/2009, 27.Jg., pp. 8-14.

- **Assessment Round 1** explores whether security measures/research **meet the needs** of society
- **Assessment Round 2** investigates and ensures that security measures/research do **not have negative impacts** on society
- **Assessment Round 3** warrants that security measures/research **benefit** society

ASSESSMENT ROUND 1: **Ensuring security measures/research meet the needs of society**	
Effectiveness of measures: *Is the proposed measure effective in reducing an identified risk?*	POSITIVE example: The effectiveness of a proposed measure is indicated in the results of a risk-assessment: the two or three factors (1) likelihood, (2) impact and optionally (3) vulnerability constitute a "risk". The assessment of a given threat prior and, (theoretically) after introduction of the proposed measure, must indicate the effectiveness of the proposed measure in reducing the identified risk[5]. NEGATIVE example: CCTV-cameras could be introduced in a PT-system with the aim to *prevent* physical assaults. While there is empirical evidence that CCTV in PT-systems effectively reduces (or displaces) vandalism, CCTV is not effective as a deterrence against physical assaults (because these are usually committed as an emotional act, i.e. they are not planned and consequently not prevented by any CCTV).
Initiator: *Who is the initiator of a safeguard / measure? This question evaluates whether a safeguard / measure is developed due to internal considerations or upon external pressure, e.g. new or increased regulations, standards or laws or from the political arena. Are there any vested interests at stake?*	NEGATIVE example: During election campaigns in a major German city the political debate centred on security in PT; however, the resulting election-promises lacked substantiation: neither did the election promises correspond with voiced needs of PT-operators, nor with the needs expressed by PT-staff

[5] As an example for a the methodology to conduct risk assessment in PT-systems regarding serious crimes see COUNTERACT (http://www.transport-research.info/ Upload/Documents/201207/20120719_145438_7577_COUNTERACTGuidelines_lr.pdf)

ASSESSMENT ROUND 1: **Ensuring security measures/research meet the needs of society**	
	or passenger in surveys.
Legal implications: *Are there any potentially conflicting legal aspects regarding the proposed safeguard / measure?*	NEGATIVE example: ▪ The (introduction of) CCTV-systems in a PT-system, which technically enables the tracking of passengers could conflict with the law of the member state. ▪ The (introduction of) rules and procedures for security staff of a PT-operator with (implicit) aspects of profiling could conflict with the law of the member state. ▪ The (introduction of) procedures for ticket controls in PT-systems, e.g. while retaining people in the course of such controls, could constitute a form of coercion.
Privacy Issues and Data protection: *Are there any potentially negative impacts particularly with respect to privacy issues and/or data protection regarding the proposed safeguard/measure?*	NEGATIVE example: ▪ See example above: tracking of passengers. ▪ The practice of storing video-images (CCTV) may negatively impact on Privacy and Data protection. ▪ The practice of storing and exchanging personal data, e.g. of fare-evaders, may conflict with privacy issues or data protection.
Ethical issues: *Are there any potentially conflicting ethical issues regarding the proposed safeguard/measure?*	NEGATIVE example: The expulsion of homeless people in order to improve the perceived security of passengers during critically cold winter-days/nights from warm and secure places (e.g. underground-stations) without alternative raises ethical concerns.

ASSESSMENT ROUND 2 Ensuring security measures/research do not have negative impacts on society	
Freedom of association: *Are there any potentially negative impacts particularly with respect to freedom of association regarding the proposed safeguard / measure?*	NEGATIVE example: ▪ The potential misuse of CCTV against the association of PT-employees by the management of the PT-operator. ▪ The potential misuse of CCTV by law-enforcement agencies against legal demonstrations, e.g. screening of passengers.
Socio-economic aspects: *Are there any potentially discriminatory implications with regard to socio-economic aspects concerning the proposed safeguard / measure?*	NEGATIVE example: Increasing security patrols and the consequent expulsion of homeless people from PT-premises (e.g. for the purpose of increasing subjective security). See example above for ethical issues in round 1.
Ethnic and Cultural aspects: *Are there any potentially discriminatory implications with regard to ethnic and / or cultural aspects concerning the proposed safeguard/measure?*	NEGATIVE example: The (introduction of) procedures for profiling of passengers e.g. for ticket controls.
Non-Citizens: *Are there any potentially discriminatory implications with regard to Non-Citizens concerning the proposed safeguard/measure?*	NEGATIVE example: The (introduction of) procedures for profiling of passengers, e.g. for ticket controls.
Religious aspects: *Are there any potentially discriminatory implications with regard to religious aspects concerning the proposed safeguard/ measure?*	NEGATIVE example: The (introduction of) procedures for profiling of passengers e.g. in counter-terrorism regarding reconnaissance-missions.
Disabled: *Are there any potentially discriminatory implications with regard to disabled people concerning the proposed safeguard/measure?*	NEGATIVE example: ▪ The (introduction of) turnstiles (e.g. with the aim to decrease fare-evasion) but with non-functioning alternatives for wheelchair-bound passengers. ▪ Written security instructions or announcements for passengers that disabled might not read or hear.
Age related aspects: *Are there any potentially discriminatory implications with regard to age concerning the proposed safeguard/measure?*	NEGATIVE example: The (introduction of) procedures for profiling youngsters, e.g. for ticket controls.
Gender aspects: *Are there any poten-*	NEGATIVE example:

ASSESSMENT ROUND 2 **Ensuring security measures/research do not have negative impacts on society**	
tially discriminatory aspects with regard to gender issues (including sexual identity) in connection with the proposed safeguard/measure?	The (introduction of) procedures for profiling male (youngsters), e.g. for ticket controls.
Mitigating Measures: *Are there any mitigating measures possible and foreseen in case the proposed safeguard / measure has any negative implication(s)?*	POSITIVE examples: ▪ CCTV coverage (introduced e.g. for countering vandalism and collecting evidence for court cases in case of abuses among passengers) may pixel out / blur out the driver-seat in the bus. ▪ Some PT-operators expulsing homeless people from their premises (in order to increase subjective security) offer alternative places for the homeless (in cooperation with governmental and non-governmental organisations), where they can seek shelter from the elements.
Implications for relevant stakeholders: *Are there any potential impacts on relevant stakeholders caused by the proposed safeguard/measure and would they be positive/negative?*	POSITIVE examples: ▪ Improved objective and subjective security (achieved by security-measures and safeguards) may contribute to increasing ridership and thus revenues, which is in the interest of the PT-operator as well as the (city-) government and therewith of tax-payers (who need to subsidise deficits of PT). ▪ The (introduction of) security measures may contribute to improved cooperation among several PT-operators and/or among PT-operators and law enforcement agencies and/or other actors, e.g. soccer-clubs with which the PT-operator cooperates for the transport of football fans, etc.
Information and engagement of stakeholders and interested parties: *Are stakeholders and interested parties adequately informed and engaged in a meaningful way?* • Local communities • (Local) Governments • State agencies • Law enforcement agencies	*POSITIVE and/or NEGATIVE example:* PT by its very nature is involving many different stakeholders. This means on the one hand that stakeholder-involvement is almost always practiced (to a certain extend), but on the other hand that stakeholder-involvement is hardly ever comprehensive. Often, the (introduction of) security measures in PT are a result of (or accompanied by) round-tables. A typical

<table>
<tr><th colspan="2"><b>ASSESSMENT ROUND 2
Ensuring security measures/research do not have negative impacts on society</b></th></tr>
<tr><td>• Other (Public) Transport Operators
• Security Providers
• Others</td><td>example is sharing of domestic authority (in stations used by rolling stock of different PT-operators). This measure is kick-starting dialogue among PT-operators and between PT-operators and law-enforcement authorities, etc., while passengers and local communities are often not engaged in this process.
NEGATIVE example:
The expulsion of disadvantaged groups from PT-premises drives these people into the adjacent quarters affecting these local communities.</td></tr>
</table>

ASSESSMENT ROUND 3 **Ensuring security measures/research benefit society**	
Customer satisfaction and subjective security: *Are there any potentially negative/ positive impacts on customer satisfaction and subjective security regarding the proposed safeguard/measure?*	POSITIVE examples: The (introduction of) reasonable presence of PT-staff (where appropriate service staff instead of security guards) will improve the objective and subjective security of passengers. NEGATIVE example: The (introduction of) massive presence of (armed) security staff may improve objective security but negatively impact on subjective security.
Staff moral/satisfaction and subjective security: *Are there any potentially negative impacts on staff moral/satisfaction and subjective security of staff regarding the proposed safeguard/measure?*	POSITIVE examples: The (introduction of) reasonable presence of security-staff will improve the objective and subjective security of PT-staff (like drivers or station managers). NEGATIVE examples: ▪ The (introduction of) inadequate behaviour of security staff towards certain target-groups may escalate and create an aggressive atmosphere, which could negatively impact on objective and subjective security of other PT-staff (like drivers or station managers), when working alone. ▪ The (introduction of) security-procedures may complicate and slow-down working-routines, and therewith constitute additional workload for PT-staff, already struggling with work-overload.
Image and reputation: *Are there any potentially negative/ positive impacts on the image of the public transport operator and its reputation caused by the proposed safeguard/measure?*	POSITIVE examples: ▪ The (introduction of) well-selected and trained security staff, which combines service- and security-functions, will positively impact on the image and reputation of the PT-operator. ▪ Awareness raising campaigns (e.g. regarding terrorist threats in PT) will improve vigilance among passengers and improve image and reputation in case that they are well-done and compatible with local customs and practices.

ASSESSMENT ROUND 3 **Ensuring security measures/research benefit society**	
	NEGATIVE examples: ▪ The (introduction of) inadequately trained security-staff may negatively impact on the image and reputation of the PT-operator. ▪ Awareness raising campaigns (e.g. regarding terrorist threats in PT) will induce a feeling of insecurity among passengers and negatively impact on image and reputation if poorly done or not compatible with local customs and practices
Media-perception: *What is the expected perception of media and opinion former regarding the proposed safeguard/measure?*	See: Image and reputation above See: Image and reputation above
Politics: *Will there be any political consequences caused by the proposed safeguard/measure and would they be positive/negative?*	POSITIVE example: The successful (introduction of) security measures will positively impact on image, reputation and thus revenues of the PT-operators, and consequently reduce the subsidies paid by tax-payers NEGATIVE EXAMPLE ...and vice versa
Reaching of strategic/operational goals and adhering to compliance rules: *Is the proposed safeguard / measure in line with the company´s overall strategic and operational goals as well as compliance rules?*	POSITIVE example: The (introduction of) security measures like emergency and crisis management is embedded in a corresponding and long-established safety- and security culture in the company, constituting a supportive environment. NEGATIVE example: The proposed safeguard is obviously not more than a “fig-leave” for the management, pretending to engage in security and/or shifting responsibility onto others
Reduction of health threats: *Is the proposed safeguard / measure likely to increase/ decrease the safety at work and operational safety?*	POSITIVE example: The (introduction of) de-escalation training for front-line staff in PT-organisations (e.g. drivers, station-managers...) will lower the number of incidences with assaults, traumata, (physical) injuries, and will increase job-satisfaction and self-esteem.

ASSESSMENT ROUND 3 Ensuring security measures/research benefit society	
	NEGATIVE example: The (introduction of) additional security-tasks for inadequately trained staff put the staff at risk.
Full lifecycle assessment and data availability: *Is it possible to assess the whole lifecycle of the proposed safeguard/measure and is reliable / best data on the proposed safeguard / measure available?*	POSITIVE example: The safeguards are well established in other PT-operations, where they have been positively tried and tested.
Monitoring, evaluation and review: *Are monitoring, evaluation and review adequately planned?*	POSITIVE example: For monitoring and evaluating the (introduction of) safeguards, proper evaluation-criteria can be defined. The evaluation and review needs to be adequately planned e.g. by comparing the development of surveys on subjective security of passengers and staff (prior and after the introduction of safeguards).
Operational Aspects / Embedding in processes and procedures: *Is it possible to smoothly integrate the proposed safeguard/measure to everyday business? Is there a risk of follow-up expenditures in other processes or departments due to the proposed safeguard/measure?*	NEGATIVE example: The (introduction of) additional security-tasks (e.g. drivers who shall conduct security-checks at remote terminal stations), might slow down processes and thus constitute an additional burden for PT-staff (already carrying a work-overload). In this case the tasks do not benefit the staff in question and therefore are doomed to fail.

This set of questions is neither comprehensive, nor does it constitute a blueprint for SIA. Nevertheless, it is a starting point for exploring the relevant dimensions of societal impacts regarding security measures or research in the field of PT.

How SIA can look like and what benefits the active integration of SIA can deliver, will be described in the following chapter. The case study is about the PT security research project V-SICMA and will elaborate some of the lessons learned during its course.

3 A case study from Public-Transport Security Research

V SICMA

SPONSORED BY THE
Federal Ministry
of Education
and Research

Awareness Raising & Competence Building of Public Transport Staff in Countering Terrorism and Serious Crime by Creating Virtual Realities in Interactive, Serious, 3D-Gaming

The lessons learned in V-SICMA show, how social impact assessment (SIA) can contribute to a security-research project, not merely by identifying potential negative side-effects, but by opening up new insights and solutions, adjusting and focussing research targets and by doing so, fostering the applicability of research.

V-SICMA[6] is the name of a research-project, funded by the German Federal Ministry for Education and Research's National Security Research Programme, in which a consortium of eight partners from social-science and humanities, industry, consultancy, law-enforcement as well as security organisations and public transport operators were developing demonstrators for awareness-raising and security-trainings of public-transport (PT) staff[7]. The V-SICMA demonstrators are simulations of relevant security (and safety) scenarios, which were delivered in two formats, addressing different target

[6] V-SICMA stands for „ V-SICMA: Sensibilisierungs-, Bewertungs- und Handlungstraining für Sicherheitsmaßnahmen in öffentlichen Verkehrsunternehmen, beispielhaft für kritische Infrastrukturen “, which translates into English: **Awareness Raising & Competence Building of Public Transport Staff** in Countering Terrorism and Serious Crime by Creating Virtual Realities in Interactive, Serious, 3D-Gaming; see: http://www.bmbf.de/de/22460.php

[7] The consortium consisted of three core-members: Hamburg-Consult GmbH (a public transport consultancy leading the consortium, conducting basic-research in the field and developing the 3D-board-game based simulation), Industrieanlagen-Betriebsgesellschaft mbH (IABG – the industry-partner developing the 3D-computer-based simulation), and Verein für sozialwissenschaftliche Forschung & Beratung (the social science and humanities partner, assigned with conducting the SIA); associated partners were the three German public transport operators Hamburger Hochbahn AG, Münchner Verkehrsgesellschaft mbH and Rhein-Neckar Verkehrs GmbH; Hamburger-Hochbahn Wache (the security-provider of Hamburger HOCHBAHN) as well as a law-enforcement entity were complementing partners. VDV-AG Security, the Security-working-group of the German umbrella-organisation of public transport operators closely collaborated with the V-SICMA project.

groups within PT-organisations: (1) interactive, three-dimensional computer-simulations for individual training of drivers and front-line personnel and (2) interactive board-game simulations for group learning, focussing on PT-staff working in operation-control centres.

Fine-tuning the target of the research-project and integrating organisational aspects

The original idea of the V-SICMA project was to cover prevention, detection and mitigation of security-threats to PT-systems with a focus on measures targeting human resources, i.e. training of staff. Since the consortium was comprised of members from different professional backgrounds, it was agreed to take a rather broad approach and look at classical training tools and organisational measures alike. It became clear in the early stages of designing the study that all measures developed to handle terrorist attacks involve a change in the organisational structure of PT.

Threat assessments forming the basis for security research and development projects often are not very well defined. Major attacks on critical infrastructures like PT are rare events and the database for the analysis is limited. Drawing conclusions for preventive measures from a few single cases is difficult. The problem is that evidence based standard solutions cannot be derived from these few cases.

What also became apparent soon was the open nature of the system under investigation. Therefore, any techno-centric approach aimed at prevention of a major attack was doomed to fail due to this open nature of PT-systems. The SIA experts spent considerable time with the stakeholders involved in the project to understand how the "system" operates on a daily basis. This produced evidence that led to a slight re-design of the original research plan. The focus shifted from "prevention" to detection and mitigation. Taking a systems approach and focusing on organisational procedures, we developed a model of cognitive division of labour. This model started from the assumption that a large distributed metropolitan public transport system is governed from a central hub (i.e. the Operational Control Centre/OCC). While the individual employees like station managers, drivers, security guards or maintenance workers are performing their assigned and clearly defined routine tasks with little discretion, decisions affecting the whole system and reaching beyond defined routines (like stopping a train at a station or ordering the clearing of a platform in case of emergency) are taken in the OCC. The members of the OCC take their decisions on the basis of the information they receive through different communication channels (intercom, video, sensors, mobile phones) from different sources such as field operatives, passengers, etc.

Regarding the security problem of a major terrorist attack, the control centre team has to integrate the incoming information to analyse and understand what is happening in the system and decide what kind of action is appropriate.

Excursus: *What is happening in our metro-system?*

Several real incidences disclose the difficulty for staff in Operational Control Centres (OCC) of metro-systems to understand, what has been happening in their system.

One example are the suicide-attacks targeting London Underground on 07.07.2005: due to loss of communication it took the OCC a considerable time to understand, that the trains in the tunnels had been subject to a terrorist- attack.

Even more challenging for the staff in the OCC in Tokyo was to diagnose the Sarin-attacks on the underground-system in 1995 by the Aum Shinrikyo sect. Despite previous attacks with chemical weapons in Japan by this apocalyptic sect, the staff of Tokyo's subway-operator was not aware of the possibility of such an attack occurring. Consequently, the chemical-attack was not identified quickly and some of the affected trains continued servicing up to 100 minutes after the attack had started, so that the number of victims among passengers and workforce increased accordingly. Staff and passengers had neither been sensitised about potential terrorist threats nor had they been trained how to recognise them or how to react effectively. Inadequate internal and external communication and coordination further delayed the recognition of the threat and the efficient response.

Furthermore, there is a considerable pressure on all staff in PT-systems to maintain smooth operation. This is particularly challenging since even minor disturbances can have major effects in tightly knit complex systems like a metro-system. Consequently, the threshold for any emergency action is rather high.

Against the background of this simple model we started to develop ideas how to improve the "receptivity" of the system and particularly how to improve the cognitive division of labour among all actors involved in optimising the complex decision process. In doing so, we focussed on technical and organisational dimensions alike.

SIA-ing the security problem and including the insights from bottom-up

What made this particular project V-SICMA successful from an SIA perspective was the integration of an SIA approach from the very beginning. This of course is always contingent upon the openness and responsiveness of the consortium. Integrating the field operatives, i.e. the end-users of any innovation or technology from the very beginning and taking their point of view serious was prerequisite. Often the view of ground-level personnel is considered as biased, limited and narrow. Instead, the experts' opinion is given more weight. While it might be true that the field operatives do not present the problem in an elaborate technological vernacular, they can contribute important insights. What helped to better understand the security problem in such a bottom-up way was the very extensive empirical and ethnographic work at the beginning of the study. Observing the crews in the control centres over several shifts and having them explain the routines of their work created important insights into the logic and functioning of the overall system. Joining security and maintenance workers on their daily work rounds and talking to them about their problem solving strategies broadened the problem description considerably.

This ethnographic empirical micro approach changed the abstract problem description (threat and vulnerability assessment) in a substantial way. It helped to refocus the project from prevention to detection and appropriate reaction. The Ground level staff had developed their own theories about dangers and threats. They decided, based on their experience, which situations required special attention. They filtered incoming information and events to decide when urgent action was needed. But as could be shown, they had difficulties in identifying the signs of a major serious terrorist attack since they framed all events against the background of trivial and minor disturbances of routine activities and performance. Serious warning signs drowned in the noise of routine problems. Developing training measures to sensitize staff members in this regard became a main task of the project.

SIA as a performative attitude

SIA is a methodological and theoretical framework, but *doing* a good SIA requires a proper performative attitude to be successful. R&D projects often follow a rather crisp and narrow path of action, laid down in flow diagrams and governed by rigid timelines for deliverables. SIA is a productive irritation trying to keep the process of research open and responsive for new insights, ideas and criticism emerging in the course of work. Given the typical design of research in the security field, SIA often sides with those actors, whose voices are not easily heard in the research process. This however should not be understood as a partisan approach. As Zygmunt Bauman[8] has pointed out, social scientists should not entertain an attitude of the philosopher kings claiming a superior knowledge. Rather, their task is to translate between different epistemic or cultural communities. Often technology experts, administrators, field operative and legal experts talk past each other and SIA can help to improve mutual understanding and find common ground for shared definitions of tasks and problems. While this does not always create a consensus satisfying all participants, SIA can follow a strategy C.W. Mills once termed clinical sociology[9]. This means through acting more like mediators, the SIA experts can make hidden or implicit conflicts explicit and hence accessible for rational discussion.

[8] Zygmunt Bauman, 1989, Legislators and Interpreters: On Modernity, Post-Modernity and Intellectuals. London, New York, Wiley

[9] C. Wright Mills, 1959 (2000), Sociological Imagination, Oxford, Oxford Univ. Press

Lessons learned in doing SIA in V-SICMA

Regarding our experience with research on terrorist attacks there are a few lessons to be learned. First of all, a close observation and analysis of daily routine work provided important information for the research and particularly for SIA. Since security work is local and includes cooperation, activities and involvement of many different actors at different levels, an ethnographic approach to "security work" is often a good path into the heart of the problem. On close inspection, it turns out very often that trivial organisational adaptations can have tremendous security relevant effects. In V-SICMA we discovered that a re-organisation of communication channels and strategies within the control centres substantially improve the ability to detect a potential major attack in the system. What we also found out was that "security" was understood very differently in the organisation. From the perspective of the management, security is a problem of accountability. For the ground level staff, increased security measures are often perceived as a nuisance, interfering with entrenched routines. The most important lesson to take home from a number of research projects on security in organisations is that a sustainable improvement of security measures always involves a more or less dramatic change in organisational *cultures* and *routines*. This is a key area for every SIA activity. Often "security" is like a one-hit-wonder. Triggered by a research initiative, the organisation and staff members put the topic for a short time high on the agenda only to return to old routines at the end of the research. Hence a follow-up and if possible a continuous support for organisational implementation of specific measures can help to improve the positive effects.

4 Conclusions

Public transport is a vulnerable critical infrastructure and security in PT is a relevant and complex problem with many dimensions: stakeholders, (vested) interests, threats and countermeasures. As these dimensions are plentiful and interrelated, SIA is particularly important with regard to security measures and research in PT. This includes identifying and highlighting threats and opportunities as well as positive and negative (side- or even side-side-) effects of potential safeguards. It can also open up completely different approaches for achieving comparable goals, e.g. by introducing service-staff instead of security guards or technical equipment where appropriate.

The case study V-SICMA showed how SIA can explore the perception and acceptance of security-measures at all levels and in different functional areas within PT operations. Doing so required (in this case) drawing an organisation-ethnographical picture of security-awareness against multiple, partly competing business objectives and institutional frameworks. Paradox constellations were to be analysed regarding the organisational and individual perception and treatment of potential incidents with an extreme impact versus frequent incidents of minor severity – and their effect on staffs' risk-awareness and the establishment of routines.

SIA in V-SICMA was a bottom-up approach, based on fieldwork for close observation and analysis of the daily routine work of PT-staff. SIA revealed that the re-organisation of communication channels and strategies within the OCCs of PT operations could substantially improve their coping abilities and support the "hardening" of so-called "soft-targets" like PT-systems. However, the sustainability of security-improvements in PT-systems requires successfully installing and constantly fostering a safety- and security culture.

In the V-SICMA project SIA contributed – among others – to open up new insights and solutions, and even adjust and focus research targets. Preconditions were the close collaboration of all partners from the very beginning and the openness and responsiveness of the members of the consortium. Experiences gained in V-SICMA. Lessons learned and examples provided in the first part of the paper demonstrate the feasibility as well as the mutual benefits of integrating societal dimensions into security measures and research-projects.