

MICROMATERIALS AND NANOMATERIALS

A Publication Series of the Micro Materials Center
at Fraunhofer IZM and Fraunhofer ENAS
in cooperation with EUCEMAN, The European Center for Micro- and Nanoreliability

ISSN 1619-2486 | issue 10 2009 | 50,00 €

Editor-in-chief
B. Michel, Berlin and Chemnitz

Editors of this issue
M. Künzel, Berlin
B. Michel, Berlin and Chemnitz

International Advisory Board

H. Reichl, Berlin
M. Bauer, Teltow
J. Dual, Zurich
H.-J. Fecht, Ulm
J. Felba, Wrocław
T. Gessner, Chemnitz
K. Kishimoto, Tokyo
A. Leson, Dresden
J. Liu, Gothenburg
N. Meyendorf, Dayton
M. Pecht, College Park
R. Pufall, Munich
E. Suhir, San Jose
W. Totzauer, Mittweida
J. Villain, Augsburg
B. Weiss, Vienna
M. Werner, Berlin
E. Wolfgang, Munich
S.-W. Yu, Beijing
G.Q. Zhang, Eindhoven

Technical Editor
T. Winkler

safety and security systems in europe



10
2009

proceedings of 3rd international
conference

MICROMATERIALS AND NANOMATERIALS

10
2009

A Publication Series of the Micro Materials Center
at Fraunhofer IZM Berlin and Fraunhofer ENAS Chemnitz
in cooperation with
EUCEMAN, The European Center for Micro- and Nanoreliability

in this issue

- 2** Introduction
- 11** Opening Plenary Papers
- 27** Advanced Detection with High-Level Radiation
- 33** Economical and Legal Aspects
- 43** Advanced Detection of Chemicals and Explosives
- 57** Human Factors in Security Applications
- 67** Autonomous Vehicles
- 75** Plenary Papers II
- 85** Signal and Image Processing
- 93** Biohazards
- 107** Communication and Networks
- 119** Advanced System Concepts
- 140** Poster
- 142** EUCEMAN – Recent Activities
- 143** About Micromaterials&Nanomaterials

IMPRESSUM

MICROMATERIALS AND NANOMATERIALS

A Publication Series of the Micro Materials Center at Fraunhofer IZM Berlin and Fraunhofer ENAS Chemnitz

editorial office:

Micro Materials Center

Fraunhofer Institute IZM Berlin

Volmerstr. 9B, 12489 Berlin

phone: +49 (0)30 6392-3610

fax: +49 (0)30 6392-3617

e-mail: bernd.michel@izm.fraunhofer.de

homepage: www.micromaterialscenter.com

editor-in-chief: B. Michel, Berlin

editor of this issue: M. Künzel, Berlin

B. Michel, Berlin and Chemnitz

technical editor: T. Winkler

copyright: © MMCB Berlin 2009

© goldenbogen verlag, Dresden

pre-press and publishing: goldenbogen, Dresden

printing: Druckhaus Dresden GmbH

ISSN 1619-2486

V-SICMA: Requirements and Solutions for the Adaption of Work Processes and Training of Employees Using new Technological Solutions

Dr. Matthias Mueth

Hamburg-Consult GmbH, Hamburg, Germany

1. Public Transportation and Terrorism

Public transport systems are considered as "soft-targets". Worldwide, the frequency of attacks against public transportation has increased drastically over the last decades. Worse, the perpetrators' perfidious tactic seems to work out, as terrorist attacks on transportation targets are significantly more lethal than terrorist attacks overall.¹

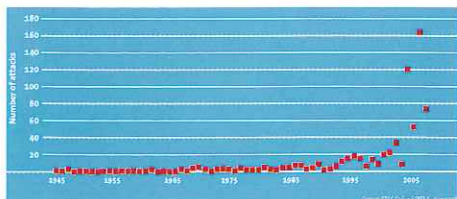


Figure 1: Number of attacks on public transport systems worldwide. Source: ASSTRA, May 2008

Threats for public transport systems are far from one-dimensional. The list of potential offenders is diverse, ranging from "simple" criminals like extortionists (like in Dresden 2003), mentally deranged suicide (like in Daegu 2003), and apocalyptic sects (e.g. Aum in Tokyo 1995), up to the diverse categories of individual or organised terrorists (Islamist, Ethno-nationalist/Separatist, Left-/Right-wing or Single-issue²). Similar diverse are the tactics and weapons they apply.

While the prevention of terrorist attacks clearly is the prime-responsibility of governments, the public transport operations are accountable for their passengers and staff.

This requires them to acknowledge the threat and ensure the highest level of prevention and preparedness.³

Of course, it will never be possible to fully rule out all security-threats. However, there are numerous examples demonstrating the feasibility of "hardening" soft-targets successfully, and for this purpose, the most important resource of public transport operators is their well-trained workforce.

2. The staff is the key factor – good and bad experiences in handling critical situations

Success or failure in detecting and countering attacks on public transport systems in the past proved the importance of adequately trained and alert personnel. Without going into detailed analysis of case-studies, some obvious lessons must be drawn.

For good reasons London Underground has been praised for their effective response to the suicide-attacks on 07.07.2005. The employees of the operator had been well prepared by decades-long IRA-terrorism. In addition, the established organisational and procedural set-ups had been well-tested in large scale exercises (London Resilience Exercises). So, the solid preparation of organisation and staff was the precondition for the successful crisis-management, demonstrated e.g. in the efficient evacuation of 250.000 passengers out of 500 trains (without major incidences), the crisis-communication, the support of relief units, and finally the quick resumption of services.

Bags with improvised explosive devices (IED) have been successfully identified as suspicious in some cases as the one planted by an extortionist at Dresden Central Station in 2003. Contrary in Koblenz and Dortmund in 2006, when IEDs in bags had been placed in regional trains by Islamists, and were not identified as dangerous. Fortunately, due to technical mistakes the IED in the regional trains did not explode. In the successfully prevented case of Dresden, the staff recognised the bag on the platform as suspicious, trusted their gut feeling, and alarmed the authorities. A canine confirmed explosive substances. The remarkable aspect is, that this particular suitcase was identified as suspicious out of hundreds items left behind in trains and stations every week. Obviously, the subjective recognition of threats by experienced staff who trust their assessments can be of invaluable importance. Cautious sensitisation of personnel can support this ability. In addition, systematic plausibility-checks (as practiced in different ways e.g. in London and Hamburg) may support the employees' judgements. The simultaneous attacks with IEDs hidden in bags on commuter-trains in Madrid 2004 also demonstrated the importance for cautious sensitisation of staff and passengers regarding threats from terrorism and serious crime, in combination with the need to establish effective channels of communication facilitating the reporting of suspicious items or behaviour.

The analysis of the Sarin-attacks on Tokyo's underground-system in 1995 by the Aum Shinrikyo sect reveals several shortcomings. Despite previous attacks with chemical weapons by the apocalyptic sect, the staff of Tokyo's subway-operator was not aware of the possibility of such an attack occurring. Consequently, the threat was not identified quickly and some of the trains continued servicing (up to 100 minutes after the attack), so that the number of victims among passengers and workforce increased accord-

ingly. Staff and passengers should have been sensitised and informed about potential threats and how to recognise them. Inadequate internal and external communication and coordination further delayed the recognition of the threat and the efficient response.

An arson attack by a suicidal in Daegu/Korea in 2003 turned disastrous, killing 192 people, due to a fatal combination of factors. Next to non-fire-resistant materials of trains and stations, missing and insufficient emergency-equipment, major misperceptions and wrong decisions by train drivers and OCC-staff were to blame. Frequent false-alarms had numbed the staff to alarms, and the real alarm was ignored. Comprehensive training of personnel and real exercises could possibly have uncovered some of the systematic deficiencies behind, and could have inserted the needed competences and confidence among staff, to enable an effective response and avoid the panic, which occurred.

The few examples suffice to demonstrate the wide spectrum of potential assaulters (extortionists, apocalyptic sect-members, suicidal, terrorists, etc.) as well as the wide range of weapons they use for their perfidious aims (arson, IED, chemical, etc.). Qualified staff makes the decisive difference for safeguarding themselves, passengers and material values. The precondition for the staffs' adequate response is their basic knowledge and understanding of potential threats combined with a training in time.

3. Obvious needs and determining framework

Among critical infrastructure it is public transportation, which is most vulnerable, and where the need for protection as well as rescue of persons is most crucial. Public transport operators and their personnel shoulder extensive duties and responsibil-

ities in preventing and mitigating attacks from terrorists and other perpetrators.

In contrast to (unintended) safety-threats where safeguards and trainings are established and of highest standards, the training needs for countering (intentional) security threats are often not yet met ideally. There are manifold reasons for that, but two aspects stand out:

- (1) Public transport operations particularly of medium and small size are often unfamiliar and insecure regarding the "nature" of these "new" threats and the means to counter them, and
- (2) more often than not they simply lack the resources to accomplish demanding additional responsibilities (resources such as manpower, time, fees for training-courses/trainers, and most important business-interruptions for real-exercises).

Both aspects particularly hold true, when trainings should not only be conducted as conventional ex-cathedra teaching, but state of the art trainings and further education shall be applied, in order to achieve best learning results.

Real exercises are considered most effective regarding knowledge transfer into working-environments. However, they tend to be most expensive – especially when they need to be applied for qualifying high numbers of staff.

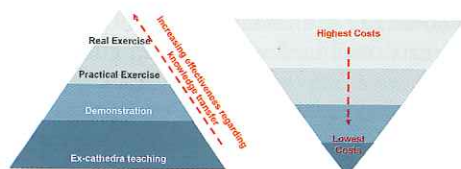


Figure 2: Effectiveness regarding knowledge transfer into working-environments versus costs of different training formats

"You have to invest in people, and then rely on them – you've got to invest in technology, but don't rely on it", said Tim O'Toole, Man-

aging Director of London Underground, after the attacks on 7th July 2005.

Neither could or should human resources supersede technology, nor vice versa. The key to success clearly lies in the right balance of high- and low-technology, and technology has – among others – a decisive role to play in developing human resources to its full potential, as becomes evident in the following paragraph.

4. Solving the dilemma

As stated above, public transport staff constitutes the first line of defence in countering attacks by recognising threats, communicating them, evacuating trains and stations, protecting themselves and passengers, showing and directing arriving rescue-forces, etc. Doing so, public transport operations are forced to shoulder more and more responsibilities in "new" and additional fields, where – in contrast to safety aspects – they often lack experience. In order to fulfil these extra tasks, their numerous staff must be adequately prepared, i.e. sensitised and qualified. This requires considerable resources given to quite a numbers of staff, in times when funds are scarcer than ever before. Not to mention the organisational challenges to train e.g. a chemical attack. This burden of additional tasks, scarce resources and the superiority of expensive real- and practical-exercises over simple ex-cathedra-learning is creating a dilemma for transport operations that shall be tackled by innovative technology that improves the quality of staff-training at minimised costs. V-SICMA is the name of a research-project, financed by the German Federal Ministry for Education and Research's Security Research Programme, in which a consortium of eight partners from social-sciences, industry, consultancy, law-enforcement as well as security organisations, and public transport operations are taking up to solve

this dilemma by developing a demonstrator for security-trainings of public-transport staff, that is an interactive, three-dimensional computer-simulation of relevant scenarios.



Figure 3: A precondition for public transport operations to train their numerous staff is an effective training tool at minimal costs. Real- und practical exercises are proven learning formats – but at prohibitive expensive costs. This dilemma is solved by a research-project V-SICMA, which develops a demonstrator for a simulation-tool, which replaces costly and difficult real- and practical exercises with equally learning-effective virtual realities.

The interactive and simulation-based, three-dimensional visualised modules are the core of the training concept for different categories of public transport employees, which comprises different schooling-formats regarding assaults against public transport systems. Each schooling-format has its strengths and weaknesses, and the advantages of the respective methods will be brought together and made use of. V-SICMA combines research in various fields starting with psychology and behavioural science, information technology, security-research, educational science, public transportation and social science.

Psychology and behavioural science are focussing on individual as well as group-dynamic human behaviour representation including crowd riot control and their handling (individuals and masses). Soft skill assessment of personnel assigned for crisis management, decision-making processes and communication within complex and in-transparent crisis-situations accompanied by time pressure and lack of information, are among the research-topics in this field.

Information technology and techniques for three-dimensional modelling, computer graphics, game-level design, interactive storytelling and the inclusion of educational aspects to develop so called serious games and enable game-based learning are topics to deal with further. Innovative is – among others – the development of a simulation based learning environment, whereby the public transport staff gets the possibility to train interaction with passengers, other transport-staff, security- and rescue-teams, and possibly perpetrators in a consistent scenario-setting. Moreover, to sensitize the public transport staff to potential threats, dangerous or unusual situations can be trained and effects of own decisions and behaviour can be experienced in the virtual scenarios without physical risk for their and public lives. These simulation based three-dimensional learning-scenarios are based on current scientific research and cutting-edge technological for the improvement of security-qualifications of public transport staff.

Security-research needs to assess the present organisational and procedural practices, define the relevant threats and scenarios, develop ideal types of organisations and practices for public transport operations of different sizes, and define the content of the curricula for different target-groups (i.e. the different functions of staff on strategic, tactical and operational level) including – among others – communication-aspects within and between organisations (transport operator and rescue-/security-teams).

Educational science needs not only develop and assess curricula, profiles of requirements and qualification regarding contents of security in public transportation, but assess and comprehensively evaluate different formats of security-training. Effectiveness and cost-efficiency of conventional trainings must be compared with interactive, simu-

lation-based trainings. So far, the technical-didactical relevance of behaviour modelling has never been evaluated for security-trainings.

Public transportation has a long tradition in all (unintentional) safety matters, whereas (intentional) security threats are relatively new to most stakeholders in the field. Actual needs and the limiting/determining factors by the general framework and specific requirements need to be systematically analysed and taken into account, in order to come up with solutions that really suit and gain acceptance.

Social science must explore the acceptance of security-measures at all levels and in different functional areas within public transport operations, and draw an organisation-ethnographical picture of security-awareness against multiple, partly competing business objectives and institutional frameworks. Paradox constellations are 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.

The demonstrator of such a training tool, which will be developed in the V-SICMA project, constitutes an innovative technological solution for urgently needed security trainings of employees in the most vulnerable of all critical infrastructures, public transport. It has the potential of overcoming the most important obstacles for public transport operations in meeting the security-challenges of the 21st century, by providing training, that is especially developed for security threats, that is of highest learning-effectiveness, almost as high as real exercises, though at minimal costs, because it does not require the shutting down of (parts of) the systems or business interruption.

For these reasons, the approach is an ambitious technological solution to pressing challenges and of greatest practical applicability at the same time.

- ¹ MTI Report 01-07 (2001): "Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices", by Brian Michael Jenkins and Larry N. Gersten. Mineta Transportation Institute. San Jose.
- ² EUROPOL (2009): "TE-SAT 2009. EU Terrorism Situation and trend Report". European Police Office. The Hague.
- ³ UITP (2003): Urban public transport and Anti-terrorism Security. Expert Round Table Brussels, 11/12 December 2003. Synthesis and Conclusions. Brussels.

Contact:

Dr. Matthias Mueth
Hamburg-Consult GmbH
Spohrstrasse 6
22083 Hamburg
fon ++ 49 – (0) 40 – 27 166 563
fax ++ 49 – (0) 40 – 27 166 410
e-mail: m.mueth@hamburg-consult.de