



DELIVERABLE D6.1

Briefing for EC/DE workshop: System-of-Systems Demonstration & Experimentation for Mass Transport Security

September 2009

Author:
E. Anders Eriksson (FOI)

PUBLIC

Grant Agreement number :	218264
Project acronym :	DEMASST
Project title :	Demo for mass transportation security: roadmapping study
Partners:	FOI (SE, coordinator), Ansaldo STS (IT), CEA (FR), Diehl (DE), EADS Astrium (FR), FFI (NO), Fraunhofer (DE), INECO-TIFSA (ES), SINTEF (NO), TECNALIA-INASMET (ES), THALES Security Systems (FR), TNO (NL), and VTT (FI).

Reviewed by:

J-F Sulzer (Thales)

Content

Executive summary	2
Introduction	4
Scope of the FP7 Security of mass transportation programme	6
What mass transportation?	6
Target mass transportation systems: A broad range of urban transport but focusing on rail in megacities	7
What security missions?	7
Defining threat focus: An all hazards approach including catastrophic terrorism and represented by a few carefully selected scenarios.....	9
What solutions?	10
Understanding systems of systems.....	11
System-of-systems architecture for mass transport security	13
Operational systems – definition and analysis	13
Security systems – definition and analysis.....	14
System-of-systems development methodology.....	18
Demonstration projects ≠ demonstration activities	18
System-of-systems demonstration and experimentation.....	19
Exploiting the synergies from the full range of experimentation methods: from “live” to in silico experimentation	20
MTSDEP design and implementation.....	22
Criteria for programme design	22
Operational and security systems in relation to the MTSDEP	23
MTSDEP design.....	25

Executive summary

This report was originally written as input to the March 2009 workshop organised by EC and the German federal government to inform the drafting of call text for the FP7-SEC mass transport security demonstration programme. Or more precisely for the “real” demo activities of the so called phase II, with the current project DEMASST being the phase I road-mapping study. Subsequently the report was updated to reflect the published FP7-SEC work programme (29 July 2009) as well as DEMASST’s work in the intervening period. Still this is very much work in progress, with final results due in May 2010.

DEMAsST’s understanding of the problem of security of mass transportation (in the phase II call defined as urban and regional public transport) is characterised by, on the one hand, very tough requirements in terms of acceptable costs and traffic delays, on the other a very heterogeneous situation in terms of legacy systems both within and between regions, a wide scope of risks and threats, and great variety of present and future security solutions. While it is immediately clear that not every factor combination of legacy systems * risks & threats * security solutions can be treated in real-world experiments and demonstrations, any successful approach to mass transport security solutions must still find a way to handle this whole space of possibilities. Modelling and simulation is an indispensable tool for this – which in no way

negates the need to test solutions in a number of real cities; likely higher than the three given as lowest limit in the call.

We also discuss the meaning of “systems of systems”, a terminology used in the call text and previously in the ESRAB report. We understand the idea as being to achieve coherence at mission level while retaining heterogeneity at system level – in contrast to highly integrated systems. Typically a highly integrated system can be made very cost-effective for a narrow range of tasks. In contrast a system-of-system approach has its strength when confronting a wide range of tasks, solvable by composing the constituent systems in different ways. This fits well the complexities outlined above.

With real-life experimentation and modelling & simulation as extreme points, a number of intermediate options like test-beds and man-in-the-loop simulators are identified, as well as certain types of “non-experiments” like exploitation of so called natural experiments. To handle the reality of many important situations being too difficult, dull or dangerous for an all real-life experimentation approach (the Three D’s somewhat modified from robotics), a successful demo programme must exploit the full range of methodologies and their synergies.

The report also presents a provisional system-of-system architecture for mass transport security consisting of seven transport and nine security systems (designated A-G and H-P, see below for examples), all quite broadly defined. Together with the thinking on the Three D’s, the different types of experiments (and non-experiments), and the need to handle physical as well as time critical information flows, this leads to some conclusions regarding programme design:

In principle, for systems that are relatively isolated cost efficiency suggests separate projects. For systems that are strongly coupled cost efficiency instead suggests joint projects. If diversity is great this could comprise several experimentation platforms in settings spanning this diversity. Specifically, the analysis suggests that five systems form a strongly connected core representing high requirements in particular on time critical info exchange, while being reasonably amenable to live experimentation:

- B. Major interchange (typically intermodal)
- C. Passenger information systems (system-to-customer and peer-to-peer)
- I. Risk assessment-based command and control
- J. Comprehensive threat detection
- K. Preventive/early intervention.

Hence these system areas ought to be addressed in (one or several) joint projects capturing at least important parts of their interactions. This said it should be clarified that the focusing on these five systems in no way means that all the rest can be safely disregarded. Quite the contrary a serious Mass transport security programme must have access to state-of-the-art knowledge in all the identified 16 system. And whereas the more generic ones are hardly reasonable candidates for funding from a Mass transport security programme beyond interface work, others like, say, tunnel rescue operations could very well merit such funding.

Introduction

DEMASST is the phase I (road-mapping) study of the Mass transport security programme funded under FP7-SEC.

Due to problems regarding the security scrutiny negotiations were delayed and DEMASST started quite late – in January 2009. With an earlier start-date the study could by now have been completed. In the present situation instead DEMASST strives to inform phase II as it evolves. While the disadvantages of such delay are obvious, arguably there is also an advantage in that the issue will be higher on the agenda, hopefully meaning an increased interest of stakeholders to engage in conversation on Mass transport security Research, Development and Innovation (RDI). And despite the very considerable internal resources of the DEMASST consortium, learning from others is key to success.

DEMASST therefore strives to provide input useful to:

- EC and MS for the various steps of the phase II work – from call text preparation to negotiation – and perhaps project review
- prospective phase II consortia (most deliverables and workshops will be public)
- to the selected phase II project(s)
- to the wider mass transport security community, e.g. in the form of identifying “low-hanging fruit”, i.e. improvements possible to implement even without demo activities, as well as guidance for research also in areas to immature to now include in demo activities
- to the security RDI community at large..

Having said this it should also be said that the DEMASST member organisations are not neutral with regard to phase II, they are most certainly interested in bidding, but with a strong interest in open and fair phase II competition. Therefore we find it important to work with public deliverables and open workshops whenever possible, and to involve a wide range of stakeholders via workshops and interviews. An important background to this is that the interest of DEMASST partners does not end with the current FP7 demonstration programme. If this programme does not help in creating an enhanced European security innovation system – in mass transport and for most partners also quite generally – the work will have been wasted from the strategic point-of-view despite the EU funding possibly received. Hence, DEMASST’s prime concern is helping to define a model for sustained security system innovation. For this it is of utmost importance to have a successful demo programme in mass transport security. Who gets to do what in that programme is in the long run a lesser concern.

The present report was presented in preliminary form (WD6.1) at the workshop convened to inform the drafting of call text for the phase II programme. This workshop was held in Berlin 18 March 2009 and it was organised jointly by EC and the German federal government. The preliminary paper was prepared in a short period of time based on the expertise of the consortium and a few invited experts at workshops.¹ The present version implicitly reflects the work that has been ongoing in DEMASST between March and now, which will shortly

¹ WD6.1 is available on DEMASST’s website www.demasst.eu. See also WD6.2 there for a brief survey of relevant resources available on Internet.

manifest itself in a number of deliverables. However, D6.1 is not different in nature from WD6.1; it is a thought piece, not a detailed technical account. It will then be more systematically elaborated throughout DEMASST, building on the diverse strands of work as indicated in Figure 1, to appear as the final roadmap at the end of the project in May 2010.

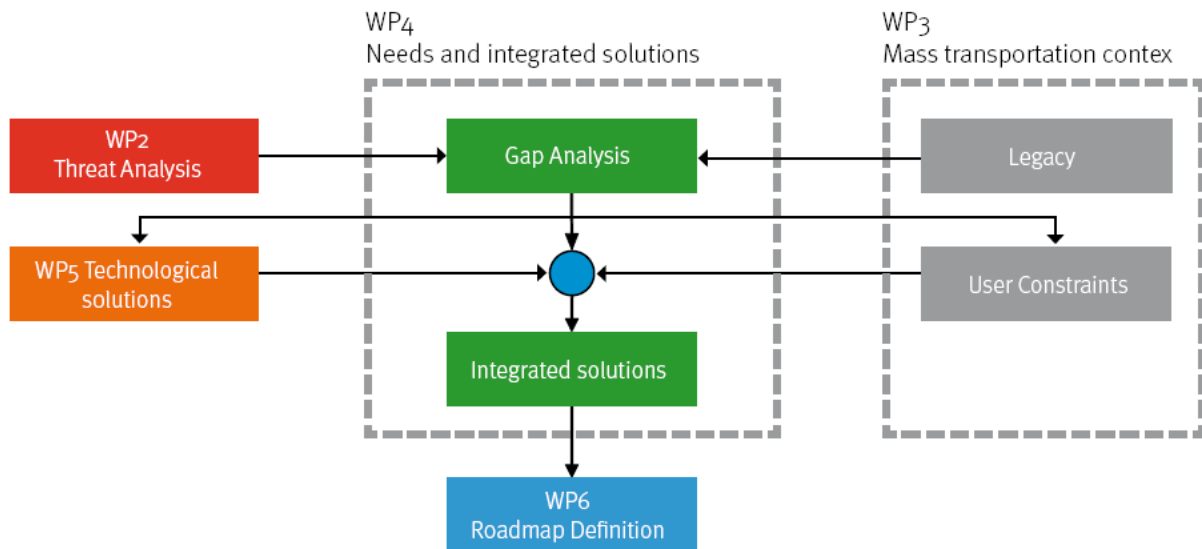


Figure 1. Workpackage structure of DEMASST

In terms of content the main development over WD6.1 is in the scoping achieved in the following chapter. The rest of the report outline is presented at the end of that chapter based on this analysis.

More editorially – and linked to the above development – D6.1 relates to the published call text for phase II (cf. Annex 1) where WD6.1 was written as a discussion of the Commission’s non-paper intended to ignite debate at the Berlin workshop. While this was the obvious choice for a presentation at that same workshop, retaining discussions of bygone aspects of a paper long ago superseded by the various stages of development of the call text felt awkward. Then on the other hand it was natural to await the final version of the call text, which was published 29 July 2009.²

² Also in D6.1 reference *is* occasionally made to the non-paper. This is in particular in respects where the non-paper arguments are judged to provide an interesting context to the call text. When this is the case, the non-paper material is presented so as, hopefully, not to require the access to the non-paper itself.

Scope of the FP7 Security of mass transportation programme

This chapter discusses the scope of the called phase II programme in the following respects:

- What specific (types of) mass transportation systems should be considered?
- What kind of security missions (e.g. threats) should be considered?
- What kind of solutions should be considered?

It is furthermore argued that these three aspects jointly suggest a suitable way to understand the ‘system-of-system’ level of security solutions. ESRAB introduced the demonstration programmes to deal with this level, but neither ESRAB nor the work programme goes very far in explaining this, either in general or for mass transport security.

What mass transportation?

The call squarely identifies the focus of the demo programme as “urban and regional public transportation.”. In the non-paper a number of compelling arguments for this were provided:

- A. Other aspects of (system-of-system) transport security are covered by other FP7-SEC work like the planned DP “Logistic and supply chain security” for freight and the IP topic on Airport security called in 2008.
- B. Urban public transport is in line with the definition of “mass transportation” used in other EU work.
- C. Political priority is on urban transport security in the wake of the Madrid and London bombings
- D. Insufficient relevant research so far:
 - In particular the volumes of passengers are orders of magnitude greater in urban transport than for major airport,³ hence rendering direct “solutions transfer” from the latter, more researched domain infeasible.
- E. European dimension by virtue of the similarity of problems across big cities in Europe and hence a potentially very important EU-wide market.

It should be noticed that the type of transport where most security investments are made is air. As commented above the much smaller transport flows there – as well as the naturally much fewer access points and the higher traveller acceptability of delays due to less frequent trips – make it difficult to directly transfer solutions from air to urban transport. Selecting air transport security as focus would render a very different project than with urban transport, even though some security characteristics are akin (compared to other walks of life also air transport deals with very big streams of people).

In terms of societal functions the main role of public urban and regional transport is daily commuting to work. Here public transport competes with and complements cars – and of course bicycles and walking. It could be argued that also these provide “mass transport”. However, the overlaps in terms of threats and security solutions are limited and therefore possible to handle as “add-ons” when necessary.

An aspect given some prominence in the call is the interchanges between long-distance – sometimes cross-border – and urban/regional transport. However, the volumes concerned are

³ London and Paris local transport have ca 7 bn passengers annually, Heathrow airport 68 mn.

much smaller than for purely intra-regional transport and the difficulty in separating the cross-border related elements out render this an only supporting argument.

However, focusing on the **intermodal interchanges** where intra-regional and long-distance transport – some of it cross-border – meet is sound in the sense of going for the hardest problems one can hope to solve, the solutions of which are likely to help solve also many easier problems.

Other problems of urban transport compared to long distance are the many, hard-to-secure access points and the high sensitivities to cost in systems with typically partial tax funding.

But, again, these major challenges also suggest the possibility of transferring successful urban transport security solutions *to* other domains like air transport.

Target mass transportation systems: A broad range of urban transport but focusing on rail in megacities

All types of disruptions will have the most far-reaching effects on people and economies if in a megacity. In smaller urban areas the margins are wider and it is much more doable for people to substitute car, bike, or walking for a troubled urban transport system.

This does in no way imply that medium sized cities should be neglected. At least non-terrorist threats are equally likely to hit these. And, whereas perpetrators of catastrophic terrorism will prefer megacities as more symbolic targets, a high security level there but not elsewhere may induce target substitution.

With a sufficiently generic methodological approach, utilising Modelling & Simulation as will be outlined in what follows, it should be possible to generalise results well beyond the specific locations of experiments and demos. For example, even if megacities are of particular importance this does not imply that all the actual experimentation has to take place in such cities. In fact smaller cities are likely to provide more tractable demo platforms. This said it is important to be aware of differences between systems that may require testing in different environments, to make sure that solutions are usable for different cities (but one example of different environments is that the distance between stations in underground train systems can vary significantly between different systems, rendering different incident response strategies suitable).

The work programme requires a testing phase in “at least 3 real cities,” different in terms of cultural background and urban public transport system. Despite what was said above the ability to generalise results this number seems on the low side in terms of capturing the variety of European public transport.

What security missions?

The key security relevance of mass transportation is two-fold:

- Mass transportation systems, particularly under rush-hour conditions, are characterised by very high densities of people, otherwise only to be found in major events like football matches. The latter type of events also constitutes another major security challenge for mass transportation systems, with different passenger behaviour patterns than for commuting. These two situations suggest that accidents as well as attacks by, e.g., terrorists in mass transportation systems have the potential to create very major casualties.
- Mass transportation systems – together with private commuter transport – are a critical infrastructure for employees to get to their workplaces, meetings, etc. Even though disturbances to this function do not create danger of life and limb as would be the case, e.g., for water supply, the economic consequences are very large particularly in the largest urban regions where the scope for substitution of public transport is very limited.

A remark here is that while a major attack on travellers is likely also to cause infrastructural service dysfunctions – not least due to scare and suspicion of new attacks – the possibility of causing major economic impact without harming people may render purely technical disruption attacks (e.g. cyber) an attractive option for activists interested in maximising economic fallout while minimising human casualties. This is not a type of aggressor that first comes to mind in an era characterised by exceptionally blood-thirsty jihadist terror, but, as always, preparing for the “previous war” is seldom the right way in dealing with intentional insecurity.

Starting with the first bullet, the situation with suspect suicide bombers – i.e. person-borne IEDs⁴ (PB-IED) – in or closing in on a big urban transport hub, can in many respects be seen as the worst-case challenge of the mass-transportation area. Spreading of lethal CB agents is another very challenging scenario.

Scenarios like these will have to be treated in any serious mass transportation security demo programme, at least as long as they are seen as politically plausible.

Therefore it is important to include reactive handling at all phases of an antagonistic threat in the mass transport security demonstration. The possibilities for early detection as well as the means by which authorities can get an accurate situation picture during the event must be tested. Another important function in handling (in particular) intentional insecurities is the forensic investigations that take place after an event in order to determine who was responsible for the attack.

It is also important to test the extent to which the mass transportation system is robust against multiple, near-simultaneous attacks against it as well as the extent to which some of these threats can be detected early, for example during reconnaissance at the scene by prospective attackers.

However, focusing only on this type of worst challenge is not a good approach. In fact the call requests a “holistic and systematic all risks approach”. How shall we understand this?

⁴ Improvised explosive devices.

First it is suggested already by the above observation that mass transport has characteristics making it attractive both for the human casualties maximising (first bullet) *and* for the human casualties minimising/economic impact maximising (second bullet) types of threat actor. Further, mass transportation systems are the locus of a whole range of other hazards, including fire, spreading of disease, theft, assault, gang-fights, vandalism, etc., which are of great concern to many passengers and therefore an impediment to public transport fully realising its market potential.

In addition high-end security solutions are, simply said, easier to sell if they can also – at least partly – be applied to a wide range of lower-end security and safety problems. From this perspective, focusing only on the worst case scenario is seldom a good approach in security RDI activities. The optimal solution for the worst case is very seldom either completely irrelevant or perfectly applicable for other threat scenarios. Hence high-end security solutions can add value by also being applicable to a wide range of lower-end security and safety problems, but this typically requires some further attributes to the solution. Therefore a **modular approach** – is particularly fruitful in this regard, where different systems may take on somewhat different roles for different types of challenge, and where the combined effect may differ dramatically.

It is also worth noticing that this economies of scope⁵ perspective is applicable not only to the build-up of systems but also to the operational side. An all hazards approach here avoids contingencies falling between chairs or getting fouled up in processes of transfer of responsibility. Also, having continuously to deal with real contingencies is good from an operators' training and readiness point-of-view.

Defining threat focus: An all hazards approach including catastrophic terrorism and represented by a few carefully selected scenarios

Based on the above there are strong arguments for the mass transportation demo taking an all hazards approach including the worst types of threat scenarios but also a wide range of lower-order contingencies.

This does, however, not mean that “all” threat scenarios (whatever that would mean), or even very many, need to be played out in real exercises. Instead a small sample, but sufficiently representative of a much wider set of scenarios to allow generalising of results, must be selected.

DEMASST includes development of a threat data base with a parameterised threat model to allow systematic navigation and the identification of representative subsets of the whole threat space. It is also discussed in what follows how Modelling & Simulation resources are needed to help in generalising results.

⁵ While the more standard concept “economies of scale” focuses on the gains from making a larger number of the same item, “economies of scope” is about the gains from coordinating the making of different types of items, having some similarities.

What solutions?

First of all it is clear from the call as well as the ESRAB report that what is sought for is ‘system of systems’ solutions. The meaning of this will be further discussed in the following section, but one important aspect is that we are not discussing technology alone. Non-technical (at least in part) areas mentioned in the call include passenger interaction, staff training, and operation procedures. Other aspects mentioned in the call are the economic implementability of solutions and the appropriateness of security measures with respect to given legal, cultural and societal environments.

Another important attribute of solutions is their **maturity** or **readiness level**. One pertinent passage in the ESRAB report reads:

research path 3 — systems of systems demonstration (multi-mission): the challenge of integrating a number of systems in which the integration and demonstration aspect represents the majority of the work, and challenge, to be undertaken; these are intended to be ‘flagship’ demonstration programmes providing a federative frame to coalesce research in areas of significant European interest.

This suggests that we must be talking about relatively mature technologies (inasmuch as we are talking about technologies at all, cf. above); it does not make sense to engage in extensive integration and system-of-systems level demonstrations for futuristic technologies.

Figure 2 gives a perspective on this and on the relationship between demonstration programmes, integration projects, and capability projects. The corresponding figure of the ESRAB report also clarifies that it is the role of capability projects to improve the maturity level of capabilities, one would assume such that they can be included in integrated solutions at system and system-of-systems level. Of course it does not make sense to see the Security research programme as a closed, self-contained system. Therefore, e.g., in the mass transportation security programme, capability and system level solutions must in no way be developed in dedicated projects, but may come from other areas of R&D, as well as be already industrialised, in other words available off-the-shelf. If this were not the case a mass transportation security demonstration programme would be hard to achieve given the relatively limited dedicated efforts so far at capability and system level.

On the other hand, if system-of-systems solutions are locked-in with today’s mature capabilities we are in for major problems in the future. Rather, just as it was argued above that the solutions sought in the programme must be applicable beyond the specific threats and the specific cities and regions that feature in the work, they must also be able to absorb and effectively utilise other types of capability, not least emerging and futuristic ones.

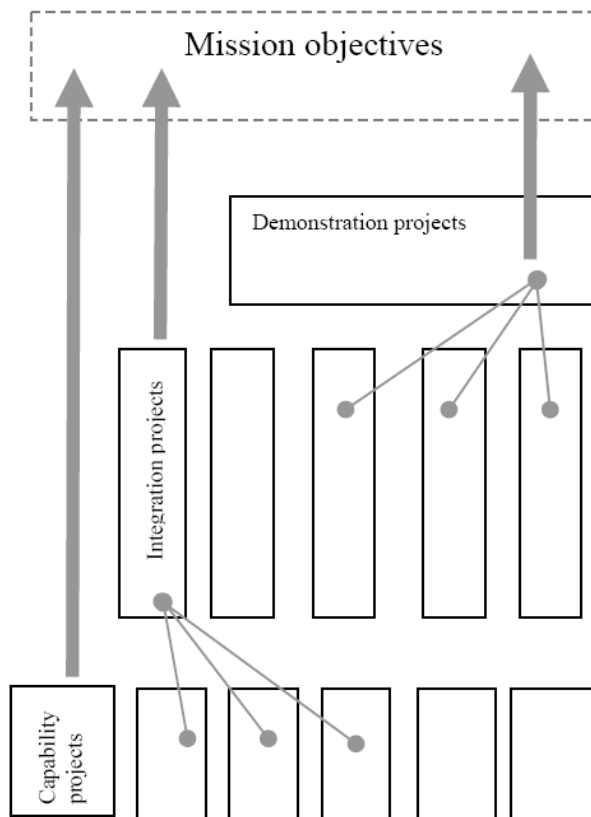


Figure 2. Relationship in principle between the types of project in FP7-SEC (from work programmes)

Understanding systems of systems

From the work in DEMASST so far it is clear that the ESRAB system terminology, essentially of military origin, sometimes creates confusion and disbelief when confronted with the mass transport sector. It seems that many tend to understand systems-of-systems as something exceptionally highly integrated and perhaps even harmonised to European uniformity. While more harmonisation likely would be useful in some respects, say communication with passengers for the benefit of non-local passengers or aspects of first-responder tactics to be able to share highly specialised and expensive resources, on the whole a strive for uniformity would make very little sense in a sector where solutions naturally and for good reasons differ considerably even between cities in the same country or region.

Fortunately the idea of system-of-systems solutions, arguably, is precisely to achieve coherence at mission level while retaining heterogeneity at system level. At least this interpretation is well in line with ESRAB and supported by many scholarly sources.

For example, a “[s]ystem of systems is a collection of task-oriented or dedicated systems that pool their resources and capabilities together to obtain a new, more complex, 'meta-system' which offers more functionality and performance than simply the sum of the constituent systems.”⁶ We here understand functionality as *what tasks* can be achieved, and performance

⁶ http://en.wikipedia.org/wiki/System_of_systems

as *how cost-efficiently* the tasks can be performed. Of course a highly integrated system can typically be made very cost-effective for a narrow range of tasks. In contrast a system of system approach has its strength when confronting a wide range of tasks, solvable by composing constituent systems in different ways, as enabled by an overall architecture and standardised interfaces.

A system of systems is typically characterised by the following properties:

- operational independence of elements
- managerial independence of elements
- evolutionary development
- emergent behaviour
- geographical distribution of elements.⁷

Due to this, modelling and analysing systems of systems typically involves:

- inter-disciplinary study
- heterogeneity of systems
- networks of systems.⁸

Based on these types of characteristics, it is reasonable to conceive of mass transport as a system of systems already at the level of a given city or region. Or for that matter mass transport security, which can be understood as the combination of the mass transport system-of-systems in general (but taken from the specific point-of-view of security) and dedicated security systems. In line with this, in the next chapter we develop a simple **system-of-systems architecture for mass transport security**.

We have argued above that a system-of-systems approach that solves just a few security missions, for just a few cities, only using today's technology could hardly be judged as an adequate constituent of the Security research programme. Yet, applying terms with sufficient rigidity, this is precisely what will happen in any demonstration programme with a budget constraint.

The solution to this apparent paradox lies in our ability of extending experimental results – and non-experimental empirical knowledge – by theory and modelling. Therefore in the chapter after next we develop a **system-of-systems development methodology** combining these strands.

In the final chapter mass transport security **demonstration programme design and implementation** is discussed based on the other chapters of the report.

⁷ Maier, M.W., "Architecting Principles for System of Systems," Systems Engineering, Vol. 1, No. 4, 1998, pp. 267–284.

⁸ <https://engineering.purdue.edu/Engr/Research/Initiatives/SoS/>

System-of-systems architecture for mass transport security

This chapter presents the systems that will subsequently be the level of analysis in this paper. We see the mass transport security system-of-systems as consisting of two types of system:

- the “normal” operational systems
- the dedicated security systems.

The ensuing security is obviously a combined effect of operational and security systems, and both types therefore need to be considered in the demo programme.

The systems being used here are defined so as to be quite abstract and generic. Many, if not all, must in a more detailed analysis themselves be understood as systems-of-systems. However, for this preliminary work we have found this level of abstraction the appropriate one.

Operational systems – definition and analysis

In line with its urban public transport focus, the call identifies the following modes as included in the task:

- metro
- tram
- short distance regional rail transport (e.g. RER-Paris and the S-Bahn)
- city busses
- water buses
- airport shuttles.

These modes of urban transport all have their infrastructures such as tunnels and bridges, as well as the traffic controlling and regulating systems. Some of these are shared with private cars – and for that matter with freight vehicles.

Intermodal interchanges – so called neuralgic nodes – have already been identified as a key type of infrastructure from a security point-of-view. This is true both because of high passenger densities making them likely targets for all kinds of passenger-related problems, and because of their importance as key nodes in the transport network. A major problem in a major hub will affect also those passengers who need to pass it. A major interchange is a complex system in its own right. What is of particular interest here is how passengers flow through the interchange.

Parking areas and repair shops for vehicles constitute a system that can be of interest for attackers wanting to plant bombs or other devices for release of dangerous substances, or sabotage vehicles to disrupt traffic.

IT and communication systems are in today’s world always necessary to consider in security work. This includes both the ICT systems required for the operation and control of the above – sometimes referred to as SCADA,⁹ and the passenger information systems.

⁹ Supervisory Control And Data Acquisition

Passenger information systems must today be seen as falling into two categories – the system-to-customer systems and the peer-to-peer systems.

From a security point-of-view the former could enable cyber attacks on the SCADA systems (when traffic information is transferred from the SCADA systems to the passenger info systems, there may be back-doors from passenger information to SCADA systems).

The peer-to-peer passenger information systems (which of course are generic mobile communication applications that become passenger information systems when people choose to input information on urban transport systems in them; examples are sms text messages and micro-blogging such as twitter, not to mention innovations yet to come) could become a very major driver of change in mass transport security. Both negatively by providing new ways for panic to arise, for hooligans to swarm in on whatever target, or for terrorists to detect signs of countermeasures being taken, and positively by providing new avenues for promoting constructive traveller behaviour in difficult situations. As has been shown in recent history (terrorist attacks in Mumbai), many details about ongoing catastrophic events will be micro-blogged about in real-time. It is important to investigate how this information could be used to enhance the situation picture of responders. It is also important to determine how the ability of passengers to communicate with each-other can influence their behaviour during an incident.

More systematically we can identify the following levels and systems from the operational side:

- A. The whole urban/intra-regional transport system including also private means of transport inasmuch as there are opportunities for substitution between private and public transport (network level)
- B. The major interchanges (typically intermodal), which are passed by both many passengers and many transport platforms on different lines
- C. Passenger information systems (system-to-customer and peer-to-peer, cf. above)
- D. Lines and roads including smaller stations and other entry points, tunnels, bridges, etc.
- E. Vehicles/transport platforms
- F. Vehicle parking areas, repair and maintenance shops, etc.
- G. Technical support systems (control, power supply, ventilation, etc.) including SCADA systems.

Security systems – definition and analysis

As the relevant operational systems were analysed in the previous section, it is also necessary to discern the relevant security systems, which together with the operational systems will build up system-of-systems solutions. A list from the “non-paper” can be of some assistance here even though it is not made for exactly this purpose:

1. Security systems designed to meet specific requirements for mass transportation networks, transfer nodes and platform interiors;
2. Interoperability of different security systems managed by different operators and/or between different EU countries;

3. Comprehensive threat detection systems fusing data across diverse and distributed networks and analysing threats via spatial/pattern recognition techniques. Detecting, tracking and tracing individuals, crowds and objects within, and across, transport systems, while respecting the personal integrity of individuals;
4. Post-event situation analysis systems capable of rapidly accessing and piecing together different multi-media and digital data to re-enact a sequence of event;
5. Common operational picture integrating and displaying data from a diverse set of sources on optimised man machine interfaces utilising intelligence based alarm management;
6. Neutralisation and containment systems for attack avoidance, suppression or nullification.¹⁰

Note first that items 1 and 2 are not about specific security systems, but rather cross-cutting issues of great relevance.

In what follows items 4 and 6 will be subdivided into multiple elements.

Of these **preventive and early intervention** deserves special attention. What we have in mind here is intervention before many passengers have been affected by – or even noticed – a real or potential attack. This can mean preventive intervention against a suspect PB-IED or quick reaction after suspect release of a B agent or in case of fire.

Item 3, **comprehensive threat detection systems**, is of utmost importance to any innovative mass transport security solution. The security systems must be able to use and exploit heterogeneous information from many different sources, ranging from sensors of different kinds (e.g., image and video, signals and communication intelligence, CBRN detectors) to intelligence information from databases and open source information collected from the web (cf. below). This requires the development of adequate tools to integrate and fuse the information from the different sources. Particular emphasis must be placed on how to correlate information about the same entities/events from different sources, e.g. for tracking and tracing, and on

¹⁰ The “non-paper” list has been retained since the effort needed to implement the work programme version of the list have not been judged as worthwhile. These are the additions with comments on how they fit in the suggested architecture:

- Exploring ways of interconnecting urban transport data systems based on electronic ticketing/payment (for example: Oyster Card – London, MOBIB – Brussels, NAVIGO Paris, and other similar) with other security systems; *belongs to operational systems*
- Preparedness and design for resilience; *inserted at beginning of item 4, preparedness belongs to several security systems, design for resilience is seen as an aspect of several operational systems*
- ...handling the interagency aspects of mass transport security and utilising intelligence-based risk assessment and alert systems; *inserted in item 5, covered in particular by item I below.*
- Optimized interactions with the passengers, with regard to the newest consumer IT technology; *cf. item C above*
- Intervention and operations technologies wherever appropriate to cover synergies of security and safety and cost-effectiveness, *cf. items K and N below.*
- Improving the protection, hardening and resilience of existing and new infrastructures related to mass transportation, *cf. design for resilience in this list*
- New tools (e.g. simulation, virtual and augmented reality) to improve the training of the staff; *cf. item P below*
- Recommendations for operation procedures in case of a security situation, *cf. item I below.*

how to ensure that all information has the right quality markings (in terms of uncertainty and other factors).

Item 5 is reformulated to **risk-assessment based command and control**, with common operational picture playing a key role but also risk-assessment – the ability constantly to make sound trade-offs between on the one hand passengers’ security and safety and on the other their comfort and uninterrupted travelling in a setting where threat detection systems will never be free of false alarms.

The just mentioned problem also points to the importance of a system type absent in the “non-paper”, viz. **intelligence**. Intelligence systems are external to mass transport *per se*, but good understanding of the ability to get advance information on threats, threat agents, etc. is key to the design of security solutions. Further, as alluded to above, “RED ALERT ALWAYS” systems don’t work in reality so some level of access to intelligence to guide risk-assessment is a prerequisite for any security system aiming at proactively engaging high-level threats. Also intelligence systems have a more hands-on role in supporting threat detection systems in recognising suspect individuals, substances, threat scenarios, etc.

Another system type added relative to the “non-paper” is **post-incident intervention and restoration of services**.¹¹ Damage assessment is an important part of post-incident handling. The situation assessment systems should provide means to evaluate the extent of damages and suggest the best ways of restoring services.

There are several important characteristics of emergencies including catastrophic terrorism that, in particular, mass transport security command and control, threat detection, and intelligence systems must be able to handle. Threats may not be isolated in time and space, but instead manifest themselves in a sequence of events. Proper intelligence functions might help to detect threats as early as possible. Such early threat detection should include both attempting to discover signs of an immediate attack (on the scale of minutes or hours before the attack) and intelligence investigations to detect earlier (e.g., detecting preparations or reconnaissance before an attack). There will be many different pre-cursor events before an attack. Intelligence and abnormal behaviour detection systems play an important part here. It is vitally important that attempts are made to reduce the number of false alarms about attacks that are raised by the security systems. A balance must be reached between the sensitivity of the system and long-term consequences of too many false alarms.

The security systems have to be able to handle multiple attacks against the same or different infrastructure systems. This makes it necessary to include a resource allocation part of the command and control system.

During the attack, situation assessment systems must help the human decision-makers achieve situation awareness in order to optimise the allocation of resources to save as many lives as possible and restore service as soon as possible.

¹¹ Cf. “Intervention and operations technologies...” in footnote 10

In most emergencies, several agencies will be involved. The demonstration programme must take inter-agency questions regarding data sharing and shared responsibilities into account. The issue of intelligence-sharing between governmental intelligence agencies and typically private or municipal transport operators is a particularly complex issue.

During the emergency, appropriate systems for communication with other agencies and customers must be in place. Systems for quickly finding relevant and scarce rescue-equipment that might be shared between many agencies in Europe would be of interest (e.g., equipment for rescue from long tunnels might be a shared resource among several European countries. In an emergency, the nearest location of necessary materiel must be quickly established.).

Special care must be taken on how to alert emergency personnel. An important aspect is how to ensure that emergency personnel, who might be dependant on the damaged infrastructure in order to get to their stations and equipment, are able to get to work.

Information that is given out to press and customers (also cf. above) must be appropriately filtered. System-to-customer communication systems are vital in post-incident and restoration of services phases. Here, it is necessary both to communicate information about what is happening to passengers in order to help them remain calm and to communicate the best ways that passengers can help each-other in the emergency.

Summing up we operate with the following list of security systems:

- H. Intelligence
- I. Risk assessment-based command and control (cf. 5 above)
- J. Comprehensive threat detection (3 above)
- K. Preventive and early intervention, i.e. intervention before many passengers have noticed a potential attack (part of 6 above)
- L. Passive and automatic protection (part of 6 above)
- M. Cyber defence (part of 6 above)
- N. Post-incident intervention and restoration of services
- O. Forensics (contains elements of 4 above)
- P. Learning and training (contains elements of 4 above).

System-of-systems development methodology

This chapter discusses in relatively generic terms – but in view of the problem at hand – methodology for system-of-system integration. This question leads to a case for a Demonstration and Experimentation Programme, utilising by necessity a whole range of experimental methods from experiments in real life through to fully computerised simulation.

Demonstration projects* ≠ *demonstration activities

A system demonstration is arguably an exercise where something like a prototype of a system is tested under real-world conditions and hopefully found to function satisfactorily. In the FP7 context *Demonstration activities* are defined as “activities designed to prove the viability of new technologies that offer a potential economic advantage, but which cannot be commercialised directly (e.g. testing of products such as prototypes).”

This means that a demonstration activity requires something that is already functioning in, say, a laboratory setting, e.g. after a substantial amount of Framework Programme RTD activities. Also note that RTD is potentially more advantageous than demonstration in terms of EU financial contribution,¹² reflecting a demo being closer to market and hence having higher commercial value. For this to be true of course also requires a commercial demand potential, which may fail for structural reasons to exist for many security products, particularly for high-end threats like terrorism.

Particularly considering the limited dedicated research so far in the mass transport security area (cf. above) it does not seem likely that a demonstration programme there could consist to a particularly high degree of demonstration activities.¹³ In fact a more fitting name would be “system-of-systems integration project”. With that perspective it is natural to expect that a so called demonstration project would consist of a lot of RTD activities – more precisely system-of-system integration – leading up to a final demonstration campaign, just as one would expect in a CP or IP.

An explanation for the apparent fact that many seem to take for granted that a DP should be predominantly demo activities may be that much of the system integration RTD work necessary just like demonstration has to take place as **experimentation** in close contact with real operational activities.

Hence we suggest **Mass Transportation Security Demonstration and Experimentation Programme** (henceforth referred to as **MTSDEP**) as a more appropriate term for the so called demo programme. In the following sections system-of-system demonstration and experimentation will be discussed in generic terms but with an eye to the specific mass transport context.

This said it is necessary to appreciate the legitimate concern that a major R&D activity with public funding will have to provide some proof of results compelling to a broad group of

¹² A maximum of 75% under certain conditions as opposed to 50% for demonstration.

¹³ Unless basing demonstrations on off-the-shelf capabilities to a degree threatening the innovation content.

stakeholders – and also to the public at large. However, knowledge accumulation and not propaganda should be the organising principle for a MTSDEP. Emphasising demonstration at the expense of knowledge accumulating RTD experimentation one runs the risk of the “Potemkin village”, i.e. organising big and expensive events that absolutely have to look good and therefore cannot really allow the risk levels optimal from the learning point-of-view.

System-of-systems demonstration and experimentation

There is no absolute demarcation between systems and systems-of-systems. It is, however, obvious that the latter term is intended to capture a higher degree of systemic complexity, and an operational definition might be that a system belongs to the “professional territory” of a single (main) specialism while operation – not to mention development – of a system-of-systems requires interdisciplinary integration across several specialities.

By virtue of being more complex *per se* a system-of-systems will typically also have a more complex relation to external conditions than a single system. This follows from the simple fact that different constituent systems will typically interact with different facets of the external world.

Further, a system-of-systems is typically capable of handling a broader range of tasks than a single system, even though this is not a logical necessity.¹⁴ Above we have argued for an “all hazards approach” – hence a very broad range of tasks – for the FP7 MTSDEP.

The inescapable – and typically multidimensional: internal, environmental, task-oriented – complexity of systems-of-systems makes a naïve approach to demonstration and experimentation defunct. The combinatorial complexity of possible combinations will produce an insurmountable volume of experimentation¹⁵ work if one were to plough through it all.

Fortunately combining real world experimentation with computer simulation provides a response to much of the complexities of systems-of-systems. In fact this is an approach applied widely in today’s world. To take but one example, physical wind-tunnel experiments are today used mainly to calibrate simulation models, and the bulk of aerodynamic experimentation is hence done on computers – or, if one prefers Latin, *in silico*.

¹⁴ UK air defence as developed in the early WWII era is often cited as the first example of a system-of-systems of the complexity discussed here, with anti-aircraft artillery (AA), Spitfire fighters, radar sensors, and command and control centres as the main constituent systems. This early example did, however, not have a particularly more complex task structure than AA alone.

¹⁵ Considering that demonstration can be seen as a special case of experimentation, we henceforth prefer the latter term unless when it is necessary to make a distinction, e.g. due to FP7 type of activity regulations (cf. footnote 12).

Exploiting the synergies from the full range of experimentation methods: from “live” to in silico experimentation

In the previous section we saw one important reason for relying on computer simulation – or rather on a combination of real world experimentation and simulation – viz. that computer simulation allows a much faster work-pace in exploring possible combinations of conditions.

Robotics has its **Three D’s** for when to choose robots rather than human workers, viz. dirty, dull and dangerous. As an adaptation of this list to the situation of choosing between computer simulation and live experimentation we would suggest *difficult*, dull and dangerous. Here **difficult** would stand for the needs of coordinating all the many aspects of a system-of-system setting, and **dull** for the above-mentioned practical impossibility of going through the very large number of relevant combinations that is often the case in a systems-of-systems setting.

The third D, **dangerous**, in the MTSDEP context can represent danger of life and limb but also the uncontrollable and normally unacceptable knock-on effects of major delays in a transport system experiment, as well as the negative psychological impacts likely to arise in passengers subjected to seemingly threatening situations. Also other ethical problems of experimentation can be counted under this D. One strand of such problems is invasion of privacy caused by various detection and identification systems. Another is the risk of panic if an experiment causes passengers to believe that a real attack or other major incident is in the making.

While the previous paragraph demonstrates that dangerous is another matter, typically to do with ethical aspects, dull and difficult are both more or less the same as “expensive”. Hence, at least theoretically, there is really a trade-off between the additional validity from real-world over *in silico* experimentation vs. the additional cost. As the wind-tunnel example suggests the result can well be a mixed strategy with some real-world experimentation and a lot of computer simulation. (Even though the physical scale-model experimentation used in wind-tunnels seems to be of less relevance to our current area of interest; nowadays in R&D, railway models can so to say completely replace the model railways.)

As discussed above Modelling & Simulation also have an important role to play in transferring results to new types of threat and to new cities and regions.

Broadly speaking we suggest distinguishing between at least the following **types of “experiments”** in the widest sense of the word:

1. “Live” experiments under conditions of ongoing real operations
2. Experiments in real operational setting but not under conditions of real operation (e.g. experiments in a terminal not yet opened or closed over night)
3. Experiments in dedicated facilities emulating real operational settings (e.g. training facilities or decommissioned real facilities)
4. “System-in-the-loop” simulation test-beds; the traditional is hardware-in-the-loop but the concept is here broadened also to allow systems to be, e.g., software-based cyber defence

5. Man-in-the-loop simulation (including Virtual Reality applications); here humans are included as decision-makers in an otherwise *in silico* setting
6. All computer simulation.

In addition to experimentation types lower on the list being less costly and less ethically problematic and hence responding to problems of the difficult, dull and dangerous, they also allow higher levels of **experimental control**.

There are also certain types of “non-experiments” that need to be considered in a MTSDEP context:

Exploitation of “natural experiments” – not all phenomena are amenable to planned experimentation. Here observations from real operations are crucial, e.g., for calibrating models. This is particularly true for abnormal situations, which could be representative of (aspects of) threat scenarios being considered, and which would be forbiddingly dangerous to set-up as live experiments. Another problem can be illustrated by way of example: potentially detection of human anxiety could be a useful element in a security system. However, experimenting on actors *trying to play* anxious would not be a credible approach to evaluating and developing such detection systems. Another case in point is information fusion systems trying to recognise threat scenarios; also here it would seem that work has to rely in large measure on real cases rather than cases made up by the researchers themselves and therefore not necessarily capturing, e.g., true terrorist logic.

“Discursive experiments” – theoretical physics has its thought experiments – in German *Gedankenexperimente* – made famous by Einstein. Both in setting up and in analysing the results of “real” experiments it is important with high-quality such “theoretical” work. However, whereas theoretical physics is traditionally the realm of the sole genius, system-of-systems problems due to their interdisciplinary nature typically require effective group work. Methods for this range from simple discussions on whiteboard over manual gaming and structured brainstorming exercises, through to sophisticated computer supported formats, which link over to *in silico* experimentation.

MTSDEP design and implementation

In this chapter we bring together the two previous ones by applying the System-of-systems development programme methodology to the System-of-systems architecture

Criteria for programme design

A key question for MTSDEP design is whether to have a single phase II project or many, perhaps operating as some kind of federation.¹⁶ Another but related issue is whether to have many or few experimentation platforms (maybe just one)?

In order to address these issues in a systematic way we discuss the following set of possible criteria:

- **Intensity and time criticality of information exchange between systems under real security operations.** Separating in the DEP (Demonstration and Experimentation Programme) systems for which this criterion is high would be very problematic since that situation calls for continuous system integration efforts.
- **“Experimentability” in real life.** As discussed above not all systems are likely to be available for real life experimentation. If system X has strong links to system Y but is less “experimentable” (e.g. experiments on X can only be made *in silico* or in testbeds whereas experimentation under conditions of real operations is possible on Y). This will mean that the info exchange intensity realised in experimental work will be less than under conditions of real security operations. This will in turn reduce the need for close cooperation, perhaps allowing system X to feature in a project focusing on Y to be represented by a simulation model.
- **Continuity of physical flows.** In addition to information flows come of course physical ones like passengers or vehicles. One example can be to track a terrorist suspect entering at an outlying station via perhaps several changes to a target main interchange. While this aspect does have some relevance this will turn out below to be fairly limited, and not too difficult to ascertain when experimenting with real operational systems.
- **Cost efficiency.** The relevance of this should be obvious to all.
- **Diversity in terms of technical and socio-cultural legacy.** Again a rather obvious criterion.

The combined logic of the criteria could read something like this.

For systems that are relatively isolated – in terms of information exchange and “experimentability” – cost efficiency suggests a separate project. If diversity is great this could comprise several experimentation platforms in settings spanning this diversity (in cases with low “experimentability” typically testbeds) in one or possibly several projects.

For systems that are strongly coupled in the same sense as above cost efficiency instead suggests joint projects. Again if diversity is great each project could comprise several experimen-

¹⁶ An FP7 example of a federation of D&E projects in SMART-CM and INTEGRITY in the supply chain area.

tation platforms in settings spanning this diversity (in cases with high “experimentability” typically instrumented real operating facilities) in one or possibly several projects.

Operational and security systems in relation to the MTSDEP

This section discusses the relevance of the various experimentation methods to the operational and security systems identified above. Also the above criteria are discussed.

Comprehensive threat detection (J) is a function very much in need of “live” experimentation. What is needed here is very extensive data collection for a wide array of detection and data fusion systems. Since real-world systems with big passenger flows add many problems beyond the laboratory – and considering that this type of testing can be done without disturbing passenger flows¹⁷ – part of a real urban transport system should be instrumented and utilised for this type of experimentation. Ideally a high-tech line in a metro-system – e.g. Paris – could be used with a hub, some more outlying stations and some cars, hence incidentally taking care also of aspects of systems D and E as well as the continuity of passenger flow; an important function of comprehensive threat detection is tracking and tracing.

A high tech system can represent also more low-tech systems since they can be emulated by deleting parts of information only available in the high tech system. In principle a similar argument can be made with regard to legal availability of data. This gives at least some control on the variety of legacy aspect. Using a single main experimentation platform is economically beneficial in that it allows background noise to be controlled during a very long run of experiments on potentially very many different subsystems where data also needs to be experimented with at the fusion level.

In spite of the arguments for a single main platform, some validation of results in other transport systems is warranted. It will also be necessary to have some instrumentation for threat detection experimentation in a number of other transport systems for experimentation on system K.

Major interchanges (B) are already identified as a key area of concern. The main aspect of concern here is how passengers flow in the interchange and how this may affect consequences of incidents as well as how it interacts with other systems; B has strong time critical links with in particular C, I, J, and K and some type of links to all other systems.

Experimentation on B would mainly mean changing the layout of the facility to affect passenger flow. This is not dangerous but may be rather difficult and dull.

Since major interchanges come in many different shapes and sizes, and since passenger behaviour is likely to vary by culture, several experimentation platforms will be necessary.

¹⁷ For the purpose of the present analysis screening of individual passengers is counted as pre-incident intervention. Admittedly, however, this could in principle be used as routine surveillance technique – at least at the level of sampling.

Passenger information systems (C) affect – in likely progressively increasing measure – passenger behaviour linked in particular to B, I and K. The key question here is how to ascertain passengers being competent and active security partners. Here it is the likely strong dynamics in the field, which makes experimentation relatively difficult, at least in terms of achieving predictability of future developments. As for B socio-cultural variety suggests a multi-platform approach.

Preventive and early intervention (K) is an extremely demanding task – consider for example a situation with suspect PB-IEDs or release of CRB agents in a metro system or a riot situation with suspect trouble-makers.¹⁸ Development of such concepts and systems is dangerous and would mostly have to take place in dedicated experimental facilities, also useful for training purposes, and *in silico*. However, such experimentation with just a limited number of figurants will fail to capture many of the real effects in an environment with large passenger flows; the main problem for the bulk of passengers would be separation and evacuation. Therefore pre-incident intervention seems like a problem area in particular need of large-scale experimentation. Links are strong with B, C, I, and J. In some scenarios (like the PB-IED) the latter functions here as “target acquisition”. Preventive and early intervention can of course also affect vehicles/transport platforms (E), e.g. since a suspect terrorist is able to board a vehicle, as well as smaller stations and other entry points (D).

The same arguments apply as in B and C for multiple experimentation platforms.

Intelligence (H) as well as Risk assessment-based command and control are both very important functions in relation to surveillance and intervention. Knowledge on the intelligence function is an important input to the other functions and in particular to command and control. Conversely improved knowledge on the other functions will benefit the intelligence function via more precise intelligence requirements. However, the intelligence function is generic and its development is not a likely main part of a mass transportation security exercise. It is naturally developed in conjunction with the command and control function (I) as well as comprehensive threat detection (J).

Cyber defence (M) can be analysed largely along similar lines as H.

Risk assessment-based command and control (I), in contrast to intelligence, is a natural key part of a mass transportation experimentation project. It is not in need of direct participation in “live” large-scale demos with live passenger streams as discussed for pre-incident intervention. Information from such exercises will, however, be invaluable for achieving realism in simulated command and control demonstration and experimentation exercises.

Experimentation on command and control systems – of course operating off line – is a commonplace occurrence and hence easy to achieve. Similar arguments apply as in B, C and K for multiple experimentation platforms.

¹⁸ Note that here some of the threat detection systems are likely to convert into “target acquisition” systems for preventive intervention.

Post-incident intervention and restoration of services (N) can also be extremely demanding. Consider for example a situation of rescuing an exploded train full of passengers in a tunnel with suspected left behind IEDs (LB-IED). This situation very much calls for dedicated experimental – and training – facilities. The need for large-scale demonstrations is arguably similar to that for pre-incident interventions (K). However, it is in practice very difficult to achieve in an ethically acceptable way the types of effect that would in reality prevail in a very serious post-incident situation (large numbers of shocked and perhaps injured passengers).

Passive protection systems (L) – e.g. fire protection or person access controls – typically carry very limited need for experimentation beyond functionality and basic ergonomics. However, in a panic situation some passive protection systems may cause problems. Pre-incident intervention (K) experiments seem, again, the best way of bringing out such problems.

Development of **Forensics (O)** and **Learning and training (P)** systems is another natural key part of a MTSDEP. In terms of output the coupling of these systems to the time critical tactical modes of systems H, I, J and K is not strong. However, O and P build on input from in particular I and J and P informs all the other systems in strategic time scale.

Transport network (A) is clearly a very important level in terms of disruptive effects. However, here already existing transport flow models should be relatively easy to adapt. There is limited need of detailed information from other system levels as to the reasons why a particular node or link is unavailable or operates at limited capacity. Information on passenger transport demand behaviour under conditions of serious threats or disruptions are important but can only be estimated based on “natural experiments” – doing “real” experimentation at this level would be far too dangerous. Operationally this level is connected in particular to I.

Lines and roads (including smaller stations and other entry points) (D) and **vehicles/transport platforms (E)** were mentioned above in connection with comprehensive threat detection (J) and preventive/early intervention (K).

Vehicle parking areas, repair and maintenance shops, etc. (F) and **Technical support systems including SCADA (G)** have not been mentioned above. These and aspects of D and E not covered under J and K are seen as relatively stand-alone problems.

MTSDEP design

As can be seen from Figure 3, the above analysis suggests that five systems form a strongly connected core representing high requirements in particular on time critical info exchange, while being reasonably amenable to live experimentation:

- B. Major interchange (typically intermodal)
- C. Passenger information systems (system-to-customer and peer-to-peer)
- I. Risk assessment-based command and control
- J. Comprehensive threat detection
- K. Preventive/early intervention

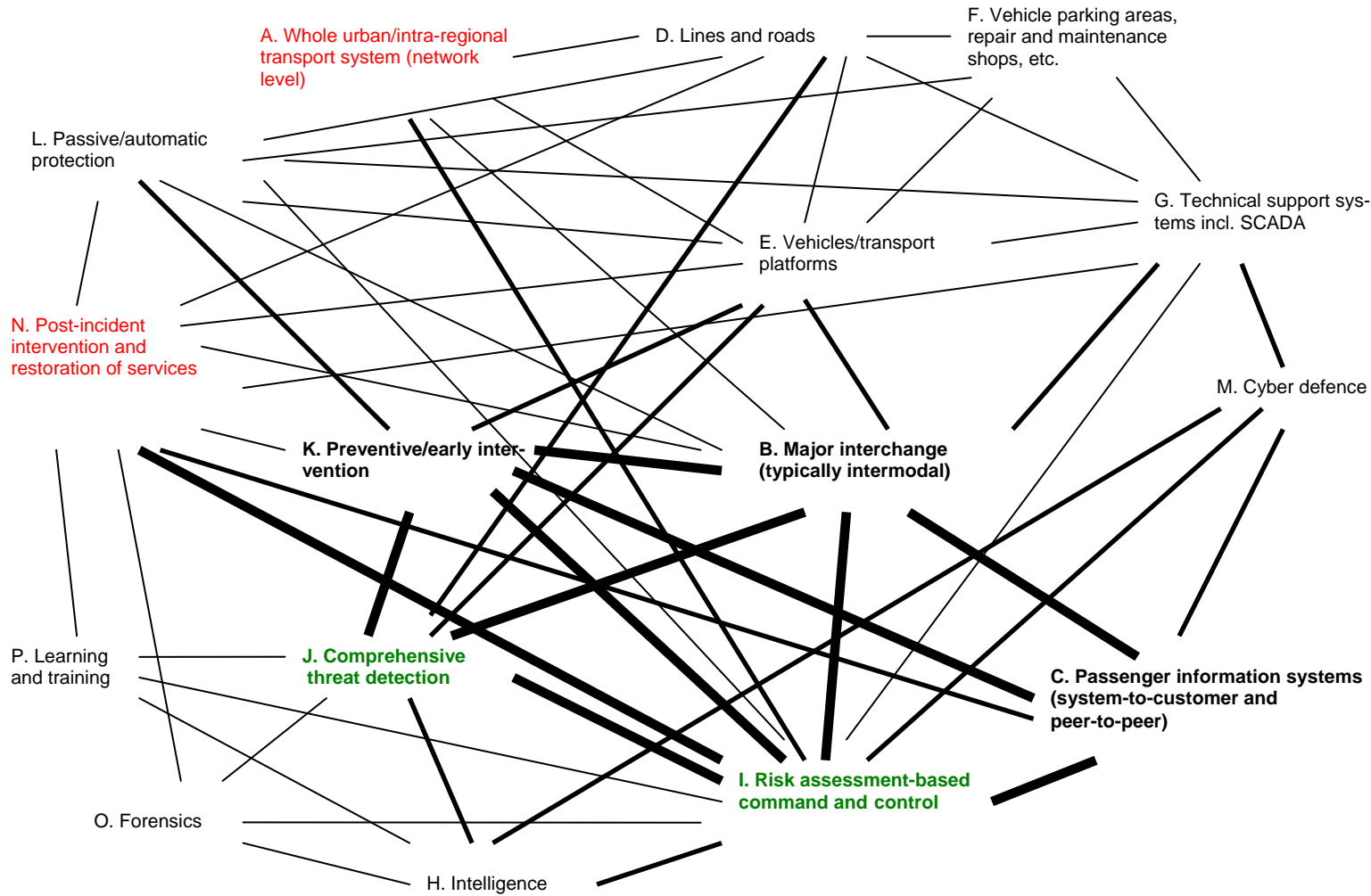


Figure 3. A first MTSDEP system-of-systems map.

Thickness of links indicates intensity and time criticality of required information exchange under operation

Colour codes for 'experimentability'
Green: real life experimentation relatively easy
Black: real life experimentation possible only with limitations
Red: real life experimentation essentially impossible

Hence these system areas ought to be addressed in (one or several) joint projects capturing at least important parts of their interactions.

As for the diversity criterion it was found that this property is pronounced with regard to B, C, I, and K but not so much for J. This suggests a multi-platform structure where all platforms are roughly equally able to experiment on B, C, I, and K, but where one platform has the lead on J. Results on J would then need to be fed from this reference platform to the others.

This said it should be clarified that the focusing on the five systems does in no way mean that all the rest can be safely disregarded. Quite the contrary a serious Mass transport security programme must have access to state-of-the-art knowledge in all the system areas listed above. And whereas the more generic ones – either on the transport side like A or on the security side like H and M – are hardly reasonable candidates for funding from a Mass transport security programme beyond interface work, others like, say, tunnel rescue operations (part of N) could very well merit such funding.