A Concept for Interoperability of Security Systems in Public Transport

Sebastian Kurowski
Fraunhofer IAO
sebastian.kurowski@iao.fraunhofer.de

Jan Zibuschka
Fraunhofer IAO
jan.zibuschka@iao.fraunhofer.de

Heiko Roßnagel
Fraunhofer IAO
heiko.rossnagel@iao.fraunhofer.de

Wolf Engelbach
Fraunhofer IAO
wolf.engelbach@iao.fraunhofer.de

ABSTRACT

In the field of public transport, operators and first responders collaborate in the prevention of and reaction to security issues. In order to optimise their specific daily operational business needs in a timely manner heterogeneous information and communication systems are deployed. In case of an incident however it is crucial that the various involved parties exchange relevant information to develop a shared understanding and act in a coordinated way. Yet, heterogeneous communication and information system infrastructures often hinder this crucial flow of information. To address this shortcoming it is crucial to enable the design of interoperable system-of-systems approaches in this domain. This paper describes a conceptual model to construct system-of-systems environments in the domain of security in public transport. By building on the results of several European research projects this concept offers a starting point for modelling and documenting individual systems inside a system-of-systems architecture.

Keywords

Interoperability, public transport, security, system of systems architecture

INTRODUCTION

In public transport and especially large urban hubs, various transport operators, first responders and public authorities collaborate in the prevention of and reaction to security issues. This setting is also characterized by heterogeneous information and communication systems, each optimized for its specific daily operational business needs. Security issues are only one aspect of these broader requirements. In this situation, security relevant information is often hard to differentiate from non-security relevant information. Furthermore, the domain of security in public transport has various collaboration scenarios, comprised of various stakeholders (COPE 2009a) and different information types depending on the situation regarded. Recent events have demonstrated that public transport can be subject to various security incidents, and outcomes may be quite severe due to the volume of passengers (Roßnagel and Junker 2010). Therefore, it is crucial that the various involved parties exchange relevant information to get a shared view and understanding of the situation and act in a coordinated way in critical situations (Chen et al. 2008). Yet, the lack of flexibility in structure and semantics of the underlying information and communication infrastructure remains an obstacle to achieving this goal (Engelbach et al. 2010).

This paper presents a concept for interoperability of information systems. The building blocks of this model are distilled from a survey on interoperability in projects researching security in public transport (Kurowski et al. 2011). We use Turnitsa's conceptual levels of interoperability (Turnitsa 2005) as a framework for our consolidated model of interoperability for information systems in public transport security. This consolidated concept is employed as basis for the interoperability notation of the European large-scale demonstration project SECUR-ED which aims at creating an interoperating information system for public transport security (Sautter et al. 2012).

We will start by giving an overview of related work regarding conceptual levels of interoperability and results from previous projects in the domain of public transport security. We then present our interoperability concept and provide in depth descriptions of the relevant building blocks identified in the survey of research projects. We provide a short discussion and outlook before concluding our findings.

RELATED WORK

Conceptual Interoperability

ISO/IEC-2382-1 defines interoperability as "the capability to communicate, execute programs or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units". Hence interoperating systems have the capability to interact with other systems, forming a larger functional unit, a system-of-systems.

The "levels of conceptual interoperability model" (Turnitsa 2005) addresses this issue by offering a classification of interoperability capabilities. Originating from the domain of simulation, this model allows both the identification of system maturity with regards to interoperability, and the definition of goals for interoperating systems. The first level (Level 1) is labelled technical interoperability, meaning the ability of two distinct systems to connect. Although they may share the ability to communicate simply having a connection does not include the ability of interpretation or even collaboration. Hence, the following levels represent increasing ability of the involved systems to understand information arriving from other entities (Syntactic interoperability - Level 2), or even interpret the exchanged information, hence exchanging knowledge (Semantic interoperability – Level 3). Reaching this level may enable a wide range of applications, e.g. automatic translation between different languages or glossaries. Pragmatic interoperability (Level 4) requires interoperating systems to be aware of others' procedures and routines, enabling a capability-oriented approach to information processing. Systems operating on the fifth level, dynamic interoperability, would be aware of the assumptions and constraints other systems are using.

For the domain of security in public transport, awareness of constraints and assumptions might refer to the specific capabilities and operational procedures of the different participating stakeholders. E.g. police officers may have a different view on a building than fire brigades since both follow different goals (catching criminals vs. evacuation) and therefore may interpret and use information differently. Finally when reaching the sixth level of conceptual interoperability, documentation of the whole system, including all structures involved and their interrelations is required, enabling interpretation and further development and adjustment by other stakeholders.

Interoperability of information systems in Public Transport Security

The interoperability concept, as part of the SECUR-ED interoperability notation, used several research projects in order to identify and distil building blocks. Such blocks are meant to be used along the levels of the conceptual interoperability model to facilitate the design of interoperable socio-technical systems-of-systems, while taking into account the complexity of the domain of security in public transport. This complexity originates from various stakeholders and scenarios creating an environment in which highly complex and dynamic collaboration and communication structures depend on types of incidents as well as phases in the emergency lifecycle (Ritchie 2004). Therefore, the present research included projects with a focus on incident ground collaboration (COPE 2009a) and incident management (COUNTERACT 2009b). The methodology used for identifying potential elements for the interoperability concept in SECUR-ED as well as a detailed description of those elements is provided in (Kurowski et al. 2011). In the following we will therefore briefly introduce the identified elements from the surveyed projects which were later synthesized into building blocks. This resulted in an integrated interoperability model which will be introduced at the end of this section.

(COPE 2008) described various collaboration scenarios and the participating entities, including systems and stakeholders. The structure of collaboration between entities in these scenarios already implies a basic system-of-systems design. (COPE 2009a) offers a description of so-called concepts of operations (CONOPS). Those are used as descriptive tools for formal understanding of the distributed roles, their collaboration, capabilities and limitations. The CONOPS usually operate on the level of pragmatic interoperability. Field level security plans (COUNTERACT 2009a) specify the more general CONOPS, applying methods, routines, stakeholders and structures to a certain security asset and / or scenario. The organizational interfaces describe generic collaboration structures and interfaces between different types of organization (COUNTERACT 2009a). This information enables both the creation of a typology of the involved stakeholders on an organizational level, and a derivation of applicable metadata for information exchanges between the parties.

In terms of technical systems, most of the surveyed projects focused on sensor systems. Although a wider range of technical systems may be involved in the domain of public transport security, sensing systems are information retrievers, enabling interpretation of environment states. Hence such systems are very interesting when focusing on the domain of security where detection is a crucial point for mitigating an incident (Asimakopoulou 2010).

(Kurowski et al. 2011) derived various ontologies from the sensor systems presented in (COPE 2009b; COUNTERACT 2009b; DEMASST 2009, 2010). The ontologies were aggregated, creating a typology of sensor systems which we present in the next section.

All identified elements from the surveyed projects were aligned with the model from (Turnitsa 2005), creating an integrated model for interoperability which is shown in Figure 1. The figure shows the usage of each identified asset in the conceptual interoperability model, along its potential contents. While those concepts (roles or their implied limitations from the scenario-based use cases in (COPE 2008), agreements from the interfaces and states derived from procedures of the field level security plans in (COUNTERACT 2009a)) enable establishment of dynamic interoperability, the concepts of operations, and the derived sensor system ontology enable pragmatic interoperability by showing procedures in terms of capabilities, adaptabilities, constraints and legal issues. Semantic interoperability is enabled by using the professional terms which is described in the concepts of operations, metadata derived from the interfaces and use cases from the use case descriptions and the field level security plans.

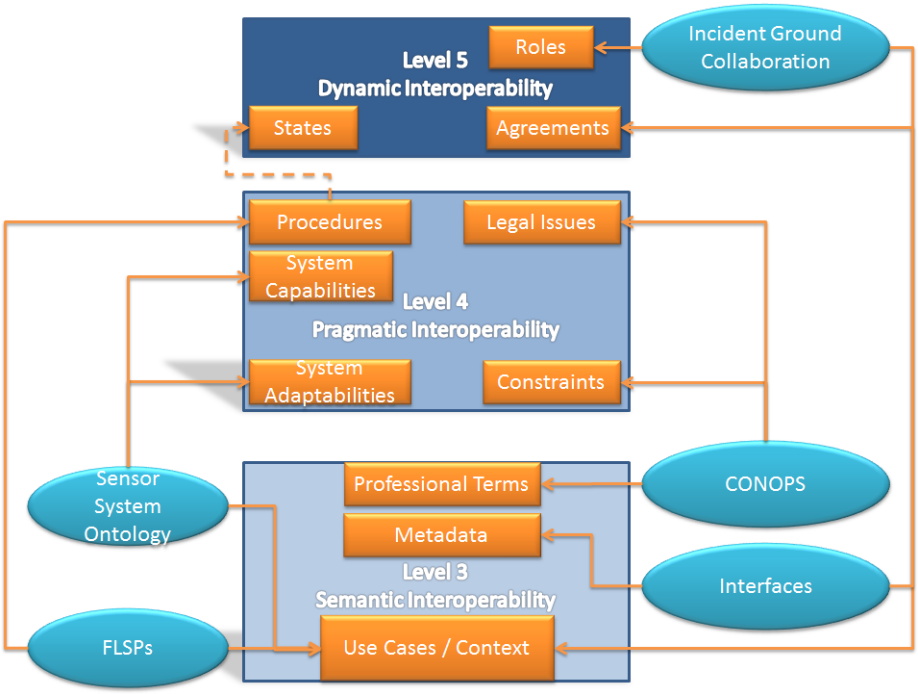

Figure 1 Integrated model for interoperability (Kurowski et al. 2011)

In the following we will show how the elements described in Figure 1 were synthesized into generic interoperability objects, enabling the development of a modelling and notation approach for interoperable system-of-systems supporting security functions in public transport.

CONCEPT FOR INTEROPERABILITY OF INFORMATION SYSTEMS

We define four interoperability objects (Information System, Intermediary, Interface, Role) which represent typical system capabilities such as program execution, information processing and communication. As an abstraction of the individual elements, those generalized interoperability objects can be applied to a wide range of use cases (see Figure 2).

A role interoperability object is modelled using the user object as known from UML use case diagrams. This allows for further correlation of the roles with specific use cases, creating a context of the information system and its use. This is very relevant as most cities considered in SECUR-ED are characterized by multi-operator-settings, where independent organizations organize public transport while following their individual business targets. Roles also enable modelling socio-technical influences (Hollnagel 2002) in system-of-systems design which is especially important in supporting emergency response where collaboration does not only take place among technical systems but also along individuals who act partially based on the information given by information systems (COPE 2009a).

An information system interoperability object can represent a wide range of entities: (1) a single sensor, (2) a network of identical sensors, (3) a network of different sensor types, (4) an IT-System, (5) a network of IT systems, (6) an organization.

This addresses the problem of various levels of abstraction that may be present in stakeholders descriptions of a system-of-systems (e.g. interoperability can be between many organizations or between many technical systems) by offering modelling capabilities applicable on a wide range of granularity levels (e.g. an information system can consist of several roles, intermediaries and (recursively) information systems).

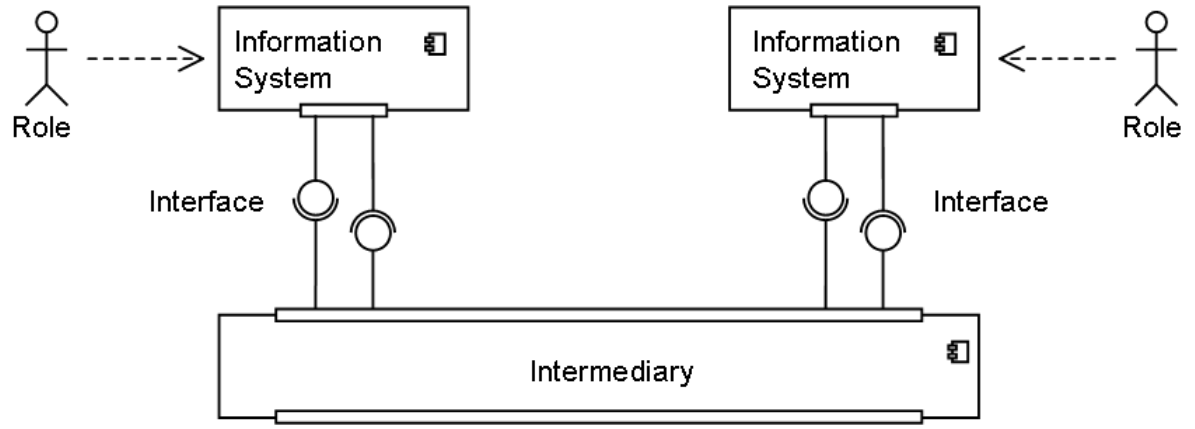

Figure 2 The SECUR-ED interoperability objects

Interfaces provide communication capabilities between systems and therefore are considered as an interoperability object. In Figure 2, interfaces are represented using the UML interface object (Born et al. 2004). Thus, information on how the information is transmitted and how another system can communicate with the information system hosting the interface can be represented. This offers capabilities to express aspects of semantic, pragmatic and dynamic interoperability (Turnitsa 2005) in the design.

Finally, the intermediary interoperability object supports modelling of extended communication capabilities, e.g. translation services, identity management or simply as proxies for information transmission. Intermediaries in our context are information systems that serve the sole purpose of supporting the interaction between information systems. It allows for modelling of the procedures used for this interaction which are not part of the information systems involved on the levels of semantic and syntactic interoperability (Turnitsa 2005).

Using these interoperability objects, along with the underlying elements identified in related research projects, we will in the following present building blocks while offering a concept for modelling interoperability in the domain of public transport security.

BUILDING BLOCKS FOR INTEROPERABILITY

Metadata for describing Roles and Information Systems

Table 1 and Table 2 provide the attributes used for annotation of the interoperability objects "information system" and "role". Both assets were derived using the aforementioned Concepts of Operations (COPE 2009a; COUNTERACT 2009a) and Field Level Security Plans (COUNTERACT 2009a). By aggregating elements from these sources, the development of a generic template for this metadata was possible, reflecting both a generic view on the entity regarded and its used context (e.g. by notating "definition of threats" or "security training and exercises").

Attribute	**Example / Explanation**
Organisational structure	Overview on the structure of the organisation
Legal basis	The organisations rights and laws applying to it. Which extra rights does this organisation have?
Security operating methods	Includes security operations under elevated threat conditions (i.e. ad-hoc safeguards, standard levels of security, threat levels), available safeguards and a description of security operations (involved interfaces, management, rules of engagement, means and methods)
Auditing	Who is responsible for auditing and reviewing these contents? Which processes apply to it?

Attribute	**Example / Explanation**
Professional terms	Meaning of terms, such as security systems, procedures, position holders, assessments, risk management, security, security means, field level security.
Risk reduction measures	Actions as response to risk assessment outcome
Available interfaces	Which interface does this organisation support?
Field level security plans	List of available field level security plans
Security typology	Controlled system, open system, level of security
Maintenance of metadata	Who is maintaining this metadata? Who is responsible for updating the information?
Systems, assets & components	Which systems, assets and components are contained in this organisation? For instance, a police department uses other systems than a railroad station.
Risk management policies	Restrictions and rules from risk management.
Communication strategy	List of strategies regarding information receivers
Definition of threats	Basic definition of the threat levels. What does this organisation mean with severe or high threat levels?
Security training and exercises	List of used security training scenarios and correlated exercises

Table 1 High level metadata for describing roles and information systems

Attribute	**Example / Explanation**
Professional terms	See High Level Metadata
Legal basis	Legal basis for operating
Organisational structure	Structure on ground level
Rules of engagement	What does this operational unit aim at? What should be avoided?
Tasks under routine conditions	Includes routine operations (security handling of people, preventive measures, supervision and control, information security, security observations, security searches, communication and reporting, deterrence and security deception), a list of security procedures, communication diagrams for the tasks, a list of security exercises, immediate actions during emergencies, lists of security monitoring systems, logistical support and involved equipment
Activity objectives	Objectives regarding deterrence, detection, response and prevention

Table 2 Operational unit metadata

The High Level Metadata enables meta-modelling of units, organisations, systems and other components in the system-of-systems architecture. Yet, operational units require a more specific description of information, resulting in additional attributes (COUNTERACT 2009a). This concept supports these different requirements by leaving out organizational assets, like service agreements (e.g. “Maintenance of metadata”, see Table 1) and adding new attributes, such as the objectives of this particular unit. The operational point of view of the metadata is presented in Table 2:

Using the reference projects and the sensor ontology, an aggregation regarding sensor systems and their usages was created. This aggregation becomes especially important with regard to the outcome of the evaluation performed during COPE. Here a supporting information system was created, using a wireless sensor network of various specific sensor systems. The system is described in (COPE 2009b) along with its evaluation. Two points become very important under the aspect of an interoperable ICT system-of-systems infrastructure. Regarding the sensors, the “dependability of the overall system (sensors, network, interface) is important” (COPE 2009b). Furthermore, the “sensors must be reasonably priced” (COPE 2009b) and the “specificity of sensors” (COPE 2009b) comes into play, since it is “impossible to have sensors for all substances” (COPE 2009b). This led to the assumptions that the system-of-systems approach must rely on more generic sensor systems in order to

increase fault tolerance and improve the overall handling. Also, the implementation of the system-of-systems approach is supported by fair pricing of the components used.

Typology of sensor systems

From the information derived from the surveyed projects we also constructed a hierarchical typology of sensor systems (see Figure 3) respecting the IED roadmap given in (DEMASST 2010). The distance of an individual sensor system from the root of the hierarchy correlates with the specificity of the sensor, along with required training.

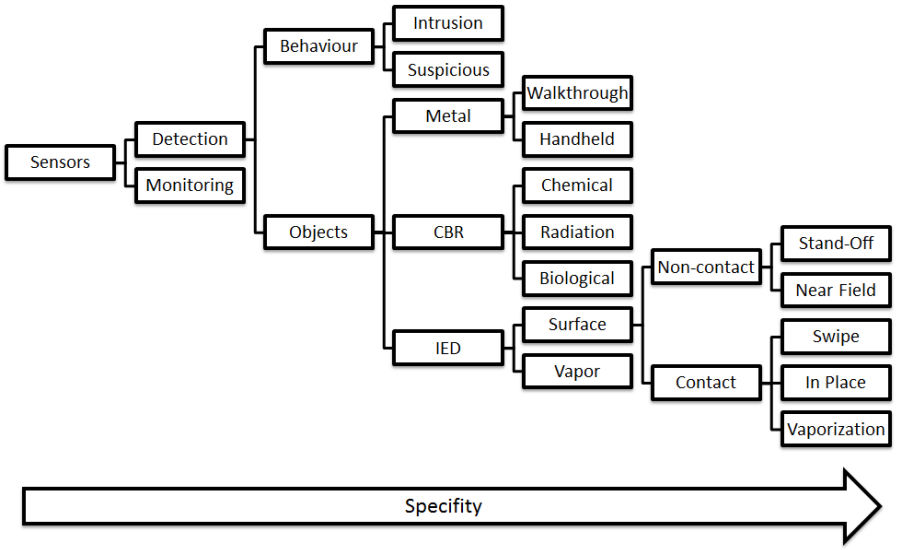

Figure 3 Sensor systems typology

The structure of the typology aims at reflecting the purpose of the systems included. Such information can be used to determine which sensor systems and which use cases are correlated. Additionally, it may serve as basis for an approach to evaluating sensor systems and comprising systems-of-system. Additionally, various generic use cases can be derived from the second level structuring of the hierarchy. These use cases can be used for evaluating sensor systems regarding their purpose, while respecting the evaluation outcome given in (COPE 2009b). The use cases include: area monitoring, chemicals detection, biological materials detection, radiation detection, IED detection, metal detection, intrusion detection, suspicious behaviour detection. In order to respect the requirements captured in (COPE 2009b) those dimensions are assessed using the following attributes: no support, usable with adjustments, usable with special training, fully usable. These are just some possible usages of our approach beyond the modelling of sensor systems as an interoperating information system object.

Scenario based role typology

We also provide a typology of role objects, based on the results of (COPE 2009a). The use case descriptions in (COPE 2009a) were used in order to identify the participating stakeholders. These stakeholders can be subdivided into Incident Ground Teams and External Organisations. One might argue that the response to an incident does not cover all actions during the post incident phase. However, by including the generalized user as a role representing external organisations it becomes possible to model all involved parties with the aggregated role typology. Figure 4 shows the aggregation of the incident ground teams which includes all parties involved in the operational aspects of resolving an incident.

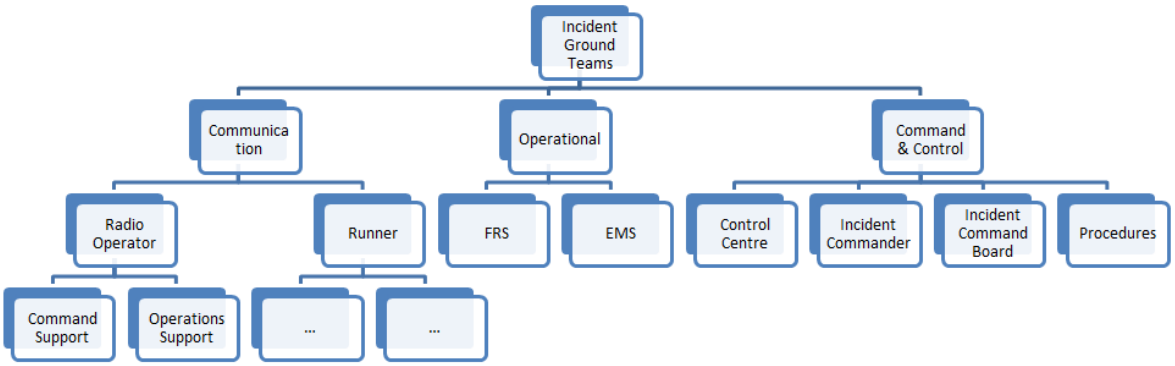

Figure 4 Aggregation of incident ground team roles

For external organisations, we employ a similar structuring approach with no domains given. While the responding units on incident ground level are focusing on operational targets, external organisations can also have more generic tasks like general planning or resource provision (see Figure 5), making it hard to provide a comprehensive typology for this aspect.

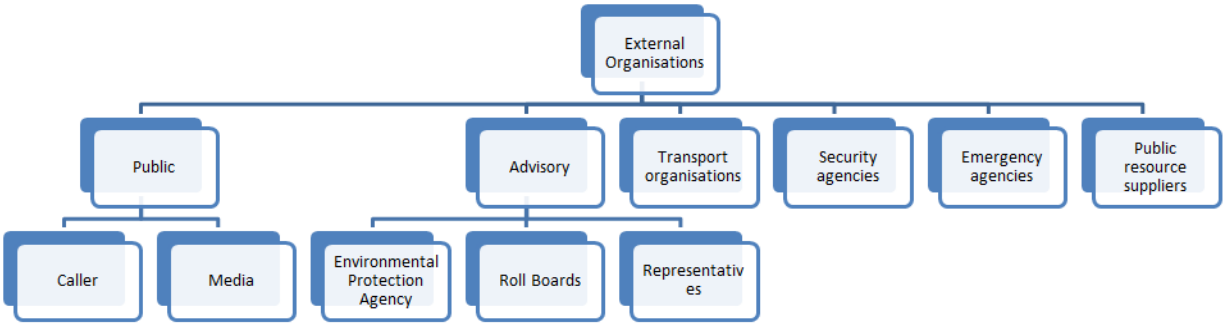

Figure 5 Aggregation of external organization roles during mitigation

Inter-organizational interface descriptions

(COUNTERACT 2009a) defines basic requirements for interfaces with external organisations, from which we derived the initial needed meta-information for those interoperability objects. By combining these requirements with the presented metadata the following interfaces were defined (see Figure 6). We assume that in each security organisation a concept for operations was defined including both high level and operational definitions. Furthermore, the roles involved in the security process should be defined as well as the person responsible for managing the processes and the processes involved.

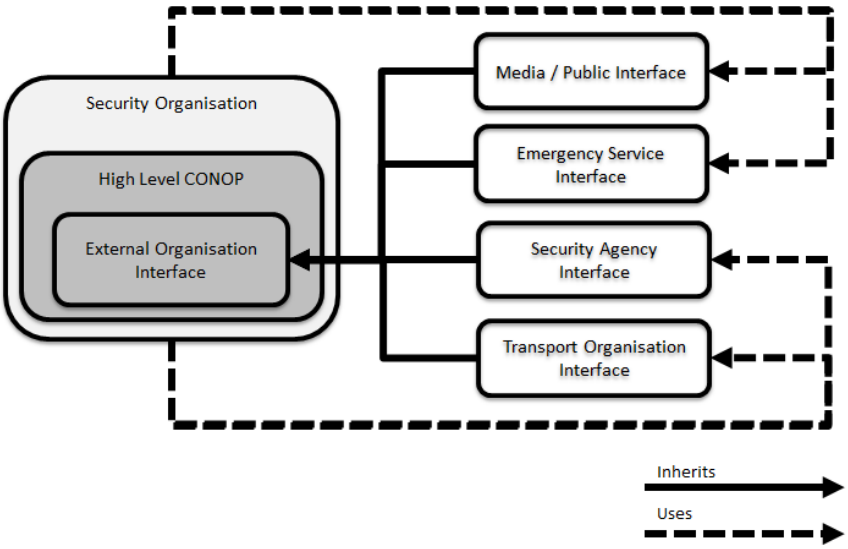

Figure 6 Inter-organizational interfaces

By including the Concept of Operation which also serves as the basis for the high level metadata in Table 1 and by reviewing the contents included, a correlation between these contents and the requirements made from the interfaces became observable. This led to the interface overview as seen in Figure 6. The following describes a generic interface as derived from this overview. The list can be used for later specific interface implementations.

- Organisation

  A basic description of the organisation and methods for accessing the information needed (i.e. dictionary for intermediating services). This description includes information on the structure of the organization, its legal form, implemented security operating methods, auditing arrangements, professional terms used and in particular the security typology including terms used in securing the organization. Furthermore, information is required on the implemented risk reduction measures and risk management policies (e.g. which measures and policies are used in this organisation), the available interfaces for communicating with this organization with their required protocols. In order to provide information on the organizations' interoperability capacities and embeddedness in information chains, information on the implemented system assets and components as well as the communication strategy is required. While the first focuses on system compatibility, being aware of the organisations' communication strategy is important for establishing true collaboration.

- Generic Interface

  The generic interface is an abstraction of all interfaces the organization provides. Individual interfaces within different types of organisations inherit meta-information from the generic interface. The description of this interface therefore includes decisions on the specific interface, available protocols, supported processes of the organization implementing this interface, arrangements such as service level agreements, the organisational power of the interface owner, the roles involved in using this interface, the responsibilities regarding the interface users, information on who is responsible for managing this interface and finally how secure this specific interface is (e.g. if encryption is offered).

  The security agency interface specializes the generic interface and is also described by the level in the organisation where the communication takes place, the type of communication (i.e. informative, initial, pushing or pulling), whether the contact is continuous, which security clearance level is expected, a description of the information which is being communicated by this interface, the time scale in which the communication is being processed and finally the communication equipment used for communication.

  The emergency services interface focuses on capabilities enabling collaboration, rather than information security (as the security agency interface). For communicating with emergency services, the interface must include a description on the expected information, how the service is supported, which relationships between this particular service and other services exist, the responsibilities for maintenance, information security and information clearance, arrangements for incident response regarding the specific interface and finally for ensuring compatibility of technical equipment between the communicating entities.

In the case of communication with a transport organization the interface includes more generic information on the number of infrastructure managers involved, whether a specific rail or road is used by multiple PTOs, what geography and topography the track or area lies in, how the population is distributed around the area or track and how the involved public transport operators communicate, what security and incident response routines are implemented at this particular transport operator (e.g. for evacuation), and how the public transport operator communicates with the public.

In order to model communication with the media and the public, the interface description focuses on information clearance responsibilities and announcement procedures.In such cases information is used which consists of who is coordinating and authorizing the information exchange and finally who is responsible for executing the information exchange.

These interface descriptions allow a generic security service to collaborate with security agencies, emergency services, transport operators and the media, while offering information on how to exchange and retrieve information, how to cooperate and how to inform the public controlled.

DISCUSSION & OUTLOOK

This contribution presents a generic concept for interoperability between entities in public transport security, regardless of their technical or non-technical nature, such as cameras, organizations, incident ground teams or sensor systems. This concept serves as a framework allowing the understanding of intra and inter-organizational IT interfaces across different administrative, business and operational structures as well as across technological environments. Within the SECUR-ED project this early interoperability concept served as a starting point to understand the relevant dimensions. It offers classifications and descriptions of typical interoperability objects found in public transport security. It further defines an approach for separating the systems involved in a system-of-systems architecture while based on the levels of the conceptual interoperability model (Turnitsa 2005). It offers high-level templates for describing Information Systems, Interfaces, Intermediaries and Roles. To this end, a wide range of related European research projects were surveyed and the identified system typologies aggregated, resulting in a comprehensive and useful concept for engineering interoperable security systems-of-systems. However, the domain of security in public transport is characterized by various entities, heterogeneous systems and various involved parties which may change significantly depending on the situation and the region. Therefore we cannot say the approach is truly comprehensive. Yet, the developed concept and its included interoperability objects were generalized and served as the basis for a more general interoperability notation for public transport in SECUR-ED (Sautter et al. 2012).

CONCLUSION

By using a widely acknowledged model for interoperability (Turnitsa 2005) and results of various European research projects, the SECUR-ED interoperability concept for information systems offers modelling capabilities for the complex domain of security in public transport. Both bottom up and top down approaches are enabled in modelling. By employing modelling approaches for socio-technical systems, e.g. (Hollnagel 2002), and by regarding both technical and social systems, interoperability modelling beyond the borders of pure technical information transfer is offered, also covering the domain of human collaboration. Hence the issues of system-of-systems engineering in complex security theatres can be addressed , since social, technical and socio-technical collaboration as well as their inter relations can be modelled.

ACKNOWLEDGMENTS

The authors gladly acknowledge this research was funded in part by the European Commission under the seventh Framework Programme (Grant agreement no: 261605, SECUR-ED, Research area: SEC-2010.2.1-1 Security of mass transportation - phase II). However, the results presented here reflect the views of the authors only.

REFERENCES

Asimakopoulou, E. 2010. "Advanced ICTs for Disaster Management and Threat Detection," In *IGI Global*, N. Bessis (ed.), .

Born, M., Holz, E., and Kath, O. 2004. *Softwareentwicklung mit UML 2*, Munich: Addison-Wesley.

Chen, R., Sharman, R., Rao, H. R., and Upadhyaya, S. J. 2008. "Coordination in emergency response management," *Communications of the ACM* (51), pp. 66-73.

COPE. 2008. *Use Case Descriptions and a Human Factors Engineering Framework* (Deliverable No. D2.1), COPE.

COPE. 2009a. *Comprehensive Model of First Responder Operations & Concept of Operations* (Deliverable No. D3.1), COPE.

COPE. 2009b. *HF-based Design Inputs to COPE Technology - Conceptual and Empirical Considerations of Common Operational Picture* (Deliverable No. D2.2), COPE.

COUNTERACT. 2009a. *Public Transport Security Planning - Organisation, Countermeasures & Operation Guidance - Part C: Systems and Equipment - Design Strategies and Considerations* (Final Report No. PT5), Counteract.

COUNTERACT. 2009b. *Public Transport Security Planning - Organisation, Countermeasures & Operation Guidance - Part B: Security Operations Planning - Development of Operational Concept, Field Level Security Plans, Procedures and Training* (Final Report No. PT5), Counteract.

DEMASST. 2009. *Current technological solutions and relevant research* (Deliverable No. D5.1), DEMASST.

DEMASST. 2010. *Report on Potential Integrated Solutions* (Deliverable No. D4.4), DEMASST.

Engelbach, W., Frings, S., Roßnagel, H., and Zibuschka, J. 2010. "Peer-to-peer Integration of Security-oriented IT -Systems in Public Urban Transport," In *Proceedings of the 5th Security Research Conference, 2010*Presented at the 5th Security Research Conference, Berlin.

Hollnagel, E. 2002. "Cognition as control: A pragmatic approach to the modelling of joint cognitive systems," *IEEE Transactions on Systems, Man and Cybernetics*.

Kurowski, S., Roßnagel, H., Zibuschka, J., and Engelbach, W. 2011. "A survey of European interoperability research in urban transport security,"Presented at the Conference on Mobility in a globalized World, Iserlohn, Germany.

Ritchie, B. W. 2004. "Chaos, Crises and Disasters: A Strategic Approach to Crisis Management," *Tourism Management* (Tourism Industry:25), pp. 669-683.

Roßnagel, H., and Junker, O. 2010. "Evaluation of a Mobile Emergency Management System: A Simulation Approach," In *Proceedings of the 7th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2010)*.

Sautter, J., Roßnagel, H., Kurowski, S., Engelbach, W., and Zibuschka, J. 2012. "Interoperability for Public Urban Transport Security: The SECUR-ED Interoperability Notation," In *Proceedings of the 9th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2012)*Vancouver, BC Canada.

Turnitsa, C. D. 2005. "Extending the Levels of Conceptual Interoperability Model," In *Proceedings IEEE Summer Computer Simulation Conference*Presented at the IEEE Summer Computer Simulation Conference, CS Press.