SECUR-ED

SECured URban transportation - European Demonstration

D22.1: Interoperability Concept

Description and illustration of the overall picture towards interoperability of capacities towards security in public urban transport, allowing orientation for SP3 and SP4 activities

Document identification	
Date	10/01/2012
Version	5
Related SP / WP	SP 2 / WP 22
Lead Participant	Fraunhofer IAO (FHG)
Contributors	Dr. Wolf Engelbach, Sebastian Kurowski, Jan Zibuschka (FHG), Didier von den Abeele (ALS), Dr. Volker Isbert (THA), Arnoud de Jong, Dr. Erik Vullings (TNO)

Reference	SCR-WP22-D-FHG-002
Dissemination Level	PU
Status	Issued
Related Deliverable	D22.2, D22.3, D22.4, D22.5
Lead Author	Dr. Heiko Roßnagel (FHG)
Reviewers	Mariangela Lamberti, Annarita Tedesco (ANS), Carolin Büttner (DBA), Lindsey Barr (UITP)

This document is issued in the frame and for the purpose of SECUR-ED project. This project has received funding from the European Unions's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261605.

TABLE OF CONTENTS

1 Abstract

In the field of public transportation and in large urban hubs such as metro or train stations, transportation operators and first responders collaborate in the prevention of and reaction to security issues. In order to optimise their specific daily operational business needs, heterogeneous information and communication systems are used. In case of an incident, however, it is crucial that the various involved parties exchange relevant information to get a shared understanding and act in a coordinated way in critical situations. Yet, heterogeneous communication and information system infrastructures often hinder this crucial flow of information.

This deliverable D22.1 describes a conceptual model that can be used to construct system of systems environments while taking into account information dependant systems in the domain of security in public urban transportation. Such an abstract definition of interoperability supports SECUR-ED in dealing with a diversity of security challenges, technologies and organisational procedures. This early interoperability concept serves as a starting point to understand the relevant dimensions. It will be further elaborated during the project towards a system-of-systems architecture. We present a comprehensive interoperability concept for a security meta system in public transportation, covering underlying approaches and theories, individual building blocks and an abstract conceptual framework integrating those components. A modelling approach is presented, offering capabilities of representing Information Systems, Interfaces, Roles and Intermediaries, while respecting the context of the interoperating system architecture and the exchanged content. We built on the results of earlier projects investigating different focus areas within this research field. We integrate those early results and synthesize them on a homogenous level of abstraction. This results in an overall concept, giving first insights in modelling and design requirements of an interoperable system.

2 References

2.1 History

Version	Date	Author	Main Changes
0.1	20.5.11	FHG	Document created
0.2	01.6.11	FHG	First Internal Draft
0.3	16.6.11	FHG	Second Internal Draft
0.4	22.6.11	FHG	Third Internal Draft
0.5	27.6.11	FHG	Final Internal Draft
0.6	29.6.11	FHG	First Draft to be delivered to WP Partners
0.8	17.7.11	TNO	Input from WP Partners
1	18.7.11	FHG	Version for Review
2	27.7.11	FHG	Final Version after Review
3	09.08.11	THA	Version submitted to EC
4	18.10.11	FHG	Integration of UITP comments : P13 & 61: Citing the year of publication, not the year of last upload: P13 “The relevant ISO standard (ISO 1993)” - P61: “ISO. 1993. ISO/IEC 2382-1:1993 Information technology - Vocabulary - Part 1: Fundamental terms.” P22: Sentence added under *6.18 Protectrail* based on UITP suggestion: “Not to be confused with RAILPROTECT developed with urban rail operators: **“**Innovative Technologies for Safer and more Secure Land Mass-Transport Infrastructure under Terrorist Attacks”. RAILPROTECT is relevant for SECUR-ED under WP23. See http://elsa.jrc.ec.europa.eu/showproject.php?id=13)” P40: Sentences deleted from *6.2.6 Current Situation in Mass Transport Security* based on UITP suggestion : “It is important to mention that no standards exist on this issue yet. Moreover, no interconnection and interoperability throughout Europe exist yet.”
5	10.01.12	THA	Version submitted with batch 1

2.2 List of Acronyms

CCTV	Closed Circuit Television
CONOP	Concept of Operations
COPE	Common Operational Picture Exploitation
COUNTERACT	Cluster of User Networks in Transport and Energy Relating to Anti-Terrorist Activities
CBR	Chemical, Biological; Radioactive
DEMASST	Demonstration Project for Mass Transportation Security
EDS	Explosives Detection System
EMS	Emergency Management Service
EXDEP	Explosives Detection with energetic Photons
FRS	First Responder Service
GUI	Graphic User Interface
ICT	Information and Communications Technology
IED	Improvised Explosive Device
IGRIS	InteGRail Information System
IM	Infrastructure Manager
IR	Infrared
IT	Information Technology
MODURBAN	Modular Urban Guided Rail Systems
NOAH	Network of Affined Honeypots
PTO	Public Transport Organisation
SAW	Surface Acoustic Wave Sensors
SECUR-ED	Secured Urban Transportation – European Demonstration
SoS	System of Systems
SP	Sub-Project
WP	Work Package
XRD	X-Ray Diffraction

2.3 Referenced Documents

The following documents are referenced

R[1] – SCR-WP22-DEL-002 – Interoperability Notation

R[2] – SCR-WP22-DEL-003 – Interoperability Syntax

R[3] – SCR-WP22-DEL-004 – Interoperability Semantics

R[4] – SCR-WP22-DEL-005 – Interoperability Framework and Guidelines

3 Introduction and Motivation

In public transport and especially in large urban hubs such as train stations, many transport operators and first responders collaborate in the prevention of and reaction to security issues. They use heterogeneous information and communication systems, optimised for their specific daily operational business needs and where security matters (if foreseen) are only part of. This also implies that it is sometime very difficult to sort the security information from the mass of information available.

At the same time, 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). In case of such incidents, 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 (Dantas and Seville). However, heterogeneous communication and information system infrastructures often hinder this crucial flow of information (Engelbach, Roßnagel, and Frings 2010).

SECUR-ED brings together 39 European partners from different backgrounds in public transportation and civil security from operators, industry and research. Being a demonstration project, security enhancing technologies and systems will be put to practice and demonstrated in four major urban European cities – Madrid, Paris, Milan and Berlin; additional tests will be conducted in cities like Brussels, Lisbon, Istanbul and Bucharest.

A major challenge will be to demonstrate the consistency of those security solutions, since the different stakeholders like vendors, transport operators and security organisations do not necessarily share the same understanding of threats, relevant information and IT-interoperability. Moreover, societal and legal concerns define a very diverse environment of mass transportation in the states and cities across Europe (UITP 2010).

Therefore, this deliverable D22.1 addresses a general concept of interoperability between information dependant systems regardless of their technical or non-technical nature, such as cameras, organizations, incident ground teams or sensor systems, in the domain of security in urban transportation. Within SECUR-ED it addresses the level of a given city or region, but the objective is not to interoperate between cities and regions. Such an abstract definition of interoperability supports SECUR-ED in dealing with a diversity of security challenges, technologies and organisational procedures. The interoperability concept concentrates on the interoperability of Information Systems, but keeps this broader context in mind. This concept must enable the other Sub-Projects to implement coherent steps towards a general approach of mass transportation security.

The interoperability concept is a framework that allows the understanding of intra- and inter-organisational IT-interfaces across different administrative, business and operational structures as well as across technological environments. Within SECUR-ED, this early interoperability concept serves as a starting point to understand the relevant dimensions. It will be further elaborated during the project towards a system-of-systems architecture (interoperability framework).

In order to cope with potential changes to the overall concept during the runtime of the SECUR-ED project (mainly because of to the refinement of the details of interoperability), the contents of this deliverable D22.1 will be continually refined towards a system-of-systems approach in D22.5.

The remainder of this deliverable is structured as follows. We will first identify the relation of this deliverable to the other activities in SECUR-ED in Chapter 4. This includes a brief overview on the Sub-Project 2, where the interoperability concept is embedded, and on the role of this concept inside the Work Package focusing on interoperability (Work Package 22). Following these relations we will derive the requirements that this concept must fulfil in order to ensure the highest additional value for the other activities using the outcomes of the interoperability concept.

While keeping these requirements in mind, we will focus on researched general interoperability concepts in Chapter 5, including an overview and details on the levels of interoperability from (Turnitsa 2005), concepts of interoperability in service oriented architectures and general system-of-systems design constraints. These assets are regarded under the aspect of their value for the interoperability concept. In Chapter 6 we focus on related research projects and their contributions towards an interoperability concept. We give a brief overview on the research projects, their contents, goals and possible benefits for SECUR-ED. Some of these projects provide further input for the interoperability concept. These results are then described, along with their possible usage for the later definition of building blocks embedded in the concept. The overall SECUR-ED interoperability concept is presented in Chapter 7, along with its elements and their usage. A brief insight in possible usages of the elements and on possible notations is given. The interoperability notation itself will be described in more detail in deliverable D22.2.

In order to use this concept for the special demands of security in mass transportation, building blocks are presented in Chapter 8. These blocks consist of the aggregated and interpreted results of the research projects introduced in Chapter 6. Additionally, a brief overview on the contents and potential income for interoperability is presented. Readers who are mainly interested in how to model interoperability should therefore skip Chapter 6. These building blocks provide the foundation to model the environment for further development of interoperable systems, while focusing on the special topic of security and mass transportation. The building blocks are explained in the order of the interoperability elements given in Chapter 7. After providing an overall concept and building blocks for further modelling, we will conclude our findings by reflecting the contents of this deliverable in Chapter 9.

4 The Relation to Other SECUR-ED Activities

This Chapter reflects the role of this deliverable in the context of SECUR-ED and derives the relevant requirements for the interoperability concept. The reflection focuses on the role of this deliverable inside the Work Package 22 (interoperability) and on the relation to Sub-Project 2 (SP2), where this deliverable and its correlated Work Package 22 (interoperability) are embedded, with regard to the other Sub-Projects inside SECUR-ED.

4.1 SP2 within SECUR-ED

The approach of SP2 within SECUR-ED is to develop a framework, which allows generalizing inputs from different cultures, disciplines, business structures and operational models, technological environments and perceived threats. This framework provides a common orientation that needs to be filled with specific content in the following SPs. In addition, the framework itself provides general concepts that should encourage novel security solutions in IT and operations. Therefore, the framework is not specific to one of the scenarios, capacities or cities, but defines a common abstraction level for all of the SECUR-ED topics. By providing common concepts and notations, it supports the intention to stay consistent within the whole project. This needs to be detailed per capacity, per city and per scenario.

Being a demonstration project, the project design of SECUR-ED follows the approach to provide early versions for different topics such as organisational procedures, interoperability concepts and technical architectures. These early documents serve as a starting point for the discussion in SECUR-ED, they are not intended to be final results. They especially support the establishment of a shared understanding of the relevant differentiation dimensions and abstraction levels for the approaches in all the involved WPs. In the long run, the common framework should allow to identify similar challenges and to gather possible solutions within a shared view of the situation. In this sense, the framework is also intended to guide the final assessment and validation.

Within SP2, three work packages exist that are closely interrelated. WP21 addresses the operational and organisational guidelines and structures; moreover it provides an overall security risk management methodology. This is the context in which the interoperability approaches (WP22) need to prove their value. WP23 tackles the chances and challenges for the modelling and simulation of security aspects in public urban transport. This should be oriented both at the structures of organisational guidelines and interoperability concepts of the previous WPs and could on this basis help to evaluate alternative approaches to the same threat.

4.2 D22.1 within WP22

The objectives of the Work Package WP22 are described as follows: *"This activity is providing both a concept of interoperability and a generic technical system-of-systems architecture. It checks use cases on this approach, provides architecture notation methods and suggests technical and organisational guidelines. The outputs will be specified for distinct capacities (in SP3, e.g. video or hypervisor systems) and in the demonstration cities (in SP4, e.g. Milan or Paris), and the experiences of SP 3 and SP 4 are integrated into an updated interoperability concept."* (SECUR-ED 2009)

The approach is defined as follows: *"The system-of-systems approach aims to allow the interoperability of several independently designed IT-systems and implementing different organisational concepts on top of them. It should be able to handle a wide range of operational tasks and security issues".* (SECUR-ED 2009)

Within the WP, the first task 22.1. "Interoperability concept: common picture" has the following description: *"The task reviews existing system-of-system approaches in security projects related to urban public transport (e.g. DEMASST, IntegRail, PROTECTRAIL, Modurban, MODSAFE, COUNTERACT, NOAH, VeRSiert) and reflects them towards the SECUR-ED vision. The results of this task will be textual descriptions and graphical representations of a common picture. This provides a reference for all other WPs in SP3 and SP4."* (SECUR-ED 2009).

Based on this overall concept, the other tasks of WP22 elaborate more details with a specific focus:

- *"Task 22.2: Interoperability notation: functional interface specification language The task provides a common functional interface specification language covering use case notation, interface description and system definition. This interoperability notation allows each WP of SP3 and SP4 to describe in the same granularity their roles, activities, IT-components and IT-interfaces*
- *Task 22.3: Interoperability syntax: technical architecture*
  The task describes the generic concepts for technical integration. This syntactical interoperability approach covers architectural interface concepts, recommends the use of standards and suggests common data modelling approaches based on data description languages. It will not go into the details of specific technologies, such as video standards, nor the individual demonstration city infrastructure.
- *Task 22.4: Interoperability semantics: business approach*
  The task is based on definition and description of standard roles and generic security use cases. For the different roles and use cases it elaborates how the relevant activities can be principally supported in the system-of-systems architecture, i.e. which systems and interfaces are used, how the approach supports the use cases and fits to the business integration approach.
- *Task 22.5: System-of-systems architecture and guidelines*
  The goal of this task is to gather feedback and experiences regarding the concept, the syntax and semantics of interoperability. It especially collects the feedback from SP3 (capacities) and SP4 (demonstrations). On this basis, guidelines and suggestions will be generated that address relevant stakeholders such as IT-industry, government, public authorities, first responders and transport operators." (SECUR-ED 2009)

Therefore, this deliverable D22.1 provides the following result: "Interoperability Concept: Description and illustration of the overall picture towards interoperability of capacities towards security in public urban transport, allowing orientation for SP3 and SP4 activities." (Perreal, 2009).

Along the tasks described above, the following deliverables are created during Work Package 22:

- *Deliverable 22.1: Interoperability Concept: Description and illustration of the overall picture towards interoperability of capacities towards security in public urban transport allowing orientation for SP3 and SP4 activities.*
- *Deliverable 22.2 Interoperability Notation: Common functional interface specification language: The deliverable is providing a project-wide common functional interface specification language with templates and guidelines for use case notation, interface description and system definitions.*

- *Deliverable 22.3 Interoperability Syntax: IT interoperability concept with architecture diagrams and interface definitions. It includes interoperability guidelines to SP3 "within capacities" and SP4 "between capacities".*
- *Deliverable 22.4 Interoperability Semantics: Use case descriptions and their usage of the interoperability syntax, defining the semantics of the system-of-systems approach and considering progress in SP3 and SP4.*
- *Deliverable 22.5 Interoperability Framework and Guidelines: General interoperability concept, IT syntax and business semantics considering results in SP3 and SP4, including enforcement guidelines to industry, government and operators.*

(SECUR-ED 2009)

The overall outcome of this Work Package 22 is the view of interoperability on a "*Concept Level*", defining "*How security can be achieved*", by using "*Shared vocabulary and conceptual models*" and providing "*the methods to the project*" (SECUR-ED 2009). Therefore the deliverables together create the basis for further development of interoperability in general and interoperable systems.

Since interoperability is a central aspect in SECUR-ED, not all its dimensions are covered in WP22. Related activities and project results within SECUR-ED towards shared concepts of interoperability are among others:

- Privacy and protection of civil rights (SP1)
- Involving advisory groups and ethical group (SP1)
- Consensus on implementable recommendations (WP11)
- Terminology (WP21)
- Organisational structure, strategy and tooling for managing security risks (WP21)
- Federated Simulation (WP23)
- Best practices from railway and bus market (SP3)
- State-of-the-art-technologies in related industries (SP3)
- Risk assessment guidelines and software (WP31)
- Competence requirements and training suggestions (WP38)
- Specific IT Architecture (WP41)
- Demo city specific scenarios (WP42-45)
- Demo city description, incl. IT and use cases (WP42-45)
- Methods and tools to set up consistent security oriented demonstrations (WP51)
- Benchmarking assessment of each solution and technology as applied in SP4/5 (WP54)
- Consistent guidelines for implementing security systems (SP5)
- Recommendations about selecting the right capacities with regard to expected performance (SP5)

4.3 Requirements for the Interoperability Concept

The concept is supposed to be used in the context of security challenges and must be able to handle a wide range of operational tasks and security issues, but does not necessarily need to be restricted to this domain. Ideally, the SECUR-ED solutions developed with the background of this concept should offer improvements also for the everyday transport operations business. It should also be able to handle the setting of a broad range of different institutions involved,

which are mainly public mass transport operators and first responders, but can be others as well.

The focus of the interoperability concept is on Information Systems, but related aspects should be tackled as far as necessary for a shared picture, since interoperability should be motivated by security activities and processes. The concept should also allow discussing different organisational concepts on top of Information Systems. In addition, it is intended to enable the reflection about coherence at mission level while accepting heterogeneity at system level.

The interoperability concept moreover should help to address interoperability challenges in the following SPs, such as:

- Do we need and how should we design a common middleware?
- Do we need and how should we handle different access rights in crisis situation?
- How do we realize the transfer and aggregation of data?

Within this project context, the main requirements for the interoperability concept can therefore be summarised as follows:

- The concept should be abstract enough to fit for the different technologies, organisational settings and crisis management phases
- The concept should be simple enough to be easily understood
- The concept should be flexible enough to be used and adapted in different WPs
- The concept should be focused enough to not interfere with the topics addressed in other WPs

This also implies that the common picture is not specific to one supplier's architecture, one country's legislation, one security challenge, one city and its public transport organisation or any given IT environment or legacy system. It should instead reflect approaches towards the interoperability of independently designed Information Systems and towards modularity in the sense that the same solution elements can be used for different purposes in different contexts. Thus, it should reflect both sophisticated and simple solutions and organisational concepts in different cities.

5 General Interoperability Concepts

In this Section we take a look at approaches and concepts towards interoperability and system of systems beyond the security domain. We will sketch the most important concepts which will be used as a basis for our interoperability concept, described in Chapter 7. To be able to understand the interoperability concepts described, one should be aware of the meaning of interoperability itself.

A lot of approaches have been undertaken to define interoperability. Following (Hrebicek 2006), interoperability is defined by the IEEE Glossary as "*the ability of two or more systems or components to exchange information and to use the information that has been exchanged*". However this can include connected systems which are able to use the information input of other systems in order to process results. Although this already draws an extensive picture of interoperability, the levels of interoperability as in (Turnitsa 2005) see simple connections as being the lowest form of interoperability. Furthermore, aspects from system-of-systems engineering and from information management, including user relevant views on information exchanges of the systems, are included in these levels. Therefore, this definition does not draw a complete picture of interoperability as required by the interoperability concept for SECUR-ED.

The relevant ISO standard (ISO 1993) defines interoperability as "*the capability to communicate, execute programmes, 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*". The picture drawn by this definition pays respect to the users' requirements and therefore to the interpretation of information. This also includes semantics and the structure of the information exchanged and is therefore more complying to the requirements to this interoperability concept as stated in Chapter 4. However, the definitions so far focus on interoperability as a sole task of the systems participating, leaving out special roles for translating information and their semantics in order to achieve an adaptable structure.

(Wegner 1996) refers to this by defining interoperability as a "*scalable form of reusability, being concerned with the reuse of server resources by clients whose accessing mechanisms may be plug-incompatible with sockets of the server. Plug compatibility arises most literally with electrical appliances that require both static compatibility of shape and dynamic compatibility of voltage and frequency*" Additionally, he adds that „*If there is no direct match, interoperability of electrical appliances can be achieved by adapters and transformers*" (Wegner 1996). This defines adapters as part of an interoperable system, being responsible for translating the information to a format that can be understood by other participating systems. Furthermore, by introducing matters of reusability (Wegner 1996) widely complies with (Turnitsa 2005) by paying respect to the engineering knowledge implied by the overall interoperable system.

As will be shown in Chapter 6, the topic of security in mass transportation includes several domains and therefore different and partially non disjunctive requirements on information and knowledge. Therefore, this concept pays respect to the definitions as described by (ISO 1993) and (Wegner 1996), focussing on the requirements of engineers, embedded systems and users.

In order to enable structured engineering methods in the different fields along the issue of interoperability, Section 5.1 presents different levels of interoperability. However the here presented levels are not the only definitions available. (Cullen et al. 2009) consider a definition

breaking down the issue of interoperability on the levels of political goal setting, shared cognition and physical communication. However, this definition does not allow any distinction between technical and non-technical issues of interoperability and is therefore not further taken into account.

Within this Section, we will start by describing the different levels of interoperability by (Turnitsa 2005) in Section 5.1, followed by an insight into interoperability concepts of service oriented architectures in Section 5.2 and general constraints and models of system-of-systems design in Section 5.3.

5.1 Levels of Interoperability

Originating from the domain of simulation, the levels of interoperability from (Tolk and Muguira 2003) have fast emerged to a widely known standard (W. G. Wang, Tolk, and Wang 2009). In the original version from (Tolk and Muguira 2003), the levels hereby focused on the provision of data and the description in the interface, distinguishing between « Harmonized Data and processes » (Level 4), « Aligned Dynamical Data » (Level 3), « Aligned Static Data » (Level 2), « Documented Data » (Level 1) and « System Specific Data » (Level 0). Level 0 represents the state of isolated, non-communicating systems, while the grade of interoperability rises with growing documentation (Level 1), compliance of reference models (Level 2), system approaches (Level 3) and finally the definition of a shared conceptual model, resulting in an overall consistency of semantic of data (Level 4),.

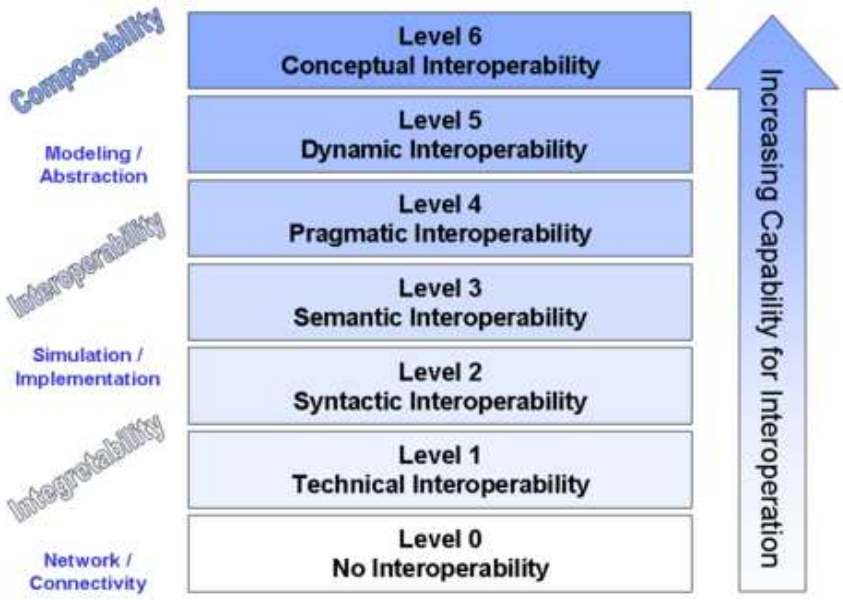

Figure 1 Conceptual Interoperability Model as described in (Turnitsa, 2005)

However, over time the definition was extended, focusing not only on data and interfaces but the involved actors of the interoperating systems and their implementation. Figure 1 shows the extended model as defined in (Turnitsa 2005). Like (Tolk and Muguira 2003), the first level (Level 0) here describes isolated actors, which are not communicating at all. When coming to Level 1, basic communication is established (i.e. by connecting two or more systems). This communication requires a communication protocol (Turnitsa 2005), which still complies with the requirement of documented interfaces and data (Tolk and Muguira 2003). Following Level 2, a common data format is required, complying with the requirement of a common reference model (Tolk and Muguira 2003). A basic communication protocol is used on this level to

structure the data. On Level 3, semantics of data are introduced, sharing the meaning of data over the systems' actors. (Selvage et al. 2006)'s approach to achieve semantic interoperability is described in more detail in Section 5.2. At the next level (Level 4, pragmatic interoperability), the systems' actors are required to be aware of other actors' procedures and methods. This can either be reached by documentation or harmonization of the used procedures and methods (Tolk and Muguira 2003). By doing so, the context of the information shared becomes visible. Finally, when attaining dynamic interoperability (Level 5), systems are aware of the assumptions and constraints existing inside the other systems. This means that a system must be aware of state changes which can occur in other systems during communication, hence respecting the effect on the results of the overall system. With respect to data, the fifth level already describes a sophisticated state of data processing, since structure, context and the effect of information is regarded. The final and sixth level defines the conceptual interoperability itself as an interoperability of system concepts. On this level, a system is fully specified and independent from its implementation. This requires full documentation of the involved systems' conceptual models, which enable interpretation by other engineers. Additionally this enables transferring of the interoperability model to other areas, i.e. other cities. While the first five levels focused on provision and sharing of knowledge on data and information processing in the system-of-systems architecture, the sixth level emphasizes the provision and sharing of knowledge on the development, implementation and maintenance of the architecture.

5.2 Service Oriented Architectures

Using service oriented architectures, standardized interchange formats can be used to enable interoperability of systems. However, with a growing number of services and correlated domains, semantics becomes a key factor for successful interoperability. (Selvage et al. 2006) approach this problem by proposing the usage of enterprise data models (EDM). Such models define the complete basis and format for exchanging and understanding the data used for communication inside an organisation (Kini and Manjaiah 2010), or in our case inside the system-of-systems. However, the nature of applications as well as the changeability of the involved stakeholders can become crucial, since semantics can be lost or not even captured. Also, according to (Selvage et al. 2006), detailed data models can lead to over-definition, to redundancies and most importantly to too large timescales, missing important changes in the process, while capturing the semantics between the datasets involved. In order to bypass these problems and to achieve semantic interoperability between the services, three patterns are proposed.

The **point-to-point semantic integration** maps the meaning of data between the data sources, without a centralized data model. Furthermore, the services themselves handle the semantics required for communication. This opposes the Hub-and-spoke semantic integration, where a central lookup is required.

The **master data management pattern** integrates the mapping of semantics into a centralized communicator. In this approach, the central platform for communication intermediates between the services and ensures the understanding of the data. However, the industry information model uses a similar approach, hence leaving out the communicating instance. Here the mapping is done by the format. Therefore, this pattern must be regarded more as an interchange approach, rather than one for interoperability.

In the **semantic web approach** for interoperable semantics, the communication and the establishing of data understanding is done according to the point-to-point pattern. This

approach differs in the way that a standardized description language is used rather than a data model. This allows transformations between the services by intermediating applications while reducing the data amount and development times.

5.3 System-of-Systems Design

Another research stream that is strongly relevant for the interoperability concept presented in this deliverable is System-of-Systems (SoS) design. Keating et al. define SoS as *"a metasystem, comprised of multiple (…) autonomous complex subsystems that can be diverse in technology, context, operation, geography and conceptual frame."* (C. Keating et al. 2008). However, Keating also notes that *"the concept of system of systems is poorly defined, and in fact tautological, since systems themselves are in fact considered to be comprised of subsystems and therefore a system of systems is itself just a system"* (C. B. Keating 2005). However, system-of-systems engineering can still offer interesting perspectives and insights, especially in cases that match the properties associated with such scenarios, such as those postulated by (Sauser and Boardman 2008), namely Independence, Decentralization, Network-Centricity, Heterogeneity, and Indeterminism, as illustrated in Figure 2.

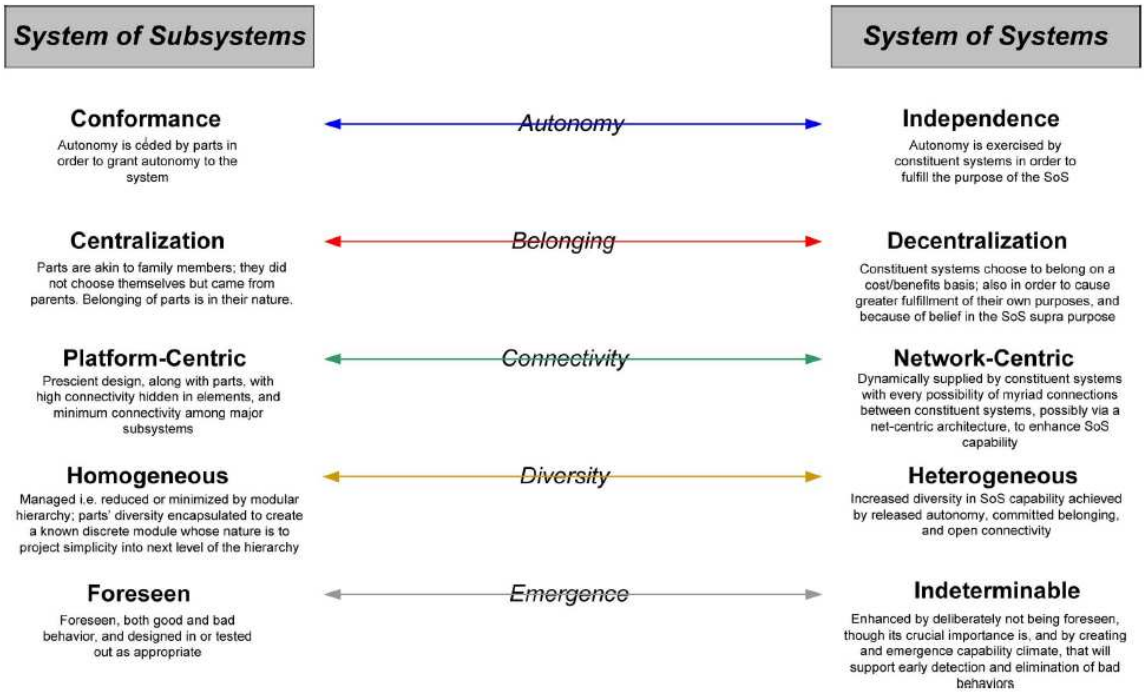

Figure 2 Properties of SoS (Gorod, Sauser, and Boardman 2008)

Keating also provides a description of what he calls "logic levels" in SoS engineering: System Philosophic, System Axiomatic, System Methodological, System Application, and System Method (see Figure 3).

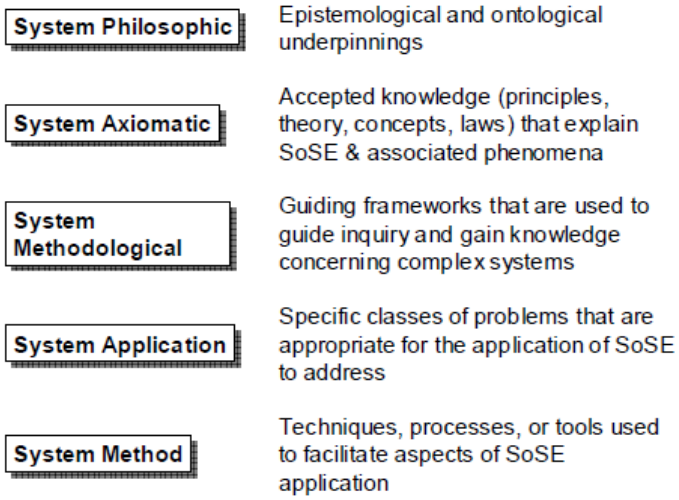

Figure 3 SoS Logic Levels (Keating 2005)

Those align quite well with the approach taken by SECUR-ED. This deliverable deals with the philosophic, axiomatic underpinnings of the SoS approach to be taken in SECUR-ED, and serves as the definitive reference for the epistemological and ontological underpinnings of the project. It also provides a collection of knowledge on the System Axiomatic level.

However, as DeLaurentis and Callaway put it, *"Much confusion still remains about words and phrases for system-of-systems type problems, let alone the best modeling approaches for dealing with them. While pockets of organisational restructuring may address this challenge for particular projects, there is a lack of systematic thinking at the basic level about how to address the challenges"* (D. DeLaurentis and Callaway 2004). First steps towards applying those principles in the area of civil security and public transport have been taken in works such as (D. A. DeLaurentis 2005) or (Eriksson 2009), whose results along with the results of other past and current projects, were integrated in the interoperability concept presented here. Hopefully, this systematic integration of results will lead to a broader intellectual foundation for system-of-system frameworks in public transportation.

6 Interoperability Elements in Related Projects

6.1 Description of Related Projects

With regard to interoperability in the research area of security in public mass transport, public security and mass transportation in general, a lot of different research projects have to be considered. Although none of these projects describes a concrete interoperability concept or approach for the field of public mass transport, several conclusions on involved roles, communication, sensor systems and general structures of collaboration can be made. These results have been an essential source for the identification and description of the relevant building blocks, described in Chapter 8. The following gives a brief overview on the most relevant research projects and their focus.

6.1.1 DEMASST

As a Phase 1 “DEmonstration project for MASS Transportation security” (DEMASST), embedded in the 7th European Framework Programme, DEMASST provides precursors for SECUR-ED regarding current technology and current situation research. Its focus was hereby on security in public mass transport with emphasis on terrorist attacks. It was funded with 956 558 Euros by the European Union with the consortium comprising TNO, TIFSA, INECA, Thales, VTT, Fraunhofer, SINTEF, INASMET, the Norwegian Armed Forces, Astrium, Ansaldo and the CEA. During the project, sensor systems and technologies were identified, along with its technological readiness level (TRL) (DEMASST 2009a). This overview on current technological solutions, such as behaviour detection systems, can be used in later phases of SECUR-ED in order to identify suitable technological solutions for the demonstrator work packages. Additionally, a survey of people involved in public mass transport security was performed (DEMASST 2009b). The survey provides an overview of the current situation in mass transportation security, when coming to requirements for external communication, used systems and involved parties in operations during routines, emergencies and more general incidents.

Considering the general concept of interoperability in SECUR-ED, such results are used to describe elements in the interoperating system by deriving metadata. The project also defines an abstract concept of interoperability by creating a system of systems map for mass transport security (Eriksson 2009). Although this map describes an approach on interoperability in mass transportation security, the project focuses on topics rather than actors and processes. Therefore, this map must be seen as a signpost for the general development. This can be done by defining the basic goals of the interoperating concepts: « Intelligence », « Risk assessment-based command and control », « Comprehensive threat detection », « Preventive and early intervention », « Passive and automatic protection », « Cyber defence », « Post-incident intervention and restoration of services », « Forensics », « Learning and training ». These basic goals comply with the emergency lifecycle from (Ritchie 2004) and should be regarded during further design of the system.

6.1.2 COUNTERACT

Similar to DEMASST, the project “Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist aCTivities” (COUNTERACT) focuses on public mass transport systems. But in contrast to DEMASST, COUNTERACT considers security on a more general level. Although COUNTERACT focused exclusively on terrorism, an all-hazards approach was used in the development of tools such as awareness campaigns or guidelines for conducting risk assessment in public transport networks (COUNTERACT 2009c) and general collaboration tools during incidents and catastrophic events (COUNTERACT 2009a). Embedded in the 6th European Framework Programme, the projects’ funding was 4.480.640 Euros and the consortium consisted of UITP, the European Commission Joint Research Centre (JRC), the Institute for Transportation Linkoeping, Associazionne Transporti (ASSTRA), Energy Solutions, M3 Systems, the National Technical University of Athens, the International Union of Societies for the Combination of Rail and Road Transportation, SAFEXPERT, the Ministry of Interior, Fire & Rescue of the Czech Republic, I-SEC Homeland Security B.V., Deutsche Bahn and DHL Worldwide Network. Additionally an active User Group made up of security practitioners from European public transport operators guided the direction of the project, making its results more widely acceptable and applicable.

COUNTERACT gives a definition of the general security management system and details on sensor systems, field security plans, concepts of operations and security procedures. Additionally general interfaces for communicating in a public mass transport environment are described (COUNTERACT 2009a). The more general approach also includes involvement of the infrastructure managers in the incident response and preparedness routines. This leads to a more holistic view on the data involved. The interfaces introduced in (COUNTERACT 2009a) and the security management system in (COUNTERACT 2009b) respect geographical information and inter-organisational collaboration between different public mass transport providers as well. This more holistic view on the shared data can provide a key for creating the syntactic and semantic interoperability during D22.3 and D22.4.

6.1.3 COPE

Focusing on emergency response, the project for Common Operational Picture Exploitation (COPE), embedded in the seventh framework programme, dealt with the collaboration and support of the involved parties at the ground-site (COPE 2009a). The consortium consisted of VTT Finland, BAE Systems UK and Sweden, the University of Dublin, UTI Group Romania, GMV Portugal, the Centre for European Security Strategies (CESS), the General Inspectorate for Emergency Situations (IGSU) and the Emergency Services College Finland. It includes approaches on the analysis of cognition and decision making in teams (COPE 2008).

Based on this analysis, several use cases were created and describe the collaboration of the persons involved at the ground site in case of emergencies. There is no general specialization on certain fields of security like mass transportation. Consequently, the provided use cases can only give a general understanding of collaboration and roles involved. Based on the outcome of the research, an incident response support system was developed, which makes use of wireless sensor networks (COPE 2009b). Through evaluation of this system by incident ground staff a picture on the requirements of presentation and sensing was drawn. In case of the development of user interfaces for decision support and information aggregation, this input becomes important, since it reflects the requirements of the involved parties at ground level

and therefore their acceptance of the system. The results from (COPE 2009a) were used in this deliverable, creating a building block for describing roles in the overall interoperability concept.

6.1.4 Modurban

Embedded in the European Unions' 6th Framework Programme and with a funding of about 10 million Euros, Modurban focused on Modular Urban Guided Rail Systems. Its consortium consisted of the Metro of Lisbon, the Metro of Madrid, Ansaldobreda, Rhein Consult, Ansaldo, Technical University of Dresden, ATAC Romania, Siemens Transportation Systems, UITP, Knorr-Bremse Rail Systems, London Underground Ltd., Ferrocarril, Navecom, Prague Public Transit Co. Inc., University of Valenciennes, Kite Solutions, BVG, University of Chile, Metro of Warszawik, Budapest University of Technology and Economics, Dimetronic, Bombardier Transportation, Elta, Frensistemi, Esterel, Rheinische Bahngesellschaft, Funkwerk Information Technologies, Thales Rail Signalling Solutions, Régie Autonome des Transports Parisiens, ALSTOM Transport, National Institute for Research on Transportation and its Security Issues, the Joint Research Centre of the European Commission, University of Newcastle and the Alma Consulting Group.

The main focus of the project was the communication between devices embedded in train systems as well as communication media and interoperability of devices in and among train systems (MODURBAN 2009). By doing so, approaches were developed for creating autonomous train systems and passenger information systems (MODURBAN 2008). Although the interoperability of components is emphasized, the level of detail regarding the systems involved is more necessary for later development of interoperating systems, rather than developing and defining a general concept for interoperability in the field of security in public mass transport which was not addressed in this project.

6.1.5 VeRSiert

As a research project focusing on security at large public events, VeRSiert deals especially with managing the information along the security lifecycle. The project was financed by the German Ministry for Education and Research and funded with 2.7 million Euros. The consortium consisted of the NVR Nahverkehr Rheinland GmbH, KVB Koelner Verkehrs-Betriebe AG, the City of Cologne, ARC Airport Research Center GmbH, Vitracom AG, the University of Wuppertal and the University of Stuttgart.

The developed solutions offer information management capabilities for all participating actors. Additionally, mobile solutions are provided for mitigation in the post incident phase, offering visitors faster evacuation and information capabilities (Roßnagel, Zibuschka, and Junker 2010). The assets created for the development of these services provide an overview on the integration of semantic web technologies and social media (Roßnagel and Zibuschka 2011), while taking into account the different roles correlated with all phases of an event, including public security organisations and first responders (Roßnagel, Zibuschka, and Junker 2011). In regard to inter-organisational cooperation, the VeRSiert-project developed a web portal that supports the planning of public events and provides communication facilities for inter-organisational information exchange (Engelbach et al. 2010) (Engelbach, Roßnagel, and Frings 2010)

6.1.6 NOAH

As an IT security project, embedded in the 6th European framework program and with a funding of around 1.5 million euro, the European "Network of Affined Honeypots" (NOAH) aims at the development of an alert system for potentially malicious internet traffic. Its consortium consisted of Alcatel, DFN-Cert, University of Amsterdam, Hellenic Telecommunications and Telematics, Technical University of Zurich, Virtual Trip Ltd. and the Trans-European Research and Education Networking Association.

The project work consisted of designing a system of so called honeypots implemented at home computers, which forward sequences of recorded malicious internet traffic to central servers for further processing. All honeypots use different detection engines, creating a distributed approach on assessing the time criticality of processing of network traffic sequences (NoAH 2006a) (NoAH 2008). The decision algorithms implemented in the honeypots and the distributed cognition along the system (NoAH 2006b) can provide input for the implementation of the decision support. The overall outcome is an assessment of the current threat level in the Internet. Along the system design, additional output was produced, such as research on state-of-the-art systems and their respective interoperability and monitoring capabilities (NoAH 2005). Although IT security plays an important role in the design of an interoperating system, the results of NOAH are too specific to be used in this deliverable. However, the algorithms (NoAH 2006b) and the overall architecture (NoAH 2006a) (NoAH 2008) may provide valuable input for the concrete implementation of the interoperating system and its decision support components.

6.1.7 Integrail

As a project coping with performance optimization, in terms of "*capacity, average speed and punctuality, safety and the optimised usage of resources*"(InteGRail 2010) of railway systems, embedded in the 6th European Framework Programme, the project for INTElligent integration of RAILway systems aimed at enabling "*sharing of information to increase efficiency and quality and support the business objectives of the Railway Undertaking and Infrastructure Manager*", ensuring "*that the right information is available at the right time in the right place*", identifying the "*ways of using the information more effectively for maintenance optimisation*", identifying "*ways of combining and using information effectively for management requirements*", ensuring "*that the information can be transmitted effectively to the decision makers*" and demonstrating "*that creating the right information and sharing it will enable improvement*" (InteGRail 2010). The project was not involving any urban mass transportation systems. The contributors avoided replacing existing systems but using them to create a system-of-systems architecture, in order to achieve the goals mentioned. Although the basic goals of this project do comply with the basic definition of interoperability as mentioned in Chapter 5, no deliverables were available to the contributors of this deliverable. Therefore this project was not taken into account while creating the building blocks.

Integrail aimed at fulfilling these goals by providing deliverables on "*Proposals for Standard(s) for data and information models for Railway Operation Rolling Stock, Infrastructure and Traffic Management*" and an "*Architecture and information sharing platform for the railway domain*" capable of providing "*information adapted to the needs of the user*", "*efficiently using state of the art Information and Communication Technologies (ICT)*", a "*Communication Framework compatible with the innovation of communication technologies or solutions and following the*

stable migration directions in this field", "*Example functions or information systems that use the architecture concept (IGRIS), the communication framework (ICOM) and the standardised information model (Railway Domain Ontology, RDO).*", "*Demonstration Service to support On-line decision making*" and a "*Demonstration Service to support Strategic and Tactic decision making.*" (InteGRail 2010). The project also implemented the research findings in a demonstrator, in order to verify system function performance, the "*collaboration of IGRIS with 'pre-existing, legacy' information systems*", reusability of the "*IGRIS architecture*" "*across the demonstrations*" and to measure the "*growth of performance*" regarding "*one or more railway business processes*" by using "*Key Performance Indicators*" (InteGRail 2010). The project was funded by the European Comission with 10.999.647,57 Euros, involved ten European Countries, as well as, Chile 39 Participants contributed to the project including UNIFE Belgium, Alstom France, AnsaldoBreda Italy, Bombardier and the Siemens AG Germany, D'Appolonia Italy, FAV Germany, DeltaRail Netherlands, Ansaldo STS Italy, CAF Spain, Nortel Networks Germany, Laboratori G. Marconi Italy, Atos Origin Italy, Mermec Italy, TrenItalia Italy, RFI Italy, ATOC United Kingdom, Ceské Dráhy, a.s. Czech Republic, MAV Hungary, Unicontrols Czech Republic, Strukton Railinfra Netherlands, Deuta-Werke Gmbh Germany, Heriot Watt University United Kingdom, IMEC Belgium, OFFIS University of Oldenburg Germany, Televic nv Belgium, Seebyte Ltd United Kingdom, Kontron nv Belgium, University of Chile – Centro de modeliamento matematico Chile, INRETS France, Wireless Future Italy, University of Birmingham United Kingdom, ADIF Spain, Corridor X Austria, Network Rail United Kingdom, Prorail Netherlands, SNCF France, UIC France, Réseau Ferré de France and FAR Systems Italy. The project ended in 2010.

6.1.8 PROTECTRAIL

Embedded in the 7th European Framework Programme, the Railway-Industry Partnership for Integrated Security & Rail Transport named Protectrail focuses on providing "*a viable integrated set of security solutions*" with the focus on rail transportation systems (PROTECTRAIL 2011). The approach hereby considers the perspective of "*layered 'system integration'*", in order to "*address this main goal*" of solving "*the railway security problem*" by "*dividing the global mission into a limited number of submissions that respond to well identified needs / concerns of rail operators, within a framework of general coherence and integration of technical and organizational solutions*" (PROTECTRAIL 2011). Although the problem addressed offers the potential for developing interoperability concepts, the project has just started recently. Therefore, no deliverables are yet available to the public and this project was not included in developing the building blocks. Protectrail is funded by the European Comission with 13.115.064 Euros and is planned to end in 2014. The consortium includes Ansaldo STS Italy, TNO Netherlands, Selex Elsag Italy, UIC France, Selex Sistemi Integrati Italy, Bombardier Transportation Germany, Alstom Transport France, Thales Communication and Security France, SARAD Germany, UNIFE Belgium, MORPHO France, DuctIS Germany, ZSSK Slovakian Railways Slovakia, LITRAIL Lithuanian Railways Lithuania, ITALCERTIFIER SCpA Italy, PKP PLK Poland, D'Appolonia Italy, ELBIT Systems Israel, FUNDP Belgium, EPPRA France, Kingston University United Kingdom, SODERN France, Smiths Heimann France, CEA France, ISL France, TCCD Turkish Railways Turkey, MER MEC Italy and SNCF France. Not to be confused with RAILPROTECT developed with urban rail operators: "Innovative Technologies for Safer and more Secure Land Mass-Transport Infrastructure under Terrorist Attacks". RAILPROTECT is relevant for SECUR-ED under WP23 (See http://elsa.irc.ec.europa.eu/showproject.php?id=13).

6.1.9 Modsafe

As a project of the 7th European Framework Programme, the MODular urban transport SAFEty and security analysis approaches interoperability from a different perspective of creating an environment with interchangeability capabilities, hence standardizing the domain of urban transportation to a degree where systems can, not just interact with each other, but be replaced as well. Hereby "*safety requirements, safety models, responsibilities, roles, safety approvals, acceptance and certification schemes*" are addressed (MODSafe 2011). The project also respects the connection of such assets to activities involved in safety and risk assessment of urban transport systems. In order to achieve this state-of-the-art systems and procedures were analysed and "*merged into harmonized and agreed joint safety packages*" (MODSafe 2011). Missing elements were added in order to "*strengthen excellence of European surface transport*" (MODSafe 2011). Hereby a "*coherent and agreed Hazard Analysis and Risk Analysis*" approach should be provided (MODSafe 2011). The project is currently being processed and started in September 2009. It is supposed to end in August 2012 and is funded by the European Commission with 3.469.161 Euros. Its consortium is consisting of TÜV Rheinland Intertraffic GmbH Germany, TÜV Rheinland Consulting GmbH Germany, Société Technique pour l'Energie Atomique AREVA France, Budapest University of Technology and Economics Hungary, Bombardier Signal GmbH Germany, Institut National de Recherche sur les Transports et leur Sécurité France, Alstom Transport SA France, Régie Autonome des Transports Parisiens France, Technische Universität Dresden Germany, Union Internationale des Transports Publics UITP Belgium, Association of the European Railway Industry UNIFE Belgium, Université de Valenciennes et du Hainaut – Cambrésis France, Thales Rail Signalling Solutions Inc Canada, KITE Solutions s.n.c. Italy, Dimetronic SA Spain, Rail and Bus Consultants GmbH, Ansaldo STS France, Transports Metropolitans de Barcelona SA Spain, TelSys GmbH Germany, London Underground Limited United Kingdom, Metro de Madrid SA Spain and Université de Technologie Compiègne France.

6.1.10 SECUREMETRO

Embedded in the 7th European Framework Programme, the small to medium scaled research project SECUREMETRO aims at "*Increased safety, security and resilience of metro vehicles from terrorist attack by explosives and firebombs through materials choices and design, thereby increasing resilience and reducing the impact of attack on passengers, staff, infrastructure and property.*" (NewRail 2011). It does so by developing "*validated materials selection and design strategies for building metro vehicles with intrinsic security features*" (NewRail 2011). The European Comission is funding this project with 2.710.714 Euros and its consortium is consisting of Bombardier Transport, Regie Autonome Des Transportes Parisiens, Explosivos Alaveses, STAM SRL, Istituto Affari Internazionali, Fundacion Inasmet, Institut National De Recherche Sur Les Transports Et Leur Securité, Suncove SA, Fundación Ferrocarriles Espanoles and the Metro Warszawskie. Since no deliverables were accessible, the project was not included during the further research of the related projects.

6.2 Selected Aspects of Related Projects

All of the projects described in the previous Section provided valuable input for the definition of an interoperability concept. In particular, COPE, COUNTERACT and DEMASST provided the most relevant deliverables in regard to general interoperability and building blocks. By analysis of these projects, requirements in the domains of sensor systems, communication systems, actors and structures could be obtained. These dimensions generally define interoperability, and also take into account both, technical systems and human factors. Following these dimensions, the most important reference projects were mapped, resulting in Figure 4.

.

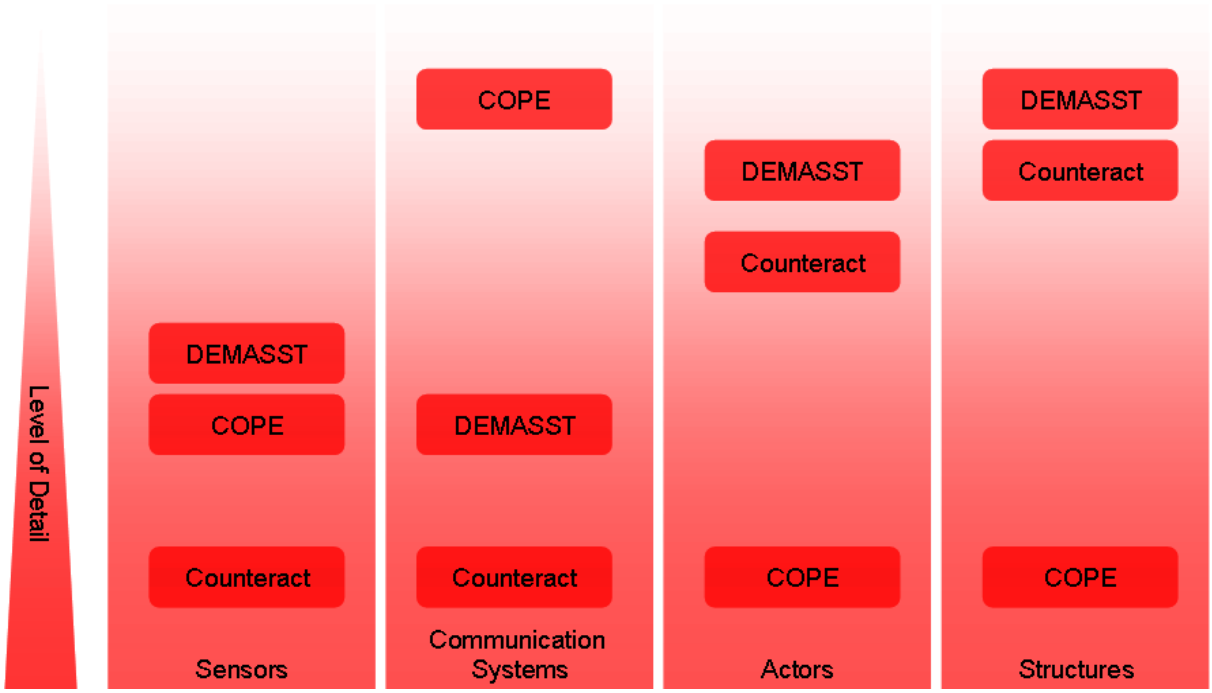

Figure 4 Level of detail of reference projects in certain domains

Using this figure, it becomes visible that all projects provide valuable input for a domain of interoperability. The most important contribution to our interoperability approach came from analysis of the projects COPE and COUNTERACT. Especially in the field of sensor and communication systems, combining the output of COUNTERACT and DEMASST provided with (COUNTERACT 2009b) and (DEMASST 2009a) creates a broad view on available systems and their relationships. COPE, as a project regarding ground site incident management in the post incident phase of the incident life cycle, focuses in (COPE 2008) more on actors and along with (COPE 2009a) on structures involved in the collaboration during the incident. In the following we will provide an overview on the potentially useful assets identified in these reference projects. Hereby each asset is presented along with its providing project. For each asset the potential use for the general interoperability concept is further described. Although these assets already give a brief insight in the elements of the general concept, they are not yet fully usable. Therefore, Chapter 8 shows these results after analysis, combination and partial aggregation, resulting in concrete building blocks for the interoperability concept. The following provides an overview on the assets identified, which contribute to these building blocks for the further interoperability concept. The following list of

assets is not ordered as the overview given in Figure 4 but by their corresponding project. It covers the aspects of Incident Ground Collaboration, Sensor Systems, Concept of Operation, Filed Level Security Plans, Interfaces with other Organisations and Current Situation in Mass Transport Security.

6.2.1 Incident Ground Collaboration

Reference Project(s)	COPE

By analysing incident ground processes, COPE provides several use cases including collaboration in the post incident phase (COPE 2009a). Like the overall project, these use cases emphasize the roles directly involved in resolving the incident or the catastrophic event. Hereby the use cases described include:

- Incident ground organisation
- Tactical mode & risk assessment
- Management of human resources
- Resource management (non-human)
- Command & control devolution
- Coordination with other agencies
- First responder & emergency services collaboration
- First responder & police collaboration
- Fire attack
- Water management
- Search & rescue
- Command hand over

These use cases give an overview on the persons communicating and collaborating, hence showing potential for further requirements of interoperability on the operational incident ground level during the response to the incident. Therefore, they can serve as an asset for further design and implementation of the overall system-of-systems in SECUR-ED. However, since the focus of this deliverable is the concept of interoperability, only the roles participating in the use cases are extracted in the following:

- Hazardous material / chemical material responsible

  As an external responsibility, this role serves a consulting purpose if hazardous and/or chemical materials are involved in the incident. Advisory is provided regarding the potential threats, damage and awareness when resolving the incident.

- Control centre

  As a central asset, the control centre is responsible for coordination and incident resolving initiation. It serves as an intermediating tool between first responders, emergency services and callers.

- Incident commander

  The incident commander is involved in organizing the incident ground and decision-making regarding the whole area of the incident.

- Incident command board

  The incident command board is important during preparation in the pre-incident phase and communication with the media and/or public during the post-incident phase.

- Sector commander

  The sector commander, as a specialisation of the incident commander, is responsible for certain areas inside the incident ground, organising staff and actions while processing the decisions made by the incident commander to a more detailed level of operations.

- Operations commander

  This role is responsible for executing the decisions of the sector commander. The operations commander is directly involved in organizing their team and decision making at ground level.

- Command support officer

  The command support officer assists the operations commander.

- Senior police officer

  The senior police officer communicates with other teams and handles decision making processes, while operating at the incident ground.

- Command support radio operator

  The command support radio operator handles all communication done with the operations commander by the command support officer.

- Command support runner

  The command support runner is responsible for the on-site communication between the teams.

- Operations command radio operator

  The operations command radio operator handles all communication done with the sector commander by the operations commander.

- Operations command runner

  The operations command runner is responsible for the on-site communication between the sector commanders.

- Fire-fighter

  The fire-fighter executes the decisions handed over by the operations commander. Additionally, it is one of the roles recognizing changes and requirements at the incident ground.

- Senior medical officer

  The senior medical officer is part of an emergency service team.

- Regional emergency centre

  The regional emergency centre handles communication with the media, as well as treating wounded.

- Other emergency agencies

  See regional emergency centre

- Company key holder

In case other companies are involved, the company key holder grants access to the required rooms (i.e. in case of a fire).

- Caller

  The caller is one of the instances, initiating the incident resolving process.

- Electric

  Abstract role for the electric company. Handles power cut-off if needed.

- Water

  Abstract role for the water company. Handles water cut-off if needed.

- Gas

  Abstract role for the gas company. Handles gas cut-off if needed.

- Environmental protection agency

  If the incident involves chemical or hazardous materials, the environmental protection agency handles risk assessment and decontamination of the contaminated area.

- Nominal roll board

  As an asset used in organizing, preparing and executing incident response, the nominal roll board provides an overview on which first responding assets are at the incident ground site. Therefore it offers valuable resource planning capabilities.

- Visitor roll board

  Like the nominal roll board, the visitor roll board provides an overview on assets at the incident ground. But in this case the board gives an overview on all non first responding assets involved. Therefore it also offers valuable resource planning capabilities, since it provides information on potentially threatened persons, for example.

- Media

  The media is a generalized communication asset between first responders, emergency services and the public.

6.2.2 Sensor Systems

Reference Project(s) (ordered by priority)	DEMASST, COUNTERACT, COPE

Sensor systems become important when the retrieval of information from the systems' environment is required in order to react or support decisions. However, when implementing such sensing systems along with other applications, databases and users, the semantics of the information communicated along the system becomes important. With sensor systems, this means that the interpretation of the data is required. Sensing systems can provide data on general or explicit objects, such as general chemical agents or an improvised explosive device. This makes a more general view on sensor systems necessary. Therefore, when referring to sensor systems in this document, the unit of a sensor and its interpreting appliance is meant. By doing so, a view on sensor systems as information providing assets can be obtained, rather than dealing with raw data.

All of the projects define a various amount of sensor systems, whereby each project, depending on their scope, focuses on different levels of detail. COPE, for example, uses sensor systems as part of a decision support system at ground site (COPE 2009b). Although very specific sensors are being used, they are not further described. However different sensor systems are mentioned, also including non-technical systems.

In COUNTERACT a more detailed view on sensor systems is provided in (COUNTERACT 2009b). Since the main focus of this project is on terrorism, the systems focus more on behaviour and detection of hazardous or explosive material. DEMASST includes this also in its deliverables (DEMASST 2009a) and (DEMASST 2010), although the level of detail provided by this project is larger. Here we find various sensor systems along with their technological readiness level. All sensor systems found in the reference projects were generalized to their functions of either monitoring a certain area/status or detecting anomalies regarding objects and persons. The monitoring Section must be understood as a supportive data supplier, for example a Closed Circuit Television (CCTV) camera monitoring a hallway, without any further interpretation. Detection enhances the monitoring by interpretation and acting on the basis of the sensor data supply. Therefore, the ontology distinguishes between systems that provide data (Monitoring) and systems that deliver information on which basis an action can be performed (Detection). Such systems can include technical solutions, such as behaviour detectors along with CCTV, while the CCTV alone would be a monitoring sensor system (see Figure 5).

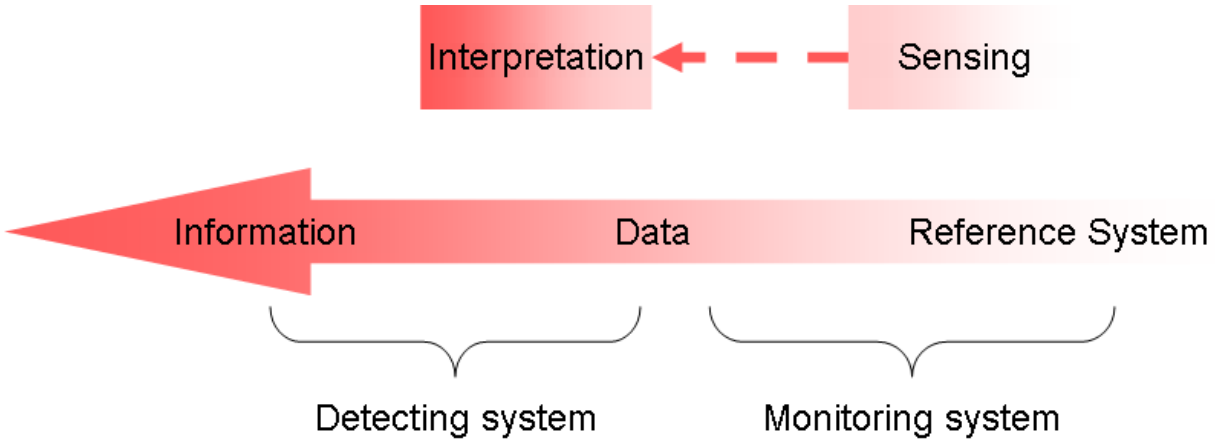

Figure 5 Definition of sensor systems

Using this, a further classification is possible. The “Detection” part can be split into the detection of objects (chemical, radioactive, biological or metal detection) and the detection of behaviour. Behaviour can include the detection of intrusion in certain areas as well as detecting suspicious behaviour of monitored people. This ontology provides a benefit regarding the identification of suitable sensor systems, while taking into account their adaptability and ease of integration into an overall interoperable system.

Figure 6 provides an overview on this ontology. When regarding the levels, detection and monitoring use-cases become the main nodes. This is due to the ontology emphasizing the usage of a sensor system, since it was assumed that sensor systems comply with one usage and if not, that all usages for this system can be aggregated (i.e. because they share some attributes). Here the distinction between detecting and monitoring systems, regarding their ability to either deliver data or information becomes visible. While the detection Section provides specific use cases that are aimed towards the detection of behaviour (suspicious

behaviour or intrusion) and objects, the monitoring Section does not contain any further use cases. In the latter, we find Closed Circuit Television (CCTV) Monitoring as an asset, which contains multiple attributes. These attributes show the different variations of CCTV Monitoring, which are applicable for various use cases (i.e. thermal / infrared cameras can be used to monitor areas during night operations).

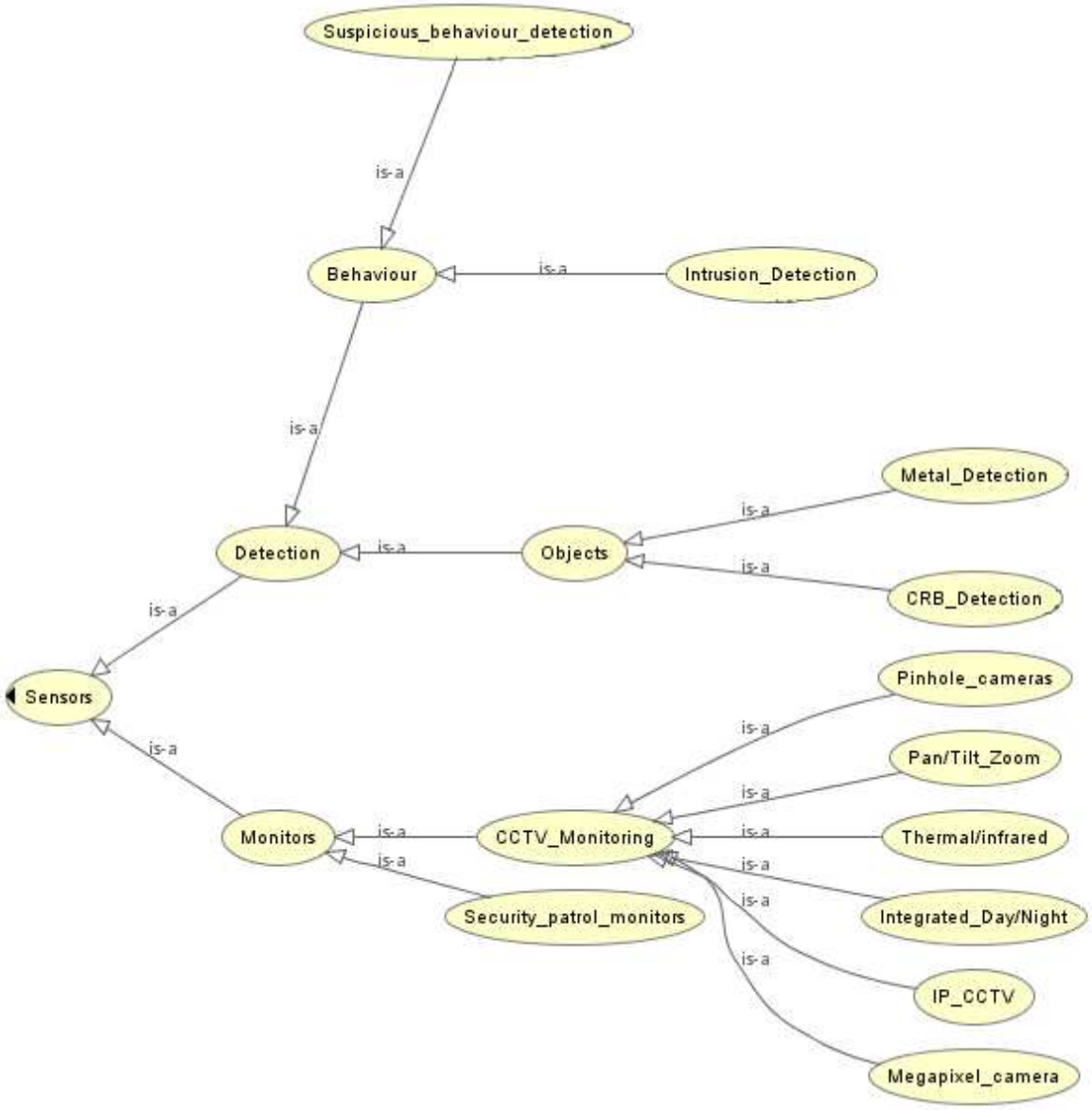

Figure 6 Overview on top level categories and attributes

The systems researched in the area of detection focus mainly on the detection of behaviour and objects. Figure 7 shows the two involved use cases in detecting behaviour. The intrusion detection mainly lists assets found in (COUNTERACT 2009b), while assets for the use of suspicious behaviour detection are mainly from (DEMASST 2009a). We can find various attributes for the solutions, such as detection by line-crossing detection, detection of tailgating or of left behind, removed or placed objects. When coming to the general detection of objects, systems listed in (DEMASST 2009a) are mainly able to detect objects by their direction, pace or speed.

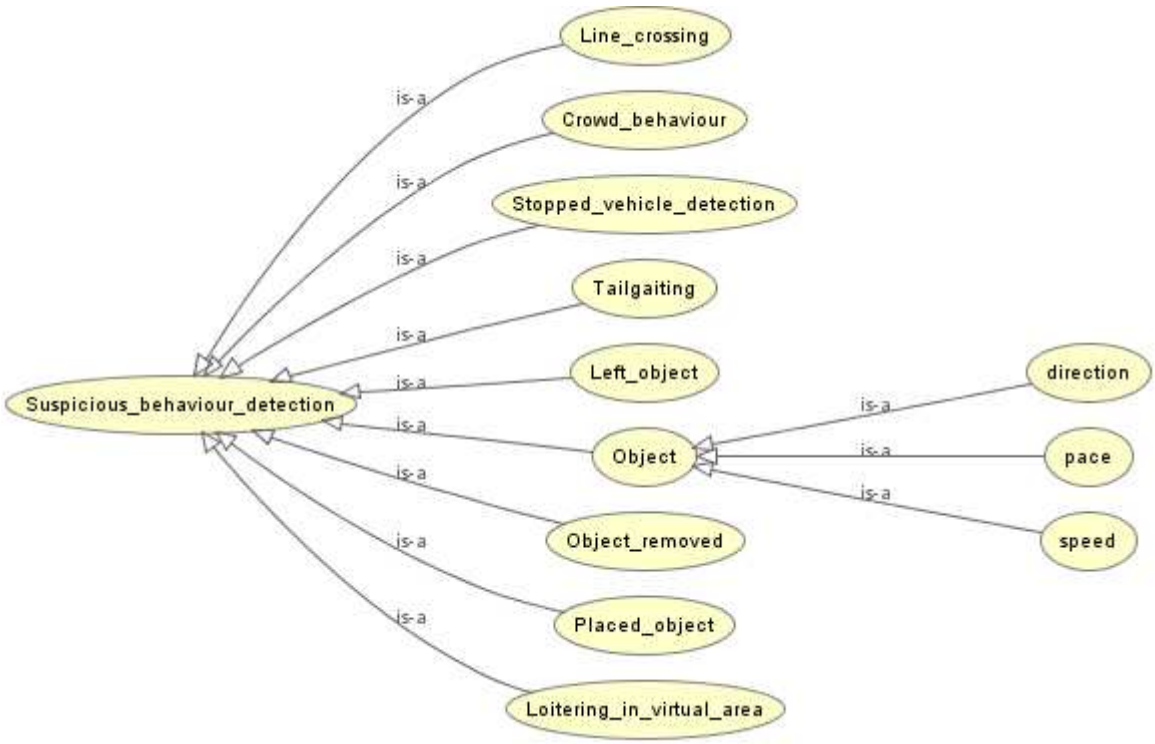

Figure 7 Elements of detecting suspicious behaviour

This specialization makes sense, since it allows systems to be correlated with one or more attributes of behaviour detection. Additionally, an overview is provided on what the listed technologies in (DEMASST 2009a) are able to process. (COUNTERACT 2009b) gave an overview of various sensors for intrustion detection, such as photo electric beams or radar sensors. Many sensor systems listed here share the same technological basis. For instance, active and passive infrared sensors both use infrared wavelengths for sensing. Since this aggregation can be made, according to the technical structure of the Sensor System and the in-depth analysis of the systems is beyond the scope of this deliverable, no further specialization was made, except for the dual technology sensors. This object may generalize every sensor system, containing of two different sensor types (see Figure 8).

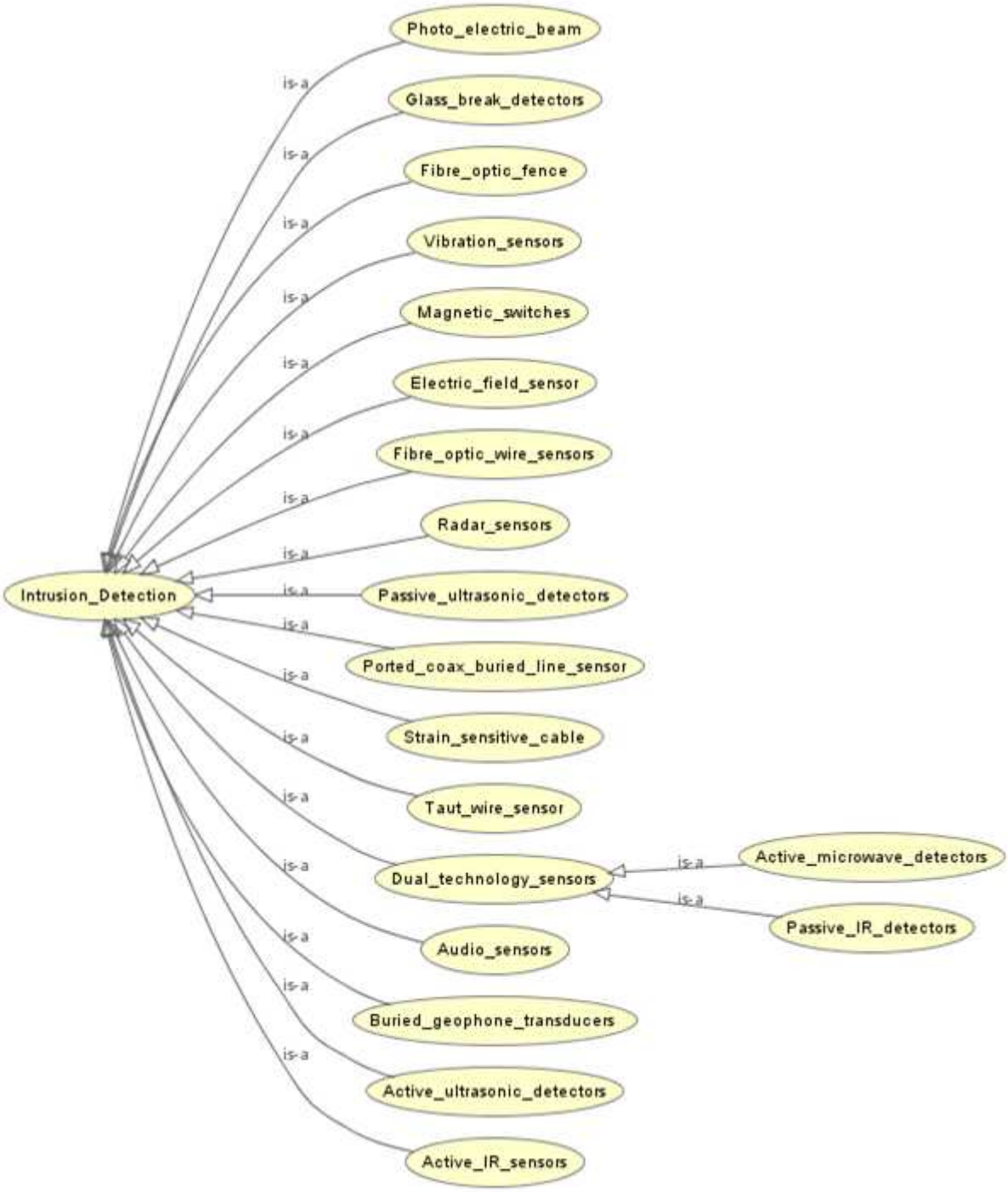

Figure 8 Elements of intrusion detection

The third use case in the detection Section is the detection of objects (see Figure 9). This is split up into the detection of metal and the detection of chemical, radioactive and biological agents, taken from both (DEMASST 2009a) and (COUNTERACT 2009b). The roadmap for improvised explosive devices as described in (DEMASST 2010) are not included, since this ontology was mainly aiming at providing an overview on the technologies presented in the reference projects. This roadmap was used in combination with the ontology resulting in the building block description in Section 8.1.3. Regarding the detection of chemical, radioactive and biological agents, special methods such as the x-ray diffraction measurement (XRD-X-Ray) are included. Detection of Chemical agents presents various technologies for detecting

explosive devices (DEMASST 2009a). Since there are no other chemical agents referred to in neither (DEMASST 2009a) or (COUNTERACT 2009b), there are no other methods included here. For Section 8.1.3, only the use cases up to the second specialization are used in the building blocks.

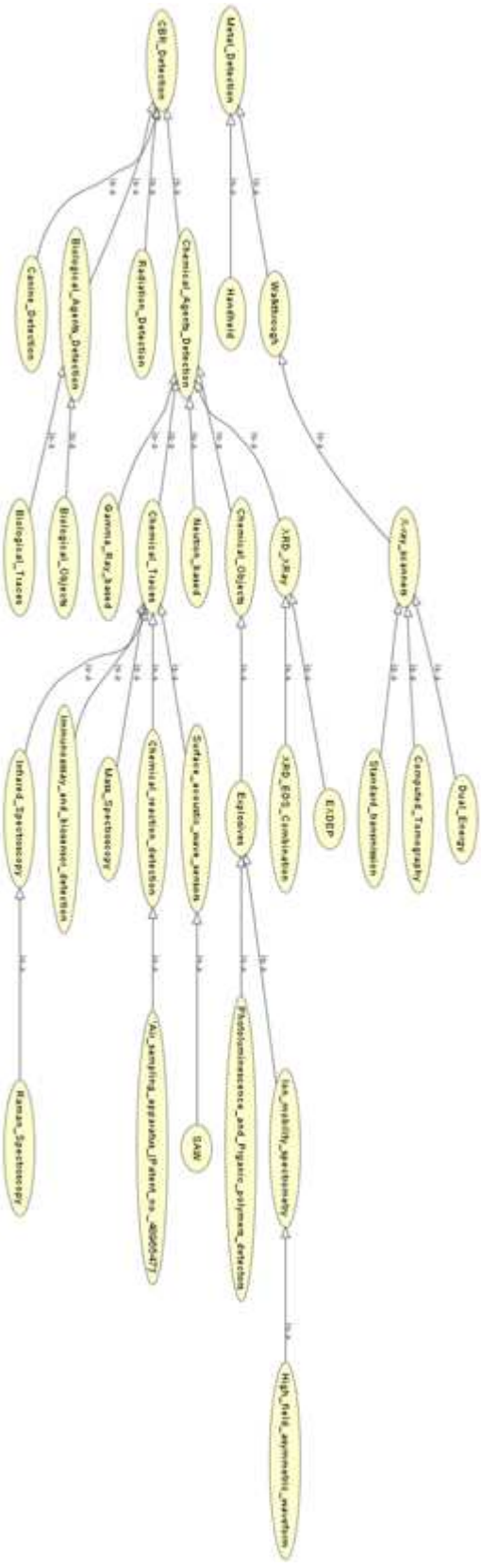

Figure 9 Elements of object detection

6.2.3 Concept of Operation

Reference Project(s)	COUNTERACT

According to (COPE 2008), maintaining common ground during operation and planning phases along the emergency lifecycle is a core process when responding on ground level. Therefore, the concept of operation (CONOP) describes basic information required for collaboration (COUNTERACT 2009a). Such concepts offer the opportunity to derive metadata for the required interfaces of the system. The concepts are described on an operational and high level, offering metadata for both ground-site communication and inter-organisational communication.

When regarding more generic information in emergency response and security organisations, the high level concept still offers capabilities for implying and therefore accessing the information with more detail, while not over-defining the information container itself. This makes the concept on this level very interesting for later interface implementations and design. The high level concepts include the following assets:

- Organisational structure

  Description of the organisations' structure for which this concept was defined. This may include the organisations hierarchy, its processes, its communication structure, and its institutions. For example information could be gathered on whether this organisation provides a quality management system or whether the persons communicating with this organisation can communicate with each other.

- Legal basis

  The organisations' rights and laws applying to the organisation and the situation. For example an emergency service has extra rights in public traffic during emergency response operations. This information container would contain which rights apply to this organisation, on which basis it can operate and what it cannot do.

- Security operating methods

  Security operations in general, security operations under elevated threat conditions, available safeguards and equipment. The security operations include used interfaces, a description of the management, the means and the methods involved. The security operations under elevated threat conditions include ad-hoc safeguards, the standard level of security, rules of engagement and the threat levels defined.

- Auditing

  Describes who is responsible for reviewing and assessing this concept, as well as the processes involved in auditing.

- Professional terms

  Include the definition of terms regarding the security systems, security procedures, position holders, past assessments and risk management results, security means and field level security plans. Therefore this asset includes the definition of all assets somehow correlated with the security organisation.

- Risk reduction measures

  Actions taken as response to risk assessment results.

- Interfaces

  Existing interfaces in this organisation.
- Security procedures

  Description of existing security procedures.
- Field level security plans

  Description of existing field level security plans.
- Security typology

  Assessment of the organisation as a system. Includes the level of security and the organisation type regarded as being an open system or controlled system.
- Maintenance of CONOP

  Describes which persons are responsible for updating the concept of operation.
- Systems, assets & components

  Description of systems, assets & components existing and available in the organisation.
- Risk management policies

  Restrictions and rules from risk assessment.
- Communication strategy

  Strategy for communicating with the public.
- Threat definitions

  Basic definition of threat levels.
- Security training and exercises

  Definition of training procedures and cycles.

Regarding the ground level, the operational concepts of operations define basic routines and actions taken at the incident ground. They aim more at the collaboration of teams and personnel at ground site rather than collaboration between different organisations. These operational concepts include:

- Activity objectives

  A general definition of objectives, which have to be elaborated. They include objectives on deterrence, detection, incident response and prevention.
- Tasks under routine conditions

  Includes routine operations, list of security procedures, a communication diagram, a list of security exercises, immediate actions taken during emergencies, a list of security monitoring appliances and the security training implementations. The tasks also include the logistical support of incident ground teams. Routine operations refer to the security handling of people, preventive measures, supervision and control, information security, security observations, security searches, communication & reporting and deterrence and security deception.
- Rules of engagement

  The rules of engagement describe what incident ground teams should aim at, what is allowed and what should be avoided during incident resolving.

- Organisational structure

  This is the structure of the organisation to which this concept applies. In this case, the structure would probably describe a certain operating unit at ground level, its internal hierarchy and its internal communication means. For example, how a fire-fighter communicates with his commander.

- Legal basis

  The legal basis for operations performed. What can this particular unit do at ground site ? Are there any extra rights ? What mustn't this unit do ?

- Professional terms

  Same as in the high level concept, but describing the understanding of terms for the specific unit.

This concept played an important role in defining metadata for the interfaces and / or mediators in the interoperability concept.

6.2.4 Field Level Security Plans

Reference Project(s)	COUNTERACT

Apart from the more general concepts of operations, field level security plans, as described in (COUNTERACT 2009a) focus more on objected assets, such as passenger stations, depots or operations control centres rather than the executing organisation. Therefore the focus is more on the objected assets and their role during incident response, prevention and deterrence. Consequently, a field level security plan, as presented in COUNTERACT, includes:

- Description of the facility and its surroundings

  A geographical and semantic description of the facility itself and the facility's environment. Includes which systems are found in and around the facility.

- Operational and commercial functions

  The role of this facility. For example an emergency in a relay station will have a larger impact on the connected households than a burning house.

- The facility's level of security

  Are there any special security plans already existing? How is the threat level for this particular facility?

- Analysis of the critical infrastructure in the facility

  Is there any critical infrastructure existing in the facility? For example a gas pipe inside a burning house can lead to extensive damage during the emergency. Units must be aware of risks correlated with this infrastructure.

- Threats and tactics analysis

  Which threat levels apply? Which particular threats are correlated with this facility? How can first response units respond to these threats?

- Routine security plans

  Which operations apply to daily work? For example, monitoring of the facilities' environment.

- Immediate actions in emergencies

  Which operations are taken when an emergency occurs?

The field level security plans can be categorized in being specific or generic. The generic field level security plans include types of facilities but no specific facilities. For example, a generic field level security plan would refer to the actions taken in case of an (unknown) emergency at a power plant, but not in case of a specific emergency at a specific power plant.

The routine security plans describe operations carried out under routine conditions. This includes activities regarding deterrence, access control, security searches & patrols, security handling of persons, baggage and vehicles, actions to increase public awareness and information security.

Immediate actions in emergencies refer to actions such as crowd management, immediate response, self defence and the cooperation with first responders.

Along with the concepts of operations, the field level security plans are combined to metadata in Sections 8.1.1 and 8.1.2, since both define information needed for preparedness and response to emergencies and incidents.

6.2.5 Interfaces with Other Organisations

Reference Project(s)	COUNTERACT

COUNTERACT defines in (COUNTERACT 2009a) interfaces by requirements. All communication with external organisations is first generalized to include assets like general and case specific policies, high level decisions, secure access and basic documentation. Documentation hereby refers to the documentation of

- Interfaces

  Which interfaces exist and which protocols are used for communication?

- Supporting processes

  Which processes deliver information for this particular interface ? Which processes pull information from this interface and which processes are pushed by the information delivered by this interface?

- Arrangements

  Arrangements regarding the interchange of information between the two organisations. Are there any obligations created along with the exchange of information ?

- Organisational Power

  Power and impact of the organisation holding this interface, as well as of the external organisation.

- Individual Power

  Power and impact, or more general the hierarchical position, of the persons or systems involved in the interchange by this interface.

- Roles

  Roles participating in the interchange (i.e. firemen and police office)
- Responsibilities

  Responsibilities involved in the interchange (i.e. information security due to person based information exchange)
- Management of Interfaces

  Responsible persons for managing the interface. This can include supervision, auditing and administration.

This generalization is further used for specializing interface requirements of other organisations. In case of security agencies, which include ministries, national security agencies and intelligence agencies, the requirements refer additionally to the office / facility Section level, whether an individual or a whole office or facility communicates by using this interface, if a continuous contact is required and which level of security clearance needs to be considered.

The information security becomes very important in this case, therefore additional meta-information describing information needed, the timescale in which the information is needed and the communication equipment is included. However, the emergency services focus of the requirements is put more on the communication and interoperability. Therefore, the compatibility of technical equipment and the security incident response arrangements play an important role. Additionally, coordination responsibilities, relationships between the organisations and the support of specialist security responders must be considered.

As a research project focusing on response to terrorist actions in public transportations requirements for communicating with other transport organisations are additionally defined. Hereby the number of infrastructure managers and the rail / road usage by multiple public transport organisations is considered. As in the field level security plans, information on operational requirements and on the objected / protected assets is emphasized. Therefore additional information on geography, topography and the population distribution is required. This complies with the requirements for security management systems as found in (COUNTERACT 2009b). Here GIS (Geographical Information System) data, representing the facility and its environment, is an important part of the data displayed, enabling planning, response and awareness capabilities depending on the environment regarded. In order to be able to coordinate the information flows in case of the public transport organisations, the communication and the media must be considered as well. Finally, the security and incident response routines become an important part of this interface. Regarding the communication with the media or the public, the coordination of information, the responsible Role for authorizing the publishing of this information and the responsible Role for publishing itself must be identified. The main goal of the interface dealing with the communication with passengers is establishing confidence, achieving a secure operation and applying additional security controls. When creating an interface for the communication with passengers, these three requirements should be met.

6.2.6 Current Situation in Mass Transport Security

Reference Project(s)	DEMASST

As a project creating the prerequisites for SECUR-ED, DEMASST provides information on the current situation (DEMASST 2009b). Analysis of the current situation regarding security in public mass transport is crucial, when coming to the identification of currently used technologies along with their use cases.

According to this analysis, delinquency was identified as the most likely threat, followed by vandalism and terrorism. Regarding the vulnerabilities along these threats, external interfaces are necessary which pay respect to the vulnerabilities of information and communication infrastructures. Interfaces with external organisations, in the following referred to as external interfaces, are just partially found, while internal interfaces generally exist. Those interfaces, which are already implemented, do already comply with an available interface standard.

Additionally along this survey, the absence of external interfaces in the following procedures was identified:

- Analysis of vulnerabilities
- Detection, Tracking, Tracing of abnormal behaviour
- Other recognition technologies
- Detection & Identification of unwanted entities close to critical infrastructure
- Monitoring of entry points
- Unattended luggage detection
- Surveillance

7 The SECUR-ED Interoperability Concept

This Chapter describes the general interoperability concept of SECUR-ED. Interoperability in the sense of this concept is the ability to interact in a meaningful way. It is intended to provide a common starting point for the work in all SPs.

This shared picture should avoid misunderstandings in the communication between the partners and activities of SECUR-ED. It is intended to be used for the specification in the different WPs for the capacities and the demonstration activities. The experiences during the project will be gathered and used to improve this initial concept towards a final approach of a system-of-systems architecture.

The interoperability concept is one of the foundational components of the SECUR-ED vision, along with the organisational and operational procedures that will be defined in WP 21. There, among others, the roles will be further detailed, and definitions presented for scenarios, threats and other relevant objects that are related to the interoperability concept presented here. A notation for this interoperability concept will be provided in D22.2.

7.1 Context and Content of Interoperability

The general interoperability concept needs to be adapted and further refined for the relevant environment, which consists of Context and Content for each capacity and demonstration city. In this Section the general properties of Context and Content are described.

7.1.1 Context for Interoperability

Within SECUR-ED, the interoperability concept focuses on collaboration between roles. Among others, the following distinctions are relevant to understand the Context of the collaboration:

- Is the collaboration within one or between several departments or organisations? (see 8.2.2)
- Is the collaboration vertical (on the same level of hierarchy) or horizontal (different levels of hierarchy)? (see 8.2.2)
- Is the collaboration within one kind of actors or across different kind of actors (e.g. transport operators and first responders)? (see 8.2.2)
- Is the collaboration relevant in critical situations only or also for daily routine operations (e.g. with respect to crisis management phases)? (see 8.1.1 / 8.1.2)

The collaboration has a purpose or intention. For SECUR-ED, to react with several organisations consistently in case of a security challenge (threat) could be a relevant example. Therefore the risk and vulnerability that are addressed as well as the current threat that should be solved need to be stated. Moreover, the phase within the crisis management cycle (Ritchie 2004) is relevant (prepare, prevent, react, recover). In addition, it may be helpful to mention the related business processes and procedures of the involved roles, e.g. for monitoring, alarming or commanding.

In general, the Context for SECUR-ED is also influenced by the nature of public urban mass transport operation, which is characterised by many access points, frequent stops, large geographical areas, and in large cities daily millions of passengers (UITP 2010). It is also often

characterised by the multi-modality with a large fleet of vehicles of different type (bus, tramway, metro, train) (UITP 2010).

The Context itself is not a building block within our interoperability concept, but part of the meta-information of such building blocks or the scenario as a whole. This Context of the collaboration will be further elaborated in Task 22.4 “Interoperability Semantics”.

7.1.2 Content to be exchanged

The interoperability levels explained in Section 5.1 draw a picture of interoperability as a matter of content (Turnitsa 2005). Interoperability becomes more sophisticated as semantics and syntactic of the data exchanged rises. Therefore, Content can be distinguished on the following levels:

- Data, e.g. numbers and codes send by a sensor
- Information, e.g. numbers in a specific syntax, describing each number as being a temperature
- Knowledge, e.g. the interpretation of that temperature as being critical.

The stage of the Content exchanged has many implications for the details of the interoperability, giving hints on what the systems involved are capable of (i.e. a system capable of interpreting a temperature and trigger a certain action is more sophisticated than a system that is simply able to receive and display structured data). This also implies the documentation needed, e.g. exchange methods, schemas or ontologies, in order to assure the exchange of the Content on one of the levels described. The exchange of Content may happen in critical situations only (which then have to be declared somehow) or permanently, covering all crisis phases (e.g. prepare, prevent, react, recover). The exchange of Content is probably related to defined processes, procedures or activities of the involved roles. Referring to the level of knowledge, and thus representing the level of semantic interoperability in (Turnitsa 2005), Content may become a by-product of processes correlated with the interoperable system. In such processes the interpretation of information may depend on the predecessor’s actions. We therefore recommend, when referring to the Content itself, to model its flow using directed graphs. This ensures that the Context of the information, embedded in the process or its involved roles, is being preserved. An undirected modelling of Content flows may lead to misunderstanding or misinterpretation, since it may not be possible to capture the Context attached to the process.

The Content itself is not an object, but describes the usage of the objects with more clear examples. The Content to be exchanged will be further elaborated in Task 22.4 and Task 22.3 covering the semantics and syntactic of interoperability.

7.2 Definition of Interoperability Objects

The interoperability concept is focussed on the interoperability of Information Systems. These Information Systems are related to organisational Roles. Information Systems also have Interfaces that allow the connection to other Information Systems. These Interfaces are almost never directly connected, but use intermediaries. Intermediaries are a specific kind of an Information System. Therefore, the relevant objects of the interoperability concept are:

- Information System
- Role

- Interface
- Intermediary

The relevant relations between these objects are:

- Role and Information System
- Information System and Interface
- Interface and Intermediary

An overview of the objects and relations is given in the following Figure 10.

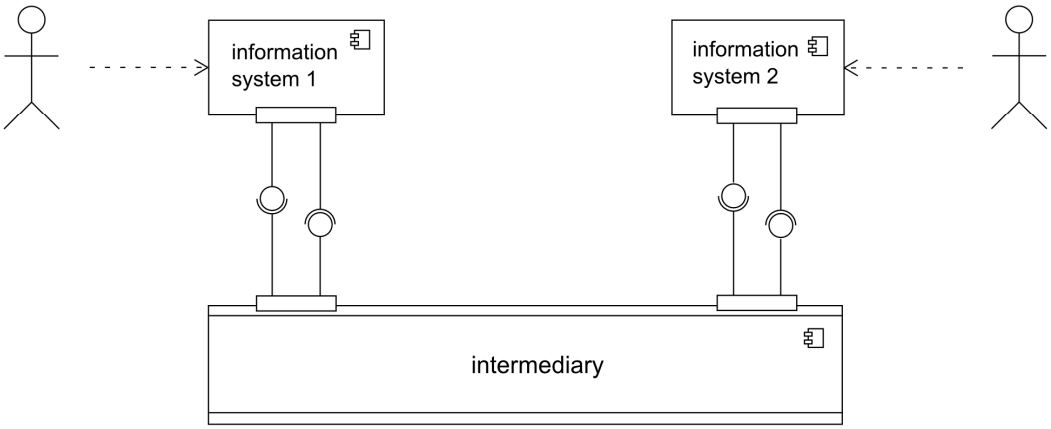

Figure 10 Interoperability objects and their possible relations

For each of these relations, multiple instances of the relation are possible in both directions. For example, each Role can be connected to many Information Systems, and to each Information System many Roles can be connected. Not all relations need to exist, e.g. there might be Information Systems without any Interface (except a GUI), or Roles without Information System.

Deliverable 22.2 will provide a notation to describe the objects and their relations.

7.2.1 Information System

An Information System in the sense of this concept can be discussed at different levels of granularity, for example:

- A single sensor
- A network of identical sensors
- A network of different sensor types
- An IT System
- A network of IT Systems
- An Organisation

This is a relevant approach towards the system-of-systems-architecture, since it allows the properties of such systems to be considered on different levels of granularity. Figure 11 presents the possibility to include the sub systems included in an Information System, hence offering detailed modelling capabilities on every level of detail regarded. However, this aggregation is further described during deliverable D22.2 along with the Interoperability Notation.

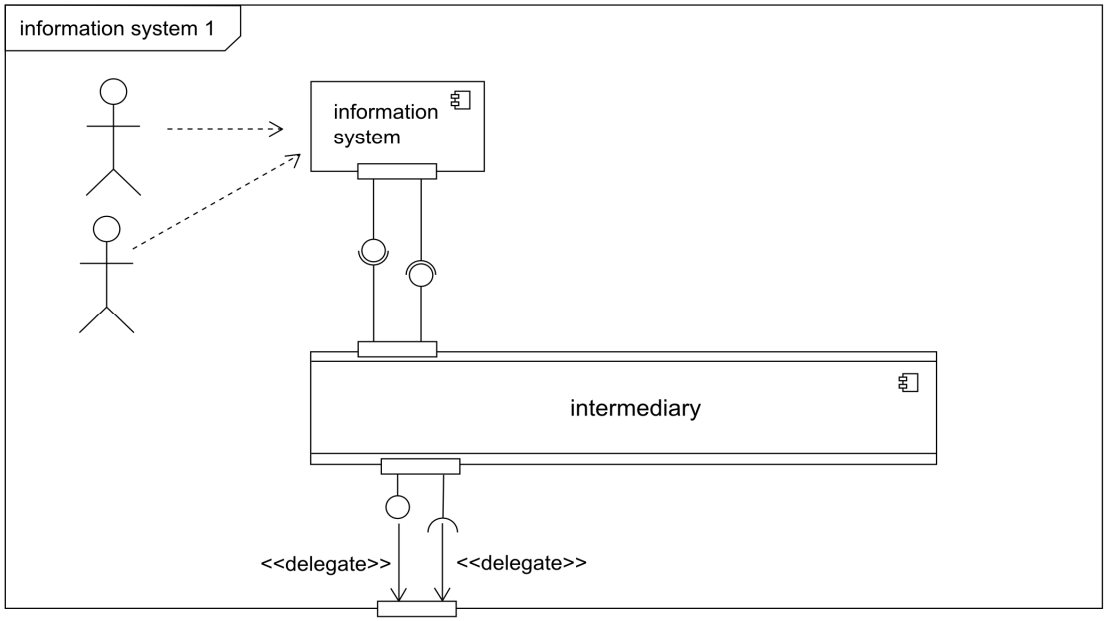

Figure 11 Information System 1 consists out of other building blocks including two Roles.

7.2.2 Role

Each Information System can have relations to several Roles. Most SECUR-ED cities are characterised by multi-operator-settings with shared responsibilities, but with different company cultures and business targets.

Regarding the usage of information, there can be relations between the Roles, and it is possible to describe Roles on different abstraction levels, e.g. for complete organisations and event groups of organisations (such as the transport operators) or for the responsibility for distinct tasks within each organisation, as required by the metadata described in Section 8.2.1. The Roles will be further elaborated in WP 21.

The overall approach of SECUR-ED is based on the understanding that qualified, trained and motivated staff is needed to solve security challenges, and Information Systems can just support their activities. The details for these preparation aspects are elaborated in WP21.

7.2.3 Interface

Each Information System can have several Interfaces that allow interaction with other Information Systems. In this interoperability concept, the object Interface does not describe the user interface but is only intended to describe Interfaces between Information Systems. Due to the possibility to model systems of different granularities, by using the Information System object, a generic description of Interfaces cannot be given. However, Interfaces on an organisational level are described in Section 8.2.2.

The syntax of such Interfaces will be further elaborated in D 22.3 Syntax.

7.2.4 Intermediary

A specific instance of Information Systems is the Intermediary. It is an Information System itself that serves the sole purpose to support the interaction between other Information Systems.

Intermediaries can be seen on different levels, for example:

- Network infrastructures (cable, wireless)
- Enterprise Service Bus
- Adapters

The existence and the design of the Intermediary have a strong influence on the overall interoperability approach in a dedicated city and for the specification of their Interfaces. Especially the Enterprise Service Bus, which is a communication platform that offers several services, may handle challenges such as access rights and identity management, harmonisation of time stamps, location information and reference data, data aggregation, fusion and processing. This pins down the overall task for this specific Information System to ensuring semantic and syntactic compliance in communication of two Information Systems. For this reason, this kind of an Information System is modelled separately within the SECUR-ED interoperability concept.

Furthermore, its sole purpose of ensuring communication between two Information Systems does not necessarily imply the correlation with a special Role. Therefore, this object is not attached to a special Role and does not offer any information presentation and general management tasks regarding a certain user, nor respecting any end-user requirements. It is only dedicated to ensure semantics and syntactic communication between two Information Systems. Hence an Intermediary offers Interfaces, for communicating with the Information Systems involved.

The details for the Intermediaries in the demo cities will be defined in SP4, and probably for specific capacities also in SP3.

8 Building Blocks for Interoperability Objects

Along with the defined interoperability objects, the outcome of the examined research projects can be used to further specify the interoperability objects. The following Sections describe building blocks to define the contents of the interoperability objects. Those blocks have been derived from the research projects described in Section 6.2 by combination of their outcomes and further interpretation. Therefore, they provide modelling opportunities for use cases contained in the reference projects. The building blocks are hereby aggregated and interpreted, in order to suit the specific requirements of the SECUR-ED interoperability concept, as stated in Section 4.3. They are listed in the following in the order of the correlated interoperability object.

8.1 Information Systems Building Blocks

Regarding the information transmitted through the Interfaces, metadata comes into play for describing and correlating the information gathered. While following the information through an interoperable system-of-systems architecture, semantics becomes especially important in order to understand or trace information. To describe every organisation, the following Sections 8.1.1 and 8.1.2 give an overview of necessary metadata. The information contained inside the metadata can serve as a container. Examples are provided for each attribute for a better understanding. Section 8.1.3 defines an aggregation for further classification of sensor systems. In this concept, sensor systems are regarded as a specialization of Information Systems. Figure 12 shows this special relationship of sensor systems and Information Systems apart from the other Interoperability objects.

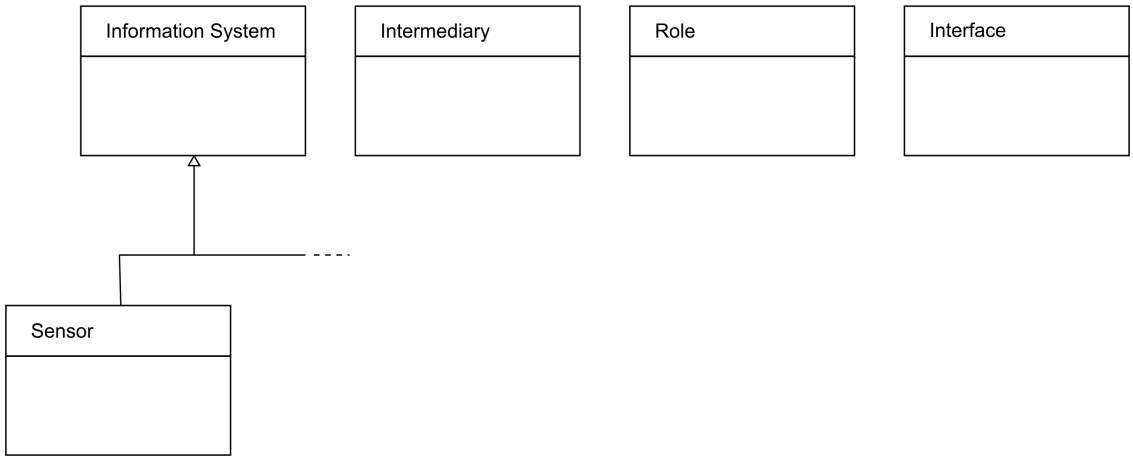

Figure 12 Relation of Sensor Systems and Interoperability Objects

In the context of interoperability in public mass transport security, sensor systems are a key entity for the overall concept, since they are the only systems able to provide information about the situation. Especially in situation-aware and incident-resolving phases of the emergency lifecycle as in (Ritchie 2004), such systems must be considered very important. Therefore the building blocks respect both the metadata required on an organisational level of detail and sensor systems, although both are not on the same level of detail from a technical point of view.

8.1.1 High Level / Metadata Describing the Organisation as a Unit

Outcome of reference project(s)	COUNTERACT
Correlated interoperability object	Information System, Roles

Due to the possibility to model systems of different granularities, using the Information System object, this metadata describes possible information containers for organisations involved in security and first responding services. The metadata was hereby derived using the Concept of Operation and Field Level Security Plans as presented during Sections 6.2.3 and 6.2.4.

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?
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 & 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

8.1.2 Operational / Metadata Describing Operational Units

Outcome of reference project(s)	COUNTERACT
Correlated interoperability object	Information System, Roles

Although 8.1.1 already provides an overview on the information requirements of organisations involved in the system, for the reaction to an incident at ground level the information required differs in detail. Therefore, Table 1 provides an insight in possible information correlated with incident ground teams. This distinction in generic metadata (organisational) and operational metadata complies with the distinction of the Concepts of Operations and Field Level Security Plans, as in (COUNTERACT 2009a). From the operational point of view the metadata can be listed as the following:

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 & 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

8.1.3 Sensor Usage and Type Aggregation

Outcome of reference project(s)	COPE, COUNTERACT, DEMASST
Correlated interoperability object	Information System

Using the reference projects and the sensor ontology as a result of the research projects outcome, 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” (Norros et. al. 2009) and the “specifity 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.

Towards a sensor systems ontology, a correlation between the depth of the sensor system inside the ontology and its specifity along with possibly required training can be assumed. Furthermore by respecting the IED roadmap given in (DEMASST 2010), an ontology aggregation was created (see Figure 13).

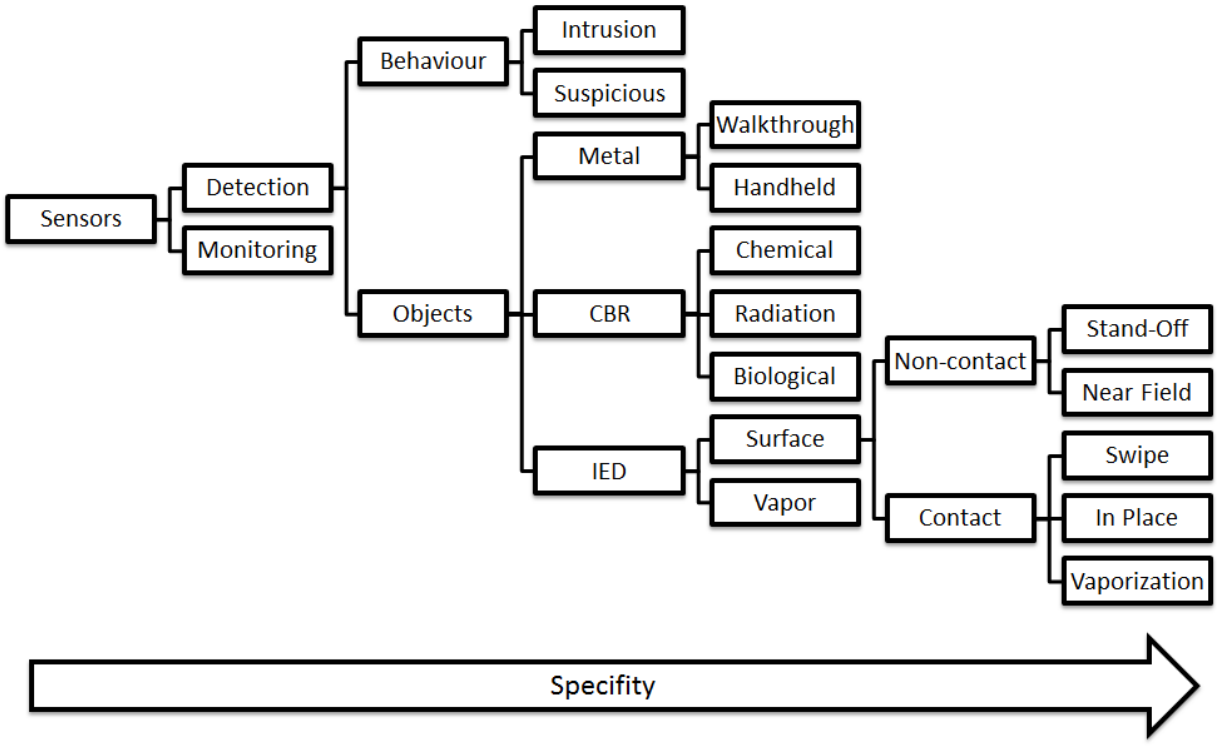

Figure 13 Sensor ontology aggregation

By using this aggregation, the classification of sensor systems can be done and correlated with the metadata of a sensor system. The ontology 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, when using the second level of the original sensor system ontology, an approach for evaluating sensor systems can be done. In the second level various generic use cases can be derived. 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 hereby include:

- Area Monitoring

  Security Monitoring of a limited area: no detection capabilities are included. For example, a simple CCTV sensor system would provide this basic functionality. Only when used in combination with a human or a special IT-system, this sensor would provide detection capabilities. This complies with the definition of detection and monitoring, given in 6.2.2, where monitoring is only the simple transfer of data.
- Chemicals Detection

  Is the system capable of detecting generic chemical agents?
- Biological Materials Detection

  Is the system capable of detecting generic biological materials?
- Radiation Detection

  Can the system detect radiation?
- IED Detection

  Is the system specialized to detect improvised explosive devices? The assumption made in this dimension is similar to the definition of monitoring and detection. Hereby a system must be explicitly able to detect an improvised explosive device not just anomalies or chemical agents.
- Metal Detection

  Is the system able to detect metals of any kind? For example, X-Ray scanners are included here.
- Intrusion Detection

  Can the system detect intrusion in a limited area? For example, a CCTV monitoring system along with a specialized IT-system.
- Suspicious Behaviour Detection

  Can the system detect suspicious behaviour in a limited area?

In order to respect the requirements captured in (COPE 2009b), those dimensions are assessed using the following attributes:

- No support

  The system does not support this use case at all.
- Usable with adjustments

  With special changes to the system, the support of this use case is given. For example, CCTV Monitors can be used for detection, when combining with a specialized IT-system.

- Usable with special training

  If the CCTV monitoring systems are not combined with an IT-system, but with a human operator, special training for using this system becomes necessary.

- Fully usable

  The system is out-of-the-box usable for this purpose.

8.2 Role, Interface and Intermediary Building Blocks

Regarding the Role, Interface and Intermediary objects, defined in Section 7.2, building blocks have been identified for each category. The following describes these building blocks, starting with the Roles aggregated from the use cases of (COPE 2009a).

8.2.1 Role Descriptions

Outcome of reference project(s)	COPE COUNTERACT
Correlated interoperability object	Role

During the COPE project a picture was drawn on the roles involved in incident resolving at ground level. By analysing these roles, potential for further aggregation was identified. This aggregation sums up the roles involved at the incident ground. Additionally by respecting the interfaces given during COUNTERACT, a first overview on all necessary roles can be given.

These roles can be substituted in Incident Ground Teams and External Organisations, whereas organisations are regarded as i.e. companies, when regarding an incident from the incident ground levels point of view. One might argue that the response to an incident does not cover all actions during the post incident phase. However, by including the generalized role of external organisations it becomes possible to model all involved parties with this role aggregation. The following Figure 14 shows the aggregation of the incident ground teams, which include all operating parts involved in resolving an incident.

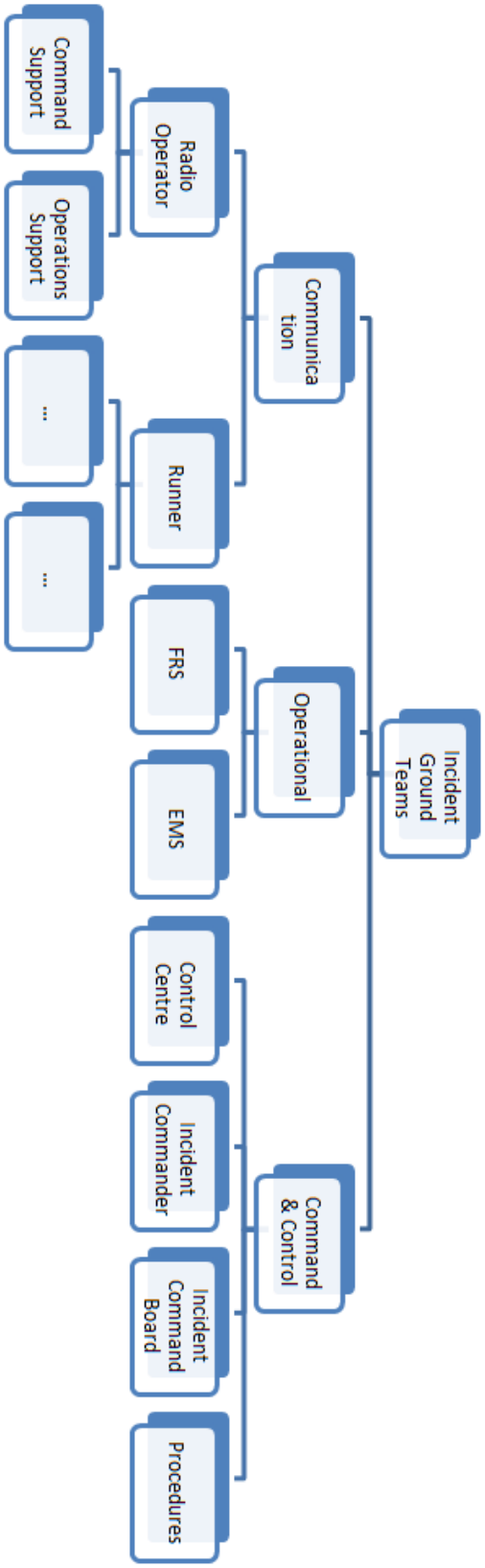

Figure 14 Aggregation of incident ground team roles

For external organisations, there are 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 15).

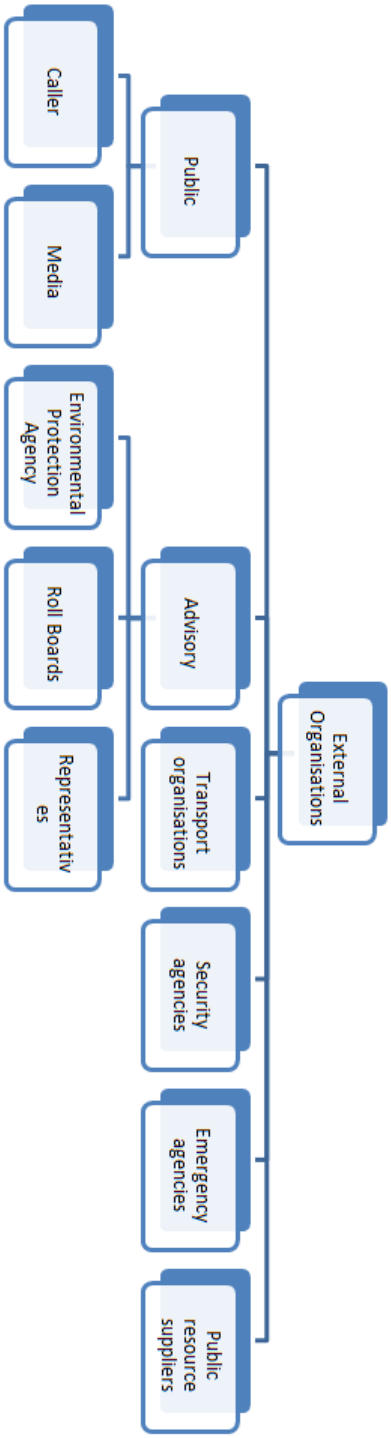

Figure 15 Aggregation of external organisation roles

8.2.2 Interface Descriptions

Outcome of reference project(s)	COUNTERACT
Correlated interoperability object	Interface

By defining basic requirements for interfaces with external organisations, COUNTERACT gives initial information on the information needs. By combining these requirements with the

Concepts of Operation, also given in COUNTERACT, the following interfaces were defined (see Figure 16).

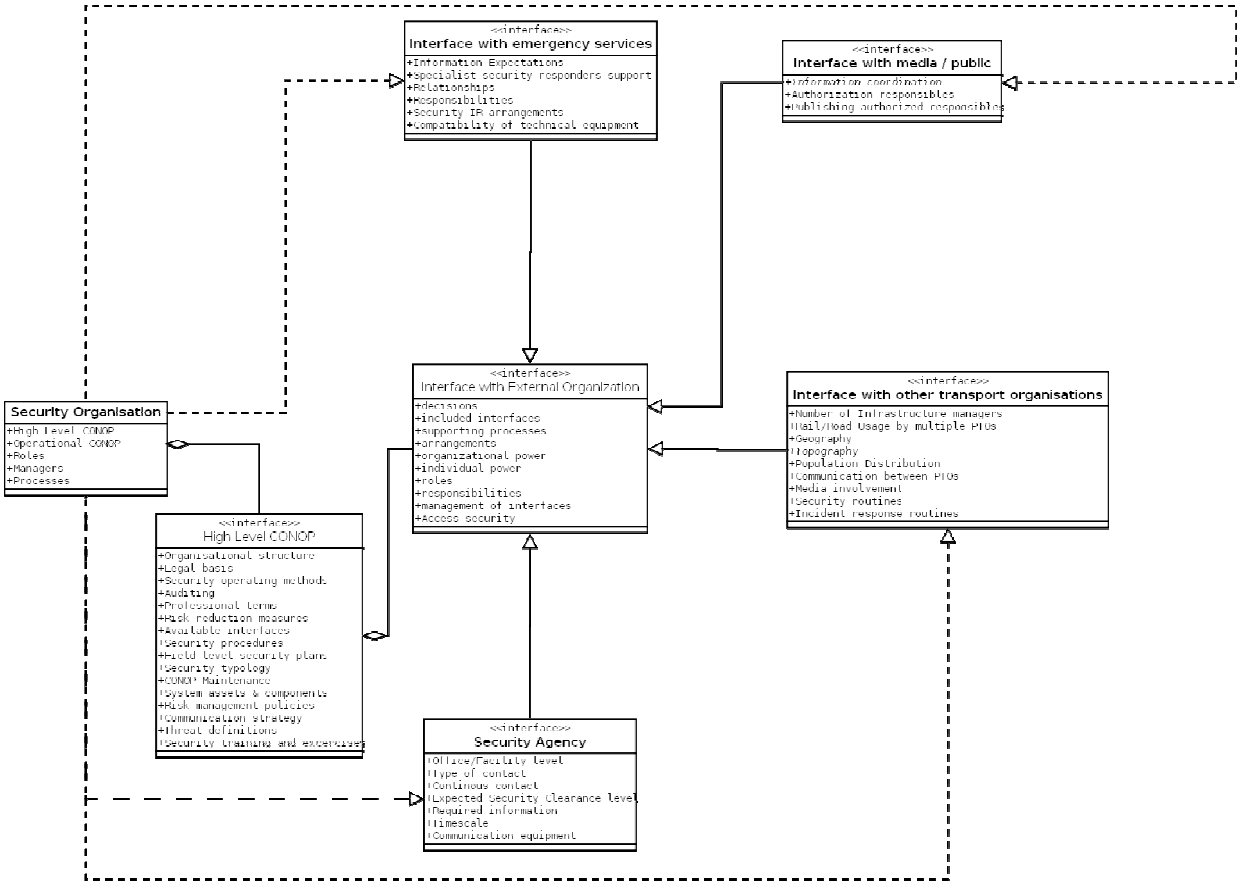

Figure 16 Interorganisational Interfaces

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. However, by including the Concept of Operation, which also serves as basis the for the high level metadata in Table 1,and by reviewing the contents included, a correlation of these contents with the requirements made by the interfaces became observable. This led to the interface overview, as seen in Figure 16. The following describes a generic interface as derived from this overview. The list can be used for later XML implementations.

- Organisation

  Basic description of the organisation and methods for accessing the information needed (i.e. dictionary for intermediating services).

  - Structure

    Is the organisation distributed? Is the management centralized? How much managers of which kind exist?

  - Legal basis

    On which legal basis is this organisation operating?

  - Security operating methods

    Which methods are used to maintain security in this organisation? Implies the level of trust for this organisation.

- Auditing

  Are the processes audited? When was the last audit? What was optimized? Implies a level of trust.

- Professional terms / Security typology

  Professional terms for communication with this organisation. Intermediating assets can use this information to translate incoming information into the right format for this organisation.

- Risk reduction measures / Risk management policies

  Are measures for risk reduction implemented? If yes, which risks do they apply to? Implies a level of trust.

- Available interfaces / protocols

  Which other interfaces and protocols are offered by this organisation?

- Security procedures

  Which security procedures are available in this organisation?

- Field level security plans

  Which field level security plans are available?

- CONOP Maintenance

  Who is responsible for maintenance of this concept? Since the concept is the basis for any information access in this organisation, this attribute also implies a level of trust.

- System assets & components

  Available assets and components in this organisation.

- Communication strategy

  Basic strategy for communicating. Is information pushed or pulled? In which situations? Is this organisation announcing to the public? Do special information security requirements apply to this organisation?

- Threat definitions

  Definition of threat levels for communication (i.e. severe, high, medium).

- Security training and exercises

  Are security trainings and exercises implemented and available in this organisation? If yes, which?

- Generic Interface

  This Interface is the generalisation of all interfaces. Special interfaces with the different types of organisations inherit the information from the generic interface. Therefore, this interface is only used for generalization of information and not for communication.

  - Decisions

    Decisions regarding this interface. What will happen in the future with this interface? Is it deprecated, implying that it will not be available after future updates?

  - Included protocols

    Which protocols are available, when using this interface?

  - Supporting processes

Which processes pull or push information in this interface? Which actions apply to which processes in this interface?

- Arrangements

  User arrangements when using this interface.

- Organisational Power

  Power of the owning organisation. For example, corruption of a governmental interface might have a greater impact, than corruption of a local fire department. This is due to the greater power of the governmental organisation.

- Roles

  Which roles are involved when using this interface? Who is receiving? Who is sending?

- Responsibilities

  What are the responsibilities of the users of this interface?

- Management of Interfaces

  Who is responsible for managing this interface?

- Access Security

  How secure is this interface?

- **Security Agency Interface**

  This specialized interface includes additional information needed for communication with security agencies.

  - Level

    On which level is the communication on? Administrative level? Are individuals involved or does this interface apply to whole office levels?

  - Type of contact

    What is the type of the contact / communication (i.e. informative, initial, pushing, pulling) ?

  - Continuous contact

    Is the contact continuous? Are there intervals of communication?

  - Expected security clearance level

    What level of security clearance is required by the information communicated?

  - Required information

    Description of information that is communicated by this interface.

  - Time scale

    In which time scale is the communication being processed?

  - Communication equipment

    What Equipment is involved in the communication? For example, a wireless connection applies to other risk reduction means than a cable connection.

- **Emergency Services Interface**

  This Interface provides communication with external emergency services.

- Information expectations

  What information is to be expected? Description of the information.
- Specialist security responders support
- Relationships

  Are there any dependencies existing with other services or agencies? Is the information depending on other external parties?
- Responsibilities

  Who is responsible for maintenance, information security and clearance?
- Security Incident Response Arrangements

  What are the arrangements along with this interface?
- Compatibility of technical equipment

  What technical equipment is used? Is it compatible with other equipment and if yes, with which?

o **Transport Organisation Interface**

This interface is used for communicating with other public transportation organisations. It is basically used for information exchange on certain tracks and areas.

- Number of infrastructure managers

  How many infrastructure managers are correlated with this road? Which ones?
- Rail / Road usage by multiple PTOs

  How many public transportation organisations (PTOs) are using this track / area?
- Geography

  The geography of the track / area
- Topography

  The topography of the track / area
- Population distribution

  Population density and distribution in / around the area / track
- Communication between PTOs

  Is there any communication between the transportation organisations which are using this track/area? How is the communication established?
- Media involvement

  Are there any interfaces to the public in the transportation organisation?
- Security routines

  Are security routines implemented? If yes, which ones?
- Incident response routines

  Are incident response routines implemented? If yes, which ones?

o **Media / Public Interface**

Generic Interface for communication with the public, directly or over the media.

- Information coordination

  Who is coordinating the information exchange?
- Authorization responsibles

  Who is responsible for authorizing the information exchange?
- Publishing authorized responsible

  Who is responsible for executing the information exchange?

8.2.3 Intermediary Description

Outcome of reference project(s)	COUNTERACT
Correlated interoperability object	Intermediary

The generic description of the organisation and its available interfaces offers the capability to communicate without knowing about the structure, the clearance and security levels and the information required. Furthermore, intermediating information between different information sources is possible, since the top level description respects different languages. Although this attribute is originally intended in (COUNTERACT 2009a) for sense-making purposes between human actors, it offers capabilities for the usage in ICT systems.

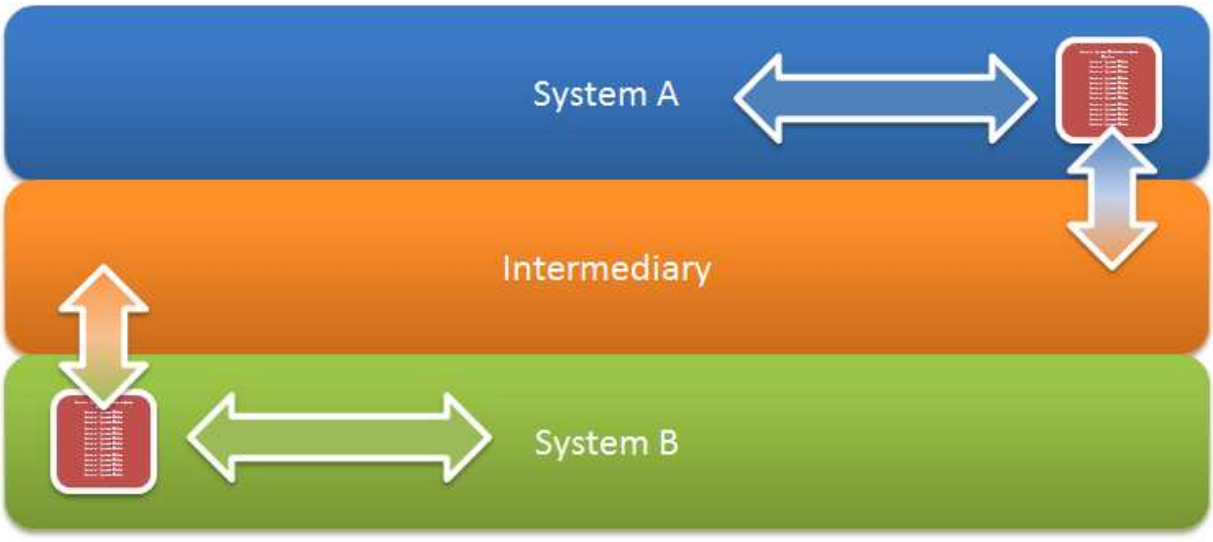

Figure 17 Intermediating between Information Systems by using the dictionary

Figure 17 shows an abstract example of intermediating between different systems or organisations by using their dictionary. In the figure, the dictionary of each system is displayed in red. The Intermediary is accessing only the dictionary for translating information syntaxes and semantics to the required format, following the point to point semantics pattern from Section 5.2. This approach offers the benefit of surpassing a central dictionary, whose maintenance effort might increase along with the number of interconnected systems and agencies.

Finally, the usage of the organisational description and its interface could result in the following steps:

1. Lookup organisational description
   Get the organisational description. Furthermore, see if the organisation complies with our targeted information receiver regarding its
   - Structure
   - Type
   - Security level
   - Tasks
2. Lookup available interfaces
   Retrieve the list of all available interfaces and select the adequate interface for the purpose of communication.
   a. Check inter-organisational communication requirements
      Is this interface suited for the information supplier? For example, a first responder service should not use an interface for security agencies.
   b. Check information security and information clearance level, if necessary.
      Does this interface offer suitable information security levels for the information transmitted? What is the clearance level for this particular information?
3. Get source dictionary
   The intermediating service retrieves the dictionary from the information sender.
4. Get dictionary of targeted service
   The intermediating service retrieves the dictionary from the information retriever.
5. Translate information and semantics
   Both dictionaries are used to translate the information and the semantics to the required output format. This ensures that both services can communicate with each other without having to look up a centralized dictionary. Furthermore the dictionaries used are easier in handling by the intermediating service, since the specialized nature of the organisation implies a smaller amount of contained information.
6. Establish communication / Transmit information
   After the information was translated, the transmission can occur. Depending on the interface, this information will most likely initiate processes and result in pushing or pulling of information in the isolated object of the whole interoperable system.

This abstract process shows basically how the organisations' description could be used to establish a communication in the interoperable system. It is aimed at the assets implemented in the overall system being as autonomous as possible. Finally, the pattern used in achieving semantic interoperability should be chosen specifically to the city and the use cases involved.

9 Conclusions

In this deliverable, we presented a comprehensive interoperability concept for a security meta system in public transportation, covering underlying approaches and theories (see Chapter 5), individual building blocks (see Chapter 8), and an abstract conceptual framework integrating those components (see Chapter 7). We built on the results of earlier projects investigating different focus areas within this research field (Chapter 6). We integrated those earlier results and synthesized them on a homogenous level of abstraction. This Chapter draws some conclusions on the usage of the interoperability concept, discusses how it tackles the requirements presented in Section 4.3, and gives an outlook to the next steps.

9.1 Usefulness of the Related Projects

All of the projects described in Chapter 6 provided valuable input for the definition of an interoperability concept. In particular, COPE, COUNTERACT and DEMASST provided the most relevant deliverables in regard to general interoperability and building blocks. By analysis of these projects, requirements in the domains of sensor systems, communication systems, actors and structures could be obtained. These dimensions generally define interoperability, while taking into account both technical systems and human factors.

The related projects contributed to the building blocks, which were created by analysis, aggregation and interpretation of the findings. Therefore these building blocks provide a point of view on security, while saving best practices researched during past projects. They should be considered as further orientation in order to achieve the best results when creating the interoperable systems.

9.2 Usage of the Interoperability Concept

This general interoperability concept should allow each WP to describe its approach, challenges and solutions in a similar way. For example:

- In SP3, the usage of a capacity can be described for different threats or scenarios, with the different existing or intended Intermediaries in the demo cities or for several organisational settings. In addition, it is possible to use the concept to elaborate the usage of the capacities for normal operational activities.
- In SP4 and SP5 for any threat or scenario the current content flow can be described and compared with the future content flow with a new capacity and/or other operational procedures. In addition, it is possible to use the concept to elaborate the reaction to similar threats on a different spatial level (e.g. station, city and region).

For such a description it is relevant that each WP decides how it adapts the general concept, e.g. in the following directions:

- Restriction of objects: limit the scope of description to a specified set of objects, e.g. only IT-Systems, Interfaces and Intermediaries.
- Restriction within objects: limit the scope of description to a specified instance of each object, e.g. only the Role of users, or only the content type data.

- Selection of objects: start with existing building blocks of potentially relevant objects and select the ones appropriate for your WP, e.g. the relevant sensor types as an IT-System.
- Specification of objects: define the types or instances of each object for the relevant city or capacity, e.g. the real-life user Roles within a demo city or the existing intermediating networks.

9.3 How the Concept Serves the Requirements

The interoperability concept within SECUR-ED follows the defined requirements as follows:

- The concept is abstract enough to fit the different technologies, organisational and settings and crisis management phases, since the same concept allows the handling of each of these challenges.
- The concept is simple enough to be easily understood, since it is limited to four objects (Information System, Interface, Intermediary and Role) and two environmental factors (Context and Content) with straight relations.
- The concept is flexible enough to be used and adapted in different WPs, which has been illustrated in the previous Section.
- The concept is focused enough not to interfere with the topics addressed in other WPs, which is done with the concentration on IT-Systems and an open relation to Roles that can be further specified by other WPs, and by not addressing specific IT-standards that are handled in WP41. Also, the notation of Context provides the opportunity to extend the view to processes and procedures or other elements that are considered relevant in following WPs.

9.4 Next Steps in WP 22

In Task 22.2, an interoperability notation will be elaborated that supports SECUR-ED to describe the situation for capacities and demonstrations according to this interoperability concept in a consistent format. In Task 22.3, the details for the interoperability syntax will be described, focussing on the IT-System, the Interface and the Intermediary. In Task 22.4, the interoperability semantics will be tackled, focussing on Context, Content and Roles.

10 Literature

COPE. 2008. *Use Case Descriptions and a Human Factors Engineering Framework*. Deliverable. COPE. December.

———. 2009a. *Comprehensive Model of First Responder Operations & Concept of Operations*. Deliverable. COPE. May.

———. 2009b. *HF-based Design Inputs to COPE Technology - Conceptual and Empirical Considerations of Common Operational Picture*. Deliverable. COPE. November.

COUNTERACT. 2009a. *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. Counteract. March.

———. 2009b. *Public Transport Security Planning - Organisation, Countermeasures & Operation Guidance - Part C: Systems and Equipment - Design Strategies and Considerations*. Final Report. Counteract. March.

———. 2009c. *Anti Terrorisms Public Awareness Campaigns*. Deliverable. Counteract. April.

Cullen, A., S. Barker, S. Case, T. Rye, B. Rossow, and E. Wilkinson. 2009. The Oasis Approach to Civil / Military Information Sharing for Disaster and Emergency Management. February.

Dantas, A., and E. Seville. “Organisational Issues in Implementing an Information Sharing Framework: Lessons from the Matata Flooding Events in New Zealand.”

DeLaurentis, D. A. 2005. Understanding transportation as system-of-systems design problem. In *43 rd AIAA Aerospace Sciences Meeting and Exhibit*, 2005.

DeLaurentis, Dan, and Robert K. “CAB” Callaway. 2004. “A System-of-Systems Perspective for Public Policy Decisions.” *Review of Policy Research* 21 (6) (November 1): 829-837. doi:10.1111/j.1541-1338.2004.00111.x.

DEMASST. 2009a. *Current technological solutions and relevant research*. Deliverable. DEMASST. September.

———. 2009b. *Current status of Security in Mass Transport*. Deliverable. DEMASST. November.

———. 2010. *Report on Potential Integrated Solutions*. Deliverable. DEMASST. February.

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

Engelbach, W., H. Roßnagel, and S. Frings. 2010. Ein Konzept zur organisationsübergreifenden Integration von IT-Systemen für die zivile Sicherheit. In *Software Engineering 2010 - Workshopband*, 379-386. Bonn: Köllen Druck + Verlag GmbH, February.

Eriksson, W. 2009. System-of-Systems Demonstration & Experimentation for Mass Transport Security presented at the Workshop to discuss the scope of Call for Demonstration Project Security of Mass Transportation (Phase 2), March, Berlin. http://www.bmbf.de/pubRD/WS_MT_Eriksson.pdf.

Hrebicek, J. 2006. Semantic Interoperability. www.iba.muni.cz/obr/File/organize/semanticka_interoperabilita.pps.

InteGRail. 2010. *InteGRail - Intelligent Integration of Railway Systems*. Final Report. InteGRail. April.

ISO. 1993. ISO/IEC 2382-1:1993 Information technology - Vocabulary - Part 1: Fundamental terms. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=7229.

Keating, C., R. Rogers, R. Unal, D. Dryer, A. Sousa-Poza, R. Safford, W. Peterson, and G. Rabadi. 2008. “System of systems engineering.” *Engineering Management Review, IEEE* 36 (4): 62. doi:10.1109/EMR.2008.4778760.

Keating, C.B. 2005. Research foundations for system of systems engineering. In *Systems, Man and Cybernetics, 2005 IEEE International Conference on*, 3:2720- 2725. doi:10.1109/ICSMC.2005.1571561.

Kini, K. S, and D. H Manjaiah. 2010. Enterprise Data Model -- A Study with Reference to Technical Institution. In *2010 International Conference on Web Information Systems and Mining (WISM)*, 2:323-326. IEEE, October 23. doi:10.1109/WISM.2010.111.

MODSafe. 2011. Description of the project. *MODSafe*. July. http://www.modsafe.eu/programm.html.

MODURBAN. 2008. *Functional Interfaces specification for Passenger Information System*. Deliverable. MODURBAN. May.

———. 2009. *MODURBAN Architecture, Description of alternatives, for publication*. Summary. MODURBAN. May.

NewRail. 2011. SECUREMETRO - Inherently secure blast resistant and fire safe metro vehicles. July. http://securemetro.inrets.fr/.

NoAH. 2005. *Survey on the state-of-the-Art*. Deliverable. European Network of Affined Honeypots. October.

———. 2006a. *Honeypot Node architecure*. Deliverable. European Network of Affined Honeypots. April.

———. 2006b. *Attack Detection and Signature Generation*. Deliverable. European Network of Affined Honeypots. May.

———. 2008. *Production Infrastructure Architecture Definition*. Deliverable. European Network of Affined Honeypots. October.

PROTECTRAIL. 2011. PROTECTRAIL - The Railway-Industry Partnership for Integrated Security of Rail Transport. (...). July. http://protectrail.eu/.

Ritchie, B. W. 2004. “Chaos, Crises and Disasters: A Strategic Approach to Crisis Management.” *Tourism Management*.

Roßnagel, H., and O. Junker. 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)*. May.

Roßnagel, H., and J. Zibuschka. 2011. Using mobile social media for emergency management: a design science approach. In *Proceedings of the 8th International ISCRAM Conference*. Lisbon, Portugal.

Roßnagel, H., J. Zibuschka, and O. Junker. 2010. “Agent-Based Simulation for Evaluation of a Mobile Emergency Management System.” *Sustainable e-Business Management*: 100–114.

———. 2011. On the effectiveness of mobile service notifications for passenger egress during large public events. In *Proceedings of the 8th International ISCRAM Conference*. Lisbon, Portugal.

Sauser, B., and J. Boardman. 2008. “Taking hold of system of systems management.” *Engineering Management Journal* 20 (4): 44–49.

SECUR-ED. 2009. Secured Urban Transportation - European Demonstration. November.

Selvage, Mei Y., Dan Wolfson, Bob Zurek, and Ed Kahan. 2006. Achieve semantic interoperability in a SOA. IBM Inc., June.

Tolk, A., and James A. Muguira. 2003. The Levels of Conceptual Interoperability Model. In Orlando, Florida, September.

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

UITP. 2010. Secure Public Transport in a Changeable World. UITP, November.

Wang, W.G., A. Tolk, and W.P. Wang. 2009. The Levels of Conceptual Interoperability Model: Applying systems Engineering Principles to M&S. In *SpringSim'09 Proceedings*. San Diego, CA, USA: SCS.

Wegner, Peter. 1996. "Interoperability." *ACM Comput. Surv.* 28 (1) (March): 285–287. doi:10.1145/234313.234424.

11 List of Figures

12 List of Tables

- End of Document-