SECUR-ED
SECured URban transportation - European Demonstration

D22.5 Interoperablity Framework and Guidelines

Document identification			
Related SP / WP	SP2 / WP22	**Reference**	SCR-WP22-D-FHG-014
Related Deliverable	-	**Dissemination Level**	PU
Lead Participant	FHG	**Lead Author**	W. Engelbach (FHG)
Contributors	T. Vandieken (FHG) F. Ebert (FHG) M. Ducharme (ALS) V. Isbert (THA)	**Reviewers**	G. Rafaeli (MTRS3) N. Blanco (CRTM) A. Söhnchen (UITP)

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

History

Version	Status	Date	Author	Main Changes
0.1	Draft	2013-09-30	W. Engelbach (FHG)	Structure and responsibilities
0.2	Draft	2014-05-09	T. Vandieken (FHG)	Concept and notation described and applied
0.3	Draft	2014-06-20	M. Ducharme (ALS)	Demonstration experiences reflected
0.4	Draft	2014-07-03	V. Isbert (THA)	Guidelines elaborated
1.0	Under Review	2014-07-04	W. Engelbach (FHG)	Integration and harmonisation; introduction, conclusion, summary
2.0 & 3.0	Under Review	2014-07-30	W. Engelbach, T. Vandieken (FHG)	Included review comments from CRTM, MTRS and UITP
4.0	Issued	2014-07-31	W. Engelbach, T. Vandieken (FHG)	Version submitted to the Commission

TABLE OF CONTENTS

1 Summary

WP22 tackled concept, notation, syntax and semantics of interoperability in the urban public transport domain. It spanned a conceptual area from security threats to interactions between different stakeholders and the usage of information systems, covering the IT-generic and IT-solution-specific challenges of data structures and understandable information in different contexts.

Task 22.5 on system-of-systems architecture and guidelines takes up the results of the previous tasks. For this purpose, selected demonstration scenarios are described in the interoperability notation language in order to check the validity and usability of the notation to address security interoperability challenges and support the generation of an interoperability framework from the diversity of project experiences. Based on these outcomes, interoperability lessons learnt from the demonstrations are elaborated and interoperability guidelines for operators, industry and politics suggested.

In the SECUR-ED project several demo scenarios have been defined and realised. This document applies the interoperability notation to one of the scenarios in the three main demonstrations that actually integrated different IT-capacities. While the initial aim was to apply the notation in order to support the preparation and execution of the demos, this was not possible since the demonstration cities already decided to use their specific ways of modelling during the start of the preparations. This resulted in the situation that the demo scenarios have been described in quite different ways, distributed over several documents. The objective of this document is therefore now to sum up and compress the content of these documents and to abstract the demo scenarios to a higher and common level. This also allows proving the validity and usability of the notation to “real world” problems.

The interoperability notation enables public transport operators and system integrators to model and reflect how relevant information exchange activities can be principally supported in a system-of-systems architecture, i.e. which systems and interfaces are used, and how the approach supports use cases and business scenarios. The interoperability notation has been mainly used within WP22, but not, as previously mentioned, in the SECUR-ED demonstrations preparation, which mainly applied local variations of the process oriented BPNM (Business Process Model and Notation) notation.

The system integration challenge of combining a variety of technological and procedural security solutions in a large scale demonstration lies in the technical integration of the various systems and in the ability to combine the strength of these devices in a global and coherent system. In the different demonstrations, the application of interoperability standards, models and formalisms therefore played a major role. While the adoption of the interoperability mind-set proved to be effective, lessons were learned related to the management of the project process, challenges of different subsystems, overall interoperability challenges, perceived benefits and training considerations.

The final interoperability recommendations therefore provide guidelines for authors and readers of interoperability specifications. Based on the experiences within SECUR-ED, suggestions are provided to handle relevant topics in interoperability specifications such as readers, tests, errors, versions, options, references, extensibility and backward compatibility. These general considerations should help the stakeholders in public transport security to better communicate about the details of interoperability, which are dependent on involved technologies, existing systems, business interests and legal context.

2 References

2.1 List of Acronyms

ATM	Azienda Transporti Milanesi
BPMN	Business Process Model and Notation
BVG	Berliner Verkehrsbetriebe (Public Transport Operator of Berlin)
CCTV	Closed-circuit television
CISEM	Centro Integrado de Seguridad y Emergencias (Madrid Command Centre for emergency response)
CITRAM	Centro Integrado de Gestión de Transporte Público de Madrid (CRTM Control Centre)
CONOPS	Concepts of Operations
CRTM	Consorcio Regional de Transportes de Madrid (Public Transport Authority in Madrid Region)
DB	Deutsche Bahn (German National Railway)
DGT	Dirección General de Tráfico (State Traffic Office – Management Centre)
DSL	Domain Specific Languages
EMT	Empresa Municipal de Transportes (Urban bus lines PTO - company of the Madrid City Council)
FLSP	Field level security plan
ICE	Inter City Express train
IDL	Interface Description Language
IED	Improved Explosive Device
IRD	Improvised Radiological Device
IT	Information technology
MOU	Memorandum of Understanding
PTO	Public Transport Operator
RATP	Régie Autonome des Transports Parisiens (Paris public transport operator)
RENFE	Suburban train services PTO
RER	Réseau Express Régional (Regional Express Network)
RFC	Request for Comments (publication of the Internet Engineering Task Force (IETF) and the Internet Society)
RFID	Radio-frequency identification

SAMUR	Emergency Medical Service in Madrid, Spain
SCNF	Société Nationale des Chemins de fer Français (French national railways)
SECUR-ED	Secured Urban Transportation – European Demonstration
THW	Technisches Hilfswerk (Federal Agency for Technical Relief Germany)
TIM	Toxic Industrial Material
UML	Unified Modelling Language
XML	Extensible Markup Language

2.2 Referenced Documents

[Asima10]	Asimakopoulou, E. 2010. *“Advanced ICTs for Disaster Management and Threat Detection”*. In *IGI Global*, N. Bessis (ed.).
[Berlin1]	K. Rothe, G. Richter. 2013. *“Detailed Scenarios for Berlin Demonstration”*. SECUR-ED deliverable WP 45.1 [SCR-WP45-D-DBA-016-05].
[Berlin2]	G. Richter, N. Arbel. 2013. *“Functional specifications for Berlin demonstration”.* SECUR-ED deliverable WP 45.2 [SCR-WP45-D-DBA-012-05].
[Berlin3]	H. Saltzman. 2012. *“Training Platform Architectural and Technical Overview”.* SECUR-ED-WP45 Project overview [SCR-WP45-B-NIC-004-01].
[Born04]	Born, M., Holz, E., and Kath, O. 2004.*”Softwareentwicklung mit UML 2”*, (1st ed.).
[COPE08]	COPE. 2008. “*Use Case Descriptions and a Human Factors Engineering Framework”* (Deliverable No. D2.1), COPE.
[COPE09a]	COPE. 2009. “*Comprehensive Model of First Responder Operations & Concept of Operations*” (Deliverable No. D3.1), COPE.
[COPE09b]	COPE. 2009. “*HF-based Design Inputs to COPE Technology - Conceptual and Empirical Considerations of Common Operational Picture”* (Deliverable No. D2.2), COPE.
[Count09a]	COUNTERACT. 2009a. “*Public Transport Security Planning - Organisation, Countermeasures & Operation Guidance - Part C: Systems and Equipment - Design Strategies and Considerations”* (Final Report No. PT5), Counteract.
[Count09b]	COUNTERACT. 2009b. “*Public Transport Security Planning - Organisation, Countermeasures & Operation Guidance - Part B: Security Operations Planning - Development of Operational Concept, Field Level Security Plans, Procedures and Training”* (Final Report No. PT5), Counteract.
[Dalga08]	Dalgarno, M., and Fowler, M. 2008. *“UML vs. Domain Specific Languages”* In *Methods & Tools* (16:2), pp. 2.
[Demas09]	DEMASST. 2009. “*Current technological solutions and relevant research”* (Deliverable No. D5.1), DEMASST.
[Demas10]	DEMASST. 2010. “*Report on Potential Integrated Solutions”* (Deliverable No. D4.4), DEMASST.
[Engel11]	Engelbach, W., Roßnagel, H., and Zibuschka, J. 2011. *“Interoperability of Information Systems for Public Urban Transport Security: The SECUR-ED Approach”.* In *Future Security 2011 Conference Proceedings*. Presented at the Future Security 2011, Berlin: Fraunhofer Verlag.
[Holln02]	Hollnagel, E. 2002. *“Cognition as control: A pragmatic approach to the modelling of joint cognitive systems”. IEEE Transactions on Systems*, Man and Cybernetics.

[Inter1]	Roßnagel, H., W. Engelbach, S. Kurowski, J. Zibuschka, D. von den Abeele, V. Isbert, A. de Jong, E. Vullings 2012. *“Interoperability Concept”.* SECUR-ED deliverable D22.1 [SCR-WP22-D-FHG-002-05].
[Inter2]	Roßnagel, H., W. Engelbach, S. Kurowski, J. Sautter, J. Zibuschka 2012. *“Interoperability Notation”.* SECUR-ED deliverable D22.2 [SCR-WP22-D-FHG-008-04].
[Inter3]	Ducharme, M., J. Boyer, A. Bruno, N. Cullin, J. Denner, N. Dromer, D. Dupré, P., M. Guichard 2012. *“Interoperability Syntax”*. SECUR-ED deliverable D22.3 [SCR-WP22-D-ALS-012-02].
[Inter4]	Vullings, E., W. Engelbach 2013. *“Interoperability Semantics”*. SECUR-ED deliverable D22.4 [SCR-WP22-D-TNO-013-03]
[Kuro11]	Kurowski, S., Roßnagel, H., Zibuschka, J., and Engelbach, W. 2011. *“A survey of European interoperability research in urban transport security”.* Presented at the Conference on Mobility in a globalized World, Iserlohn, Germany.
[Kuro12]	Kurowski, S., Zibuschka, J., Roßnagel, H., and Engelbach, W. 2012. *“A Concept for Interoperability of Security Systems in Public Transport”*. In *Proceedings of the 9th International Conference on Information Systems for Crisis Response and Management*. Presented at the ISCRAM 2012, Vancouver, Canada.
[Madrid1]	T. Melero. 2013. *“Detailed description of Madrid Demo Scenarios”,* SECUR-ED deliverable WP 42.1 [SCR-WP42-D-CTM-002-06].
[Madrid2]	T. Melero. 2012. *“Functional Specifications for Madrid Demo Scenarios”*. SECUR-ED deliverable WP 42.2 [SCR-WP42-D-CTM-003-05].
[Milan1]	S. Milanesi. 2013. *“Detailed Scenarios for Milan Demonstration”*. SECUR-ED deliverable WP 44.1 [SCR-WP44-D-ATM-029-06].
[Milan2]	S. Milanesi. 2012. *“Functional Specifications for Milan demonstration”*, SECUR-ED deliverable WP 44.2 [SCR-WP44-D-ATM-030-05].
[Milan3]	C. Dambra. 2012. *“Description of the implementation of the Milan demonstration”*, SECUR-ED document linked to WP44 [SCR-WP44-T-ANS-013-01].
[Milan4]	J. Steinkohl. *“Milan Demo - Enhanced CCTV application to protect passengers, staff and assets”*, SECUR-ED Midterm Conference Presentations [SCR-WP13-B-UNI-031-01].
[Paris1]	E. Laurens-Fonseca. 2013. *“Detailed Scenarios for Paris demonstration”*, SECUR-ED deliverable WP 43.1 [SCR-WP43-D-RTP-010-04]
[Paris2]	RATP. 2013. *“Functional Specifications for Paris demonstration”*, SECUR-ED deliverable WP 43.2 [SCR-WP43-D-RTP-011-05].
[RFC2119]	S. Bradner. 1997. *“Key words for use in RFCs to Indicate Requirement Levels”*
[Ritch04]	Ritchie, B. W. 2004. *“Chaos, Crises and Disasters: A Strategic Approach to Crisis Management”. Tourism Management* (Tourism Industry:25), pp. 669-683.
[Saut12]	Sautter, J., Roßnagel, H., Kurowski, S. and Engelbach, W. 2012. *“Interoperability for Information Systems in Public Urban Transport Security: The SECUR-ED Interoperability Notation”*. In *Proceedings of the 9th International Conference on Information Systems for Crisis Response and Management*. Presented at the ISCRAM 2012, Vancouver, Canada.
[Turn05]	Turnitsa, C. D. 2005. *“Extending the Levels of Conceptual Interoperability Model”*. In *Proceedings IEEE Summer Computer Simulation Conference*. Presented at the IEEE Summer Computer Simulation Conference, CS Press.

3 Introduction

Interoperability is a key approach to arrive at systems-of-systems that support security awareness and response in public urban transport. While interoperability has many facets, here the conceptual linkage between information systems is highlighted. Based on the understanding that the involved public transport operators and security stakeholders have their roles and procedures, the information systems enable information exchange between these partners and thus help to design and run more reliable and efficient processes.

This final deliverable D22.5 in WP22 firstly summarises the overall approach of the interoperability concept and the related notation (chapter 4). Selected demonstration scenarios are then described in the interoperability notation language to check its validity and usability for addressing security interoperability challenges and support the generation of an interoperability framework for information systems (chapter 5). Across all the SECUR-ED demonstrations, interoperability lessons learnt from the cooperation and implementation phase to bring the concepts to real live are elaborated (chapter 6). Against this background, interoperability recommendations are provided that may support transport operators, security stakeholders, supplying industries and politics to overcome the identified challenges and foster the application of integrated and beneficial solutions for interoperable security systems, especially in the agreement on relevant interoperability specifications (chapter 7).

A basic assumption of the interoperability view in the SECUR-ED is that in the field of urban public transport, first responders and transport operators collaborate in the prevention of and reaction to security issues. Hereby 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. Thus a conceptual model has been described 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 transport [Inter1, Engel11]. This comprehensive interoperability concept for a security meta-system covers underlying approaches and theories, individual building blocks and an abstract conceptual framework integrating those components [Kuro11, Kuro12].

The SECUR-ED interoperability concept has been transferred to a graphical representation and introduces a set of rules and key concepts to harmonise modelling of interoperability for the public transport and security domains [Inter2]. Based on the interoperability objects and building blocks of the concept, the notation offers capabilities for further annotation of the interoperability objects modelled, hence enabling collaboration and interpretation of this model on various stages. The notation language is based on the Unified Modelling Language (UML) and thus offers the possibility for structured modelling of the system-of-systems architecture. The notation allows expressing organisational settings as well as technical infrastructures. UML is a modelling language used in requirements and software engineering that is flexible and offers several possibilities in granularity and ways of modelling a certain aspect. An example on how to use the notation is provided in [Inter2] and [Saut12].

An interface specification language allows mass transport security information systems to communicate and exchange data in a distinct and understandable way in order to achieve interoperability between the systems. Interoperability between systems is only possible if the interfaces have been fully, precisely and clearly defined previously. That clarification of the syntax for interoperability is the role of a technical Interface Description Language (IDL).

Thus a dedicated technical IDL and data definition language has been developed in order to satisfy the needs of interoperability of the security in public urban transport domain [Inter3]. A graphical representation of each concept of the interface description language has been provided. Additionally common standards and open middleware technologies are presented to guide the definition of interfaces and description of data.

Semantics of interoperability have been added by the definition and description of standard roles and generic security use cases [Inter4]. For the different roles and use cases it is elaborated 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. A semantic definition of common tasks, roles, functionalities, and locations is delivered in order to describe the security aspects of a communication hub in a clear way. Besides this definition, a software tool was developed. The tool named RED (*“Requirements Editor and Designer”*) supports the definition of scenarios, user roles and stories in a clear and concise way, as well as describe the high-level architecture using the interoperability notation.

4 An Interoperability Framework for the Public Transport Security Domain

This chapter provides an overview about the interoperability concept and the corresponding SECUR-ED interoperability notation. The aim of this interoperability framework is to provide a structured approach to design and document the ability of information systems to interact. This specifically includes inter-organizational interoperability of systems from different stakeholders that are active in the public transport security domain. The developed concept enables system designers to model a system-of-systems architecture by defining interoperability objects and their relations and supports the structured documentation of security relevant information by providing guidelines for annotation.

The following text is a summary of [Kuro12] and [Saut12], which are based on [Inter1] and [Inter2].

4.1 A Concept for Interoperability of Security Systems in Public Transport

In the field of public transport, operators and first responders collaborate in the prevention of threats and reaction to security issues. In order to optimise their specific daily operational business needs in a timely manner, heterogeneous information and communication systems are deployed. In case of an incident however it is crucial that the various involved parties exchange relevant information to develop a shared understanding and act in a coordinated way. Yet, heterogeneous communication and information system infrastructures often hinder this crucial flow of information. To address this shortcoming it is crucial to enable the design of interoperable system-of-systems approaches in this domain. Therefore a conceptual model to construct system-of-systems environments in the domain of security in public transport was developed.

The building blocks of this model are distilled from a survey on interoperability in projects researching security in public transport [Kuro11]. Turnitsa's conceptual levels of interoperability [Turn05] were used as a framework for a consolidated model of interoperability for information systems in public transport security. This consolidated concept is employed as basis for the interoperability notation of SECUR-ED.

The interoperability concept used several research projects in order to identify and distil building blocks. Such blocks are meant to be used along the levels of the conceptual interoperability model to facilitate the design of interoperable socio-technical systems-of-systems, while taking into account the complexity of the domain of security in public transport. This complexity originates from various stakeholders and scenarios creating an environment in which highly complex and dynamic collaboration and communication structures depend on types of incidents as well as phases in the emergency lifecycle [Ritch04]. Therefore, the research included projects with a focus on incident ground collaboration [COPE09a] and incident management [Count09b]. This resulted in an integrated interoperability model.

[COPE08] described various collaboration scenarios and the participating entities, including systems and stakeholders. The structure of collaboration between entities in these scenarios already implies a basic system-of-systems design. [COPE09a] offers a description of socalled concepts of operations (CONOPS). Those are used as descriptive tools for formal understanding of the distributed roles, their collaboration, capabilities and limitations. The CONOPS usually operate on the level of pragmatic interoperability. Field level security plans (FLSP) [Count09a] specify the more general CONOPS, applying methods, routines, stakeholders and structures to a certain security asset and/or scenario. The organizational interfaces describe generic collaboration structures and interfaces between different types of organization [Count09a]. This information enables both the creation of a typology of the involved stakeholders on an organizational level, and a derivation of applicable metadata for information exchanges between the parties.

In terms of technical systems, most of the surveyed projects focused on sensor systems. Although a wider range of technical systems may be involved in the domain of public transport security, sensing systems are information retrievers, enabling interpretation of environment states. Hence such systems are very interesting when focusing on the domain of security where detection is a crucial point for mitigating an incident [Asima10].

[Kuro11] derived various ontologies from the sensor systems presented in [COPE09b], [Count09b], [Demas09], and [Demas10]. The ontologies were aggregated, creating a typology of sensor systems.

All identified elements from the surveyed projects were aligned with the model from [Turn05], creating an integrated model for interoperability which is shown in Figure 1. The figure shows the usage of each identified asset in the conceptual interoperability model, along its potential contents. While those concepts (roles or their implied limitations from the scenario-based use cases in [COPE08], agreements from the interfaces and states derived from procedures of the field level security plans in [Count09a]) enable establishment of dynamic interoperability, the concepts of operations, and the derived sensor system ontology enable pragmatic interoperability by showing procedures in terms of capabilities, adaptabilities, constraints and legal issues. Semantic interoperability is enabled by using the professional terms which is described in the concepts of operations, metadata derived from the interfaces and use cases from the use case descriptions and the field level security plans.

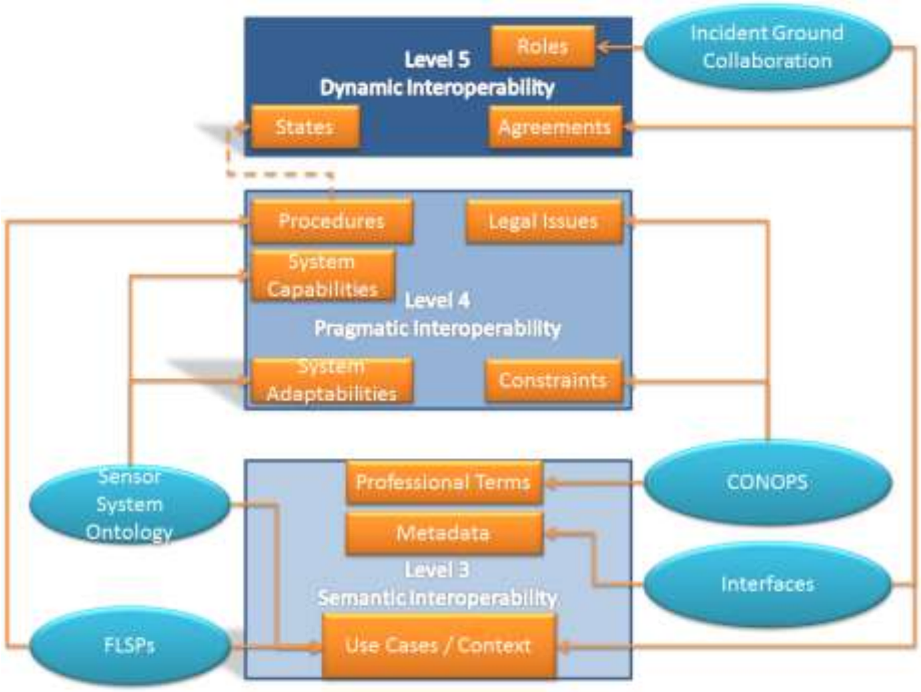


Figure 1: Integrated model for interoperability [Kuro11]

4.2 An Interoperability Notation for Security Systems in Public Transport

In this section the elements described in Figure 1 are synthesized into generic interoperability objects, enabling the development of a modelling and notation approach for interoperable system-of-systems supporting security functions in public transport.

In software and systems engineering there are essentially two different approaches to model system infrastructures. The first approach is to rely on general purpose modelling languages. The alternative is to use domain specific languages (DSL) [Dalga08]. In the present work both of these approaches are combined by relying on a proven general purpose language in UML that is enriched with domain specific guidelines for the annotation of the components.

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

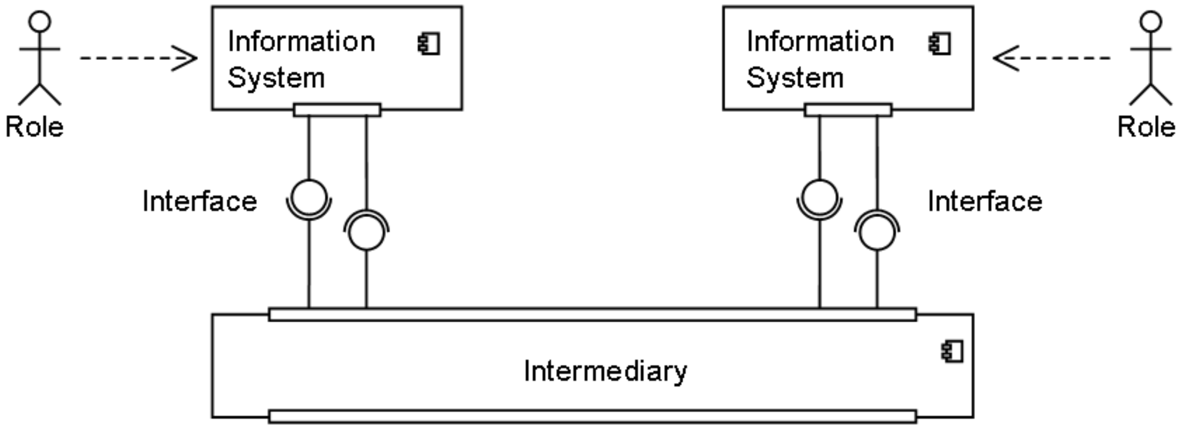


Figure 2: The SECUR-ED interoperability objects

Roles represent organisational roles that are fulfilled by persons. Every role is responsible for certain tasks and interoperates with information systems. Notated in UML the "<<use>>>"-identifier is applied to specify an interoperation between roles or between a role and an information system. Roles are notated using UML-Agents, which themselves are a special notated kind of component (see Figure 4b). Figure 3 illustrates a role, which uses two information systems. As depicted the "<<use>>"-identifier keyword may be left away.

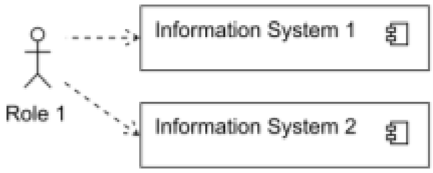


Figure 3: Simple infrastructure diagram showing a role using two information systems

An information system is an entity which processes and stores data and has a specified dependency to its environment. In urban transport a single sensor system as well as an organisational entity like a whole train station can be considered as an information system [Engel11]. Within the present notation, such a system is realized as an UML-component with an optional component icon (see Figure 4a).

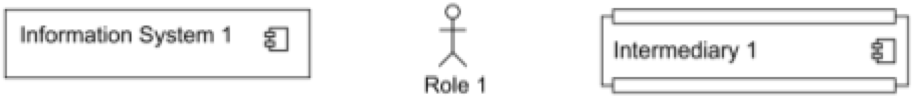


Figure 4: An information system notated as UML-component (a), a role notated as UML agent (b) and an intermediary notated as UML-component with two complex ports top and bottom (c)

As the same information system typically occurs several times in a concrete setup in public transport, a mechanism is offered to initially specify a concrete type of information system once in a classification diagram and instantiate it several times in infrastructure diagrams. The advantage of this approach is the ability to specify detailed information concerning this concrete type only once. Therefore, the designer can introduce a classification of information system types as a prerequisite of an infrastructure component diagram. This classification is specified as a component diagram typically using the UML-concept inheritance, and if required associations between information systems may also be modelled.

An interface is a gateway that allows interaction between several information systems [Engel11]. Two alternatives are offered to represent interfaces graphically, dependent on the designer's individual needs: UML-interfaces and UML-connectors. For both UML-concepts we always notate an UML-port on both sides of the interconnection.

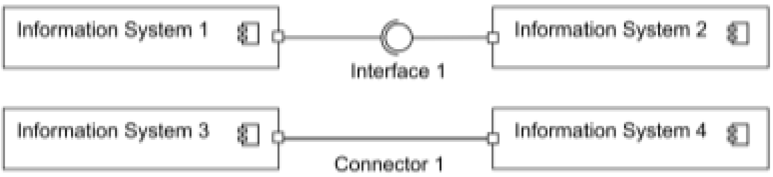


Figure 5: Interfaces notated as UML interface and UML connector

The setup outlined in Figure 5 implies that "Information System 2" realizes the UML-interface "Interface 1" in sense of the UML-identifier "<<realize>>". The depicted ball-socket-notation is a short-notation for notating an entity "Interface 1" and a realizing "Information System 2" [Born04]. If the initiative of an interconnection – no matter if organisational or technical – shall be defined as the task of one of the two parties, the UML-interface notation should be used. The other way round, the designer should be aware of the fact that modelling interoperability via UML-interfaces exactly specifies an invocation direction. If an interconnection is modelled, which aggregates several heterogeneous interconnections with several invocation-directions, the UML-connector shall be used. This saves the designer from having to notate all the particular interfaces in detail.

An intermediary is a specific information system that serves the sole purpose of supporting the interaction between other information systems [Engel11]. The intermediary is represented by using a special-notated UML-component which has always two notated complex ports on top and on bottom (see Figure 4c). This is just a notation convention in order to clearly distinguish between information systems and intermediaries and to offer the possibility to visually attach interfaces (as UML interfaces or UML connectors) from both sides of the rectangle. Conceptually there is only one complex port, which defines outer dependencies of an intermediary.

Since the interoperability notation is tailored to the domain of public transport security it must of course provide guidelines on how to document security relevant information in a complete and structured form. Based on a survey [Kuro11] detailed guidelines for annotating interoperability objects, their relations and the overall context were elaborated [Kuro12]. These guidelines are partly flexible and text-oriented and partly include a set of concrete default values. They allow designers to annotate their models with additional information specific to the security domain in a structured manner. The guidelines define a few mandatory fields but most of the fields are optional enabling designers to adapt their models to their individual needs (see Table 1). The specification of the guidelines however is beyond the scope of this notation.

Attribute	**Mandatory**	**Format**	**Example Value**
Information System Type	Yes	Single	Surveillance
Information System Description	Yes	Text	A type defining the CCTV appliances.
Purpose of Information System	Yes	Text	Surveillance of areas
Security Related Purpose	Yes	Text	See Purpose of Information System
Information System Operator	Yes	Text	FNM
Security System Typology	No	Single	Fully Controlled System
Processing Capacity Description	No	Text	25 frames per second, 468kbit/s, 800x600px
Threats to Information System	No	Text	Vandalism, Bombing
Legal and Compliance Issues	No	Text	-
Maintainability Requirements	No	Text	-
Availability Requirements	No	Text	-

Table 1 : Annotation of the information system type “CCTV FNM Type”

In summary, the SECUR-ED interoperability notation for security systems in public transport enables systems designers and practitioners to describe components and systems in public urban transport in a consistent format. One of the main purposes of the notation is to help avoid misunderstandings in the communication between different stakeholders such as operators, first responders and suppliers. By employing specialized security-oriented annotation guidelines the notation enables seamless collaboration, as all stakeholders are able to interpret the model during the various stages of the systems and system-of-systems development process.

Based on UML, the most widespread standard for expressing information system architectures in the field, the notation language offers the possibility for structured modelling of the system-of-systems architecture. The notation provides capabilities to express organisational settings as well as technical infrastructures. Furthermore, it is very flexible, easy to understand and use. The notation defines basic rules to enable the domain’s various stakeholders to understand models designed by other parties, while maintaining a high degree of flexibility. Such a set of rules and key concepts standardizing the modelling for the public transport and security domains therefore should prove beneficial in practice.

5 Demo Scenarios in the Interoperability Notation

In the SECUR-ED project several demo scenarios have been defined and realised. This chapter applies the interoperability notation to one of the scenarios in the three main demonstrations that actually integrated different IT-capacities. The selection of scenarios has been driven by the criteria to have several roles and information systems involved, and a clear picture of the expected benefits already at an early stage of the scenario definition.

While the initial aim was to apply the notation in order to support the preparation and execution of the demos, this was not possible since the demonstration cities already decided to use their specific notation of modelling during the start of the preparations. This resulted in the situation that the demo scenarios have been described in quite different ways, distributed over several documents. The objective of this chapter is therefore now to sum up and compress the content of these documents and to abstract the demo scenarios to a higher and common level, with a focus on the interoperability of information systems.

The story of each selected scenario is first described textually, then the roles and their stories are presented, and targets, threats, suspicious objects and locations extracted. Finally, the architecture of the information systems is illustrated.

5.1 Scenario Milan 1

The description of the scenario is based on the following documents: [Milan1], [Milan2], [Milan3], and [Milan4]. The scenario has been selected since several roles and IT-systems are involved, and a clear picture of the expected benefits has been described at an early stage of the scenario definition.

5.1.1 Scenario Description

The scenario is triggered by the report of an employee of the public transport operator or a citizen calling the emergency number. A person showing suspicious behavior is moving in the public transport network targeting the Malpensa airport. The person is carrying dangerous material (e.g. explosive) in his bag to perform a terrorist attack at the airport. The public transport authority wants to detect and track the person while travelling through the transport network in order to prevent the attack and arrest the person.

Roles and stories:

- ***Person showing suspicious behavior:*** As a person showing suspicious behavior I want to perform a terrorist attack at the airport using dangerous materials (e.g. explosive) in order to bring disorder to the transport infrastructure.

  As a person showing suspicious behavior I want to travel as unobtrusively as possible through the public transport network in order to be undetected.
- ***Citizen:*** As a citizen I want to call the emergency number in order to report a person showing suspicious behavior travelling through the public transport network.
- ***Public transport operator (ATM) staff:*** As a staff member of the public transport operator I want to refute the person showing suspicious behavior travelling through the public transport network, usually by questioning and additional screening. If necessary I want to report the person showing suspicious behavior in order to ensure

the safety of the people using the transport network, mainly by timely measures like evacuation.

- ***Public transport operator staff (ATM):*** As a public transport operator staff member I want to identify a wanted person using technologies like the ticketing system, RFID tracking, Bluetooth, WiFi or personal features tracking in order to find the person showing suspicious behavior.

  As a public transport operator staff member I want to identify a person that is behaving suspicious while travelling through the public transport network in order to find out if they plan to harm people or infrastructure.

  As a public transport operator I want to track a person with suspicious behaviour that is travelling through the public transport network using video tracking technologies like CCTVs in order to prevent terrorist attacks.
  If necessary I want to report the person showing suspicious behavior in order to ensure the safety of the people using the transport network, mainly by timely measures like evacuation.
- ***Public transport operator staff (TRENORD):*** As a train operator staff member I want to identify a person travelling through the transport network using technologies like the ticketing system, RFID tracking, Bluetooth, WiFi or personal features tracking in order to find the person showing suspicious behavior.
  As a train operator I want to track a person that is travelling through the transport network using video tracking technologies like CCTV in order to find out if they plan to harm people or infrastructure.
- ***Municipal authority (Municipality of Milan):*** As a community I want to track a person that is travelling through the city using video tracking technologies like CCTV in order to find out if they plan to harm people or infrastructure.
- ***Police (Milan Police):*** As the police I want to have access the information systems (like video tracking systems) operated by different organisations (public transport operator, train operator, community) in order to identify and track the person showing suspicious behavior in order to prevent criminality.
- ***Global Control Centre staff (Control Centre):*** As a global control centre staff member I want to centrally access the information systems of other organisations (e.g. video tracking systems) in order to manage emergency situations and to track the person showing suspicious behavior from a field to another one.
- ***Shop owners:*** As a general control centre staff member I want to have the CCTVs of the shop owners to be integrated into my video surveillance network in order to extend my possibilities to track suspicious people.

Targets: The person showing suspicious behavior targets the Malpensa airport.

Threats: Transport of dangerous material (e.g. explosive). This might include:

- The suspect carries dangerous materials in a bag.
- The suspect has upon himself only a few traces of dangerous materials.
- The suspect does not carry anything up to a certain point of the path, in which an accomplice gives him a bag with dangerous materials.

Suspicious Objects: The person showing suspicious behavior is carrying dangerous material. The person can be identified by:

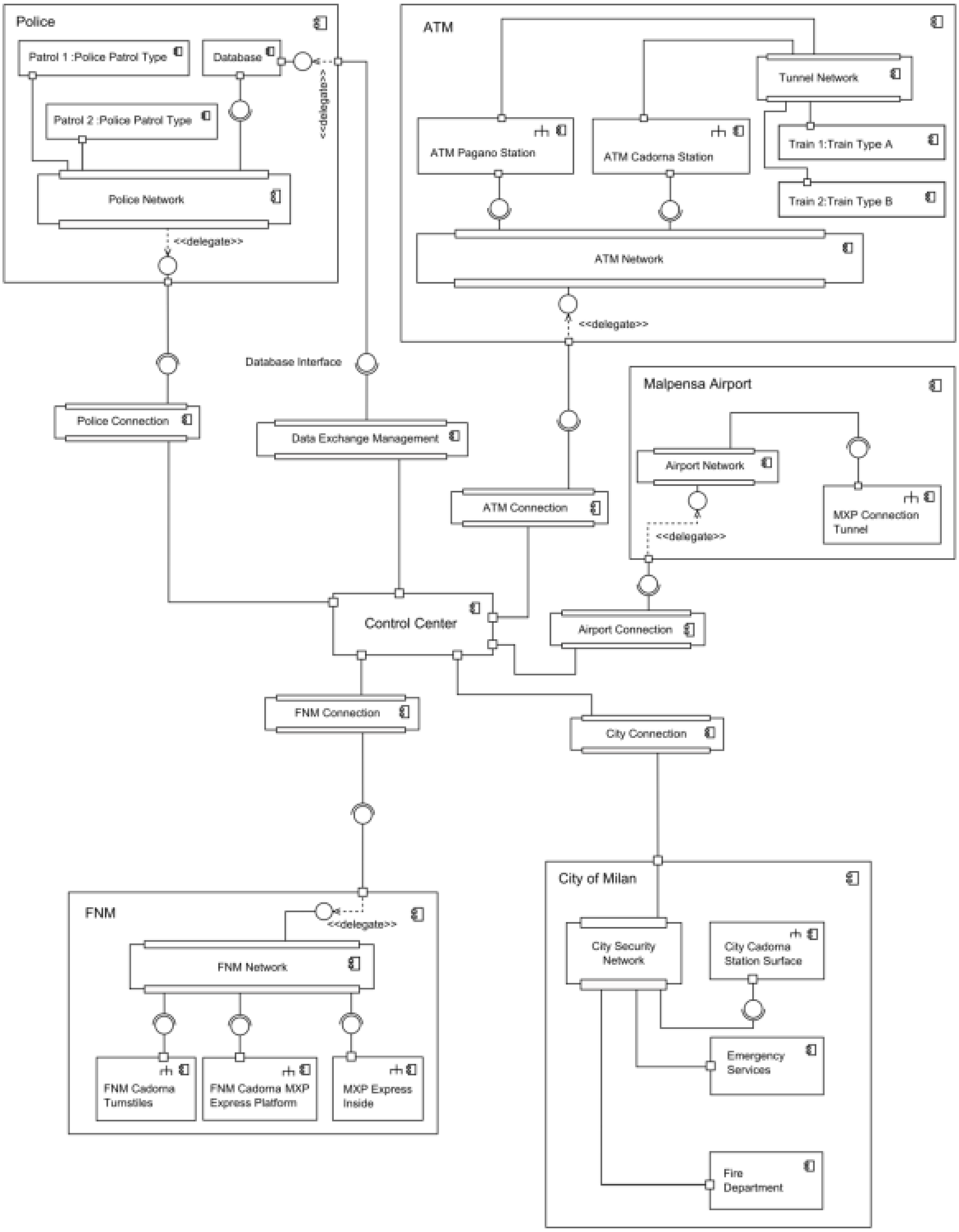
- Does not go immediately to the train.
- Dressed strangely.

- Carrying an unusual bag.

Locations: The person showing suspicious behavior passes the following locations while targeting the airport:

- Pagano station Underground Line 1
- Conciliazione station Underground Line 1 (only in transit)
- Cadorna Underground Line 1
- Cadorna square – Municipality area
- Cadorna railway station (TRENORD)
- Malpensa Express (inside the train),
- Malpensa railway station (TRENORD), consisting of a platform and mezzanine for Malpensa Airport (tapis roulant).

5.1.2 Architecture of Information Systems



5.2 Scenario Madrid 2

The description of the scenario is based on the following documents: [Madrid1], [Madrid2]. The scenario has been selected since several roles and IT-systems are involved, and a clear picture of the expected benefits has been described at an early stage of the scenario definition.

5.2.1 Scenario Description

An insurgent/vindictive/terrorist group decides to perpetrate a sabotage action (explosion) to get media exposure. This causes an operative and physical collapse of the main access of the Moncloa Interchange (BUS-VAO). The interchange has to be closed to traffic. Several people are injured as a bus catches fire. The crisis situation has to be handled according to emergency plans.

Roles and Stories:

- ***Insurgent/Vindictive/Terrorist Group:*** As an insurgent/vindictive/terrorist group I want to perpetrate a sabotage action in order to hurt people and bring disorder to the public life.
- ***Local control centre:*** As the local control centre I want to control the operation of the interchange in order to offer transport services.

  As a Local Control Centre I want to alert the Emergency Services via the incident management system (*GEIS*) in order to activate emergency routines.
- ***First intervention team:*** As the first intervention team I want to check the status of the vehicles in order to begin the work of fire extinction.
- ***Command centre for emergency response (CISEM):*** As the command centre for emergency response I want to activate the contingency plan in order to react to the sabotage act in an ordered way.
- ***Control centre of the public transport operator (CITRAM):*** As the control centre of the public transport operator I want to locate buses through the geographical information system (*SGRAF*) in order to determine the traffic interference after the sabotage act.
  As the control centre of the public transport operator I want to share information of closed interchange with the supervisor of the public transport authority of Madrid (*CRTM*) and the virtual crisis cabinet in order to enable them to react to the emergency situation.
  As the control centre of the public transport operator I want to send a message to the travellers through the passenger information system (*SGIP*) in order to inform them about the emergency situation.
- ***Supervisor of public transport authority of Madrid (CRTM):*** As the supervisor of public transport authority of Madrid I want to be informed about the emergency situation in order to be able to react appropriately.
- ***Management centre of the operating office of the state traffic (DGT):*** As the management centre of the operating office of the state traffic I want to operate the bus interchange (*BUS-VAO*) in order to fulfil the customers' transport needs.

As the management centre of the operating office of the state traffic I want to be informed about the current status of the transport operators in order to react to emergency situations.

- ***Suburban bus operator:*** As a suburban bus operator I want to be informed about the closing of the bus interchange (*BUS-VAO*) in order to inform my drivers and customers.
- ***Suburban train service (RENFE):*** As a suburban train service I want to be informed about the closing of the bus interchange (*BUS-VAO*) in order to inform my drivers and customers.
- ***Control centre of the urban bus transport operator (EMT):*** As the control centre of the urban bus transport operator I want to be informed about the closing of the bus interchange (*BUS-VAO*) in order to inform my drivers and customers.
- ***Control centre of the metro system:*** As the control centre of the metro system I want to be informed about the closing of the bus interchange (*BUS-VAO*) in order to inform my drivers and customers.
- ***Sanitary services (SAMUR):*** As the sanitary services I want to take care of injured people in order to save their lives.

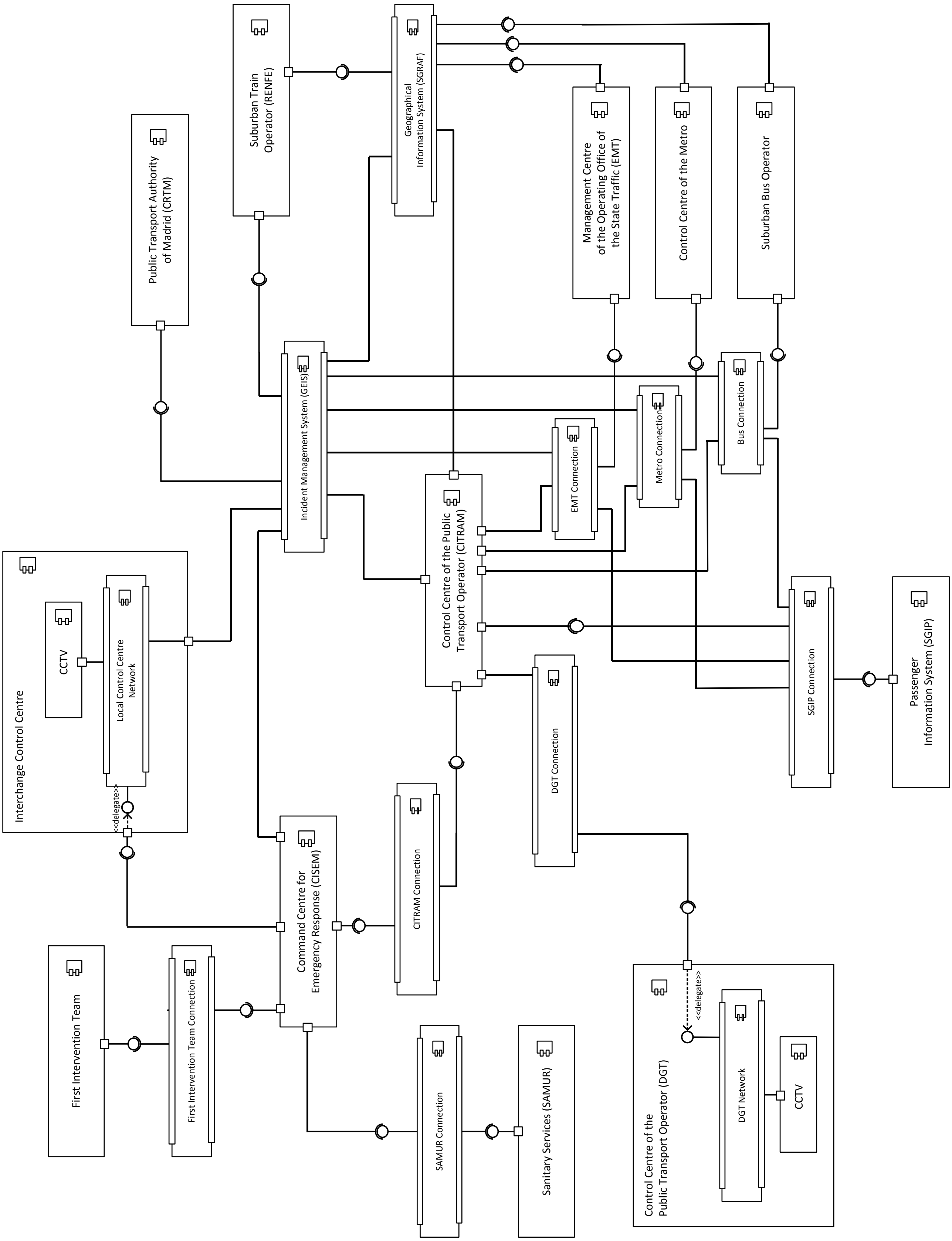
Targets: Main access of the Moncloa Bus Interchange (*BUS-VAO*)

Threats: Due to the collision, the bus suffers severe damage and is on fire. It is considered that there are injured passengers. Multiple collisions occur in string between buses circulating immediately behind.

Suspicious Objects: None

Locations: Moncloa bus interchange consists of several islands with bays for buses, connections to the Metro and a shopping and passenger services area. The sabotage occurs in the curb next to the Interchange Control Centre in heavy commuter traffic.

5.2.2 Architecture of Information Systems


Suburban Train Operator (RENFE)
Geographical Information System (SGRAF)
Public Transport Authority of Madrid (CRTM)
Management Centre of the Operating Office of the State Traffic (EMT)
Control Centre of the Metro
Suburban Bus Operator
Incident Management System (GEIS)
Bus Connection
Metro Connection
EMT Connection
Control Centre of the Public Transport Operator (CITRAM)
Interchange Control Centre
CCTV
Local Control Centre Network
<<delegate>>
SGIP Connection
Passenger Information System (SGIP)
DGT Connection
CITRAM Connection
Command Centre for Emergency Response (CISEM)
First Intervention Team
First Intervention Team Connection
SAMUR Connection
Sanitary Services (SAMUR)
Control Centre of the Public Transport Operator (DGT)
<<delegate>>
DGT Network
CCTV

5.3 Scenario Paris 5

The description of the scenario is based on the following documents: [Paris1], [Paris2].

5.3.1 Scenario Description

A perpetrator performs a toxic attack by leaving hand luggage at the departure platform of a metro station and flees with a train (based on scenario 2). This situation causes serious harm to the people waiting on the platform. The aim of the scenario is to succeed in tracking the previously identified perpetrator, to succeed in investigating and hypothesizing his next action and to apprehend him before he escapes or can take further actions.

Roles and Stories:

- ***Perpetrator:*** As a perpetrator I want to place a toxic bomb on the departure platform in a metro station ("La Défense") after using the delivery entry in order to harm people and cause chaos.

  As a perpetrator I want to flee without being identified or tracked in order to escape my punishment.
- ***Security staff of the public transport operator (RATP):*** As the security staff member of the public transport operator I want to do a video analysis of the recorded images in order to identify the potential risk and the perpetrator.

  As the security staff member of the public transport operator I want to watch the recorded video of all stations in order to find out where the perpetrator leaves the means of transport (metro train, RER (regional train), bus).

  As the security staff member of the public transport operator I want to do real-time video tracking of the perpetrator in order to localise him in the crowd and apprehend him.
- ***Security Staff/First Responder:*** As security staff/first responder I want to find and arrest the perpetrator in order to prevent him from escaping.
- ***Police:*** As the police I want to do video analysis of public CCTVs in order to re-identify and track the perpetrator.

  As the police I want to arrest the perpetrator in order to prevent him from escaping.

Targets: Perpetrator targets an undefined group of people on the departure platform of a metro station ("La Défense").

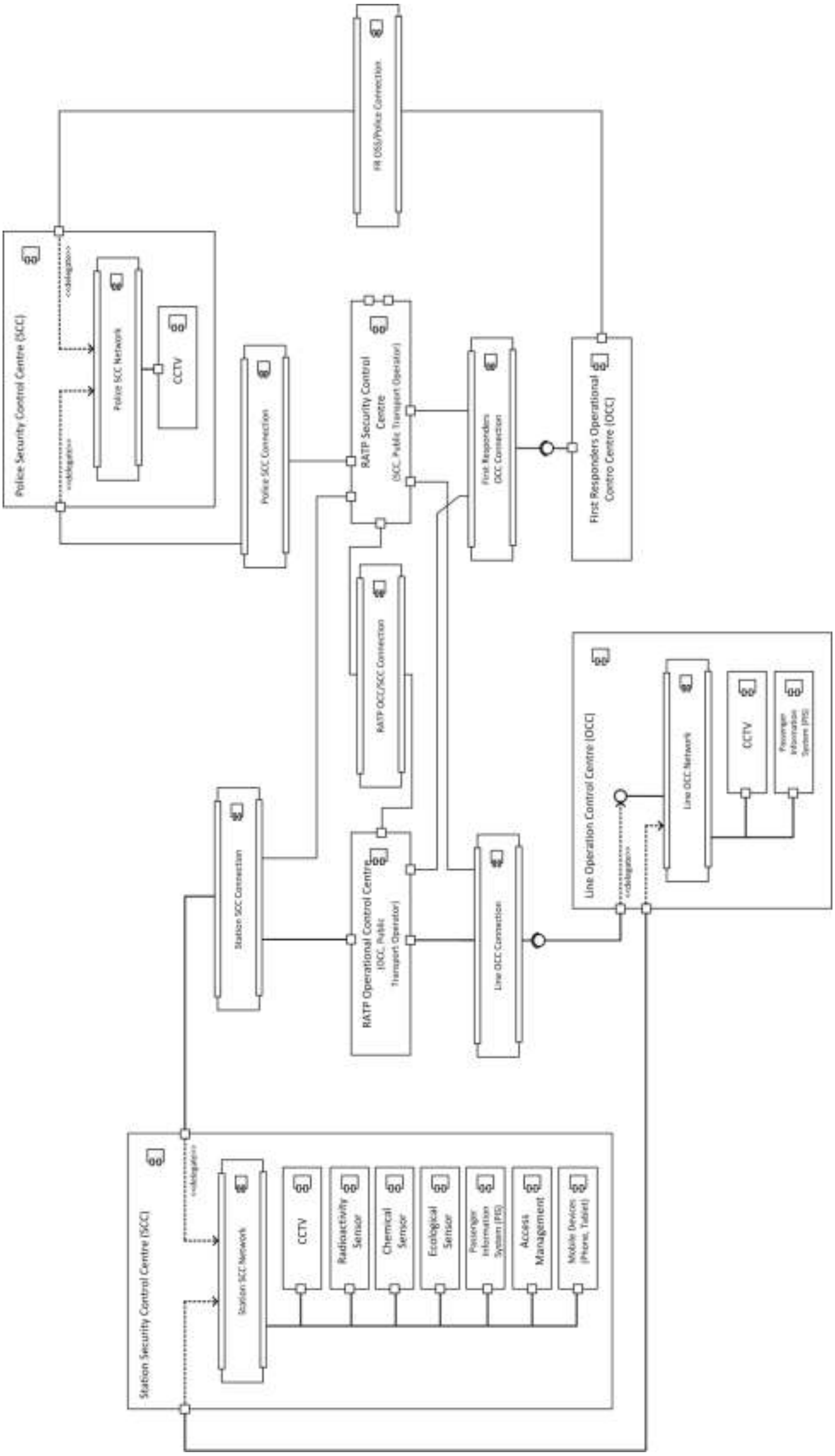
Threats: Toxic attack with a bomb containing TIM (toxic industrial material) gas.

Suspicious Objects: A hand luggage that is left on the departure platform of a metro station.

Locations:

- ***Departure platform of metro station "La Défense":*** The metro station where the toxic attack is performed. The perpetrator takes a metro line to "Châtelet".
- ***Metro station "Châtelet":*** The perpetrator leaves the train and takes the RER B to the south.
- ***Luxembourg train station:*** The perpetrator leaves the RER train and takes the bus n° 89.
- ***BFM (metro station "Bibliothèque François Mitterand") bus stop:*** The perpetrator leaves the bus.

5.3.2 Architecture of Information Systems


FR OSS/Police Connection
Police Security Control Centre (SCC)
<<delegation>>
Police SCC Network
CCTV
<<delegation>>
Police SCC Connection
RATP Security Control Centre
(SCC, Public Transport Operator)
First Responders OCC Connection
First Responders Operational Contro Centre (OCC)
RATP OCC/SCC Connection
Line Operation Control Centre (OCC)
Line OCC Network
CCTV
Passenger Information System (PIS)
<<delegation>>
Station SCC Connection
RATP Operational Control Centre
(OCC, Public Transport Operator)
Line OCC Connection
Station Security Control Centre (SCC)
<<delegation>>
Station SCC Network
CCTV
Radioactivity Sensor
Chemical Sensor
Ecological Sensor
Passenger Information System (PIS)
Access Management
Mobile Devices (Phone, Tablet)

6 Interoperability Lessons Learnt from the Demonstrations

The challenge of combining a large variety of technological and procedural security solutions in a large scale demonstration lies in the technical integration of the various systems and in the ability to combine the strength of these devices in a global and coherent system. With this in mind and putting interoperability at the centre of the SECUR-ED global objectives, an important emphasis was put in the different demonstrations on the application of interoperability standards, models and formalisms.

While the adoption of the interoperability mind-set proved to be effective in the different demonstrations, many lessons were learned applying the concepts that are quite valuable if a similar exercise is to be attempted again. They are here structured into project process, subsystems, interoperability challenges, perceived benefits and training considerations.

1) Project process

- Use of interoperability notations, syntaxes and semantics facilitated the communication between the different partners, which proved to be quite valuable in a European project involving many different stakeholders from different cultures. The PTOs preferred to use BPMN instead of UML, as they interpret the term ‘interoperability’ for their business process rather than to their IT environment.
- Since multiple possible interoperability standards exist and are documented and available, obtaining a consensus between multiple stakeholders on the approach to adopt proved to be difficult to achieve.
- The concept of interoperability being considered by many as abstract and because of differences in the technical backgrounds of the involved partners, an important informal training activity was required to ensure all parties have the same level of knowledge.

2) Subsystems

- The geographical information subsystem, although it contains and has the possibility to generate a large amount of information to exchange between subsystems, was easily integrated with other systems.
- The security subsystem currently providing the highest level of standardisation and normalisation, video protection, proved to be the hardest to integrate in the system-of-system solution.

3) Interoperability challenges

- Adoption of the interoperability framework required for the different partners providing solutions to adapt or modify their existing systems, this transition was considered difficult and time consuming for the industrial partners providing end node peripherals that are simple in nature.
- One of the criticisms often attributed to the use of interoperability standards when integrating systems is its vulnerability to cyber-attacks. The different demonstrations did not provide substantial evidence that this threat is addressed in the applied model.
- Some evidence suggests that the maintenance of a system-of-system solution might be more difficult to manage than for a closed solution, integration of system maintenance aspects should therefore be included in the interoperability application.

- Many questions were raised related to the use of cloud computing in the demonstrations to facilitate the interoperability between systems such as the security vulnerability it represented, the operational cost of this approach and the control over intellectual properties.

4) Perceived benefits

- Although the adoption of the interoperability philosophy was clearly beneficial for the industrial partners, integration heterogonous solutions in the different demonstrations, the added value was not obvious for the public transport operators.
- The railway community is considered traditionally conservative, since they are concerned with critical safety issues as a daily part of their operation. Therefore they double-check the investments, benefits and side-effects of new solutions carefully before implementing them even in a demonstration environment.
- Some evidence suggests that measuring the operational performance of a system-of-system solution might be more difficult to achieve than with a closed solution, integration of performance management aspects should therefore be included in the interoperability framework.
- Information exchange progress steps made possible by the adoption of interoperability methods might infringe on specific norms, laws or national regulations, extra care is required to evaluate these potential infringements.
- If reaching higher levels of interoperability is possible, such as pragmatic, dynamic or conceptual interoperability, this approach could be used to extend the concept outside the public transport network to first responders, public authorities and government entities.

5) Training considerations

- The use of an interoperability framework naturally favoured a more computerized solution and more abstract concepts. This often is done in the wording of IT-integrators, but not necessarily understandable for PTO. Thus, adapted training is required for operators, both for their IT-experts and for their IT-managers.
- The different training sessions held in the demonstrations were not included in the interoperability framework. It would have been interesting to include them in the approach.

Although the lessons learned in the large scale demonstrations can mostly also be applied to the additional satellite demonstrations, specific lessons were learned in these demonstrations related to the scalability of the interoperability framework:

- The additional demonstrations were very effective in adopting the interoperability framework, this raises questions about the effective scalability of the approach;
- The adoption of an interoperability framework seemed more adapted to large public network operators or groups that can more readily provide resources with the required technical background.

7 Interoperability Recommendations

These recommendations are "best practices" or "guidelines" for methods, materials, or practices towards an easier and better implementation of interoperability. The recommendations address public transport operators, industrial system providers and integrations as well as politics and governments to enforce a higher level of Interoperability, based on a more general understanding. This chapter builds on good practice used in SECUR-ED. Use of any or all elements of a recommendation is discretionary; it may be used as stated or modified by the user to meet specific needs.

These recommendations mainly concern the writing of specifications as the basis for interoperability where there is a clear expectation that these documents are precise enough to ensure that their applications are interoperable. In other words, these recommendations apply when interoperability is a matter of correct or consensual interpretation of the specification. Specification should be understood as an exact description of the particular needs to be satisfied, or essential characteristics that are required (in a good, material, method, process, service, system, or work) and which must be delivered. Specifications are written usually in a manner that enables the parties (and/or an independent certifier) to measure the degree of conformance.

Unfortunately often, specifications mix two aspects:

- If the specification is about a communication protocol (technical interoperability) (e.g. a transfer protocol, an interface) and about the behaviour of processors of this protocol, then interoperability is understood as the ability of two implementations of this specification – i.e. processors of this protocol – to communicate properly.
- If the specification is of an artefact (e.g. a business document, a process definition, a policy contract), then interoperability is understood as the ability to process this artefact with consistent results (semantic interoperability).

A large part of the confusion about Interoperability can be summarized by the question: Which aspects of interoperability fall under (a) authors responsibility, and (b) users responsibility? Too often interoperability problems arise when each party (the specification authors, the user) is over-reliant on the other party to ensure interoperability. This guideline is intended to point at the following most common interoperability traps that specification authors could avoid, or could help users avoid: readers, tests, errors, versions, options, references, extensibility and backward compatibility.

A) Readers

Who are the readers of the specification? If this is only the club of experts who spent years together coming up with a consensus on how to do business in a specific area, then the specification can be interpreted as a Memorandum of Understanding: every word conveys a well understood meaning in the club that does not need be further detailed, given the common background and domain culture of the authors (the club members). But if the specification must be read by implementers, end-users (e.g. operators), test developers or product developers who may not fully share the author’s background and expertise, then interpretation mistakes or liberties will abound.

Best Practice:

- It is best to assume that your readership will have different backgrounds. Think of the graduate intern who may have to implement it and does not have your domain culture. This will be even more likely if your standard is widely published, adopted and translated in a foreign language. Being too explicit or repetitive does not hurt – this is not the same thing as being too verbose.
- Define a glossary of terms used that gives them precise meaning in the context of this specification. Do not hesitate to use terminology definitions from elsewhere, and repeat it. Do not hesitate to redefine common terms used with a specific meaning in your context. If some unspecified features or behaviours are delegated to referenced specifications, state this explicitly and don't assume this is obvious to the readers.

B) Tests

You need to provide at least hints on how some specification requirements might be verified, otherwise test suite writers will interpret your statements as they wish, or may just ignore them. It will not be until systems are in production, that those conformance discrepancies – and therefore interoperability problems – are discovered. If there is no way to test some requirements, then conformance and interoperability hangs solely on the interpretation of your words by implementers.

Best Practice:

- Ideally, the "testing perspective" should be added to a specification in the form of a list of test assertions. These could be provided in a companion document.

C) Errors

Too often, the causes of errors (e.g. time-outs in programme loops) that an implementation may experience are insufficiently identified and covered in a specification. Errors are also a communication item in addition to drawing a clear line between expected and unexpected behaviour of features. Yet they have low priority on the agenda of authors, when the schedule is tight. Proper definition, standardization and reporting of errors are important aspects of interoperability.

Best Practice:

- A specification should include an “Errors” section that describes a list of errors. Each error type should be clearly identified, and an appropriate error message defined. For every specification requirement, it should be clear which error type applies in case of failure.
- Details about how the error is reported or transmitted may be left open. However, when several parties are involved, it is recommended to also specify:
  - Expected behaviour of a device / implementation when receiving an error notification from another device,
  - Expected behaviour of an implementation after generating such an error as the result of processing a faulty artefact.

D) Versions

Version and revision numbers of the used specification should be readily accessible for all users. Not doing so will invariably cause misunderstandings and interoperability issues over time. One may wonder: isn't that mostly an implementation issue? Only partly so: while it is the responsibility of an implementation to announce in some way which version(s) of specification(s) it supports (see the well-known “-v”-option in many command-line software tools). The specification should help make the version information that is associated with an artefact easy to access by an implementation. And when two implementations communicate, they also need a (standard) way of accessing version information about each other.

Best Practice:

- Whenever a specification concerns an artefact that is to be exchanged between devices or is portable across devices, the version information (including Revision #) should be associated in some way with this artefact, i.e. either appear in the artefact itself or be communicated on demand or prior to the exchange using other (specified) means. In Extensible Markup Language (XML) artefacts, a different namespace and/or a schema may be associated with each version or revision. However, this technique may not always prove practical and could generate unexpected constraints. An explicit version/rev element is often the best way to convey version information in artefacts, as well as a distinct command or option in processors.

E) Options

The optional character of a specified feature, when concerning an artefact that may be produced and consumed, is a common source of confusion and interoperability failure. An artefact MAY implement a feature. This clearly means that a compliant device producing such an artefact MAY omit this feature. However, any compliant device consuming such an artefact MUST be able to process this feature, should it be present (unless specified otherwise). This is the intention of the definition of the MAY/OPTIONAL keywords as stated in [RFC2119] (although this subtle interpretation is not explicit enough for SHOULD/ RECOMMENDED).

Best Practice:

- Add a section in your specification that could be titled: “General Rules for Normative Interpretation” and that clarifies how the usual ISO or RFC keywords that indicates optionality (OPTIONAL, SHOULD, RECOMMENDED, MAY…) should be interpreted from the viewpoint of a compliant artefact vs. of a processor of this artefact. It is also good practice to identify at the beginning of your specification, what are the main conformance targets that will be addressed.

F) References

Specifications refer to each other, and compose with each other. For example, a protocol layer will operate above another protocol that is defined in another specification. Or, some interface used in combination with another interface. Often the specification writer wishfully assumes a “black-box” or perfectly modular composition, and ignores the “corner cases” (error escalation, mismatched features) leaving the details to users. The degree of variability introduced by such compositions is then underestimated. As a result, users may interpret differently how the composition is supposed to operate. The composition of implementations of these specifications is a separate issue that will depend on engineering choices - but still predicated on how precisely the composition of these specifications has been specified.

Best Practice:

- For specification writers: When a specification S1 “uses” another specification S2 with the intent of not depending excessively on S2 (i.e. keeping the possibility to replace S2 with S3 later on), it is good practice to gather in a single section everything that concerns the details of composing S1-S2. This is the case of “Bindings” sections often found in appendix. This requires the addition of new error types, or the capability to “escalate” or interpret errors from the other specification. Such composition details could also be defined in subsequent, separate profiles. In any case, it should be expected that new bindings or profiles will be added over time, so it is wise to not overly tie the specification of the composition itself with the main specification body.

G) Extensibility

Extensibility makes it possible to extend either the specified artefact or the functions of a specified device. A common mistake is for specification writers to treat extension points in their specification as customization hooks that are fully out of scope and the usage of which they have no responsibility for. As a result, these extension points may be used and interfere with the core specification in ways that were not foreseen, and cause unexpected interoperability problems.

Best Practice:

- While extensions are out of scope of a core specification, how to handle failures to support an extension is not. How to gain awareness of extensions used by a partner implementation must also be considered by specification writers. How an implementation is expected to react to an unrecognized extension must also be described. If extension points should not /cannot be used to override the default feature or behaviour, this should be clearly stated. If it can override it, the specified feature should be worded to allow so (e.g. "...unless extension XYZ is used to indicate otherwise"). It is good practice to “flag” every extensibility point in a specification, e.g. in an appendix, as a possible interoperability hazard. The same precaution as for optional features applies.

H) Backward compatibility

A standard is said to allow backward compatibility, if products designed for the new standard can receive, read, view or process older standards or formats. Or, it is able to fully take the place of an older product, by inter-operating with products that were designed for the older product. [Forward compatibility (sometimes confused with extensibility) is the ability of a system to gracefully accept input intended for later versions of itself. The introduction of a forward compatible technology implies that old devices partly can understand data generated by new devices.] Assume your new specification version is not backward compatible – in general, an embarrassing fact you'd prefer users to not ask about. Yet the worse thing to do is to avoid talking about it, hoping no one will notice – which may indeed be the case in the very unlikely event where everyone migrates at the same time to the new version. Users will implicitly assume backward interoperability, and they are on their way to be disappointed and angered.

Best Practice:

- Describe precisely what are the non-backward compatible features, and on the public relation side, explain in an FAQ why it wasn’t possible to preserve compatibility. A section describing the "diff" from V(n) to V(n+1) will greatly help users of the new version to understand what they can and cannot reuse from their implementation of the previous version.

8 Conclusions

WP22 tackled concept, notation, syntax and semantics of interoperability in the urban public transport domain. It spanned a conceptual area from security threats to interactions between different stakeholders and the usage of information systems, covering IT-generic and IT-solution-specific challenges of data structures and understandable information in different contexts.

The interoperability notation enables public transport operators and system integrators to model and reflect how relevant information exchange activities can be principally supported in a system-of-systems architecture, i.e. which systems and interfaces are used, and how the approach supports use cases and business scenarios. The interoperability notation has been mainly used within WP22, but not in the SECUR-ED demonstration preparation, which mainly applied local variations of the process oriented BPNM notation. The reflection about the complementarity of both the business process (BPMN) and the technical (UML) notation has been a valuable discussion line within SECUR-ED.

The system integration challenge of combining a variety of technological and procedural security solutions in a large scale demonstration lies in the technical integration of the various systems and in the ability to combine the strength of these devices in a global and coherent system. In the different demonstrations, the application of interoperability standards, models and formalisms therefore played a major role. While the adoption of the interoperability mind-set proved to be effective, lessons were learned related to the management of the project process, challenges of different subsystems, overall interoperability challenges, perceived benefits and training considerations.

The final interoperability recommendations therefore provide guidelines for authors and readers of interoperability specifications. Based on the experiences within SECUR-ED, suggestions are provided to handle relevant topics for interoperability specifications such as readers, tests, errors, versions, options, references, extensibility and backward compatibility. These general considerations should help the stakeholders in public transport security to better communicate about the details of interoperability, which are depending on involved technologies, existing systems, business interests and legal context. In the end, these interoperability considerations aim to improve the security oriented procedures of the operators and thus the security of passengers and staff.

- End of Document -