Interoperability for Information Systems in Public Urban Transport Security: The SECUR-ED Interoperability Notation

Johannes Sautter
Fraunhofer IAO
johannes.sautter@iao.fraunhofer.de

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

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

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

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

ABSTRACT

In public transport and at large urban hubs, such as metro or train stations, transport operators and first responders collaborate in the prevention of and reaction to security issues. Within the EU demonstration project SECUR-ED a specific notation for interoperability of information systems in the domain of public transport security was developed. (In this context, the interoperability of actual operating systems is not the focus.) Based on UML (Unified Modelling Language), the notation language offers the possibility for structured modelling of system-of-systems architectures. Four interoperability object templates and their interdependencies form the underlying basis. Domain-specific annotation rules and guidelines for interoperability objects and their sub-component structures allow collaboration and interpretation of this model on various granularities and stages during a systems engineering process.

Keywords

Interoperability, Security, Public Transport, UML, Notation, SECUR-ED

INTRODUCTION

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 in the reaction to security issues. They use heterogeneous information and communication systems that are optimised for their specific daily operational business needs. Some of these systems mainly or partly also serve security purposes (Engelbach et al. 2011).

At the same time, recent events have demonstrated that public transport can be subject to various security incidents and outcomes may be severe due to the large number of passengers (Roßnagel and Junker 2010; Smith and Clarke 2000). In case of such incidents it is crucial that the various involved parties exchange relevant information to get a common operational picture (which is the same view on a current situation combined with a shared understanding) and act in a coordinated way in critical situations (Dantas and Seville 2006). However, heterogeneous communication and information system infrastructures often hinder this crucial flow of information (Engelbach et al. 2011; De Laurentis et al. 2007).

SECUR-ED (Secure Urban Transport – European Demonstration) is an EU FP7 Security demonstration project that brings together 39 European partners from different backgrounds in public transport and civil security from operators, first responders, industry and research. Being a demonstration project in four major urban European cities – Madrid, Paris, Milan and Berlin – security enhancing technologies and systems will be put to practice and demonstrated; additional tests will be conducted in several cities such as Brussels, Lisbon, Istanbul and Bucharest.

A major challenge will be to demonstrate the consistency of those security solutions since the different stakeholders do not necessarily share the same understanding of threats, relevant information and IT-

interoperability. Moreover, societal and legacy concerns define a very diverse environment of mass transportation in the states and cities across Europe (UITP 2010).

Therefore, (Engelbach et al. 2011) and (Kurowski et al. 2012) developed a concept that fulfils among others the requirement to be simple enough for a broad common understanding, to be abstract enough for the application in organisational and technical application and to be flexible enough to be used in different cities and implemented in different existing systems and technologies.

This paper shortly describes a notation based on this concept that integrates some modelling conventions in the usage of the modelling language UML (Unified Modelling Language) and utilises well-founded security-specific knowledge. In the following we first discuss related work, and then provide a specification of our interoperability notation. Subsequently, we discuss our results and provide an outlook on how the notation will be used before we conclude our findings.

RELATED WORK

ISO defines interoperability as "the capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units" (ISO 1993). The conceptual interoperability model by (Turnitsa 2005) offers a classification of different interoperability capabilities by defining 7 different levels of interoperability. Level 1 describes the technical interoperability. On this level two systems are able to connect. They may share the same protocol and are able to communicate. However, simply having a connection does not yet ensure that two software applications are able to interpret the data shared. This is achieved by sharing the same format or being able to understand each other's' data format, hence exchanging information. If this state is reached the level of syntactic interoperability is fulfilled. Semantic interoperability extends this requirement, by adding the interpretation of data, ensuring that the applications share knowledge instead of information. On this level applications are for instance. able to localize the information exchanged, allowing communication even with different glossaries or languages. Pragmatic interoperability enables the participating systems to be aware of each other's procedures and routines. Systems realizing dynamic interoperability even consider other systems assumptions and constraints, enabling them to be aware of state changes which may occur during or as a result of the communication. Finally, level 6 describes the interoperability of systems' concepts, requiring all systems to be fully specified and independent from their respective implementations. This requires full documentation of conceptual models, enabling interpretation by other engineers (Turnitsa 2005).

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 information systems in the field of public mass transport, several conclusions on involved roles, communication, sensor systems and general structures of collaboration can be made. Thereof aspects from the following fields are considered as relevant to public urban transportation: incident ground collaboration, sensor systems, concept of operation, field level security plans, interfaces with other organisations and current situation in mass transport security. These results are an essential source for the identification and description of relevant rules and guidelines for the notation described in the subsequent sections. For a detailed discussion on relevant security aspects in the field of urban mass transportation please refer to (Kurowski et al. 2011, 2012).

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) (Dalgarno and Fowler 2008). We aim to combine both of these approaches by relying on a proven general purpose language in UML that we enrich with domain specific guidelines for the annotation of the components.

THE SECUR-ED INTEROPERABILITY NOTATION FOR INFORMATION SYSTEMS

The aim of our interoperability concept and notation 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 notation has to be able to document organisational settings like hierarchies within or across organisations as well as threat and security clearance levels (Engelbach et al. 2011). Our concept enables system designers to model a system of system architecture by defining interoperability objects and their relations and supports the structured documentation of security relevant information by providing guidelines for annotation.

Interoperability Object Templates

Information system: An information system is an entity which processes and stores data and has a specified dependency to its environment. In urban transportation a single sensor system as well as an organisational entity like a whole train station can be considered as an information system (Engelbach et al. 2011). Within our notation, such a system is realized as an UML-component with an optional component icon (see Figure 1a).

Figure 1 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 transportation, we offer a mechanism 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.

Role: 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 1b). Figure 2 illustrates a role, which uses two information systems. As depicted the "<<use>>"-identifier keyword may be left away.

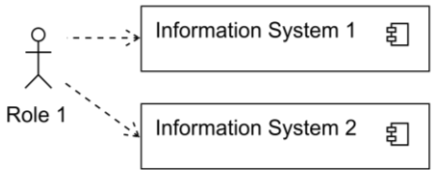

Figure 2 Simple infrastructure diagram showing a Role using two Information Systems

Interface: In terms of the SECUR-ED Interoperability Concept an interface is a gateway that allows interaction between several information systems (Engelbach et al. 2011). We offer two alternatives 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.

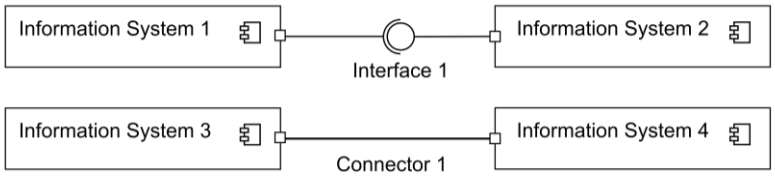

Figure 3 Interfaces notated as UML interface and UML connector

The setup outlined in Figure 3 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" (Born et al. 2004). 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.

Intermediary: An intermediary in the sense of the SECUR-ED Interoperability Concept is a specific information system that serves the sole purpose of supporting the interaction between other information systems (Engelbach et al. 2011). We represent the intermediary using a special-notated UML-component which has always two notated complex ports on top and on bottom (see Figure 1c). 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.

Guidelines for Annotation

An interoperability notation that is tailored to the domain of public transport security must of course provide guidelines on how to document security relevant information in a complete and structured form. In order to achieve this we conducted an extensive survey of relevant European projects and synthesized them on a homogenous level of abstraction (Kurowski et al. 2011). Based on these insights we elaborated detailed guidelines for annotating interoperability objects, their relations and the overall context (Kurowski et al. 2012). 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 paper.

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"

DISCUSSION AND OUTLOOK

General-purpose concepts to describe decomposition, delegation and recurring components from the Unified Modelling Language have been utilized and specified by classifications for the security domain. Furthermore, the strict separation of concerns regarding roles, information systems, interfaces and intermediaries is a benefit in direction of the organisational and technical implementation of the modelled infrastructure. The notation is flexible, can address different levels of detail and provides the ability to describe information in a structured manner where necessary and in an unstructured textual annotation where appropriate. In first presentations and discussions, the involved operators and suppliers have been able to understand the concept and the modelled infrastructure. As UML (respectively the extension SysML) is widely established in the environment of system engineers and for instance intermediaries as technical broadcast units are clearly separated, a well-founded base for a realization of modelled scenarios without obstacles is given.

Further evaluation based on a validation of the method during the practical application of the notation in the SECUR-ED demonstration scenarios in major European cities including Paris, Milan, Madrid and Berlin are foreseen. Those steps will be executed in close cooperation with all relevant stakeholders, including transport operators and systems suppliers. Further steps building on our results that will be taken within the project are to add more details for syntax (interface methods and data formats) and semantics (behaviour complementary to structure).

CONCLUSION

The SECUR-ED interoperability notation for information systems 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 proof beneficial in practice. It may also help to simplify the comparative evaluation of achievements in the involved demonstration cities and to support the transfer of innovative or established solutions from one information systems environment to another one. Further evaluation, such as validation during usage in practical implementations will follow within the project.

ACKNOWLEDGMENTS

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

REFERENCES

1. Born, M., Holz, E., and Kath, O. 2004. *Softwareentwicklung mit UML 2*, (1st ed,).
2. Dalgarno, M., and Fowler, M. 2008. "UML vs. Domain Specific Languages," *Methods & Tools* (16:2), pp. 2.
3. Dantas, A., and Seville, E. 2006. "Organisational Issues in Implementing an Information Sharing Framework: Lessons from the Matata Flooding Events in New Zealand," *Journal of Contingencies and Crisis Management* (14:1), pp. 38-52.
4. 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.
5. ISO. 1993. *ISO/IEC 2382-1:1993 Information technology - Vocabulary - Part 1: Fundamental terms*, .
6. Kurowski, S., Zibuschka, J., Roßnagel, H., and Engelbach, W. 2011. "A Survey of Interoperability Concepts for Security Systems in Public Transport," In *Proceedings of the Conference on Mobility in a Globalised World*Presented at the Conference on Mobility in a Globalised World, Iserlohn.
7. 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.
8. De Laurentis, D., Dickerson, C., DiMario, M., Gartz, P., Jamshidi, M. M., Nahavandi, S., Sage, A. P., Sloane, E. B., and Walker, D. R. 2007. "A Case for an International Consortium on System-of-Systems Engineering," *IEEE Systems Journal* (1:1), pp. 68-73.
9. Roßnagel, H., and Junker, O. 2010. "Evaluation of a Mobile Emergency Management System: A Simulation Approach," In *Proceedings of the 7th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2010)*Presented at the ISCRAM 2010, Seattle, WA, USA.
10. Smith, M. J., and Clarke, R. V. 2000. "Crime and Public Transport," *Crime and Justice: A Review of Research* (27), pp. 169-233.
11. Turnitsa, C. D. 2005. "Extending the Levels of Conceptual Interoperability Model," In *Proceedings IEEE Summer Computer Simulation Conference*.
12. UITP. 2010. *Secure Public Transport in a Changeable World*, UITP.