A SCALABLE OPEN MONITORING PLATFORM ENVIRONMENT FOR RISK MANAGEMENT

Raimar J. Scherer [1] and Gerald Faschingbauer[2]

ABSTRACT

Handling crises requires making decisions, based on sufficient knowledge about the situation. New developments in ICT enable to make the existing capacities of data and information usable in order to provide decision makers and task forces with the knowledge necessary for taking decisions as quickly as possible and hence to reduce response times considerably. Today, risk management systems are proprietary client server systems developed for particular hazards and specific scenarios, i.e. they are not open and scalable. Recent approaches have extended these client server systems to ASP technology. However, these application services, platforms and sensor systems are built on their own infrastructures, islands of functionality that cannot be easily shared and integrated in one logically common but distributed environment. In this paper we will present a concept for a novel ICT environment for a dynamically optimized management of emergency and crisis situations generated by natural hazards and industrial accidents focused on the estimation of the actual constitution of engineering structures based on sensor data and engineering models. The main idea is a Scalable open Monitoring Platform Environment which will deliver a sustainable approach for ICT-based integration and information computing and which can improve management and logistics in the aftermath of hazardous events. The architecture of the platform environment is modular and extendable, immediately available and highly distributed: this can be accomplished by the integrated combination of four main "state-of-the-art" and high potential technologies: (i) GRID technology for enhanced distributed data management and computation, (ii) Semantic Knowledge Technologies (SKT) to manage smart optimization of generalized novel risk management ontologies, (iii) intelligent self-adapting sensor networks for smart access to local information resource, combining in-situ sensors as well as human observers ("human sensors"), and (iv) Virtual Organisation / Concurrent Engineering paradigms so as to deal with multidisciplinary and dynamic work environments with multi-stakeholder involvement, that are required for monitoring of very different structures.

KEY WORDS

Risk- and Crisis Management, Platform Environment, Decision Making.

[1] Professor, Institute of Construction Informatics, Dresden University of Technology, 01062 Dresden, Germany, Phone +49 351/463-32966, FAX +49 351/463-33975, Raimar.J.Scherer@cib.bau.tu-dresden.de

[2] Scientific Assistant, Institute of Construction Informatics, Dresden University of Technology, 01062 Dresden, Germany, Phone +49 351/463-34262, FAX +49 351/463-33975, Gerald.Faschingbauer@cib.bau.tu-dresden.de

INTRODUCTION

In the aftermath of hazardous events the main goal is to save as much lives as possible. The enormous time pressure demands an all-embracing quick overview of the serviceability of the civil infrastructure, i.e. the usability of traffic lines, lifelines and essential buildings, e.g. hospitals. The necessary information can be gained from sensor data, measured at the structure. Because sensors deliver only raw data, a complete risk management system needs integration of two principal groups of components: (1) the sensor systems acquiring data that are the recorded physical facts, and (2) the application of engineering evaluation models, together with the expert knowledge to deduce information of the possible consequences from the sensed raw data. These information allow also the estimation of the remaining structural safety. The sensing and monitoring process is an embedded phase in the overall risk management process cycle shown in Figure 1. This novel ICT-based risk & crisis management model abstracts on the high-level the risk & crisis management process into 4 major status nodes where human decisions are taken beginning with sensing and continuing with information concentration towards crisis decision-making and proceeding with target-oriented information distribution to task forces and rescue teams later on. Four directed ICT-enabled processing edges represent the stepwise transition “data → information → knowledge → actions” and the change of responsibilities and actors involved. At each node new goals requiring a different focus are set up and a mapping between different data models corresponding to the different mental models of actors occurs.

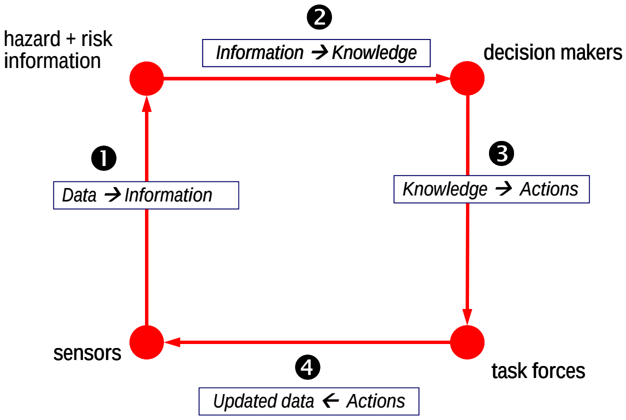

Figure 1: ICT-based Risk & Crisis Management Model

In this contribution we will restrict ourselves to the sensing and monitoring process, i.e. the deduction of hazard & risk information from the raw data from sensors, which are nowadays available for many specific measurements. They enable a time-continuous monitoring and analysis of the structural condition and thus an early recognition of changes of the structural conditions and hence derivation of remaining capacity. To date, there are a few sensor nets dedicated to public hazard monitoring, and some more operated by private or public companies, especially in the lifeline domain. However these sensor nets will most probably be growing fast in the future and hence monitoring environment technology should be (1) scalable, (2) secure and (3) already prepared to cope with the expected huge amount of sensor networks and processing work load. Furthermore in the case of a hazardous event in a mega-city the number of affected structures extends the limits which are manageable by the local engineering personnel. So an additional essential for a monitoring system is the ability to collaborative work of a large number of specialists who are spread over a wide area.

The open problem is still the combination of computation, monitoring and analysis of structures, i.e. the synthesis of the different data from different sources of information prepared by multi-physical sensor systems. This problem, which will increase with increasing number of sensors in the near future, requires a novel ICT approach. Some ideas that can help tackle such problems to raise online-collaboration on high level have been developed in the EU project ISTforCE "Intelligent Services and Tools for Concurrent Engineering." They are described in (Turk & Scherer 2001). The concept of a platform environment which is based on the ISTforCE platform and which will be presented in the following will enable the integration of distributed, multi-physical data, with supply of GRID arithmetic performance and the derivative of information on the basis of engineering models.

PRINCIPAL APPROACH

The main idea for the ICT based risk management concept is the platform environment, shown in Figure 2 that should be comprised of several logical platforms specialised from one generic ICT platform and inter-connected on the basis of semantic grid services complying with one common environment ontology.

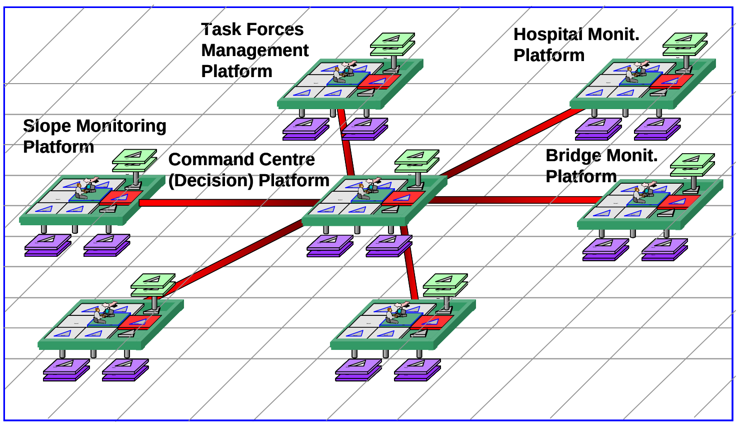
Task Forces Management Platform
Hospital Monit. Platform
Slope Monitoring Platform
Command Centre (Decision) Platform
Bridge Monit. Platform

Figure 2: Example Configuration of the Platform Environment showing the Technical Connection through the GRID and the Logical Connection of the Command Structure

This integrated platform environment should be able to (a) handle dozens to several hundreds of sensors systems (with growing numbers towards thousands on the long-term), with several dozens or hundreds of sensors each, which have to be processed and managed concurrently, (b) incorporate and utilise the know-how of several experts who should be able to process the sensed data concurrently in order to deduce valuable and reliable information about the monitored objects in their responsibility, (c) process seamlessly and efficiently the thousands of continuously updated and refined information items, representing different views of damage and hazard consequences, different quality and reliability, and different perceptions (in particular by human sensors), and manage them into one integrated information space and (d) present the synthesised high level hazard and risk information to end users and decision makers on appropriate semantic level, together with various capabilities allowing them to easily manage, protect, discover and verify this information according to specific models. The specific demand on the platform environment is the interoperability, the structuring, the availability and the efficient delivery of the information, and hence the requirements towards the management of that information, e.g. who is allowed to store information about which issues, how this information is verified and according to what models.

The roles and functionalities of the separate platforms of the platform environment shown in Figure 2 must be determined in accordance with the four phases of the risk & crisis management cycle (see Figure 1), which defines the organisational structure of the environment. The monitoring platforms, which are logical units, will be responsible for interpreting the sensed data by using formal (usually engineering) models verified by expert teams. Thus, the monitoring platforms provide an additional natural grouping mechanism reflecting the ability and the knowledge of the involved experts. Therefore, basically only domain-specific monitoring platforms are reasonable.

With this principal approach, each monitoring platform can be seen as a *logical unit* consisting of three inputs and one output.

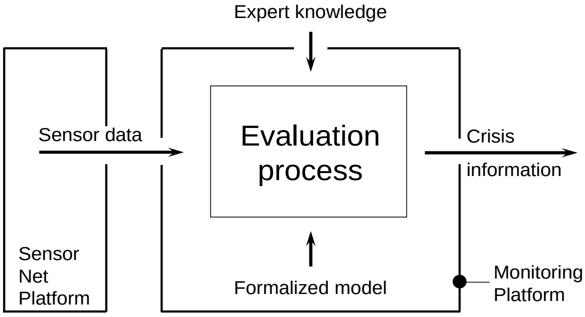

Figure 3: System Sketch of a Monitoring Platform

The formalized model is pre-defined and hence represents formalisable expert knowledge that is generally and automatically applicable. All expert knowledge about the model to transfer/interpret the data sensed is neither easily nor sufficiently formalisable. Therefore the formalized model has to be complemented by human expert knowledge, which leads to the logical definition of a generalized monitoring platform consisting of two logical units, namely:

1) One or several sensor net platforms without a permanent expert operating,
2) A monitoring platform for evaluation purposes, typically with an expert operating permanently.

The sensor net platforms only collect data, whereas the monitoring platforms give the sensed data a meaning. With this structuring, efficient operation of the overall environment will be achieved, combining the essential command, control & communication methods of risk management with appropriate principles adopted from VO and concurrent engineering methodology.

Often the formalized model can be structured in nested and/or parallel sub-models and hence the evaluation process too, however with different reliabilities. If it is possible to identify problem-dependent sub-models incl. automatically controlled variations, which are so much saturated or simple that they are considered fully reliable, then they can be applied to the related sub-tasks without expert interaction and verification, i.e. they can always be applied automatically. With the growing “intelligence” of sensor units more and more such sub-models, i.e. evaluation can be delegated to those sensor platforms. With the support of agents, this can even be done dynamically, e.g. for different operation modes, like alert, pre-warning, response, preparation, etc. These sub-tasks may be very simple tasks, like reduction of sampling by computing mean value at time window or computing Fourier, Power or Response spectra and selecting from them only a few amplitudes which may be mean values of certain frequency bands or combining two or more data sensed like evaluation of the amount of gas per time from sensed valve opening, gas temperature and gas velocity and communicate only the evaluated data, the gas flow instead of the three sensed ones.

GENERIC PLATFORM

The core of the platform environment will be provided by the generic RM platform. This platform can be extended and specialised in the various forms needed for the targeted facets of the RM cycle. As already mentioned, it is first of all a logical unit, enabling the logical grouping of RM information and services for certain specific needs.

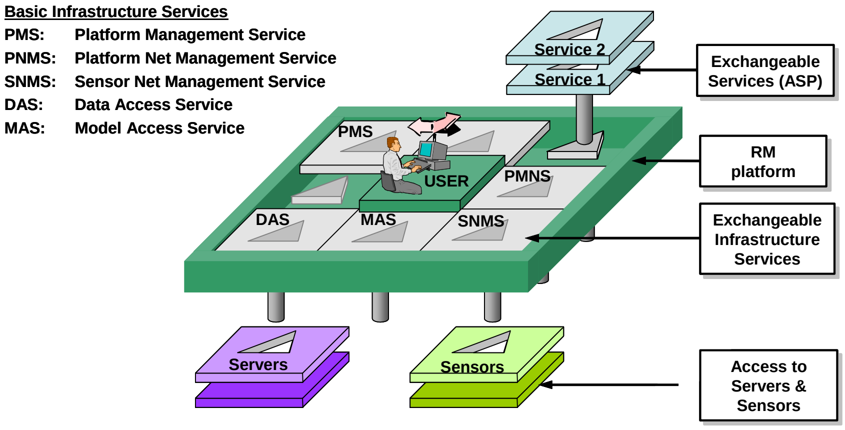
Basic Infrastructure Services
PMS: Platform Management Service
PNMS: Platform Net Management Service
SNMS: Sensor Net Management Service
DAS: Data Access Service
MAS: Model Access Service
Service 2
Service 1
Exchangeable Services (ASP)
PMS
USER
PMNS
RM platform
DAS
MAS
SNMS
Exchangeable Infrastructure Services
Servers
Sensors
Access to Servers & Sensors

Figure 4: Overview of the Generic Platform

The generic platform has two operation modes. First, it has to operate fully automatically with lower reliability or vice versa less detailedness/granularity using default values in order to quickly deliver results for alerts, pre-warning or very fast response demands, like first estimate of new or changed situation. Second, it has to operate under the guidance of an expert for high reliability, high detailedness/granularity. The sophisticated expert knowledge of human experts is needed – and this has to be applied very fast and goal-oriented. One of the biggest challenges when utilising a distributed infrastructure lies in porting existing models and applications onto the new grid-based environment without significant user effort or deep understanding of grid computing principles. Therefore, one common feature supported by all platforms of the environment should be a set of easy-to-use interfaces to capabilities offered by infrastructure grid services and technologies in order to facilitate deployment and remote control of RM models as well as cross-platform secure data exchange. Grid services and protocols will provide seamless access to other remotely available sensor, monitoring and information platforms. They will also support secure incorporation of legacy RM models and tools located in many geographic distributed platforms. This will limit significantly the need for maintaining and controlling remote legacy RM models and improve the data flow among computing units.

Nevertheless, an efficient platform management providing access to any data model and analysis tool is demanded. This is the objective of the **P**latform **M**anagement **S**ervice (PMS), managing the logistics of the selected and actual, logically combined application services and tools of the particular platform. It will be responsible for finding, configuring and launching all other infrastructure and user-related platform services, as well as for the secure user/services authentication and authorisation. Security/authentication/authorisation issues will be tackled with the help of the underlying basic grid middleware services. The necessary higher level semantics will be provided on top of available basic open-source ontology services, e.g. from the Jena framework.

From the generic platform any kind of particular specific RM platform can be deduced and instantiated. Due to the **P**latform **N**et **M**anagement **S**ervices (PNMS) any network of platforms can be established (see Figure 2). Whereas the Grid manages data and software storage as well as computing, the PNMS service manages the logical inter-connection with the other platforms of the RM environment. In particular, secure data file transfer, authorization, remote job execution, work load distribution etc. will be based on grid technology, whereas interoperability and management of the inter-platform information flow from organisational and contextual point of view will be provided by the general environment ontology services. The platform-to-platform communication has a hierarchical structure, corresponding to the RM cycle command & control structure.

The direct access to those sensor nets that have to be directly processed by the platform will be managed by the **S**ensor **N**et **M**anagement **S**ervice (SNMS). This service is needed to provide direct and fast access to the sensor net platforms and the related sensor nets, and to govern the sensor net platforms, i.e. to manipulate and reconfigure them remotely whenever necessary and possible. This can proceed automatically by means of software agents or manually by experts. In addition, the SNMS will also provide remote access to the GUI of the sensor net platforms to re-configure the sensor nets remotely.

All data sensed are stored – appropriately condensed – in a secure and safe storage on the Grid and are always accessible. The access will be managed by the **D**ata **A**ccess **S**ervice (DAS), capable of accessing data represented in XML and described according to different schemata as long as the descriptions are provided, too, e.g. as simple DTD or semantically richer XML Schema, RDF or OWL specifications. This is of high importance for the identification of damages, because system identification is based on observed changes in the object behaviour from two different monitoring campaigns, namely pre-hazard and post-hazard monitoring. Because of the non-uniqueness of the inverse problem of system identification, often several pre-hazard campaigns have to be used and hence fast access to several pre-measurement campaigns is necessary.

The **M**odel **A**ccess **S**ervice (MAS) manages the access to various models, like the engineering behaviour model, the perception model of the monitored/observed objects and also the models of the later steps, like the consequence models. Because real-structure objects or systems are often complex and multi-physical problems, the established model is only a kind of hypothesis and the models are adjusted to the measurements by the inverse problem. Hence there is never one single model but a variety of models with slight to strong variations in the crisis phase. These variations of models have to be accessed in a fast, secure way and easy to be manipulated to get high reliability of the information evaluated and the conclusions drawn, i.e. provide bandwidth and worst-case estimates. The service provides model access services being capable of accessing a group of alternative models and parts of models that are represented in XML data format and described by different schemata, like STEP or IFC. Each model may be allocated on another server and groups of models are dynamically and logically defined on high level by the end user via a risk management ontology.

All components of the platform can be dynamically configured and distributed on the Internet. They will be managed by a middleware layer comprising a set of appropriate grid-enabled infrastructure services. Hence, any application service or engineering application tool can be optionally plugged-in to the platform and can be selected individually, e.g. using ASP technology.

ARCHITECTURE OF THE GENERIC RM PLATFORM

As mentioned above, the generic RM platform is the heart of the whole environment. It consists of 4 layers (Figure **5**), built upon a basic Grid infrastructure layer.

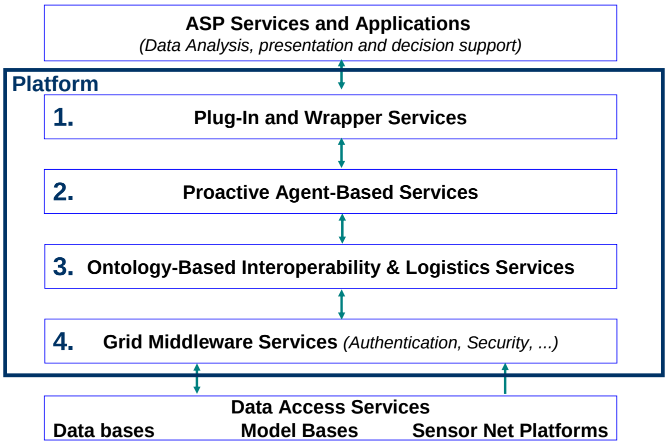
ASP Services and Applications
(Data Analysis, presentation and decision support)
Platform
1. Plug-In and Wrapper Services
2. Proactive Agent-Based Services
3. Ontology-Based Interoperability & Logistics Services
4. Grid Middleware Services (Authentication, Security, ...)
Data Access Services
Data bases
Model Bases
Sensor Net Platforms

Figure 5: Architecture of the Generic Platform

The **GRID middleware layer (Layer 4)** provides the technical integration of the RM platforms. This includes generic and specific services for single-sign-on, authentication and authorisation of people as actors in the environment, secure communication, access to heterogeneous resources etc. Moreover, these services will provide the necessary flexibility to support dynamic network configuration by enabling ad hoc addition/removal of components and point-to-point communication. This will fully eliminate communication bottlenecks of server-based solutions and, more importantly, provides the necessary prerequisite to construct a largely self-organising network. Through the Grid middleware services parallel and controlled access to the full range of available computational resources will be warranted, thereby enabling real-time execution of sophisticated analysis tasks that would otherwise not be possible.

The ontology-based interoperability and logistics services (Layer 3) provides the semantic layer of the environment. It will enable the separation and subsequent controlled inter-linking of 'technical' Grid semantics and risk management semantics. For that purpose, a novel risk management specific ontology will be needed, preferably based upon the OWL format and inter-linked by utilising concepts like namespaces with a general-purpose Grid ontology that will adapt and extend related specifications from recent and current RTD work. The risk management ontology has to serve two distinguished objectives, namely (1) the interoperability on the high semantic level of data information models, services, environment components, and (2) the organizational issues of the environment or the technical level, namely the logistics of services, selected and configured to a platform and the controlled access to these services depending on time, status of the evolving/devolving crisis and so on.

The agent-based services (Layer 2) provide facilities for proactive access to data, information and services. Agents can be used for three purposes: (1) as proactive interface to sensors, in order to pull and process data whenever it is available and not wait until it is requested, (2) for the interface between the sensor platforms and the RM service platforms, and (3) for search and retrieval of information about monitored objects which is not pre-determined by the ontology, e.g. to support task forces on site in various unexpected situations by providing ad hoc data from various initially unconsidered resources. The agent layer is not mandatory for the principal functionality of the environment, but it enhances its functionality and, more importantly, facilitates faster processing which can be a time-critical issue in a number of cases. Use of software agents typically involves commitment to a common ontology. Therefore the added value of this layer will be achieved with comparatively low effort by making use of the ontology layer 3. Moreover, there exist already basic agent systems which provide generic Grid interfaces, which can additionally facilitate the software realisation.

At last, **the plug-in and wrapper services (Layer 1)** provides a generic API for interfacing various tools and risk management services provided by third parties and used in ASP business modus on the basis of Web Service technology. Access to these services can be realised by means of state-of-the-art specifications and tools (WSDL, SOAP) whereas communication and message semantics will be ensured by respective ontology constructs. The wrapper services will have the task to "translate" risk management ontology concepts to standard SOAP queries that can be interpreted by a third-party (legacy) tool and thereby provide the bridge between basic Grid services and the various risk management analysis and decision support tools. Wrapper services will also be used to achieve proactive data and information storage and retrieval, as well as active notifications and broadcasting. For this purpose the software agent paradigm can be applied on this layer as well for the creation of wrapper agents.

ARCHITECTURE OF THE GENERIC SENSOR NET PLATFORM

A sensor net is the logical sum of tens or hundreds (or more) of sensors, usually logically structured around an object to be monitored and may be further sub-structured in mutually independent sub-systems. Each sensor net is a logical unit and hence has to be managed by a sensor net platform, which provides the functionality of the sensor components, sub-systems management, security, authentication, dynamic changing adaptation, operation on different pre-defined modes and show self-healing capabilities. Each component (sensor services, operation modes, etc.) can be identified in the GRID and hence become part of the GRID. This results in the same structure of basic layer (see Figure 6) as for the generic platform outlined above.

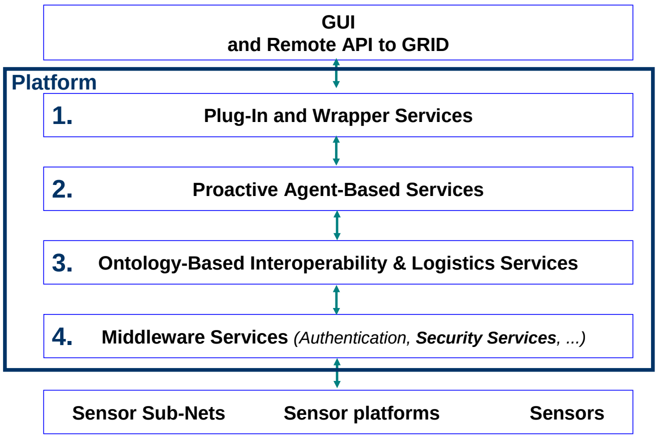
GUI
and Remote API to GRID
Platform
1. Plug-In and Wrapper Services
2. Proactive Agent-Based Services
3. Ontology-Based Interoperability & Logistics Services
4. Middleware Services (Authentication, Security Services, ...)
Sensor Sub-Nets
Sensor platforms
Sensors

Figure 6: Architecture of the Sensor Net Platform

Therefore a sensor net platform is an instantiation of the generic platform as well as all other platforms in risk management environment. However the sensor net platforms do feature some specific functionality. For instance, a sensor net platform is usually operated in the automatic modus and hence has to have very robust components and services. It does not require a comfortable GUI but a remotely operable interface to be operated by monitoring platforms. Each sensor net platform may show some individual functionalities, which may be provided by the delegation principle either through services or agents application. However, due to the requirement of robustness and high reliability in case of a hazard event some or most of these functionalities have to be coded on the sensor net platform resulting in mutually different (instantiated) platforms. Therefore several specific sensor net platforms corresponding to the specific monitoring platforms may be instantiated from a generic class sensor net platform.

CONCLUSIONS

The concept of a risk management platform environment which will enable combination of computation, monitoring and analysis of structures has been described. This platform environment will enable the integration of distributed, multi-physical data, with supply of GRID arithmetic performance and the derivative of information on the basis of engineering models. The key component of the environment is the generic platform which can be instantiated to problem specific monitoring platforms and sensor net platforms. The integrated platform environment would be able to handle dozens to several hundreds of sensors systems and incorporate and utilise the know-how of several experts in order to deduce valuable and reliable information about the monitored objects which can be synthesised and presented as high level hazard and risk information to end users and decision makers on appropriate semantic level. The interoperability, the structuring, the availability and the efficient delivery of the information would improve the efficiency of rescue measures after hazardous events considerably.

REFERENCES

Gehre, A., Katranuschkov, P. & Scherer, R. J. 2004. *Agent-enabled Peer-To-Peer Infrastructure for Cross-Company Teamwork*. In: Dikbas, A. & Scherer, R. J. /eds./ Proc. "ECPPM 2004 – eWork and eBusiness in Architecture, Engineering and Construction", Istanbul, 8-10 Sept., Balkema, ISBN 04-1535-938-4, pp. 445-452.

Gehre, A., Katranuschkov, P., Stankovski, V., Scherer, R.J. 2005. *Towards Semantic Interoperability in Virtual Organisations*, In: proceeding of cib-w78 2005 22nd Conference on Information Technology in Construction, Scherer R.J, P. Katranuschkov & S.-E. Schapke (ed.);CIB Publication, ISBN 3-86005-478-3, pp. 307-314, July 2005.

Gómez-Pérez, A. /ed/ 2002. *A Survey on Ontology Tools*. Deliverable 1.3, EU Project OntoWeb, IST-2000-29243, 96 p.

Guarino N. 1998. Formal Ontology and Information Systems. Amended version of a paper in Guarino N. (ed.) *Formal Ontology in Information Systems*. Proc. of FOIS'98, 6-8 June 1998, Trento, Italy, publ. by IOS Press, Amsterdam, the Netherlands, pp. 3-15.

Katranuschkov, P., Gehre, A. & Scherer, R. J. 2003. *An Ontology Framework to Access IFC Model Data*. ITcon Vol. 8, p. 413-437, ISSN 1400-6529. http://www.itcon.org/2003/29

Katranuschkov P., Scherer R. J. & Turk Z. 2001. Intelligent Services and Tools for Concurrent Engineering - An Approach Towards the Next Generation of Collaboration Platforms. *ITcon Vol. 6, special issue: Information and Communication Technology Advances in the European Construction Industry*, http://www.itcon.org.

Katranuschkov P., Scherer R.J. & Turk Z. 2002. *Multi-Project, Multi-User, Multi-Services Integration: The ISTforCE Integration Approach.* In ECPPM 2002 - eWork and eBusiness in Architecture, Engineering and Construction, Turk Z. & Scherer R.J, (ed.); A.A. Balkema, 2002

Miller, E. 2003. *Weaving Meaning: Semantic Web Applications*. Presentation at INTAP, November 11, 2003, Tokyo, Japan. http://www.w3.org/2003/Talks/1117-semweb-intap/

Turk Z. & Scherer R. J. 2001. Towards the next generation of civil engineering collaboration platforms. In: *Proceedings of the eBusiness and eWork 2001 Conference*. Venice, Italy.