Risk Characterization and Prototyping

Mariagrazia Fugini
Dipartimento di Elettronica e Informazione
Politecnico di Milano
Milano, Italy
fugini@elet.polimi.it

Claudia Raibulet, Luigi Ubezio
Dipartimento di Informatica, Sistemistica e Comunicazione
Università degli Studi di Milano-Bicocca
Milan, Italy
raibulet@disco.unimib.it, ubezio@gmail.com

Abstract—The paper proposes a characterization of risk and a service-oriented prototype to face emergencies situations in industrial environments. We outline the technological features of a risk environment and a service system aimed at improving safety in workplaces. To achieve this goal we overview technologies and discuss engineering issues related to risk modeling. A prototype architecture of a Risk Management System is presented, composed of layered services able to detect (corrective behavior) and to prevent (pro-active behavior) the occurrence of risk conditions in work contexts.

Keywords—risk management; emergency; service; layered architecture; risk prevention technology; sensor networks; event services.

I. INTRODUCTION

Sensor networks and wearable service technologies are promising ways to monitor and interact in physical environments to detect and react to risky situations in industrial work places [14]. Sensor and devices in a distributed system communicate environmental data regarding workers and machines from and on distributed nodes, and respond to asynchronous events communicating risky situations. Data of interest can be pre-registered to the sensor network so that the corresponding data is collected and transmitted only when needed. These functions can be treated as services because they communicate the data according to the application’s data semantics and shield the overwhelming volume of raw data from applications. To date, not much research has been performed on real-time data services in sensor networks. Despite their similarity to conventional distributed systems, sensors and software services for empowering the individuals’ lives in work areas have to exhibit real-time capabilities, and applicability in the outside space, such as in work areas, which still present a high risk of accidents. In particular, in industrial areas the most serious damages are caused by falls and by use of transportation means and machinery. The existing rules and laws prescribe the use of garments suitable for accident prevention such as jackets, shoes, or glasses. Nevertheless, the requirements for sensor networks and wearable services providing the necessary technology to signal dangerous situations are increasing continuously. This is also due to what is expected from a smart environment for security in workplaces [1, 2] which may exploit components and services [3].

The related solutions available in the literature concern both wearable devices and service-oriented approaches [4, 5, 9, 10, 12, 13]. In ambient intelligence [4], compatible enabling hardware is adopted, including fully optical networks, nano/micro electronics, sensors, RFID, software agents, affect computing, or brain–machine interfaces. Wearable objects are technologies involving efforts to create natural human interfaces i.e., supporting natural gestures and non-intrusive communications, including also socio-technical design factors, supports for human-to-human interaction and the analysis of societal and political developments in terms of stakeholders needs [5]. To enhance wearable objects, meta-content services can be developed [6] to improve information handling, knowledge management and community memory, involving techniques such as smart tagging systems and Web Services technologies. Considering Web Services in real-time applications, [7] presents a project about the application of Web Services technology in distributed real-time data delivery systems, and identifies the appropriate contexts in which such a design can be considered. The Service-oriented Device Architecture (SODA) [8] is realized through various technologies (OSGi, UPnP, DPWS, REST) and Web Services. Embedded hardware is often excluded from the deployment of Web...
Services because of the lack of resources like computing power and memory.

The paper is organized as follows. Section II introduces engineering issues for risk management through services. Our risk modeling approach is presented in Section III. Architectural issues are illustrated in Section IV, while the simulation environment is described in Section V. Concluding remarks and future developments are given in Section VI.

II. ENGINEERING IN SERVICES FOR RISK MANAGEMENT

Technological aspects related to risk management regard the possibility to implement a full-fledged distributed and flexible system. A first engineering issue concerns risk modelling of the work environment and of the events that can create dangerous situations requiring an immediate reaction. Moreover, preventive actions should be set in place so that the system behaves in a pro-active way [15]. A second engineering issue regards the technology available for risk management, which have been developed for the following categories: 1. Health monitoring: wearable objects. 2. Distribution of ambient sensors. 3. Identification and positioning.

1. Technologies for users’ health have seen many progresses through wearable objects [16], such as shoes, gloves, or clothes, which constantly monitor vital parameters (blood pressure or heart beating), evidencing anomalies and generating alarms in case of illness. Applied to industrial environments, the technology inserted in wearable objects permits an addition of functions that make the user perceive a higher usefulness and protection level. In this paper, we do not deal with design of such objects but consider them as available as described in [15]. Considering that an innovative RMS needs to exhibit both reactive (to react to risks) and proactive (to prevent risks) modalities, wearable objects need to be constructed around user profiles in terms of parameters such as age, role, and health status. The RMS has to be able to suggest which objects have to (mandatorily) be worn to provide an adequate protection to the user, and which services should be activated on the object to collect useful data to generate alarms in case of danger.

2. Considering distribution of ambient sensors in highly dangerous environments, the computation of the person’s risk level at a given time implies the need to have an instantaneous detailed knowledge of such environment. A technology allowing to cover large areas, both open and in door, and in a capillary way, allowing to capture any potential problems, is the technology of Wireless Sensor Networks (WSN). These are based on the Sensor Node, as a generic term for a set of small devices studied to permit the observation of the physical world. The interconnection of nodes occurs via radio technologies and a protocol-based architecture enabling the cooperation between different entities. This amplifies exponentially the capacities of single elements and paves the way to a wide set of new applications, among which control of industrial work areas. The main drawbacks of this technology are the limitations posed by the battery and the reduced dimensions of such device which origin constraints on the dimensions of the energetic support. Further developments have reduced the energetic consumption obtaining a life of up to 6 months for such sensors. Another problem regards privacy and security since the communication between sensors and the back end system occurs in a wireless mode with no assurance on data privacy, since the impact of data cryptography on the battery would be a serious problem. WSN can be coupled with wearable applications such as healthcare monitoring, intelligent cities, and vehicle management.

3. Identification and positioning may be tackled through different techniques among which the Radio Frequency Identification (RFId), and Ultra Wide Band (UBW) systems, and generally embedded tags with communication capabilities both towards the person wearing them and towards the servers’ area. From a technological viewpoint, tags can be used for different purposes, depending on their characteristics. The classification proposed in [11] proceeds according their power supply, distinguishing among Active Tags, which integrate batteries and transceivers; Passive Tags, which reflect the radio signal coming from an antenna or a reader and send it back adding information by modulating the reflected signal; Semi-Passive Tags, namely a hybrid solution. When the device is excited by the antenna radio beam, a tag sends back a signal powered by the internal battery. Workers entering the work area must wear the correct equipment according to which they have an associated worker’s risk level. The fulfilling of this requirement can be easily checked by tagging the objects to be controlled. Additionally, the work area can be partitioned in subareas classified at different environment risk levels.

Regarding real-time control of risk, the technologies should support the identification of the position of each worker and machinery at each moment. The fundamental technologies for such aim are GPS, EGNOS and GALILEO, and ULTRA WIDE BAND (UWB) technology [17]. In closed environments, hybrid technologies can be employed, combining UWB impulses with Wireless Routers. Positioning technologies are compared in Table I, while a basic set of used technologies in some categories of applications in summarized in Table II.

The benefits of a Service Oriented Architectures (SOA) are support to the design of a layered, distributed and flexible system able to incorporate new components easily. However, service technology cannot be implemented at all system levels (from design to implementation/deployment), due to integration and performance problems mainly at the implementation level where hard-coded solutions often need
In this paper we consider an overall service approach, assuming that some mechanisms will then be non service oriented, such as software hard-coded on devices or implemented in embedded systems.

The RMS is provided as a set of individual services that manage risk levels. The idea of modeling through services is bound to a uniform approach to all the levels of system lifecycle, where various system components as well as the environment and the persons can be seen as elements communicating via message exchange. Although at the implementation level various physical components (e.g., hardware, devices, sensors) might not have actual services on board, due to performance reasons, a uniform message exchange paradigm is useful for the standardization, cooperation, and interoperability. In this sense the service-oriented approach must be intended latu sensu, as a conceptual paradigm to identify relationships among different system elements: the effective/real implementation of such a paradigm does not imply the complete adoption of a full fledged service-oriented model. In practice a concrete RMS component, which behaves as a Service, could be set up, for optimization purposes, only using hardware components.

The risk level can be coupled with a person and a given device or area; alternatively, a risk level varies with the action the worker performs, and with his location. Therefore, the risk level is either a static measure, associated with an element of the environment, or a dynamically-computed level, associated to a given situational case.

For example, the dynamic level of risk can be controlled via choke points, where it is checked if a worker who is entering an area at a given risk level has all the necessary garments, or, conversely, if the risk level of that area is compatible with the level which the worker is cleared for.

The service layer will have precise purposes according to the peculiarity of the risk level of the work task to be completed. Moreover, the services are useful in that they can archive/record the interaction among different enterprise levels, without considering the heterogeneous platforms and devices so facilitating the gathering of all the collaborative environment information.

### Table I. Comparison among positioning technologies

<table>
<thead>
<tr>
<th>Technology</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS</td>
<td>Widely implemented. Tested and easy to be interfaced</td>
<td>High error (around 20 m)</td>
</tr>
<tr>
<td>GALILEO</td>
<td>Error reduction (around 2 m). Limited costs</td>
<td>High error. Not operative in closed environments.</td>
</tr>
<tr>
<td>UWB</td>
<td>Positioning with low error (30 cm) Low power consumptions.</td>
<td>High costs. Increased error in closed environments.</td>
</tr>
</tbody>
</table>

### Table II. Problems and solutions related to RMS in some categories of applications

<table>
<thead>
<tr>
<th>Problem</th>
<th>Tech. Solution</th>
<th>Pro</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Monitoring</td>
<td>Wearable objects &amp; wearable sensors</td>
<td>Real-time control of health status. Large set of sensors available</td>
<td>Objects should not be cumbersome and should be ergonomic</td>
</tr>
<tr>
<td>Distribution of Ambient Sensors for Ambient Monitoring</td>
<td>Wireless Sensors Networks</td>
<td>Easy implementation of any typology. No need for wiring. Can be wearable sensors.</td>
<td>Short duration of battery and consequent need of maintenance.</td>
</tr>
<tr>
<td>Identification of Objects and Tools</td>
<td>RFId</td>
<td>Widely employed technology. Easy finding of components and devices.</td>
<td>Efficient identification only with passive tags (due to high number of objects). Active tags need maintenance.</td>
</tr>
<tr>
<td>Positioning of Persons and Machinery</td>
<td>UWB + Wireless</td>
<td>Precision of 30cm even indoor.</td>
<td>High costs for acquisition of antenna and collectors.</td>
</tr>
<tr>
<td>Communication</td>
<td>Wireless</td>
<td>Easy message exchange exploiting a consolidated technology</td>
<td>Need full coverage of area.</td>
</tr>
</tbody>
</table>

In such context, for each observation level a different aggregation and presentation of information is needed. For example, when a single production cell is inspected by the RMS all information must be shown to the observer with a convenient granularity level. On the counterpart the same information could make no sense if the abstraction level of observation rises up.

Our goal is to experiment a set of wearable services integrated into a RMS able to prevent the occurrence of emergency/unsafe conditions in work contexts, and we do it through a prototype that we have implemented to simulate a work environment where workers can have mobile or radio devices on which security-related messages can be forwarded after being conveyed to servers. In such RMS, messages are:

1. Notification of a personal risk (e.g., a worker remains for too long inside an irradiation area); 2. Notification of risks/accidents which arose inside an area; 3. Notification of a risk/accident in other areas.

The treated types of alarms related to the above messages allow for dynamic computation of risk related to the instantaneous exposition of a worker to a danger, since they represent risk sources also not directly identifiable as system objects. Upon alarm generation, through messages related to the associated danger (gas, water, fire, etc.), the coordinates of ambient sensors are identified, a unique source is determined and the source coordinates are coupled with those of the alarm. Alarms can be reactive, i.e., after an accident, and proactive, i.e., able to prevent the arising of a
security problem. Table III shows some sample associations between risk events and alarms, identifying also the suitable monitoring technology and the typology of the RSM behavior.

**Table III. Reactive and Proactive Alarms**

<table>
<thead>
<tr>
<th>Event</th>
<th>Monitoring Technology</th>
<th>Alarm</th>
<th>Behavior Typology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gas leak</td>
<td>WSN – Gas Sensor</td>
<td>Gas Alarm</td>
<td>Reactive</td>
</tr>
<tr>
<td>Fire</td>
<td>WSN – Smoke/Fire Sensor</td>
<td>Fire Alarm</td>
<td>Reactive</td>
</tr>
<tr>
<td>Use of tools in dangerous areas</td>
<td>RFID and UWB Positioning</td>
<td>Security Messages</td>
<td>Proactive</td>
</tr>
<tr>
<td>Detection of lowering in heart beating</td>
<td>Wearable Objects</td>
<td>Health Danger</td>
<td>Reactive</td>
</tr>
<tr>
<td>Entry into dangerous areas without protections</td>
<td>RFID and UWB Positioning</td>
<td>Message of Danger</td>
<td>Proactive</td>
</tr>
<tr>
<td>Anomalous movement of a crane</td>
<td>UWB Positioning of machinery</td>
<td>Security Message</td>
<td>Proactive</td>
</tr>
<tr>
<td>Start of work phase in the site</td>
<td>Documentation of phases and competences</td>
<td>Messages on security set up in the areas of the site</td>
<td>Proactive</td>
</tr>
</tbody>
</table>

**III. Modeling Aspects**

**A. Characterizing Risk**

In order to identify the Risk as an entity modeled in the RMS and analytically computed, we first define Risk as a potentially negative effect on a resource (in our case, a person) deriving from ongoing processes or events. Many definitions of risk have been given in various contexts (e.g., economic and financial risk, health risk, accident risks, etc.). For our purposes, we identify risk through some properties reported in Table IV. Although these properties derive from common experience, more details are necessary to apply these definitions to the RMS. Empirically, the risk for a worker is determined by his position in the environment, by the worn protections, by security procedures, and by the presence of dangerous resources. As depicted in Figure 1, a risk element at a given time instant for a given person is computed as the Cartesian product between the person’s properties (i.e., his risk profile deriving from age, skill, experience, role, health status, and employed protections) and a given ambient resource.

**B. Risk Computation**

The risk level (here shortened with “Risk”) for a person at time $t$ is the sum of the single risk elements, obtained from a combination of all dangerous ambient resources present and active at time $t$, namely:

\[
RISK_{PERSON} = \sum_{Risk\_element} (Person \otimes Ambient)
\]

**Table IV. Properties of Risk Elements**

<table>
<thead>
<tr>
<th>Element characterizing risk</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicators</td>
<td>Each risk indicator is proportional to the expected damage.</td>
</tr>
<tr>
<td>Source of Risk</td>
<td>The protection measures are specific for each source of risk.</td>
</tr>
<tr>
<td>Damage</td>
<td>The expected damage (e.g., in money loss) is directly proportional to the entity (e.g., cost) source of risk.</td>
</tr>
<tr>
<td>Damage</td>
<td>The expected damage is inversely proportional to the distance from the source of risk.</td>
</tr>
<tr>
<td>Damage</td>
<td>The expected damage is inversely proportional to the protection measures employed by the exposed persons.</td>
</tr>
</tbody>
</table>

By unifying this definition with the properties in Table IV, we obtain an analytical expression for the instantaneous value of the risk for a person.

\[
RISK_{PERSON} = \sum_{r:Ambient\_R} \frac{P_r \cdot T_r}{D_{pr} \cdot S_r}
\]

where $P_r$ is the dangerousness of a resource $r$, $T_r$ is a coefficient identifying the type of danger of resource $r$, $D_{pr}$ is the distance between the person $p$ and the resource $r$; $S_r$ is a coefficient identifying the security procedures which are in place to prevent the damage provoked by resource $r$.

This analytical form results very useful to identify risk parameters. However, it presents some problems, namely:

- It is difficult to obtain validity ranges for coefficients from experimental data;
- Risk coefficients should not be bound to any other factor in the expression, since the worn protections and the procedures in place should offer a constant
support to the reduction of the risk for a person, independently of his distance from dangers;

- The distance parameter could make risk values oscillate out of the prescribed range. In fact, even short distances can increase the risk to very high levels; although conceptually correct, this could lead to problems during the elaboration of risk formulas.

Most of these problems can be solved through a risk function, modified from what proposed in [18] as follows.

- The security coefficient has been separated from the computation of the actual danger by subtracting a numeric valued depending of the protections used to prevent a damage caused by the considered element.
- The distance has been substituted by a Gaussian coefficient dependent on both the distance from the dangerous source and on the danger type, giving a value between 0 and 1. Such value is multiplied by the dangerousness $P_r$ of the resource in order to smoothen its contribute with the increase of the distance.

Supposing the resource be located in the origin of Cartesian axes (here bi-dimensional for simplicity), the Gaussian distribution is simple enough in that it model the maximal value exactly in the origin of danger and decreases while the distance increases. The distribution of values around the means (i.e., the standard deviation $\sigma$) denotes how flat the curve is, namely how the danger continues to influence the risk value while the distance increases. Such value depends on the type of danger linked to the resource (fire, gas, water, etc.) and hence on coefficient $T_r$. Hence, the coefficient is exactly the standard deviation by which we compute the influence of danger while the distance increases. The higher the standard deviation, the flatter the Gaussian. Finally, such function has been suitably scaled up so that its maximum coincides with point (0,1), allowing the definition of a fixed range of values ([0,1]) for the single risk element as shown in Figure 2.

The new formula of risk for a person $P$ at $t$ is:

$$Risk_{person, P} = \sum_{r:ambient\_resources} \left[ N_\sigma(D_{rp}) \cdot P_r - S_t \cdot B_t \right]$$

where $P_r$ is the danger of resource $r$; $S_t$ is a security coefficient to be subtracted from danger independently of distance (it is a risk rescaling factor); $B_t$ is a Boolean coefficient set to true when a security procedure has been performed to reduce the risk caused by resource $r$; $D_{rp}$ is the distance of person $p$ from resource $r$; $N_\sigma$ is a Gaussian function with means = 0 and standard deviation $\sigma$ suitably scaled to obtain a value in [0,1]; namely, it represents the following function where $T_r$ is our standard deviation:

$$y = e^{-\frac{D_{rp}^2}{2T_r^2}}$$

All the properties in Table IV, namely all the proportional dependencies (direct and inverse) between risk and each of its components, have been maintained. The sum of each Gaussian (having its maximum in $P_r$), scaled of a factor $S_r$, shows the trend of instantaneous risk in each point of the work environment.

**Examples**

Initially, let us assume the position of a worker can vary along a unique linear dimension represented in a Cartesian plan by X-axis. The risk is computed and represented on Y-axis. Assuming to have three dangers along such line at positions -5, 0, and 3 with variances 1, 2, and 5 respectively, the graphical representation in Figure 3 shows the risk curve as a sum of the respective Gaussian curves.

We now apply such method to the case where a worker can move freely in a bi-dimensional area $(x,y)$, i.e., on a plan on which we draw a tridimensional diagram where the Z-axis represents the Risk. We use a Gaussian bi-dimensional distribution having the following expression:

$$f(x,y) = \frac{1}{\sqrt{2\pi} \cdot \sigma_x} \cdot e^{-\frac{(x-\mu_x)^2}{2\sigma_x^2}} \cdot \frac{1}{\sqrt{2\pi} \cdot \sigma_y} \cdot e^{-\frac{(y-\mu_y)^2}{2\sigma_y^2}}$$

Supposing the means $(\mu_x, \mu_y)$ be equivalent to the position of danger and the standard deviation be equal along $X$ and
along Y, we again scale the function and simplify it as follows:

\[ z = e^{-\frac{(x-p_x)^2}{2\sigma_x^2} - \frac{(y-p_y)^2}{2\sigma_y^2}} \]

where \( p_x \) and \( p_y \) are the coordinates of danger and \( \sigma_x \) is the standard deviation. The sum of these Gaussian curves provides a view of the instantaneous risk trend in a bi-dimensional space. Suppose now we have three dangers in positions (-5, -3), (0, 1) and (3, 4) with variances 1, 2 and 5 respectively, the risk tend at a given instant is represented in Figures 4a and b.

![Figure 4a. Single Elements](image)

![Figure 4b. Risk Sums](image)

When the dimensions increase and assuming the worker can move in a tridimensional environment, it is necessary to partition the space into plans and to apply the risk computation to each plan, limiting the computations to the plan where the worker is located.

### IV. ARCHITECTURAL ASPECTS

From a high-level point of view, the relevant elements of an RMS are:

- the environment, which is composed of the physical topology of an industrial context;
- the tools and instruments available in the environment and which may participate actively or passively in a risk or emergency;
- the persons present in the environment, either workers or visitors;
- the devices, which monitor various aspects of the environment, tools, or persons, and which may receive feedbacks from the central system;
- the risks and emergencies, which may occur for various causes, among which the interaction persons-tools, the movement of tools, the health conditions of the persons, the quality and composition of the atmosphere in the environment.

To manage all these concepts, the RMS comprises the following architectural components (see Figure 5):

- an Environment Manager, which gathers all the information received from the environment; it is actually a database, enriched with information-merging capabilities in order to generate connections among information apparently not interconnected;
- a Communication Manager, whose role is to handle all the communications to and from the environment in case of a risk or emergency;
- a Risk and Emergency Manager, which consists of a Risk Detector and of an Emergency Detector, of a Catalog of Risks and Emergencies which can be addressed by the system, the Alarm Generator and the Action Generator through which the system actually manages the risks and emergencies.

![Figure 5. Main Architectural Components](image)

The RMS could potentially contain parts or components which are not fully compliant with SOA approach. In this case a particular attention must be paid to the integration of the components which are not compliant with the fully fledged SOA standard. The following corrective operations shall be taken into account:

- A service must be represented inside the platform as all the other services even if it is not SOA fully compliant;
- A service execution must be supposed by RMS in case of necessity;
- The actual service execution must be checked as well as possible by opportune means;
- In case of mixed implementations of services the part which is properly implemented (that is SOA compliant) must provide necessary integration mechanisms towards the part which is not SOA-based.

### V. THE SIMULATION ENVIRONMENT

In this section, we present the prototype of the service-based RMS implemented following the architecture of Figure 6. A simulation tool has been implemented, due to the unavailability of the necessary technologies. The aim of our simulation is to make available to the RMS all the data that would be collected by sensors using the technologies previously described. In particular, all those objects devoted to data retrieval (sensors, RFIDs, antennas, tags, and so on) have been simulated, together with their communication techniques. Figure 6 shows the conceptual separation between the actual system and the simulation system: besides simulation of technologies, the generation of data (in particular, alarm data) need to be simulated to be interpreted.
by the RMS. Hence, the prototype simulates the environment
and the communications, data, and technologies.

Note that the modules for management of risk, health and
environment (ambient) are part of the RMS, while the sensor
systems, the data communications (network) and the
portable and wearable devices are part of the simulation.
The services constituting the simulation modules are
implemented as Java classes and by static methods. The
class diagram of Figure 7 explains the relationship between
the simulation environment and the RMS. Each entity in the
System (an element to be controlled) has a corresponding
element in the Simulation. A 1:1 correspondence exists
between the object I instantiated in the Simulation and the
physical object to be controlled in the System. Figure 8
shows the main interactions between objects which simulate
risk-related events and the system reactions to such events.
For example, a person changing his position (Worker in
Simulation) causes changing the position of his PDA which
has an associated active UWB active tag which changes its
coordinates. Since positioning data are retrieved through
UWB sensors interacting with the RMS, the data exchange
between Simulation and System occurs at this stage. The
simulated tag conveys its data to the system modifying the
Active Tag object’s coordinates (see low part of the
diagram). Since the system is aware of which PDA is
associated to this active tag and which person is the PDA’s
owner, it can detect the position changing of Worker and
generate the suitable events. The same occurs for position
changing of moving objects (see Truck in Figure 8). The
Worker’s PDA has a direct link with System for message
and data exchange. All simulated sensors (Gas Sensor and
Heart Beat Sensor) have an active link to the system to allow
all values detected in the Simulation to be sent to System.

Besides the PDA class, we have modelled the Worker
class because there are various scenarios where its
characteristics (e.g., age, general health conditions,
professional preparation) play a determinant role in the risk
identification. Furthermore, it is important to know who are
the workers present at the given location when a risk is
identified. Finally, some simulated objects have no reference
to system objects. For example, Gas Pipe is in the
simulation to model the interaction with other elements of
the implementation platform to show what occurs in the
environment, but is not an active technological component
and hence has no direct link to the RMS. Such object has a
Java counterpart in the RMS, necessary for the localization
services in case, during a gas leak, the identification of the
leak source is needed.

The RMS level manages the risk values and the events. It
will contain services for risk management and values and
event handling.

---

1 Each object in the system and in the simulation is implemented in Java
1.6 in the Eclipse Galileo environment.
consider that the system is able to support risk analysis, as explained in our previous work [16]);
3. the correctness of the model, to understand what elements need to be considered in detail (e.g. the definition of user roles and profiles), which have been neglected (e.g., the typology of the work area is fundamental to fine tune the action, such as an escape, to be undertaken in face of a risk event, such as the location of an area within the environment – for instance if a window/door is available or rather the area is closed), and which cannot be managed properly yet by the RMS due to lack of details (mainly in the communications).

The evaluation of the RMS regarding services has been conducted mainly on the service approach to modeling, rather than on the evaluation of the performances of a SOA architecture (this being object of future work).

VI. CONCLUSIONS

This paper has proposed an approach to risk management in work environments. From the software engineering viewpoint, it is fundamental to identify and specify the notion of risk specific for a particular environment. The technological advances allow on one hand monitoring of different environment parameters, which are strong indicators of risky situations, and on the other hand communication of these situations and coordination of environment elements and actors. The paper has focused on risk identification, specification, and computation; risk modeling; risk simulation (because in certain application domains the simulation plays a critical role in the validation and verification of a system, due to the impossibility, or expensiveness, to directly test the real systems). Future work regards improvement in modeling and implementation using service-oriented tools modeling more complex risk scenarios.

ACKNOWLEDGMENT

This work has been partially supported by the Tekne Project and by the S-Cube European Network of Excellence in Software Services and Systems.

REFERENCES