RAMIRES: Risk Adaptive Management In Resilient Environments with Security

Mariagrazia Fugini, Mahsa Teimourikia
Department of Electronic, Information and
Bioengineering
Politecnico di Milano
via Ponzio 34/5, Milan, Italy
Email: mariagrazia.fugini@polimi.it; mahsa.teimourikia@polimi.it

***Abstract*—This paper describes the cooperative interface of *RAMIRES*, a prototype web application where adaptive environmental risks are reported in a dashboard style for risk managers. It shows monitored areas with hazards, supports managers in fully explaining the risk and its consequences, and helps in deciding the intervention to prevent the risk. It empowers risk managers in taking decisions to *mitigate* risks and therefore to improve the environment resilience. To treat risks, *RAMIRES* is *adaptive* for risk and for security. For risk, it adapts the information flow towards the monitored environment to obtain more, or different, data about the observed area at the needed detail level to understand the risk and its consequences. For security, *RAMIRES* is adaptive in that security and privacy rules can be modified dynamically to allow facing the risk e.g., through temporary increased managers' clearances. Risk, security and actors and actions involved in risk mitigation are modeled. An outline of the methodology for risk management is given. The tool interaction with the environment and with risk managers is presented using storyboards of information flows.**

I. Introduction

The purpose of this paper is to explore how to unravel environmental risks arising in a physical environment through an improved *risk assessment phase*, and how to decide on risk management actions guiding the risk managers in *preventing* accidents.

We approach risks with the aim of achieving resilience in the monitored environment. To this aim, we present the interface of *RAMIRES* (Risk Adaptive Management In Resilient Environments with Security), a web application being developed with the following goals: i) achieving an improved assessment of risk, through interactions with the monitoring devices to get more information to understand the environment state; ii) empowering cooperation among the actors involved in risk prevention; iii) evaluating the consequences of a risk and selecting the most appropriate actions for risk mitigation; iv) supporting the execution of the selected actions.

In this paper, we deal with the first two tasks, which require a so called cognitive approach to the interpretation of hazardous situations emerging from the observations on the environment, in the streamline of what is being proposed in the Internet of Things [1]. The focus is also on the evaluation of risk consequences, and of the actions which risk managers need to perform cooperatively to *prevent* the risk. The functionalities of *RAMIRES* are presented, its underlying modeling features related to the Environment, the Events, the Risk, the Consequence, the Action to mitigate the risk, and the Actors to be involved in risk mitigation are presented.

We outline a methodology for achieving resilience in the environment. The methodology includes an iterative phase of assessment of sensors-detected parameters, aimed at obtaining more, or different, information from the environment, to fully identify a risk and its consequences. In fact, in case gathered information is not sufficient to clarify the risk and its consequences (where consequences are possibly other risks, or damages to people and objects), *RAMIRES* manages requests for more information or control commands on the environment sensors, e.g., to orient them to the area at risk and to its surroundings. We have presented the study about areas configurations and spatial information giving the location of directly and indirectly affected objects in [2]. We rely on these issues, which are outside the scope of this paper.

The methodology then includes a phase of selection of actions to prevent the risk consequences and support to their execution. In fact, while some actions are automatically executed by actuators (e.g., open activation of an acoustic alarm), other, more complex, sets of actions need be executed by human operators in a cooperative way (e.g., directing people to exits, rescuing fainted persons and removing damaged obstructing objects).

RAMIRES is presented here as a cooperative dashboard helping human actors in understanding sensors signals, determining the risk type and suggesting preventive actions. *RAMIRES* is adaptive in that it adapts the *information exchange* with the environment and with/among human actors in the assessment phase, so that sensors provide additional information to determine the risk. It is also able to adapt *security*, in that both the assessment and the action execution phases might require to modify the security and privacy rules at run time (e.g., providing enhanced privileges to risk managers).

Information exchange during the *assessment phase* is modeled in terms of *Events* that are the formalization of hazards detected by sensors, *Risk* and *Consequences* (conditions that may occur upon the Risk). *Actors* are also an entity of our model, representing risk managers, while *Actions* represent the steps to be undertaken to react to the risk. A set of actions is the strategy to be executed to achieve *environmental resilience*. In the paper, we put the basis for achieving such resilience, while not modeling it directly nor measuring related parameters able to make resilience explicit as a feature. Moreover, for the time being, we do not rely on any formal language nor knowledge representation mechanism to represent knowledge acquisition.

These will be issues to be studied in further research. Here, our aim is to show the cooperative interface supporting dialogues with human actors to face the risk. Finally, we consider Security in terms of access privileges of actors in the environment. In this paper, we focus only on the grant/revoke mechanism of privileges needed by risk managers during risk handling. Security in a wider scope has been described in [2] which is leveraged.

This paper is organized as follows. Section II discusses the state of the art. Section III describes the aims of *RAMIRES* and its visualization capabilities. Section IV presents a scenario to show the methodology used in *RAMIRES* and highlights the definitions used throughout the paper. Section V defines the model entities. Section VI outlines the functional architecture of *RAMIRES* and illustrates the interactions at the User Interface (UI) level using a storyboard. Finally, Section VII presents concluding observations and future wok.

II. Related Work

The issue of collecting data from sensor networks and from monitoring devices, currently popular also under the umbrella of IoT [3], is receiving much attention, since it allows gathering huge amounts of information from a monitored environment. Languages and knowledge representation in different forms such as ontologies, are studied [4] to represent the environment, the data gathering and interpretation phases, and so on. The issue is that, sensors transmit signals at a rough level to gateways, and that interoperability platforms are usually available to map signals into events. However, environmental data need to be interpreted at a higher conceptual level than events, in order to extract valuable information about what is occurring in the monitored environment in terms of facts or, more generally, knowledge about the environment state [5].

In particular, in the field of environmental risk management, the issue of providing safety to people and physical objects according to what happens in the environment is an open issue, as discussed in [6], [7]. These go under various labels, such as smart environments, smart cities, Generalized World Entities (GWE) and other research areas [8].

With the purpose of reducing the risk exposure of a physical environment, resilience is more and more considered as a feature to be added to the monitored environment. The purpose is to achieve a balance of a physical system by constantly adapting the information flow among sensors, risk management tools and human actors to meet the needs related to understanding the risks and incidents.

A statement on the resilience of an environment corresponds to a particular incident and to the system ability to recover, within a certain response time, as well as to the analysis of composite costs and risks [9]. In recent years, resilience engineering has received attention as related to safety, in particular as related to risks. Traditional risk facing approaches are based on knowledge, reports about failures and risk evaluation, computing historical data-based probabilities. Instead, resilience engineering studies ways to empower the ability of organizations to be resilient to risks by recognizing risks and then adapting to variations, risk sources, malfunctioning and unexpected events. In [10], the focus is on defining the concept of risk, analogously to our approach, were risk is modeled as a first-level entity, and on how risk can be treated by substituting the concepts of risk probability by uncertainty, so paving the way to use the main ideas of resilience engineering in risk management.

During risk treatment, problems of security and privacy arise, where, in order to assess, and treat a risk, more information might be required than is normally available to risk managers. Moreover, security should be handled dynamically so that privileges can be granted upon need and later revoked. In this direction, [11] tackles security for IoT applications. With the objective of introducing a lightweight data management and service framework, the paper discusses how to evaluate the trustworthiness of data coming from sensors and how to set up security and privacy mechanisms for data confidentiality, integrity and anonymity in a distributed configuration.
The trade-off between the strength of security and privacy guarantees and the assurance that the required information for decision making about risk are available, and that strategies for risk treatment can be executed successfully by the authorized entities, is discussed in [12].

Considering risk and security models, the current approaches usually fail to consider risks and security vulnerabilities together, which actually arise in a combined way during a spontaneous risk information exchange. With the goal of improving risk management and flexibility in security, this paper proposes an improvement to the risk and security model we proposed in our previous research [2] and its enforcement to treat current and potential risks *before* they turn into crisis and emergencies.
Access control [13] is the suitable security policy model, since it allows changes during run-time without conceptually raising additional accidents [2]. We start from these models, in particular from the Attribute Based Access Control (ABAC) model [13] and, as a further research step, explore ways of obtaining environment resilience for improving overall sustainable welfare, safety and security of smart areas.

As for adaptive tools, that are able to adapt their logical operation or their interface to what is observed in the real world, authors in [14] tackle the run-time adaptiveness of the user interface with the view of context of use and activities. They present how new user interfaces can be generated, gathering all the information required to perform a task.

III. RAMIRES Aims and Visualization Capabilities

The way *RAMIRES* visualizes data and spaces for risk treatment and in different ways for the various actors is the focus of this paper. In fact, in risk management, visualization of the spatial location of entities is a challenging task which may include Information and Knowledge Sharing, consultative participation and the collaborative decision making [15]. While, there are great amounts of data gathered from sensor networks and monitoring systems in the environment that form Internet of Things (IoT) [1], it is critical to enable visualization of this information to different users in a meaningful way to facilitate the risk management decision-making processes. Correlated with this challenge, there is the security variation of rules to access data related to the monitored environment. Security rules (who can access which resources in which way) can vary dynamically to adapt to the risk status, and then should be recovered back to their previous state.

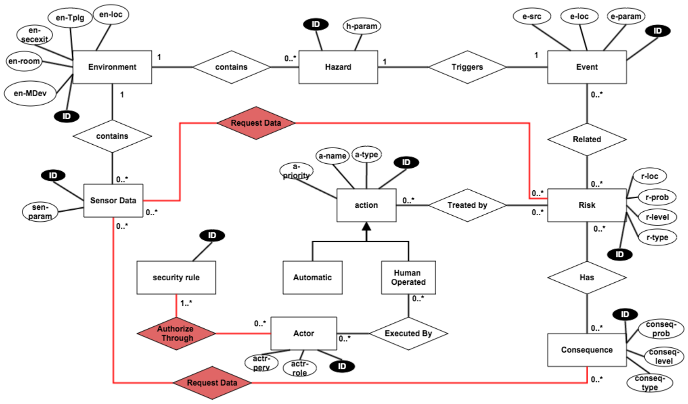


Fig. 1. ER diagram of the risk-relevant entities of *RAMIRES* conceptual model

We assume that sensors transmit data about the environment and a gateway collects data and conveys these to *RAMIRES*. The tool cooperates with an *Access Control* component responsible for varying the security rules applying to information that is being visualized, and for varying these rules according to the risk treatment needs and to the actors visualizing it to handle the risks.

RAMIRES supports cooperation in that it has to:

- interpret the environmental data and transform them not only into events, which signal a risk, but in knowledge about what has to be done to handle the risk (mitigation actions) and/or what data need to be further collected from the environment to clarify what is occurring in the environment. ”More data” means for instance that some selected sensors need be activated to get more information (e.g., sensors detecting presence of people) or redirected (e.g., a camera can be oriented and operated to observe a scene and show full images, while usually people’s visage is not shown for privacy reasons).

- select and suggest to risk managers the most appropriate risk mitigation actions. These can be selected out of a predefined knowledge stored in rules of the form $risk \rightarrow action$ or can be suggested at run time by a reasoner which is incorporated in our tool (identified as a risk management tool in [16]) and that elaborates a strategy on the fly out of the knowledge acquired at the moment the risk is detected.

RAMIRES is described by showing how it requires to elaborate knowledge about the environment and how it guides people in handling the risk using a storyboard of its interactions with i) the environment, ii) the risk managers. The storyboard diagrams are depicted as sequence diagrams and screen shots obtained from our prototype.

IV. Scenario, Definitions and Methodology

In this section, we set a scenario used to show the *RAMIRES* tool. Let us first set some preliminary definitions.

As a basic example, we have that sensors may detect the presence of smoke (hazard is likely to be *fire*) in a closed environment, and an *Event* of type Fire is issued to *RAMIRES*. In its assessment steps, *RAMIRES* determines the risk related to the Fire Event, and starts to identify the Risk type, level, area where the fire is and possible affected areas and all the risk attributes. The dependencies between the involved entities, namely persons, physical resources, sensors which monitor the environment, and actors in charge of risk management have to be determined by *RAMIRES*.
These issues in turn threaten security and privacy, because for instance clearances of risk teams need be upgraded to observe the affected areas in more detail. Therefore, we consider that security rules are adaptively modified: *granted* when the event arises and during risk mitigation (e.g. a camera is allowed to return facial details of individuals, while normally it is not) and *revoked* when the risk is concluded.

Referencing the terminology in the literature [7], we use *hazard* to define the abnormal condition in the environment, *event* to denote the signal passed to *RAMIRES* to signal the hazard, *risk* as the problem to be identified and mitigated/prevented. Risks have *consequences*, which need be evaluated in order to react by performing mitigation *actions*, and involves *actors* in charge of risk management. Backwards interactions towards the environment may be necessary to fully characterize the risk and its consequences. *RAMIRES* manages such interaction by adapting sensor data flow to understand and prevent the risks. *Security rule* is also an entity that can be modified during risk mitigation. The defined entities are shown in the Entity-Relationship diagram of Figure 1. Hazardous conditions and unknown dependencies need be treated by:

- understanding events for improved assessment;

- executing the actions to face the risk. Sets of actions constitute a *risk mitigation strategy*, which we presented in [17].

A. Methodology Outline

To show the steps of our proposed methodology, we can observe Figure 2 where we use Business Process Management diagrams to show the flow of assessment, decision, and risk management steps and the involved components. A flow of information between *RAMIRES* back to the environment (where the sensors have raised an hazard-event) is required to set interventions to mitigate the risk and limit the damages. For example, to understand a risk and its consequences, more sensor data need to be collected and evaluated, in dependence of the people positioned in the affected area, or the risk level due to the observed increased temperature in a zone, can be determined by activating other sets of sensors, or a camera to observe the area. Coming to mitigation actions, some are quite trivial, like automatic actions activating an alarm or opening emergency doors. We call these *simple actions*. Others require to get more information from the environment and to elaborate knowledge about what an event (e.g., smoke detection) actually is about: where it was generated, which people are possibly involved, which rescue teams should be sent to the affected area, equipped with which tools, vests and wearable sensors, and so on. These actions, usually to be performed by humans, can be selected only after the consequences of the risk have

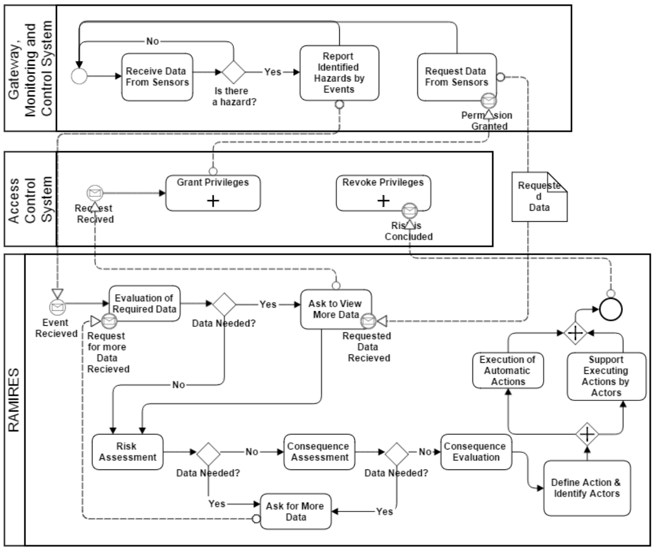


Fig. 2. Methodology adopted by *RAMIRES*

been evaluated; we name them *complex actions* to mean a set of tasks to be carried on in the style of a business process.

To understand and to execute, the Access Control System can adapt security rules, for instance, granting access privileges to risk teams to observe an area in more details or to view the positions of the employees in affected areas. Security rules are adaptively modified via *grant* of access privileges according to the risk and during the risk treatment, and via *revoke* operations on the granted privileges, when the risk has been mitigates.

We assume we are in an indoor work area where people are working with tools and moving machines (e.g. forklifts, carts or small indoor vehicles). Workers are protected by wearable sensors and safety tools, e.g., embedded in glasses, helmets, shoes, or work suit. The environment is surveilled by sensors networks, cameras, RFIDs and other environment tools (fire extintors, and the like). The environment here has the advantage that is fully described by its blueprint (we know where the emergency doors, staircases and windows exist on a map of the area). We are also under the hypothesis that people in the environment are known because they have been identified through entrance gates or badges, and hence their health status, for instance, is known (in case rescue teams have to intervene for assistance).The skills of risk managers are also known.
We assume three human actors types for risk management: a Risk Responsible (RR), a Risk Operator (RO), and a Risk Team Head (RTH). The ROs can be grouped in teams dynamically when the risk arises and assigned a RTH. Their profiles and roles are stored in RAMIRES data bases and regard their skills, experience, access privileges, and, at run time, the tasks they are involved during a risk intervention. Modeling human actors and their attributes is beyond the scope of this paper; elsewhere we have modeled actors as Subjects of the ABAC model and given their security-related adaptive attributes.

During the whole risk mitigation phases, all these actors, both tools in Figure 2 and human actors mentioned above, play a role. A risk is detected by sensors (and this part of the communication is beyond our description purposes here) and becomes an event. An event can signal a single risk (fire) or multiple risks (fire and fainted person). The event has to be processed by *RAMIRES* to be transformed into knowledge. To elaborate knowledge, the *RAMIRES* can require further information from the environment, such as getting more detailed images from a camera.

When knowledge has been fully obtained, *RAMIRES* suggests actions to mitigate the risk to the RR, RO and/or RTH. These actions, called *mitigation actions*, can be:

- automatic, like lock a firedoor, open an emergency door, activate a sound alarm;
- actions for people: these are actions that guide for instance fire brigades in moving through a smoky area, or suggesting which persons need first aid with high priority. These actions are shown on the dashboard of *RAMIRES*, e.g., provided as vocal orders emanated by the risk managers.

V. Model Entities

The main entities in our definitions are Hazard, Event, Risk, Consequences, Environment, Actor and Actions, as shown in Figure 1.

We use *Hazard* $h_i \in H$ to represent the abnormal conditions in the environment. In this work, we do not tend to model the hazards. Instead, here we simply consider a list of parameters h_{param} as shown in (1) to define the hazard. These parameters include: the source of the hazard, its location and the type of the hazard e.g. gas leak.

$$h_i \triangleq \{\{h_{param}\}\} \tag{1}$$

We use the concept of event $e_i \in E$ to signal the *hazards* in the monitored environment. Events are defined in (2), including the event source e_{src}, i.e., the component causing the event, e_{loc}, i.e., the location of the event, and the list of parameters e_{param}, namely data, extracted from the sensors, that can be used in risk assessment, such as the environment temperature, the presence of people, the number of open windows, and so on.

$$e_i \triangleq \{e_{src}, e_{loc}\{e_{param}\}\} \tag{2}$$

Risk includes the severity of the accident consequence and its probability of occurrence [7]. Risk is defined as actual or potential threats with diverse consequences that include danger, harm or loss of the environment and physical components like the infrastructures, tools and machinery, and the human entities, such as workers, visitors, etc. who reside inside the affected area. We define risk $r_i \in R$ and $i \in \mathbb{N}$ as following while R denotes the set of risks identified and assessed in the environment by *RAMIRES*:

$$r_i \triangleq \{r_{type}, r_{level}, r_{loc}, r_{prob}, \{r_{conseq}\}\} \tag{3}$$

In (3), risk r_i is considered to be identified by its type r_{type} (e.g. *fire*, *explosion*, etc.). Risk level r_{level} represents the severity of the risk defined as a qualitative attribute that accepts the values: VERY HIGH, HIGH, MEDIUM, LOW, VERY LOW. r_{loc} identifies the location with is affected by the risk r_i. While, r_{prob} shows the probability of occurrence of r_i.

Risk Consequences are considered as a list $\{r_{conseq}\}$ representing the identified results of r_i in case of occurrence. Each risk consequence $conseq_i$ as defined in (4) includes $conseq_{type}$ that is the type such as loss of life, damage to infrastructures, etc., $conseq_{prob}$, and $conseq_{level}$ that represent the probability and severity of the consequence, respectively.

$$conseq_i \triangleq \{conseq_{type}, conseq_{prob}, \{conseq_{level}\}\} \qquad (4)$$

Environment (en) is defined as an area that can be monitored to identify potential or existing risks. Specifically, as shown in (5) the environment en includes attributes such as topology en_{tplg}, the location en_{loc}, set of security exits $en_{secexit}$, set of rooms en_{room}, and the set of monitoring devices en_{MDev} that include various sensors, cameras and so on.

$$en \triangleq \{en_{tplg}, en_{loc}\{en_{secexit}\}, \{en_{room}\}, \{en_{MDev}\}\} \qquad (5)$$

Furthermore, Actor $actr_i \in ACTR$ is defined to represent the persons in charge of risk management. They get authenticated by the access control system to view required information. For the purpose of this paper, we simply consider the following actor's attributes: their set of privileges $actr_{prev}$ and their set of roles $actr_{role}$ as shown in (6).

$$actr_i \triangleq \{\{actr_{prev}\}, \{actr_{role}\}\} \qquad (6)$$

Action $a_i \in A$, represents the risk mitigation action suggested by the *RAMIRES* for risk treatment. Actions can either be automatic, meaning that they are automatically executed by *RAMIRES*, or they are human operated, in that they are suggested by *RAMIRES* to the actors and these can select which actions are the most appropriate and then are guided by *RAMIRES* in executing them. Action a_i as shown in (7), has a type a_{type} that can be simple or complex. It also includes a name a_{name} and a priority $a_{priority}$.

$$a_i \triangleq \{a_{type}, a_{name}, a_{priority}\} \qquad (7)$$

The complete set of attributes for the entities, considering their security related attributes are defined in our previously security model in [2].

A. Security and Privacy in Risk Management

As we mentioned in our previous work [2], we consider that risk can be managed only by authorized personnel having defined Security Roles. The personnel has a defined *security profile* specified according to ABAC where the attributes define the authorizations. These authorizations can change at runtime via a grant (and revoke, when the risk has been treated) mechanisms. So we speak of *adaptive security* as defined in [2]. As depicted in Figure 2, the Access Control Systems filters the requests coming from *RAMIRES*, in terms of access to environmental data, by checking the required privileges on objects against the access rule data base and allows/deny privileges. Allowed privileges are dynamically granted on a temporary basis, and later revoked. Denied privileges are those which are not compliant to security policies (these aspects are detailed in [2]).

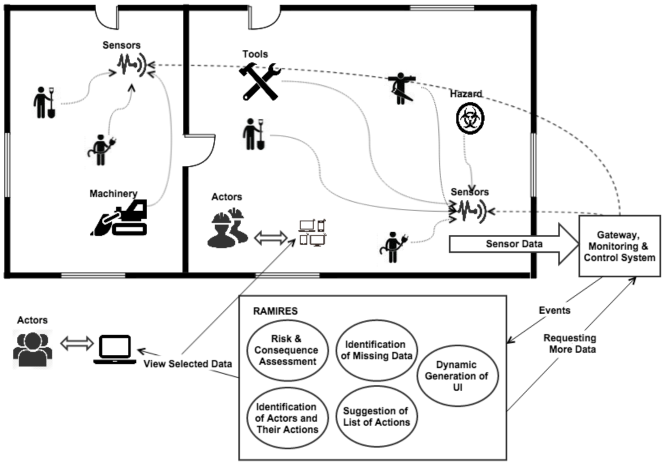
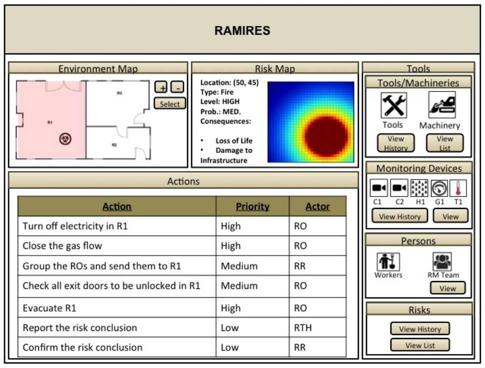

Sensors
Tools
Hazard
Machinery
Actors
Sensors
Sensor Data
Gateway, Monitoring & Control System
Actors
View Selected Data
RAMIRES
Risk & Consequence Assessment
Identification of Missing Data
Dynamic Generation of UI
Identification of Actors and Their Actions
Suggestion of List of Actions
Events
Requesting More Data

Fig. 3. *RAMIRES* functional architecture:tasks and interactions



Location: (50, 45)
Type: Fire
Level: HIGH
Prob.: MED.
Consequences:

- Loss of Life
- Damage to Infrastructure

Action	Priority	Actor
Turn off electricity in R1	High	RO
Close the gas flow	High	RO
Group the ROs and send them to R1	Medium	RR
Check all exit doors to be unlocked in R1	Medium	RO
Evacuate R1	High	RO
Report the risk conclusion	Low	RTH
Confirm the risk conclusion	Low	RR

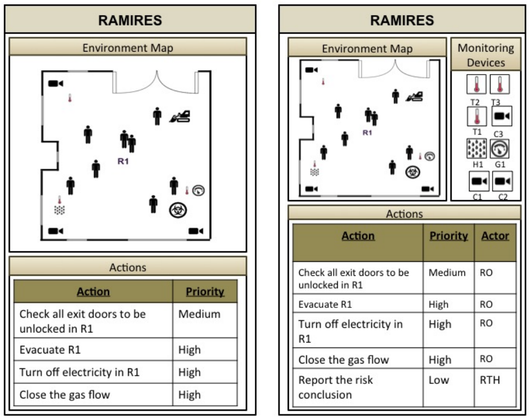
Fig. 4. Sample dashboard provided to the RR

VI. *RAMIRES* Storyboards

The main architecture of *RAMIRES* is shown in Figure 3. *RAMIRES* generates the UIs dynamically based on the risk assessment done online. The data views for each actor are generated according to the security rules ([2]). As depicted in Figure 4 and Figure 5, different information is displayed to the RR, ROs and the RTH respectively, according to their roles and privileges. The risk map is generated in *RAMIRES* using MATLAB, by employing risk probability functions. R1 denotes a room where risk is to be managed.

To understand what an event means in terms of risk, *RAMIRES* needs to produce knowledge out of events. The reasoning on risk can be:

1) Simple: like understanding the r_{type} attribute of the Risk entity. This requires to unchain the Event-Risk relationship of the ER diagram.



Action	Priority
Check all exit doors to be unlocked in R1	Medium
Evacuate R1	High
Turn off electricity in R1	High
Close the gas flow	High

Action	Priority	Actor
Check all exit doors to be unlocked in R1	Medium	RO
Evacuate R1	High	RO
Turn off electricity in R1	High	RO
Close the gas flow	High	RO
Report the risk conclusion	Low	RTH

Fig. 5. Sample dashboard for the RO (left-hand side), and for the RTH (right-hand side)

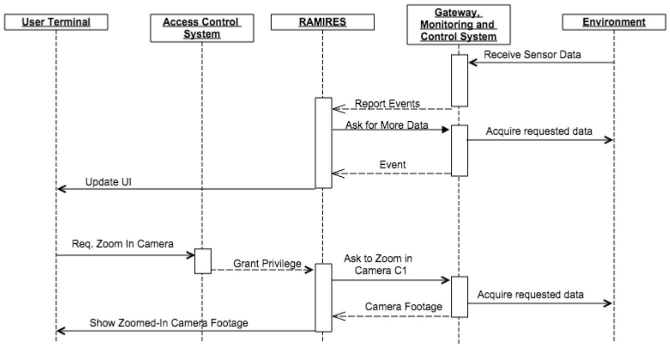


Fig. 6. A sample interaction at the presentation layer in our scenario

2) Complex: like determining what strategies to be suggested to the RR, RO and/or RTH in a list appearing on the dashboard of *RAMIRES*. Then, it is up to the actors to decide which actions to execute and in which order. In other words, we take the approach of having the system suggesting all the possible mitigation actions and leaving it to the actors the 'smart' task of deciding what to execute actually.

We will elaborate further on ways to event interpretation; for this paper, we are concerned with specifying the *RAMIRES* presentation layer, and to show a sample interaction in our scenario. A sample visualization interaction in work areas of our scenario, we consider the storyboard depicted in Figure 6, where the interaction between the user, through the user terminal, and RAMIRES is depicted, while considering also the interactions between *RAMIRES*, the Environment, the Access Control System and the Gateway, Monitoring and Control Tool. The user requests, and the requests issued by *RAMIRES* for more environmental data, due to its elaboration of knowledge performed internally and not analyzed in this paper, are both filtered by the Access Control System, which checks if the necessary privileges hold or modifies the security rules. For the sake of simplicity, in this scenario, we assume that the requested access is always compliant with security policies and is therefore always granted.

In Figure 7, we show the execution of simple and complex actions. While the simple actions are automatically executed by *RAMIRES*, all the requests should pass through the Access Control System. After the successful execution of an action, *RAMIRES* can inform the actors by updating the UIs. For execution of the complex actions that needs the interventions of the actors, *RAMIRES* first asks for updating the security rules so that actors can be granted the required privileges needed to execute the actions.

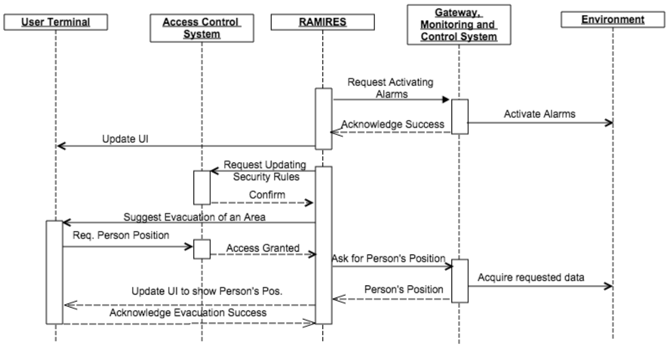

User Terminal
Access Control System
RAMIRES
Gateway, Monitoring and Control System
Environment
Request Activating Alarms
Activate Alarms
Acknowledge Success
Update UI
Request Updating Security Rules
Confirm
Suggest Evacuation of an Area
Req. Person Position
Access Granted
Ask for Person's Position
Acquire requested data
Person's Position
Update UI to show Person's Pos.
Acknowledge Evacuation Success

Fig. 7. A sample interaction showing the execution of simple and complex risk mitigation in our scenario

VII. Concluding Remarks

The paper has made a step towards achieving resilience in physical environments, like work areas, or closed spaces hosting offices, shops by setting in place an assessment phase where risk can be fully clarified to understand its consequences, and where risk managers are guided in performing risk mitigation actions. The *RAMIRES* tool has been presented as a visual interface able to ask/receive more information from the environment to decide the best risk mitigation strategies. We have presented the overall architecture of *RAMIRES* and a storyboard of its dahsboard along the phases of our proposed methodology of enhanced risk assessment and risk decisions making.

We are working on defining the business logic of *RAMIRES* which stands beyond the Presentation Layer illustrated in this paper. Further work regards the formalization of adaptive information flows and of adaptive security, as well as the interpretation of events as risks and the formalization of resilience aspects so that these become measurable.

Acknowledgment

The authors thank the Attivabili Project of Politecnico di Milano and Regione Lombardia and the Sensori National Project for funding this research.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] M. Fugini, G. Hadjichristofi, and M. Teimourikia, "Dynamic security modeling in risk management using environmental knowledge," in *WETICE Conference (WETICE), 2014 IEEE 23rd International*. IEEE, 2014, pp. 429–434.

[3] N. Bessis, F. Xhafa, D. Varvarigou, R. Hill, and M. Li, *Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence*. Springer, 2013.

[4] G. P. Zarri, "Generalized world entities as an unifying IoT framework: A case for the GENIUS project," in *Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence*, 2013, pp. 345–367.

[5] M. Rönkkö, J. Heikkinen, V. Kotovirta, and V. Chandrasekar, "Automated preprocessing of environmental data," *Future Generation Computer Systems*, vol. 45, pp. 13–24, 2015.

[6] K. Smith, *Environmental hazards: assessing risk and reducing disaster*. Routledge, 2013.

[7] N. J. Bahr, *System safety engineering and risk assessment: a practical approach*. CRC Press, 2014.

[8] M. Batty, K. W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, G. Ouzounis, and Y. Portugali, "Smart cities of the future," *European Physical Journal-Special Topics*, vol. 214, no. 1, p. 481, 2012.

[9] T. Takahashi, K. Emura, A. Kanaoka, S. Matsuo, and T. Minowa, "Risk visualization and alerting system: Architecture and proof-of-concept implementation," in *Proceedings of the first international workshop on Security in embedded systems and smartphones*. ACM, 2013, pp. 3–10.

[10] R. Steen and T. Aven, "A risk perspective suitable for resilience engineering," *Safety Science*, vol. 49, no. 2, pp. 292 – 297, 2011.

[11] S. Sicari, C. Cappiello, F. De Pellegrini, D. Miorandi, and A. Coen-Porisini, "A security-and quality-aware system architecture for internet of things," *Information Systems Frontiers*, pp. 1–13, 2014.

[12] E. Bertino, G. Ghinita, M. Kantarcioglu, D. Nguyen, J. Park, R. Sandhu, S. Sultana, B. Thuraisingham, and S. Xu, "A roadmap for privacy-enhanced secure data provenance," *Journal of Intelligent Information Systems*, vol. 43, no. 3, pp. 481–501, 2014.

[13] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to attribute based access control (abac) definition and considerations," *NIST Special Publication*, vol. 800, p. 162, 2014.

[14] C. Martinie, D. Navarre, and P. Palanque, "A multi-formalism approach for model-based dynamic distribution of user interfaces of critical interactive systems," *International Journal of Human-Computer Studies*, vol. 72, no. 1, pp. 77–99, 2014.

[15] M. Evers, A. Almoradie, and A. Jonoski, "Web based collaborative decision making in flood risk management," in *EGU General Assembly Conference Abstracts*, vol. 16, 2014, p. 15614.

[16] M. Fugini, C. Raibulet, and L. Ubezio, "Risk assessment in work environments: modeling and simulation," *Concurrency and computation: Practice and experience*, vol. 24, no. 18, pp. 2381–2403, 2012.

[17] M. G. Fugini, C. Raibulet, and F. Ramoni, "Strategies for risk facing in work environments," in *Computer and Information Sciences II - 26th International Symposium on Computer and Information Sciences, London, UK, 26-28 September 2011*, 2011, pp. 425–431.