RAMIRES: Risk Adaptive Management In Resilient Environments with Security

Mariagrazia Fugini, Mahsa Teimourikia
Department of Electronic, Information and Bioengineering
Politecnico di Milano
via Ponzo 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 environmental risks are reported in a dashboard for the risk management team. It shows monitored areas, supports risk managers in understanding the risk and its consequences, and supports decision making so empowering risk managers to mitigate risks improving the environment resilience. To treat risks, RAMIRES is adaptive regarding risk and security. For risk, it adapts the information towards the environment to obtain more data about the observed area to understand the risk and its consequences. It also adapts the user interface according to the involved actor. For security, RAMIRES is adaptive in that security rules determine the data views to different actors. The tool interaction with the environment and with risk managers is presented using storyboards of interactions.

I. INTRODUCTION

The purpose of this paper is to explore how to unravel risks arising in a physical environment through risk assessment, 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. Resilience engineering represents a different way of viewing risk management, fostering the creation of robust yet flexible systems to monitor and proactively face the risks to reverse their effects. 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) assessment of risk through interactions with the monitoring devices to understand the environment state; ii) evaluating the consequences of a risk and selecting the most appropriate actions for risk mitigation; iii) supporting the execution of actions by risk managers. These tasks require a so called cognitive approach to the interpretation of hazardous situations emerging from the observations on the environment, in the streamline of what proposed in the Internet of Things (IoT) [1].

The functionality and entities of RAMIRES are presented. Then, we illustrate the steps performed to achieve resilience, including an iterative phase of assessment of sensors-detected parameters, aimed at obtaining more information from the environment, to fully identify a risk and its consequences. For example, in case gathered information is not sufficient to clarify the risk, RAMIRES requests more information from sensors (a better image of the area at risk).

Other steps consist of: i) selecting actions for risk mitigation, and ii) supporting their execution. Some actions are automatically executed (e.g., activate an alarm); others need to be executed by human operators in a cooperative way (e.g., directing people to exits, rescuing fainted persons and removing damaged obstructing objects). In these phases, RAMIRES acts as a cooperative dashboard supporting human actors in understanding signals, determining the risk type and suggesting preventive actions, showing information to risk managers according to their roles and to their access privileges.

RAMIRES is adaptive as it adapts the information exchange with the environment and with among human actors in the assessment phase to gather additional information about risk and to personalize the user interface. It is also adaptive for security, in that risk management requires to generate views on the environment dynamically according to users’ profiles and to modify the security rules at run time, e.g., granting enhanced privileges to risk managers.

Mitigation actions aim at environmental resilience. In the paper, we put the basis for achieving resilience, while not modeling it directly nor measuring related parameters able to make resilience explicit as a feature. We consider security in terms of access privileges of actors in the environment based on their roles in risk management and according to what we have described in [2].

This paper is organized as follows. Section II discusses the state of the art. Section III gives a scenario and the definition of entities and information flow. Section IV describes the visualization capabilities of RAMIRES, its functional architecture and the interactions at the User Interface (UI) level using storyboards. Section V concludes the papers and gives future work.

II. RELATED WORK

Data collection and analysis from sensor networks, currently popular also under the umbrella of IoT [3], is receiving attention, since it allows gathering information from a monitored, or so called, smart environment. Languages and knowledge representation in different forms such as ontologies, are studied [4] to represent the environment and data gathering and interpretation phases. 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 environment in terms of facts and knowledge [5].

In environmental risk management, providing safety to people and physical objects according to what happens in the environment is an open issue, as discussed in [6], [7]. The
research issue goes under various labels: smart environments, smart cities, and Generalized World Entities (GWE), to mention a few [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 environment [9]. 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 [10]. In recent years, resilience engineering has received attention as related to safety risks [9]. Resilience is usually measured in a qualitative way employing some indicators or by empirical studies that are done on data gathered from questionnaires. The resilience indicators are studied in works such as [11]. In [12], the focus is on defining the concept of risk, analogously to our approach, where 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.

In risk management, problems of security and privacy arise, when risk assessment might require more privileges than normally available to risk managers. Security should be handled dynamically so that privileges can be granted upon need and later revoked. In this direction, [13] tackles security for IoT applications. [14] discusses the trade-offs between the strength of security and privacy guarantees, and the assurance that the required information for decision making about risk are available, from the one sided, and the fact that strategies for risk treatment can be executed successfully by the authorized entities. With the goal of improving flexibility in security, our paper leverages the security model we have proposed in [2], in the streamline of access control [15] security policy models, and in particular using the Attribute Based Access Control (ABAC) model [15] to dynamically grant and revoke privileges in smart areas.

As for adaptive tools, namely able to adapt their logical operation or their interface to what is observed in the real world, authors in [16] 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. We stem from these hints, and present our tool capabilities in the style of storyboards of adaptive interactions.

III. SCENARIO, DEFINITIONS AND INFORMATION FLOW

We set a scenario used to show RAMIRES entities and functions. We also set some preliminary definitions.

Considering a work area, such as a plant or an office building, assume we have sensors detecting the presence of smoke. In its assessment steps, RAMIRES has to determine that the signals about smoke are related to the risk of fire. Therefore, it elaborates on the Fire Event, and starts to identify the Risk attributes: type, level, location of fire (and possible affected areas) and so on.

Fig. 1: Steps of risk management adopted by RAMIRES

Referencing the terminology in the literature [7], hazard defines an abnormal condition in the environment, and event denotes the signal passed to RAMIRES to notify the hazard; risk is defined as the problem to be identified and mitigated/prevented.

Starting from these standard definitions, we elaborate on the model as follows. Risks have consequences, which need to be evaluated in order to react through mitigation actions, and involves actors in charge of risk management.

The resilience is not about avoiding risks, as they can happen at any time, but it refers to maintaining and regaining an stable state prior, during and after an event [9]. To achieve resilience, minimization of failure, early detection and treatment of hazards, minimization of consequences of a risk, and flexibility are required. By continuously monitoring the environment early detection of hazards is possible. Moreover, early and full assessment of the risk and consequences, planning of preventive strategies, and facilitating the collaboration between actors improves the treatment of risk. Finally, the flexibility and adaptiveness of RAMIRES and of the ACS to the risk facilitates the successful execution of the strategies.

To perform in a resilient manner, the following steps of risk management are considered by RAMIRES which are reported in Figure 1 where Business Process Management diagrams show assessment and decisions steps and the involved components. The Gateway, Monitoring and Control System (GMC) connects RAMIRES to the external world. As depicted in Figure 1, when there is a hazard, the GMC reports it as an event causing RAMIRES to start the risk and the consequence assessment processes. Interactions with the environment may be needed to characterize and assess the risk and its consequences. RAMIRES manages such interactions requesting new events from the environment as depicted in Figure 1. RAMIRES then proposes preventive actions that can be human operated or automatic. And it executes the automatic actions while supporting the execution of human operated actions. In case an
actor requests to view a data item that is needed in the process of risk treatment, if the adaptive security rules allow such view, RAMIRES asks the GMC for more events, and updates the dashboard so that the requesting actor is enabled to view the requested data.

Hazardous conditions and unknown dependencies need to be treated by: (i) Understanding events for improved assessment. (ii) Executing actions to face the risk. Sets of actions constitute a risk mitigation strategy (More details on risk mitigation strategies are presented in [17] where we discuss the procedure to select the proper strategies for treatment of detected risks).

As presented in Figure 1, the ACS manages security issues related to the requests by adaptively granting and revoking permissions.

For example, assume three human actors 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 are assigned a RTH. Their profiles and roles are stored in RAMIRES databases with data about 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 [2]. During risk mitigation, RAMIRES suggests actions to mitigate the risk to the RR, RO and/or RTH.

A. RAMIRES Entities

The entities composing RAMIRES, the External Environment and the ACS are depicted in the Entity-Relationship diagram of Figure 2 explained below.

![Fig. 2: ER diagram of the risk-relevant entities of RAMIRES conceptual model](image)

Relationships between RAMIRES, External World, and ACS are highlighted in a different color. Hazards in the External World trigger events in RAMIRES.

In the External World, Hazard $h_i \in H$ represents out-of-range parameters $h_{param}$ in the environment. The environment is denoted by its location $e_{loc}$ and contains sensors that monitor the environment parameters $s_{param}$.

In RAMIRES, events initialize the risk and consequence assessment phases. RAMIRES assesses the event to determine the risk. In doing this, RAMIRES might need to request more details from the External World for a full determination of the risk. Then, risk consequences need to be evaluated and later treated by actions, executed either by RAMIRES (if automatic) or by actors (if human operated).

The main entities in RAMIRES are detailed below.

An Event $e_i \in E$, as defined in (1), includes the event source $e_{src}$, i.e., the component causing the event, the location of the event $e_{loc}$, and the list of parameters $e_{param}$, extracted from sensors, that are used in risk assessment (e.g., the temperature, the presence of people, the number of open windows, and so on).

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

(1)

A Risk $r_i \in R$, where $R$ denotes the set of all known risks, computed according to a probabilistic approach ([17]), is defined as follows:

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

(2)

In (2), $r_i$ is defined by: risk type ($r_{type}$), that explains the characteristics of the risk (e.g., fire, explosion, etc.); risk
security rules. The authorization result is a tuple as each actor are generated according to the risk profiles the adaptive security rules proposed in [2].

It is possible to create the personalized visualization according to an actor on a resource. Using the authorization results, it is possible to display the associated data views representing which actions are permitted for each actor. The categories of data to be shown in the personalized dashboards are predefined. In our work environment, we have resources such as: tools and machinery, monitoring devices like temperature, humidity and pressure sensors and monitoring cameras, a map of the environment, localization data on the persons, monitoring devices and tools and machinery. Risk-related data are shown as a risk map on the UIs and the preventive actions recommended to RO and the current values of the persons on it together with the position of the monitoring devices and hazards. Instead, the RTH can also view the positions of tools and machinery, current and previously recorded data from the sensors and monitoring devices, the positions of persons in the affected environment by risk and the risk management actors on the field, and also the history of previous risks that happened in the environment.

On the other hand, the RO and the RTH have their own views, as reported in Figure 5. The RO can only view the preventive actions proposed to him/her with their priorities, and the map of the environment with the anonymous locations of the persons on it together with the position of the monitoring devices and hazards. Instead, the RTH can also view the preventive actions recommended to RO and the current values of the monitoring devices to be able to treat the risk properly. Actions have associated priorities of execution, which can be changed by allowed actors and according to predefined rules.

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

\[ \text{actor}_i \triangleq \{\{\text{actor}_{prev}\}, \{\text{actor}_{role}\}\} \]  

(3)

\[ \text{ru}_i \triangleq \{\text{actr}_{ID}, a_{ID}, \text{result}\} \]  

(5)

The ACS includes security rules (RU) to authorize actors requests (shown in Figure 2). For each security rule \( \text{ru}_i \in RU \), we consider the actor identifier (\( \text{actr}_{ID} \)), the action identifier (\( a_{ID} \)) and the authorization result (\( \text{result} \)) as its attributes, as shown in 5. The detailed model of the ACS can be found by the interested reader in [2].

\[ \text{actr}_i \triangleq \{\{\text{actor}_{prev}\}, \{\text{actor}_{role}\}\} \]  

(3)

\[ \text{actr}_i \triangleq \{\{\text{actor}_{prev}\}, \{\text{actor}_{role}\}\} \]  

(4)

\[ \text{ru}_i \triangleq \{\text{actr}_{ID}, a_{ID}, \text{result}\} \]  

(5)

IV. RAMIRES VISUALIZATION CAPABILITIES

The RAMIRES dashboard is employed to visualize the personalized risk-related data (e.g., the map of the environment, location of the risk, and sensors data indicating the risk) to the risk management team, as reported in Figure 3. In fact, in risk management, visualization of entities is a challenging task which may include information and knowledge sharing, consultative participation and collaborative decision making [18]. Since great amounts of data gathered from sensor networks and monitoring systems in the environment are available, e.g., for the 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 while preserving the confidentiality and privacy of the entities [2].

The main functional modules of RAMIRES are shown in Figure 3 that includes risk and consequence assessment, identification of missing data (so triggering a request for them from the GMC. Other functions suggest preventing strategies to face the risk, identification of suitable actors and assignment actions to them. Finally, a function consists in the dynamic generation of User Interfaces (UIs) of the dashboard, customized for each actor. RAMIRES generates the UIs dynamically based on the risk assessment done at run time. Specifically, data views for each actor are generated according to the risk profiles and the security rules. The authorization result is a tuple as \(<\text{actor, resource, action}>\) representing which actions are permitted for an actor on a resource. Using the authorization results, it is possible to create the personalized visualization according to the adaptive security rules proposed in [2].

The main functional modules of RAMIRES are shown in Figure 3 that includes risk and consequence assessment, identification of missing data (so triggering a request for them from the GMC. Other functions suggest preventing strategies to face the risk, identification of suitable actors and assignment actions to them. Finally, a function consists in the dynamic generation of User Interfaces (UIs) of the dashboard, customized for each actor. RAMIRES generates the UIs dynamically based on the risk assessment done at run time. Specifically, data views for each actor are generated according to the risk profiles and the security rules. The authorization result is a tuple as \(<\text{actor, resource, action}>\) representing which actions are permitted for an actor on a resource. Using the authorization results, it is possible to create the personalized visualization according to the adaptive security rules proposed in [2].

The categories of data to be shown in the personalized dashboards are predefined. In our work environment, we have resources such as: tools and machinery, monitoring devices like temperature, humidity and pressure sensors and monitoring cameras, a map of the environment, localization data on the persons, monitoring devices and tools and machinery. Risk-related data are shown as a risk map on the UIs and the preventive actions recommended by RAMIRES for each actor and their probabilities are reported. The security rules enforce a fine-grained access control on viewing such data.

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, and considering the risks and the security rules.

In Figure 4, the UI presented to the RR shows the environment map with the positions of the hazard. The RR can zoom-in/out with defined levels of details on the selected sections of the environment based on his privileges (see [2]). The RR has also functions allowing him to assign tasks to the RO and to the RTH. The risk map is generated in RAMIRES using MATLAB, by employing risk probability functions (see [17]). The RR is also able to view positions of tools and machinery, current and previously recorded data from the sensors and monitoring devices, the positions of persons in the affected environment by risk and the risk management actors on the field, and also the history of previous risks that happened in the environment.

The main functional modules of RAMIRES are shown in Figure 3 that includes risk and consequence assessment, identification of missing data (so triggering a request for them from the GMC. Other functions suggest preventing strategies to face the risk, identification of suitable actors and assignment actions to them. Finally, a function consists in the dynamic generation of User Interfaces (UIs) of the dashboard, customized for each actor. RAMIRES generates the UIs dynamically based on the risk assessment done at run time. Specifically, data views for each actor are generated according to the risk profiles and the security rules. The authorization result is a tuple as \(<\text{actor, resource, action}>\) representing which actions are permitted for an actor on a resource. Using the authorization results, it is possible to create the personalized visualization according to the adaptive security rules proposed in [2].
The evaluation of risk consequences is more complex, e.g., to determine what strategies or what priorities for actions should 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 possible mitigation actions and leaving to human actors the ‘smart’ task of deciding what to actually execute.

A. A Sample Interaction

As a sample scenario, we consider the storyboard in Figure 6, reporting the interactions between the users (via the User Interface) and RAMIRES, and between RAMIRES and the environment via the ACS, and GMC tool. Here, data are conveyed by sensors and mapped into an event which updates the UI. Assuming that the user requests more environmental data, such request is filtered by the ACS, which checks the profiles against his privileges. For the sake of simplicity, we assume the requested access is compliant with security policies and therefore granted. In the figure, the request is for more details from a video camera, which is executed via RAMIRES and whose results are sent back to the user.

Figure 7 shows the execution of simple and complex actions. Simple actions are those automatically executed by RAMIRES (activation of alarms in Figure 7). For the execution of complex actions, which need the intervention of actors (in Figure 7, an example of a complex action is shown as the evacuation of the environment), suggestions are made by RAMIRES that further supports the execution of the action by considering the requests of actors (in this example, opening the secured doors that is needed for a successful evacuation). After the successful execution of an action, actors can notify RAMIRES via the dashboard so to give a feedback.

B. Discussion on Qualitative Evaluation of Resilience

Evaluating and measuring the resilience is challenging, since identifying the measurable factors that contribute to resilience in various context-specific unexpected situations is
not a straight-forward task. However, there are some indicators of relative overall resilience that are defined in the literature [11], [9] in the categories of situation awareness, management of keystones strategies, and adaptive capacity. In the following, we try a qualitative assessment of how we could possibly identify and then take into consideration some indicators relevant for our context in order to improve resilience.

In the category of situation awareness, we can consider roles and responsibilities for actors, and as RAMIRES can suggest the preventive strategies based on the roles of each actors, helping to get a clear view of the risk treatment strategies that should be executed by each person. One point that should be considered is the unavailability of actors and how someone should fill their role. Furthermore, RAMIRES assesses the risk and its consequences and communicates it to the actors through the dashboard’s interface, and prioritizes the strategies that are designed to either prevent or recover from the risk consequences. Also, by continuously monitoring the environment, RAMIRES is able to detect the hazards on time. Hence, we should consider the external hazards that may effect the environment besides focusing on the internal situation factors. Moreover, we do not consider the lessons learned from past events in changing the future detection of risks.

In the category of management of keystones strategies, RAMIRES plans preventive strategies using a risk management plan and suggests it to the actors (see also [19]). This facilitates the cooperation among actors by providing them with relevant information and strategies via its dashboard.

Last but not the least, in the category of adaptive capacity, that refers to the ability of the system to adaptively display resilient behavior [11], we facilitate the actors engagement, involvement and decision making by clearly identifying their cooperative activities required to treat the risk. Through the help of the Risk-Adaptive ACS (see [2]), it is possible to grant/revoke permissions to view more details so adaptively facilitating risk management to the levels of risk, to the consequences, and to the level of skill of actors in decision making.

V. CONCLUDING REMARKS
The paper has made a step towards achieving resilience in physical environments, like work areas, or closed spaces hosting offices and 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 request/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 interactions with environment and actors along the phases of a process 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
This research was supported by RAS, Regione Autonoma della Sardegna (Legge regionale 7 agosto 2007, n. 7 Promozione della ricerca scientifica e dell’innovazione tecnologica in Sardegna) in the project DENIS: Dataspaces Enhancing the Next Internet in Sardinia.

REFERENCES