

REDIRNET – Emergency Responder Data Interoperability Network

Aurel Machalek, Dominic Dunlop
University of Luxembourg
aurel.machalek@uni.lu, dominic.dunlop@uni.lu

Zoltán Balogh, Emil Gatial, Ladislav Hluchý
Institute of Informatics, Slovak Academy of Sciences
zoltan.balogh@savba.sk, emil.gatial@savba.sk, ladislav.hluchy@savba.sk

Abstract - European states regularly experience a wide range of major crisis events, including not only environmental disasters such as major flooding, avalanches and earthquakes, but also man-made incidents involving large-scale transport-related accidents and terrorist-sponsored events. When responding to such incidents, Emergency service agencies and rescue organisations are working together more frequently to enhance their overall operational effectiveness, often requiring collaboration across state borders. The REDIRNET project benefits multi-agency joint-working by facilitating information exchange through the concept of broad-scale data interoperability.

I. INTRODUCTION

The REDIRNET solution provides true Europe-wide interoperability that is not reliant on specific technology or proprietary systems. The REDIRNET project is developing a system that provides seamless interoperability for all participating agencies via the REDIRNET socio-professional web and which includes dynamic configuration as required (Fig. 1). This level of interoperability allows emergency service agencies to provide a more effective response to major crisis incidents, ultimately leading to enhanced public safety and security across Europe.

This work is supported by European Union projects FP7-607768 REDIRNET: Emergency Responder Data Interoperability Network, VEGA No. 2/0054/12 and CLAN APVV-0809-11.

The intended users of the system are rescue teams and first responders in countries across the EU. A number of recent major incidents have highlighted the challenges that first responders face, most notably concerning interoperability barriers. These challenges must be faced in the context of the current economic and financial situation; agencies are under considerable budgetary pressures and are unable to justify the investment of significant sums of money to enhance their existing, and in some cases quite limited, interoperability capabilities. The application of REDIRNET's interoperability principles requires minimal agency resources, with the only area of investment being the development costs of the adapter needed to connect to the open source gateway.

This work is supported by the following projects: EU FP7-607768 REDIRNET - Emergency Responder Data Interoperability Network and Slovak National VEGA Project No. 2/0167/16.

REDIRNET is not only relevant to rescue and first responder teams, it is an open system and therefore all organizations, whether they are public agencies or commercial entities, can join when the operational need arises, share their information and enjoy the benefits offered by the system.

This paper describes REDIRNET's unique concept and its possible applications in industry. The overall concept is based on three main technologies: the Collaboration Web, an Interoperable Gateway, and the Secure Agents.

A. Technical approach

REDIRNET provides a platform, configuration interfaces and an open-source generic system gateway that can be modified by integrators to connect their systems to the platform. The project will provide a communication solution to exchange and share information via voice, data, images, video, CCTV and remote sensors. The platform, configuration interfaces and a generic system metadata gateway can easily be modified by an agency's existing ICT integrator to connect their system to this platform. To encourage emergency responder agencies, and also commercial organisations which are involved in major incident response, to connect their legacy systems to REDIRNET, documentation and open source sample code for the metadata gateway will be publicly available. All these features will be developed with an emphasis on the security of transmitted data and ease of integration in a user-friendly and cost-effective solution.

B. REDIRNET Components

The main focus of the current project [1] is to create possibilities for interagency communication and the sharing of first responders' data. Our system allows an agency to access a

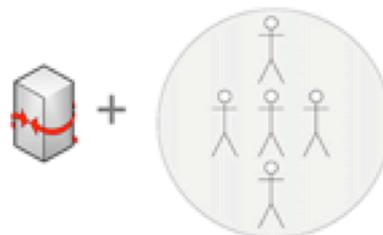


Fig. 1. Metadata data gateway combined with socio-professional networking

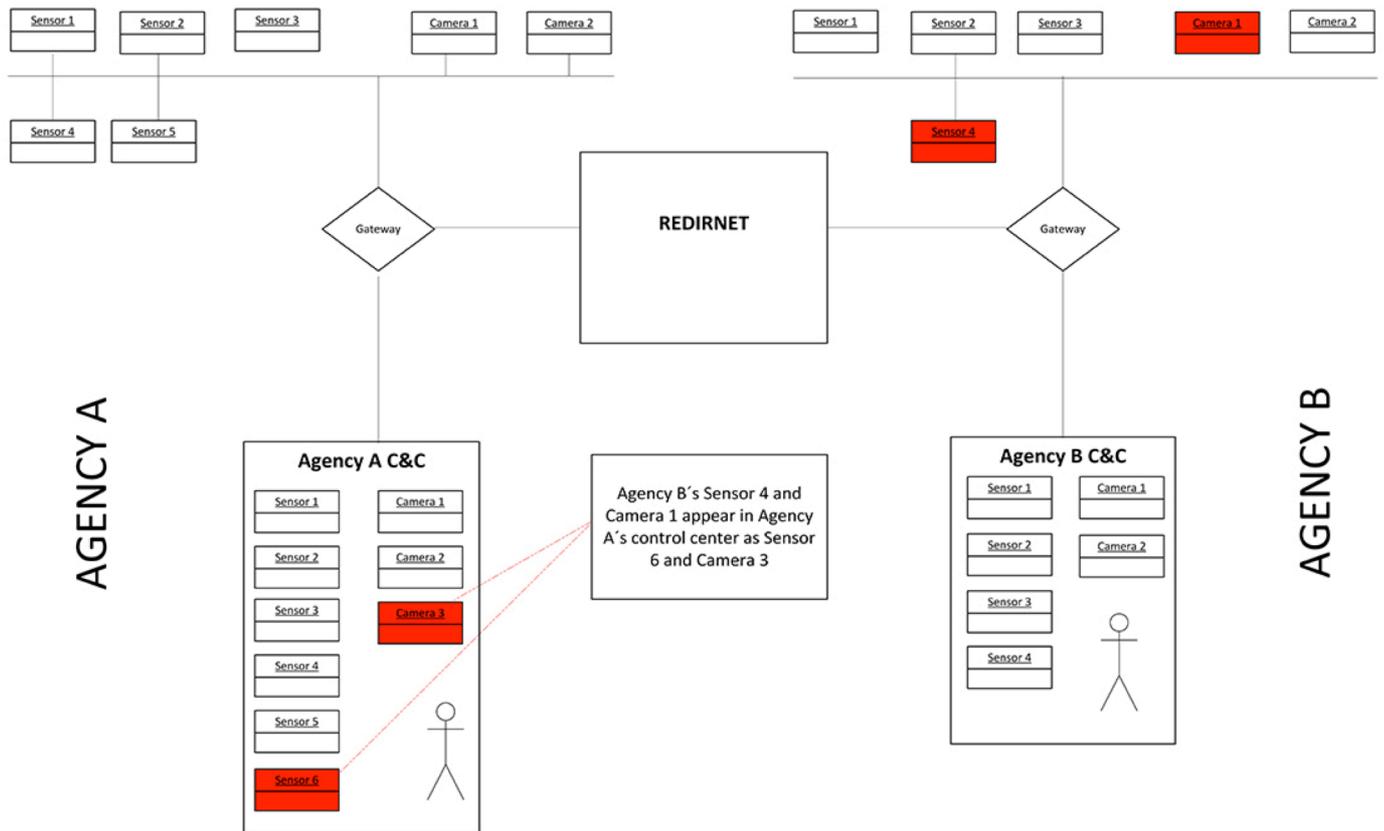


Fig. 2. REDIRNET components

partner's shared sensor data. Based on the sensor and its capability, two kinds of connection can be set up: a request/response connection is used for batched data, while a stream connection is established for a continuous data flow. It is assumed that the partner agency consuming the data is capable of processing it.

As an example, in Fig. 2, Agency B is offering data streams from Sensor 4 and Camera 1 to Agency A. This arrangement has been previously agreed between the two agencies and configured using the REDIRNET socio-professional network. The network's seamless interoperability means that Agency B's Sensor 4 and Camera 1 can be displayed in agency A's control centre beside its own Sensor 6 and Camera 3. The same is true for data displayed on Agency A field officers' handheld devices.

In order to provide agencies with the ability to share their data resources, some preliminary steps are required. The data-producing resource must be connected to some sort of translator, which can encode the data stream into a common transport protocol, and provide the correct command interface. This translator is then connected to a transport network, which can verify permissions for each user and route the stream to its destination, where it is translated into a protocol native to the data consumer and subsequently displayed.

This workflow can be achieved by a system consisting of five components:

- **Main Switch**, redirecting the communication, checking permissions and providing a logging facility,
- **Core Data Storage**, supplemented by an ontological search engine, providing database services for all data requiring storage,
- **Collaboration Web**, the user interface for the system, allowing resources to be registered and their permissions to be managed,
- **Gateways**, a client at each agency client, taking the role of mediator between the main switch and the plug-ins, and
- **Plug-ins**, drivers providing interfaces for the endpoint resources.

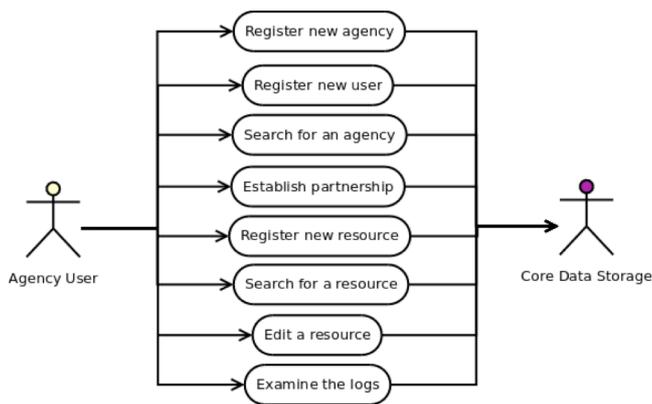


Fig. 3. Collaboration Web system operations

II. THE COLLABORATION WEB

The socio-professional networking component provides a decentralized opportunity for an interoperability network to be built and configured by its users. It also allows the interoperability network to be run without major operational costs, since the collaboration rules are set by the agencies themselves by following basic guidelines. Collaboration rules are set according mutual agreements between the agencies involved and should cover issues such as the visibility and controllability of data fields, data streams and switches. The algorithms and keys used for end-to-end encryption of the data are also set up by the agencies.

The collaboration web handles the use cases related to getting in touch with other agencies and the high-level configuration of the interconnection based on abstract roles. Typical use cases, shown in Fig. 3, are the creation of an agency profile, registration of a data resource, and configuration of permissions. The agency's authorized users can perform all these actions through a web browser. The web interface will initially provide all of the essential collaboration capabilities mentioned above, but, should the need arise, it can be extended to provide additional functionalities of the type found today in commercial applications.

In line with modern approaches to the development of web applications, we are using the MVC programming paradigm for enhanced robustness and modularity. The services of the REDIRNET core, particularly its core data storage component, will implement the model and controller functions of the paradigm, while the collaboration web itself will provide the View role.

Using the collaboration web, each agency's authorized users will be able to

- 1) register users and maintain profiles;
- 2) enter name, short-name, description, and contact information;
- 3) establish partnerships between agencies;
- 4) search for a partner agency, propose/approve a partnership, display the partners of an agency and whether a partnership was mutually approved;

- 5) search for the data resources of other registered agencies;
- 6) set up interoperability for resources with the help of the ontology subsystem, which allows the user to use the terminology native to their region or domain; and
- 7) examine log events and set the correct permissions on each resource.

III. INTEROPERABLE GATEWAY

The concept of a gateway as a link between two computer programs or system is a traditional solution when resource sharing is demanded in a multiprotocol environment. The gateway acts as a portal between two worlds, separating them (and so providing security), while allowing contact between them (by providing communication and transport). A gateway-based solution was tested, verified and successfully used in previous FREESIC project [2], confirming the usability of this mechanism in multiprotocol environments.

C. Significance of the Gateway in REDIRNET

The gateway is crucial for system integrators because it allows them to integrate the emergency agency's system into the REDIRNET platform. The open and well-commented source code makes it possible to verify the implementation and promotes trust. Additional example source code and detailed documentation help software engineers to understand the gateway in order to be able to implement their components.

D. Logical Location of the Gateway

The gateway acts as middle layer between a collection of third-party plug-ins and the REDIRNET core. Fig. 4 shows the location of the gateway relative to other components implementing control command flow and the resource transport mechanism.

The Gateway forwards control commands and data resources between core and appropriate plug-ins. The gateway also manages requests handling and encapsulating prior to forwarding to core. One gateway can handle many providing and/or consuming plug-ins.

The primary services supported by gateway can logically be split into the roles of provider and consumer.

E. Gateway as Information Provider

As an information provider, the gateway responds to requests concerning the resources that it mediates, and supplies data from those resources. To do this, it:

- Holds primary information about availability of resources provided by attached plug-in(s), and
- Uses HTTP/POST to push requested resources to proxies.

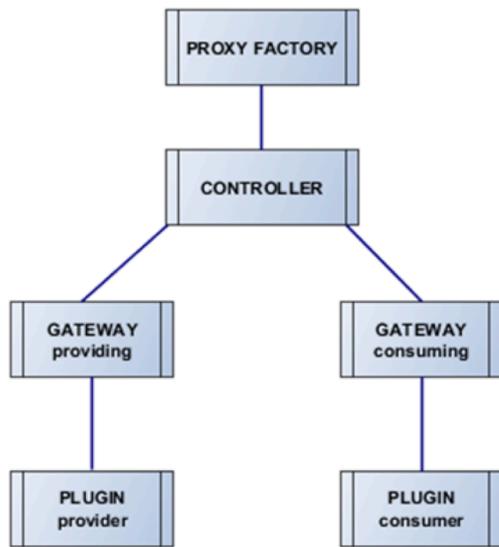


Fig. 4. Gateway in relation to other REDIRNET components

F. Gateway as Information Consumer

As an information consumer, the gateway acts as an intermediary between the controller and connected plugins. This involves:

- Pushing resource requests to controller, and
- Propagating proxy URIs to consuming plugins.

G. Required Gateway Functionality

The gateway is required to support the following methods:

- **Event.resource.changed** – If a resource change is detected by a plug-in, this event generates a message that is sent to the gateway
- **Request.login** – Ask a plug-in to provide its credentials to the gateway
- **Request.getMetadata** – Request for metadata concerning a specific resource
- **Request.getLocalTime** – Request local time for a specific resource. (“What time zone is this camera in?”)
- **Request.getRemoteResourceState** – Query the availability of a remote resource (“Is this resource available?”)
- **Request.getLocalResourceState** – Query a plug-in about the availability state of an underlying resource
- **Request.getRemoteResource** – Requests data from remote resource. Not applicable to video resources.
- **Request.getLocalResource** – Requests plug-in to provide data from its underlying resource. Not applicable to video resources.
- **Request.playRemoteResource** – Requests starting of stream on a remote resource. Applicable only to video resources.

- **Request.stopRemoteResource** – Instructs remote video resource to stop streaming. Applicable only to video resources.
- **Request.playLocalResource** – Requests plug-in to start video stream from its underlying resource.
- **Request.stopLocalResource** – Instructs a plug-in to stop steaming from its underlying resource.
- **Request.heartbeat** – Used by the gateway to check whether a plug-in is alive.
- **Request.retrieveMetadata** – Query a plug-in about metadata from a specified resource.

H. Conceptual design

The gateway communication model is based on HTTP, so both an HTTP server and a client are incorporated into the gateway as independent but cooperating processes. The HTTP client is used for gateway-to-controller communication while the HTTP server handles gateway-to-plugin communication, as shown in Fig. 4. A plugin can communicate with the rest of REDIRNET only when Gateway is connected to a controller. On other hand, a gateway with no connected plugins is functional, but of little practical use.

IV. THE SECURE AGENTS

During a large-scale crisis response there is a need to seamlessly retrieve, evaluate and exchange information from many parties and rapidly make an appropriate action based on the processed information. Moreover if the information is structured, validated and geo-located it can provide additional value. The seamless collection, aggregation, analysis and effective presentation of relevant and accurate information in the right time can greatly support crisis response. In emergency contexts, in fact a large number of actors need to collaborate and coordinate in the disaster scenes by exchanging and reporting information with each other and with the people in the control room [3]. One of the two essential major objectives of the REDIRNET project therefore is to add new smart functions to existing services, which will make the communication more effective and helpful for users. Smart functions will be provided by distributed IT systems based on an agents’ infrastructure. By fulfilling this goal, we should allow a pervasive and trusted communication infrastructure to be created, fulfilling the requirements of crisis management users and ready for immediate application. Further secure agent infrastructure (SAI) should provision a distributed service paradigm to achieve both confidentiality and access to resources. It should also provide a smart negotiating system for parameterization and independent handling of access requests to achieve a rapid reaction.

A. Architecture of the Secure Agent Infrastructure

We use a concept of Polls to manage information in the SAI architecture. A Poll is a process of smartly collecting and aggregating information using a pre-prepared configuration setup from a specific group of users or services subscribed to various communication channels. Polls are easily created using a setup procedure based on pre-created Templates in a matter of seconds. A Poll can be executed right after the setup procedure is finished or the execution can be planned for a

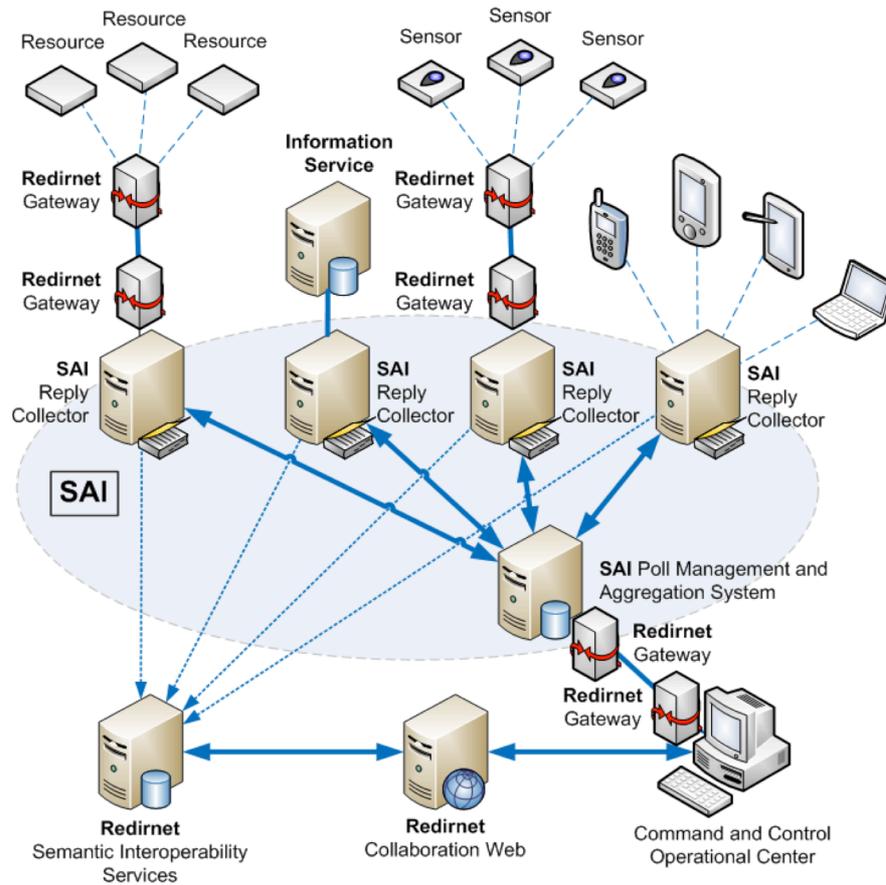


Fig. 5. The context of the Secure Agent Infrastructure in the Redirnet project

later exact date and time. Polls can be of different types such as one-time, recurrent or continuous. Depending on the type, a Poll can last an explicitly specified time or can run continuously or till a predefined rules are met. Upon the Poll execution and finish the collected information are aggregated. Based on the Poll results a report or an action can be generated. All or specific predefined subscribers can be informed about the Poll execution result. One Poll can execute another Poll to deliver required information - this way the Polls can create a simple workflow, which can be used to execute a chain of information collection actions.

The context of the SAI in the Redirnet overall architecture is depicted in Fig. 5. The SAI is two core components are: the Poll Management and Aggregation Service (PMAS) and the Reply Collector (RC). The Interoperability Gateway connects both PMAS and RCs to the overall Redirnet infrastructure. While the PMAS is primarily used as a consuming plug-in, the RCs are used as consuming as well as a providing plug-ins.

A typical sample scenario was created in scope of the Redirnet project [1] in which information collection takes place from disparate hospitals from legacy databases or from communication devices operated by the hospital staff in charge. The requirements for the hospitals are to provide appropriate treatment facilities for the injured persons in a required capacity. Additionally the hospitals must be as close

to the incident site as possible. There are Reply Collectors deployed in each hospital. The PMAS manages the collection of replies from individual RCs. Two additional components depicted in Fig. 5 are the Redirnet Semantic Interoperability Services - which provide semantic description of our RCs and the already mentioned Redirnet Collaboration Web - which is a user interface for integrating operations of different subsystems.

V. CONCLUSION

The REDIRNET is an ongoing project. The first working open source gateway has been implemented. While not all functions are yet provided, its core functionality works well, as confirmed by field testing. The initial implementation focused primarily on the resource transfer capability, and this goal was fully met.

REFERENCES

- [1] REDIRNET, Emergency Responder Data Interoperability Network. Available at: <http://www.redirnet.eu>.
- [2] FREESIC, Free Secure Interoperable Communication. Available at: <http://www.freesic.eu>
- [3] TRECARCHI, G., RIZZI, V., MARCHESE, M., VACCARI, L., BESANA, P.. Enabling Information Gathering Patterns for Emergency Response with the OpenKnowledge System. COMPUTING AND INFORMATICS, Slovakia, 29, jan. 2012. Available at: <http://www.cai.sk/ojs/index.php/cai/article/view/99>.