ARM - Adaptive Risk Management Platform for Emergency Response Operations

Mihaela Ulieru
Canada Research Chair,
Faculty of Computer Science,
The University of New Brunswick
P.O. Box 4400
Fredericton, E3B 5A3,
Canada
ulieru@unb.ca

Paul Relf
Director of Business Development
ARTIS (Applied Real Time Imaging Systems)
120 Moodie Dr.
Ottawa, K2H 9R4,
Canada
paul.relf@artisnet.com

Merv Matson
President
RightsMarket

Calgary,
Canada
MatsonM @ RightsMarket.com

***Abstract* – We introduce the Adaptive Risk Management (ARM) Platform as a versatile testbed for the development of emergency response applications. The platform consists of three powerful components encompassing M3Data, RightsEnforcer and powerful up-to-date hardware consisting of MOTES, mobile wireless devices and computer networks backed by powerful servers. On a scenario unfolding into gradually increasing complexity we illustrate how the ARM platform works.**

***Keywords* -** Emergency Response Holarchy, Command and Control, Situational Awareness, Network-Centric Operations, Secure Data Integration, Persistent Information Security

I. INTRODUCTION

This work is grounded in our previous results merging multi-agent systems with the holonic paradigm to define the concept of holonic enterprise (HE) [1]. A HE (Fig. 1) is a holarchy of collaborative enterprises, where each enterprise is regarded as a holon and is modelled by a software agent with holonic properties, so that the software agent may be composed of other agents that behave in a similar way but perform different functions at lower levels of resolution. In [2] we introduce the concept of emergency response holarchy (Fig. 1) and in [3] we propose a FIPA-based implementation. Arguing that absolute security is impossible to achieve, which calls for a risk management approach to emergency response, in [4] we expand the emergency response holarchy concept to embrace the need for adaptive risk management.

In this paper we present an architecture and implementation considerations for this novel perspective, materialized in a powerful software platform (which we will refer to as Adaptive Risk Management or in short ARM platform) which spans across three centres (all based in Fredericton): The Adaptive Risk Management Laboratory at the University of New Brunswick, the Privacy, Security and Trust Laboratory at National Research Council of Canada and the Situational Awareness Command and Control Centre at the New Brunswick Public Safety office.

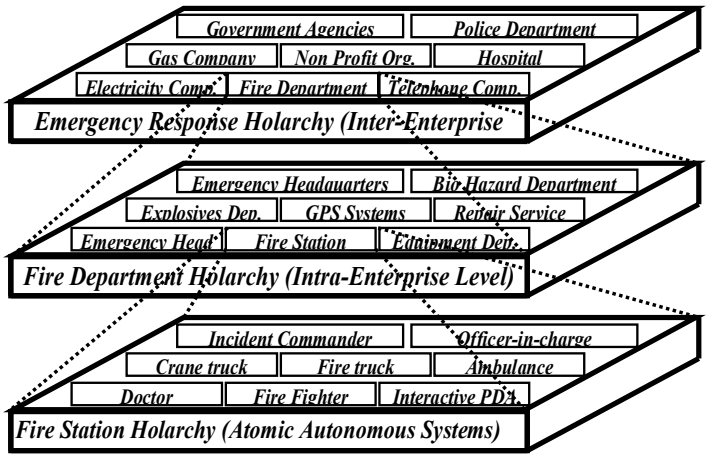


Fig. 1: Emergency Response Holarchy

II. ARM PLATFORM OVERVIEW

The ARM platform supports the quick deployment of the following application areas

1). *Enhanced Situational Awareness*: provide an integrated view of high quality, contextual information to support decision making by combining relevant information from multiple disparate sources into an integrated picture.

2). *Information Sharing / Dissemination:* support intra/inter agency information sharing and service composition through secure access to relevant information which is stored in multiple disparate repositories.

3). *Decision Support Capabilities:* apply advanced knowledge management techniques to analyze a diverse set of data to predict outcomes, make recommendations, provide notifications / warnings or even automatically take certain actions, e.g. by employing multi-agent technologies..

4). *Logistics Management:* apply advanced knowledge management techniques to analyze a diverse set of data to optimize the utilization and distribution of assets.

5). *Persistently secure documents and email messages:* enable protection, control of access operations, and tracking, wherever the document or email goes, every time someone attempts to use it, thus endlessly extending the domain of secure information dissemination and collection.

To support any of these solution categories, an approach to secure data integration must be applied. Situational awareness and information sharing directly target the data integration challenge. Decision support and Logistics management apply knowledge exploitation techniques across an integrated data set.

The two software packages animating the ARM platform are:

1). *M3Data Information Sharing & Knowledge Exploitation System (M3Data), ARTIS:* (www.artisnet.com)This flag-ship product [5] which combines a unique information integration approach with advanced knowledge management and artificial intelligence capabilities, allowing for rapid and agile deployment of Network Centric Operations. M3Data provides a unique solution which specifically targets the complex information integration and knowledge exploitation needs of Military, Intelligence, and Public Safety markets. The, Solution areas include; advanced Command and Control Applications, Information Fusion & Knowledge Exploitation, Intelligent Machine-to-Machine applications, and Secure Information Sharing. With M3Data, information flows are modeled graphically (Fig 2) to meet the application need regardless of source, target, or required data manipulation. Mapping is performed through simple icons and arrows allowing the information architect to focus on the required information flow and not the complexities of the underlying technology. This freedom allows sharing of information from any source to any target. M3Data supports a wide variety of databases, packaged applications, directory services, enterprise services, semi-structured and unstructured data.

2). *RightsEnforcer*: This suite of products of RightsMarket (http://www.rightsmarket.com/) provides persistent security, access control and complete tracking and audit capability for valuable or confidential information. The RightsEnforcer product suite works in conjunction with existing security models to provide enhanced "every time, everywhere" protection. It can grant and revoke access even after the information has been distributed and used by legitimate users [6]. RightsMarket is a provider of Persistent Information Security solutions that enable information owners and custodians to protect information wherever it goes, however it gets there. RightsEnforcer integrates seamlessly with standard email tools (such as Microsoft Outlook and Lotus Notes) to provide persistent email and attachments protection with minimal impact on user workflow.

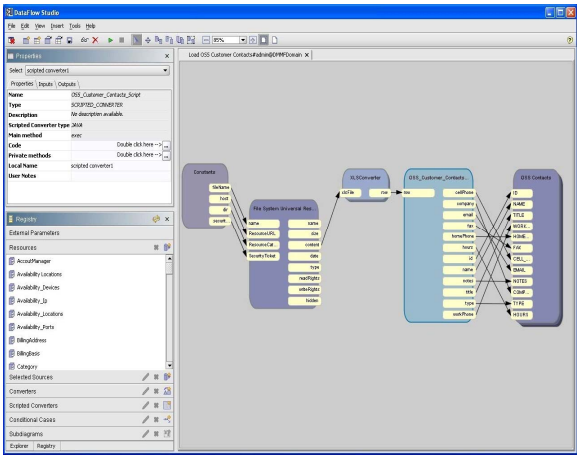


Fig. 2: M3Data Iconic Application Development

In the ARM platform ARTIS M3Data will be deployed as the secure, intelligent middle-ware solution and RightsEnforcer as the "every time, everywhere" document and email security solution.

Of the three levels of emergency management (strategic, operational, and tactical), it is the command and control element at the operational level which has a broad mandate of responsibility and need for technological advancement. The base context for the initial configuration of the ARM Platform is centered on the needs of an Emergency Operations Center (EOC). More specifically, the configuration will support capabilities which enhance EOC Command & Control of a coordinated response during a catastrophic event. Command & Control includes capabilities such as; collaborative planning, directing, coordinating, and controlling of inter-agency operations on the ground.

III. ILLUSTRATION WITH AN EMERGENCY RESPONSE SCENARIO

During a state of emergency, the scope of interoperability between various levels of government and other organizations to provide a coordinated response is tremendous, Fig. 3 [3], [2].

The nature of this problem involves many agencies within all levels of government, and first responder organizations (firefighters, police (RCMP), ambulance service, and hospitals). Extending the scenario in Fig. 3 to, e.g. a chemical fire taking place on a foreign vessel anchored in e.g. a Canadian harbor, additional agencies such as; Transport Canada and PSEPC (Public Safety and Emergency Preparedness Canada) are likely to get involved. Using our previous results [7], [8] data from multiple national sources such as; fire, EOC, RCMP, Transport Canada, and general knowledge from the Internet will be mined and integrated into an ON-LINE dynamic knowledge repository.

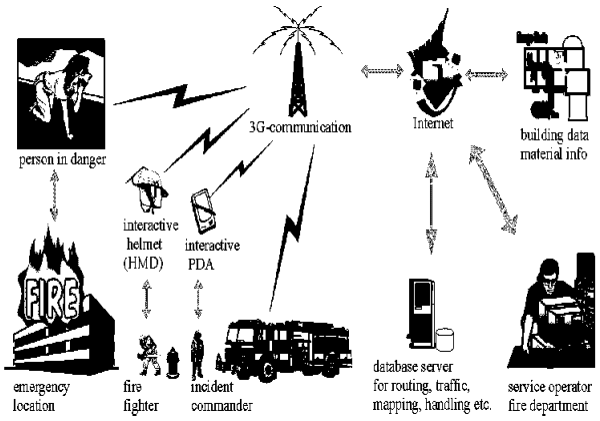


Fig. 3: Emergency Response Scenario

Within this problem domain there are many opportunities to leverage technology in support of individual organizational need and coordination across organizations. The need for research is in the realm of technology to support inter-agency coordination and response which calls for novel cross-platform mitigation techniques (Fig. 1) [3]. Current processes, applications and information systems represent substantial investments for organizations. For an information sharing system to be successful, these investments need to be preserved while still delivering the incremental value required.

Within this scenario, M3Data is deployed as a secure, intelligent middle-ware application enabling an information centric operations approach. This is achieved by first providing secure data integration within and between various operating organizations. M3Data enables compliance for strict inter-agency information sharing agreements shaped by privacy and security needs. These disparate information sources are combined and related using various M3Data libraries. Secure applications are then provided which exploit the combined knowledge to meet various needs of the EOC: Command & Control, Situational Awareness, Decision Support, and Interoperability.

Since there are many participating agencies at all levels of government, each with their own strict policies surrounding information access, a persistent mechanism which protects documents themselves (including e-mails) is required. RightsEnforcer is an application level information security solution referencing the OSI[1] and TCP/IP communication stack model and protocol. It provides file level control that is independent of location and programmable on time, even outside of the originating or host information management system. Architecturally, Rights-Enforcer is based on a client-server system; the client portion must be present to use a protected file in cooperation with the server. Whenever a user attempts to use a file, the server always asks and answers the question "What rights does this user have to this file?" Then it governs use of the file to enforce those terms of use. RightsEnforcer has been applied to documents so the rights are typically to display, print, copy-paste clear (unencrypted), and file copy clear [9]. Offline use and timed use (e.g. start next Monday for seven days) are provided for. Rights (or permissions) can be modified after distribution of the document, so a document can be disabled for everyone and a user can be disabled for all documents no matter where the documents are. Email and attachments can be persistently secured. Rights can be governed by peers and policy.

Let's assume for example that the fire is on-board a vessel which has hazardous chemicals in its cargo and the situation escalates after an explosion occurs resulting in a plume drifting towards a densely populated area. In this case the firefighting and police response will need to adjust/adapt accordingly [2]. Using M3Data, the ARM platform provides a decision support capability which monitors the events unfolding on the ship-borne fire to predict necessary response for fire and police assets. Within this context there are many possibilities.

IV. ARM PLATFORM CONFIGURATION FOR SITUATIONAL AWARENESS APPLICATIONS

Across an emergency response holarchy (Fig. 1) M3Data Information Sharing System utilizes a component based distributed architecture (Fig. 4), which allows for tremendous horizontal and vertical scaling. More importantly, it provides the ability to quickly deploy the EMO solution within computing environment constraints without compromising the operation and performance of the system.

The ARM platform enhances situational awareness within an EOC environment by providing contextually based access to information from multiple disparate data sources. Information is accessible via a geo-spatially based Integrated Intelligence Picture which acts as a decision aid during consequence management activities. Information is shared securely between multiple agency repositories and combined into a common knowledge warehouse. User credentials determine which information assets can be seen by specific roles within the EOC. The Integrated Intelligence Picture provides a capability for displaying entities within a given area of interest. For example, the location of 911 callers, hospitals, sensors, and other place names can be displayed. Users can then drill-down into these items of interest to access related knowledge which has been correlated across multiple repository types.

Fig. 4 illustrates the ARTIS Solution Architecture which is used to deliver the right information to the right user at the right time for situational awareness problem domain. It consists of:

[1] http://www.webopedia.com/quick_ref/OSI_Layers.asp
http://en.wikipedia.org/wiki/TCPIP

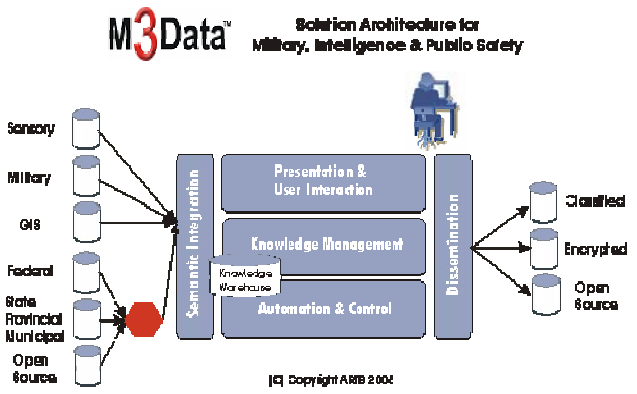


Fig 4: ARTIS Military, Intelligence & Public Safety Solution Architecture[2]

1). *Data Sources:* A wide variety of data sources are accessible to M3Data through pre-built Resource Adapters. The underlying data and meta-data are made available to the Information Architect within the graphical design studio to define any required Information Flow. This provides a graphical approach to provide syntactic and semantic integration between information sources and user applications.

2). *Sensors:* Diverse sensory input providing environmental data and awareness.

3). *Automation & Control:* Automated data processing, transfer and control within the system enable real-time applications which meet environmental, operational and performance needs.

4). *Virtual Knowledge Warehouse:* Machines and users interact with a virtual knowledge warehouse representing a combined view of information and knowledge assets within the system which they are authorized to access.

5). *Knowledge Management*: M3Data provided or 3rd Party Knowledge Management services are accessible for user and machine applications. A cornerstone in providing next generation Command and Control (C2) applications is combining access from the common Knowledge Warehouse with Artificial Intelligence algorithms (e.g. using multi-agent system technologies [4]), to enable advanced decision support capabilities for the particular emergency operation.

6). *Presentation & User Interaction:* Information must be presented to individual decision makers in context and a format which makes sense to them, such as, portal, report, e-mail, etc. This includes views and ad-hoc queries into the C2 Information System and Notifications or processes which are integrated with the system.

7). *Dissemination:* Post decision. M3Data Information Flows (Fig. 2) allow for the efficient dissemination of Response information in a wide-variety of formats or any application as required.

V. ARM PLATFORM ARCHITECTURE

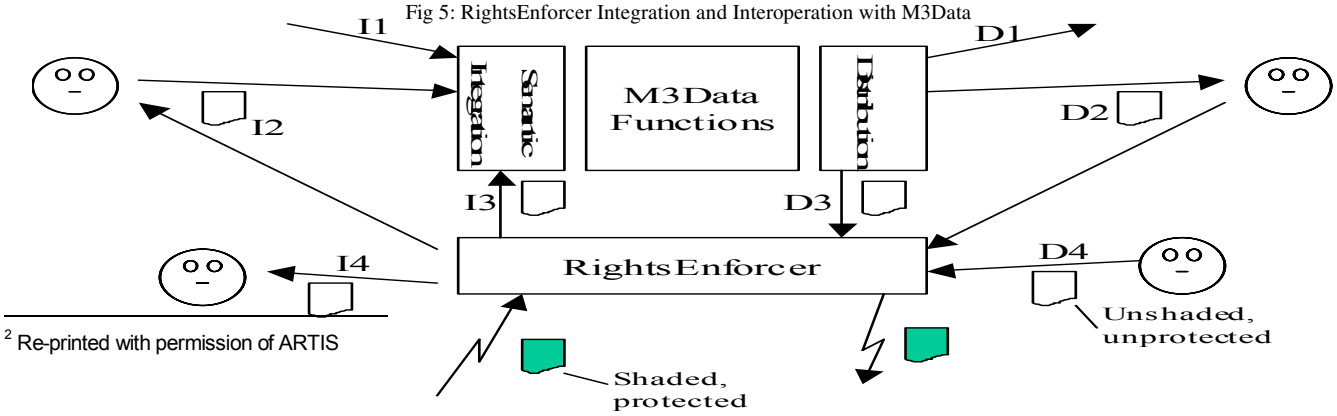
Fig. 5 illustrates the integration and interoperation of M3Data and RightsEnforcer. Several file data flows are depicted: I1 to I4 for system inbound communication, D1 to D4 for system outbound communication. An interpretation of each follows.

1). I1 – Most large volume M3Data inbound dataflow, defined and modelled databases and sensors are independent of RightsEnforcer. For example, considering the subject ship-harbor scenario, inputs might be coming from harbor-side smoke detectors directly to M3Data for integration and storage.

2). I2 – Some files carrying information destined for integrated databases are mediated by a human user of M3Data. The information is protected on the outside, beyond the domain of M3Data integrated data sources, received by an M3Data user, and input into the M3Data system in a more or less modified or interpreted form. For example, observations of trained observers of the urban conditions – road and traffic, buildings and people, weather and air quality – might be recorded in audio files in constrained but unstructured natural language. Unsynchronized, the audio files are persistently protected and emailed to central coordinators who listen, interpret and enter structured information into a database within the M3Data domain. In the future this dictating, interpreting and coding may become a specialized practice somewhat analogous to clinical data coding in medicine. To use the full power of M3Data human observation and interpretation must be applied to many complex inputs.

3). I3 – Some files of defined form and semantics are protected by RightsEnforcer outside the M3Data domain

Fig 5: RightsEnforcer Integration and Interoperation with M3Data



[2] Re-printed with permission of ARTIS

and delivered directly to M3Data without human intervention. M3Data processes them to augment databases and the knowledge base. There can be many information structures, including:

- Self describing files such as XML files,
- Web or database forms of a fixed format and semantics,
- Fielded files with a classic data processing record schema.

The first two forms carry information that can be automatically parsed and interpreted, and also read by human users. For example, ships cargo manifests are created in many different parts of the world according to different standards. While some may be available in a database integrated with M3Data, many others will need to be parsed, interpreted and added to an internal database.

4). I4 – M3Data users also receive inputs which are not bound for M3Data at all, but which must be protected. For example, an emailed query to a foreign intelligence service might be answered by a protected email but fall outside the scope of the M3Data information domain.

5). D1 – Some M3Data output is distributed without using RightsEnforcer. For example, automation and control commands to position cameras and turn on lights do not use file protection.

6). D2 – M3Data users extract a file from M3Data, manipulate, select or augment it using office software such as a word processor or spreadsheet, then protect and distribute it using push (e.g. email) or pull (e.g. Web download) network operations. For example, a central coordinator might be asked for a non-standard status report, such as the immediate availability of dockside crane operators. The coordinator can query M3Data for the current formal duty roster and off-duty operator list, but will need to phone several people to ascertain their availability and willingness to standby, type it into a report and send it off to the query source. We are currently working on the development of an automatic notification process that will replace the human operator by distributed intelligent software based on multi-agent technologies [2].

7). D3 – M3Data can use RightsEnforcer automatically, without human intervention to deliver sensitive information outside of its domain. The information can be a human readable document or a data file with defined permissions and defined life. For example, marine shipping security personnel may have a routine watch on vessels of certain registration and type and enter it into an M3Data-integrated database. M3Data routinely generates a report which it makes available in two ways: by posting it to an integrated document repository where users of M3Data can access it, and by pushing it out to certain people beyond the system user community, but with a need to know. Because this information should not be accumulated outside the document repository, the previous non-repository document is automatically disabled whenever a new one is generated.

8). D4 – Users of M3Data use RightsEnforcer to protect ad hoc communications of the knowledge synthesized in M3Data. The user will learn the information to be communicated from the M3Data system, from talking to other users, and from ad hoc sources such as telephone conversations. Then she will create an unstructured document or email and send it to those she judges have a need to know. For example, an M3Data user specializing in political and public relations studies the unfolding emergency in the harbour and composes an email with briefing and meet-the-press observations for the Minister of Transport. She sends it with RightsEnforcer persistent information security.

VI. FUTURE WORK

The ARM Platform provides a versatile template for the development of emergency response applications. The complexity in the development of such applications lies within the required knowledge engineering for this particular domain. The ARM testbed provides the much needed simplification of developing and deploying situational awareness command and control centers which are required to exploit information and coordinate response across many participating agencies. Our future work will gradually leverage the synergy of the advanced software and hardware technologies involved in the ARM platform to provide more and more complex solutions such as; using intelligent agent technologies [3] to make M3Data and RightsEnforcer fully interoperate and cooperative in the matters of single-sign on, access to RightsEnforcer protected documents by authenticated and authorized M3Data users, and the distribution to remote users by M3Data of confidential information that requires persistent protection “on the outside”.

In such dynamic, intrusive environments organizations need to be protected by strong security mechanisms, exceeding today’s web-service deployment standards. M3Data provides granular security, protecting every transaction that occurs on the system through full authentication, authorization, and audit trail. The M3Data security layer provides fine-grained access across all information assets, ensuring that both users and systems can only access information relevant to them. RightsEnforcer extends this control beyond first access to every subsequent access, local or remote.

VII. REFERENCES

[1] Mihaela Ulieru, Robert Brennan and Scott Walker, “The Holonic Enterprise – A Model for Internet-Enabled Global Supply Chain and Workflow Management”, International Journal of Integrated Manufacturing Systems, No 13/8, 2002, ISSN 0957-6061, pp. 538-550.

[2] Mihaela Ulieru, Adaptive Information Infrastructures for the e-Society, in Engineering Self-Organizing Applications, Giovanna DiMarzo Serugendo and Anthony Karageorgios (Eds.) Springer Verlag – LNAI 3464, Berlin 2005, ISBN: 3-540-26180-X , pp. 32-51

[3] Enrique M. Tognalli and Mihaela Ulieru, Pervasive Information Infrastructures for Industrial Informatics: An Application to Emergency Response Management, 3rd International Conference on Industrial Informatics, INDIN 2005, Perth, Australia, August 2005 (Proceedings on CD-Rom)

[4] Mihaela Ulieru and Paul Worthington, "Adaptive Risk Management System (ARMS) for Critical Infrastructure Protection", *Integrated Computer-Aided Engineering, Special Issue on Autonomic Computing*; ISSN: 1069-2509; IOS Press, Vol 13, No 1, 2006, pp. 63-80.

[5] Mihaela Ulieru and Dan Ionescu, Privacy And Security Shield For Health Information Systems (E-Health), Computer System Sciences & Engineering, May 2006 (http://www.crlpublishing.co.uk/Forthcsse.htm)

[6] Merv Matson and Mihaela Ulieru, "Persistent Information Security – Beyond the eCommerce Threat Model", Privacy, Security and Trust Conference, Canada 2006

[7] Mihaela Ulieru, Maja Hadzic and Elizabeth Chang, Soft Computing Agents for e-Health Applied to the Research and Control of Unknown Diseases, Information Science, Vol. 176/9, 2006 (available online September 2005)

[8] Garrett Camp and Mihaela Ulieru, InOrder – An Adaptive Visual Interface for Collaborative Knowledge Communities, International Journal of Multi-Agent and Grid Systems (submitted April 2006)

[9] Merv Matson, "A policy engine for granting access to persistently secure EHRs", eHealth 2002 Conference, Vancouver, Canada, 2002-Apr-21