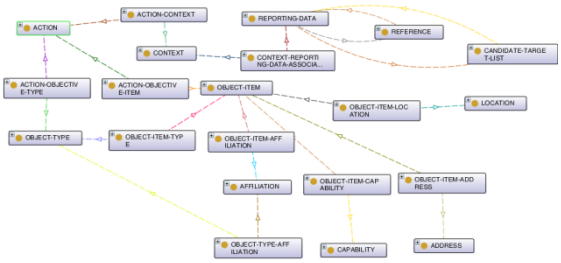
SRDC - EMERGENCY MANAGEMENT AND SECURITY

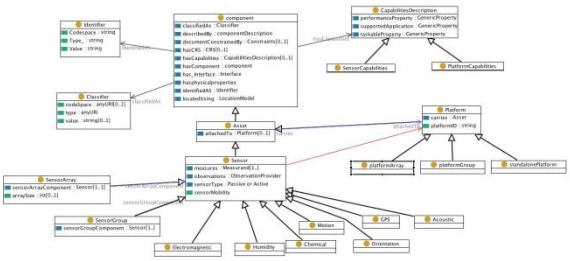
SRDC has been working on the emergency/crisis management nearly since its establishment. The team has extensive expertise in sensor management, interoperability of sensors, interoperability of command and control systems, emergency data standards and situational awareness.

RELATED PRODUCTS

SITUATIONAL AWARENESS ONTOLOGY

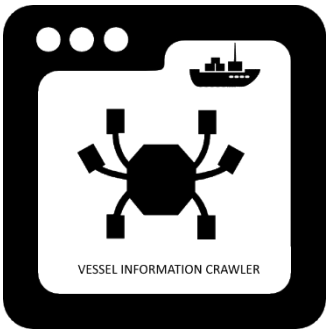


We believe that effective response to emergencies and crises depends on timely available, reliable and intelligible information. To achieve this, many different services from heterogeneous information sources, sensors, systems and organizations have to co-operate. The major bottleneck in this co-operation is the difference of the information models (and/or standards) that the emergency systems use. Therefore, we have harmonized the well-established emergency data standards into a single OWL-based Situational Awareness Ontology, which can be used as the lingua franca domain data model of the emergency/crisis management domain. The used standards are as follows:



- Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) of Multilateral Interoperability Programme (MIP)
- OASIS Emergency Data Exchange Language (EDXL)
- Open Geospatial Consortium's (OGC) Sensor Web Enablement (SWE)
- OASIS Common Alerting Protocol (CAP)

VESSEL INFORMATION CRAWLER



There are quite a number of Web sites providing information about vessels on the Internet. The information ranges from simple AIS data to sophisticated master, owner and history. There are also national online databases which contains detailed data about the ships such as captain, crew, cargo and passengers. It is a fact that more information means more situational awareness. In this respect, given the IMO (or MMSI) number of a vessel, Vessel Information Crawler tool gathers information about the vessel from the popular Web sites and stores the information to its database in terms of Situational Awareness Ontology. The stored data can be accessed through standard based interfaces.

SUSPICIOUS VESSEL BEHAVIOR DETECTOR

Suspicious behavior of a vessel is mainly identified by the operator in front of the command and control system. Therefore, the detection is totally based on human experience and gut feelings. In order to make this detection more effective, Suspicious Vessel Behavior Detector identifies the suspicious vessels automatically by inspecting their collected data. At the background the tool executes situational awareness rules (coded in Drools Rule Language), which means that the tool is highly extensible and customizable to the setting it is used on. The operators are allowed to define new rules (or edit existing ones) with user friendly interface. In this way, the organizational know-how of the operator can easily be captured and stored persistently. The tool can be integrated to any type of command and control system and ship information database as its interfaces are based on well-established standards. The Suspicious Vessel Behavior Detector has been successfully used in the scope of RECONSURVE Project pilots and deployed to Turkish Coast Guards.

C2 INTEROPERABILITY MIDDLEWARE

Today, *many different organizations having different Command and Control (C2) Systems and Sensor Systems* have to cooperate to provide effective response to emergencies and this cooperation would only be possible through interoperability. However, unless standards and well-defined specifications are used, the interoperability of these systems can be quite challenging, technologically complex, time consuming and expensive. For this purpose, we developed C2 Interoperability Middleware, based on well-established commonly used standard data models (the specifications used for Situational Awareness Ontology) and transport protocols (Web Service and Data Distribution Service). In the scope of RECONSURVE Project, the middleware have been used to establish interoperability of three Command and Control Systems. Furthermore, being based on well-known OGC SWE specifications, any type of compliant sensor system can be integrated to this middleware.

EMERGENCY PROFILE DEFINITION/SPECIALIZATION TOOL

There are commonly used standards and specifications (addressing also different layers in the communication stack) in the command and control, sensor and emergency management domains. However, there is no single specification of using these standards together in an emergency situation. These dispersed standards and specifications in these domains create a crucial interoperability challenge. To address this challenge profiling is a practical approach to achieve seamless interoperability by addressing all the layers of the communication stack in the security field. The profile concept aims to eliminate the need for a prior bilateral agreement between any two information exchange partners by defining a standard set of messages/documents, choreographies, business rules

and constraints. The profile compliant partners are able to exchange information and services among themselves in a plug & play manner. This is in contrast to the bilateral agreements that have to be settled between partners for each new exchange partner. Considering the nature of emergency management, where the responding organizations can change at run time (especially in an international intervention case), and these generic profiles permits coordination flexibility to deal with the unexpected circumstances and to prevent chaotic response to crises situations. Therefore, Emergency Profile Definition/Specialization Tool allows the users to specify profiles based on well-established standards and customize them to real-life settings.

SEMANTIC MDR

Semantic MDR EE is a web-based metadata management and data modeling tool to create and maintain common data models collaboratively either based on imported standard content models or from scratch. Through its spreadsheet based user-friendly interfaces, it hides the implementation specific details and allows the modelers to focus on the data models to be managed. The current version of the tool contains the concepts of Emergency Data Exchange Language (EDXL) and OGC SWE specifications. In this way, these standards can be customized to real-life use cases collaboratively.

SECURITY AND PRIVACY SUITE

Maritime situational awareness is a goal which cannot be reached without cooperation or exchange of information. However, the exchanged data is quite confidential such that most of the time it contains personal data and/or company data. An unavoidable amount of maritime reporting and surveillance data is qualified, in the national legal framework of European member states, as confidential. The importance of addressing these questions properly, giving them the adequate importance that they claim, is clearly the main concern. Through the Security and Privacy Suite, the participants can define the access rights to the information that they want to share. Also through the tools the confidentiality and integrity of the exchanged data are ensured. The suite is based on well-known recent security standards like Security Assertion Markup Language (SAML), eXtensible Access Control Markup Language (XACML) at the authorization and authentication level and TLS/SSL at the confidentiality and integrity level.

RELATED PROJECTS

ITEA2 – RECONSURVE: RECONFIGURABLE SURVEILLANCE SYSTEM WITH COMMUNICATING SMART SENSORS - HTTP://WWW.RECONSURVE.EU/

RECONSURVE
A Reconfigurable Surveillance System with Communicating Smart Sensors.

RECONSURVE is a reconfigurable maritime surveillance framework with multimodal smart sensors installed on various platforms forming a coherent network via interoperability interfaces. The RECONSURVE project aims to address the need to control the rapidly increasing number and complexity of maritime surveillance issues such as illegal immigration especially using small vessels, interoperability between heterogeneous systems, automated cost-

effective and efficient decision support. Although there are some maritime surveillance systems available, they lack the technical and architectural maturity to tackle all these requirements at once. Some companies have some of the RECONSURVE subsystems as individual, disparate systems; some have "unified" systems that display several data feeds all at once without the critical automated decision making and support component and yet some have an integrated system with only very limited algorithmic capabilities. A maritime surveillance system with a diverse set of smart sensors installed on various platforms forming a coherent network via interoperability interfaces would address maritime border security needs properly.

ITEA3 – APPS: ADVANCING PLUG & PLAY SMART SURVEILLANCE - HTTP://WWW.APPS-PROJECT.EU/

At present, surveillance systems in the maritime domain consist of radar and visual sensors. Whereas radar is used to detect and track vessels, the visual sensors are used for securing borders in and around large infrastructures as e.g. along a coast or in a harbor. These sensors are never used in conjunction in their full capacity and have severe limitations. Radar is only capable of detecting large vessels without getting details about the type and identity, whereas visual sensors are too static and hamper 3D capabilities. Therefore, future surveillance systems will differ significantly from today's systems in several important ways by exploiting the benefits of different sensor modalities. They will integrate high-quality (HD and 3D video), multi-sensory data inputs taken from multiple viewpoints, exchange multi-streamed data between subsystems and take action in a plug-and-play fashion, whereby the multidimensional data is analyzed in real-time. This will place unprecedented demands on networks for high-capacity, low-latency, and low-loss communication paths. The APPS project will contribute to this transition by advancing the state-of-the-art in surveillance systems in three key areas:

1. It will enable the development of plug & play solutions
2. It will enhance the sensor processing and intelligent decision-making capabilities and intelligent operator aids of such systems to achieve smart surveillance in large spaces such as coastal areas and harbors with critical infrastructures.
3. It will develop a robust communication layer over heterogeneous technologies.

FP7 – C2-SENSE: INTEROPERABILITY PROFILES FOR COMMAND/CONTROL SYSTEMS AND SENSOR SYSTEMS IN EMERGENCY MANAGEMENT - HTTP://C2-SENSE.EU/

C2-SENSE project's main objective is to develop a profile based Emergency Interoperability Framework by the use of existing standards and semantically enriched Web services to expose the functionalities of C2 Systems, Sensor Systems and other emergency/crisis management systems. C2-SENSE will assess its outcomes in a realistic "Flood Scenario in Italy" pilot to ensure that the developed technologies are generic and applicable in a real life setting.

PARTNERSHIPS

Having been active in emergency management domain, we have quite a number of contacts ranging from big private companies to emergency public institutes in Turkey:

- ASELSAN: Turkey's biggest defense company
- Prime Ministry Disaster & Emergency Management Authority
- Turkish Coast Guards
- Turkish State Meteorological Service
- Ministry of Health Emergency Services and Hospitals

TOPIC SPECIFIC CONTRIBUTIONS

DRS-01-2015: CRISIS MANAGEMENT TOPIC 1: POTENTIAL OF CURRENT AND NEW MEASURES AND TECHNOLOGIES TO RESPOND TO EXTREME WEATHER AND CLIMATE EVENTS

With the know-how gained from the C2-SENSE project, we have extensive experience on standards based communication among the first responders of emergency cases. Therefore, for this topic we can provide our experiences based on Command and Control systems interoperability. Furthermore, we can provide two use cases for extreme weather and climate events:

1. In Turkey, with Turkish State Meteorological Service and - Prime Ministry Disaster & Emergency Management Authority
2. In Italy Puglia Region, with our partners in C2-SENSE Project (Regione Puglia, Innova Puglia)

DRS-12-2015: CRITICAL INFRASTRUCTURE PROTECTION TOPIC 1: CRITICAL INFRASTRUCTURE "SMART GRID" PROTECTION AND RESILIENCE UNDER "SMART METERS" THREATS

For this topic, we can provide a Turkish smart meter use case. We have contacts from Turkish Telecom, AVEA GSM Operator, Turkish Smart Meter Producers and Turkish Electricity Distributor.

BES-01-2015: MARITIME BORDER SECURITY TOPIC 1: RADAR SYSTEMS FOR THE SURVEILLANCE OF COASTAL AND PRE-FRONTIER AREAS AND IN SUPPORT OF SEARCH AND RESCUE OPERATIONS

We have extensive experience on maritime security through the RECONSURVE Project. We can bring our experience mainly on Situational Awareness and Interoperability. Furthermore, together with ASELSAN and Turkish Coast Guards we can develop a Turkish use case.

BES-04-2015: MARITIME BORDER SECURITY TOPIC 4: DETECTION OF LOW FLYING AIRCRAFT AT NEAR SHORE AIR SPACE

Like for BES-01-2015, we have extensive experience on maritime security through the RECONSURVE Project. We can bring our experience mainly on Situational Awareness and Interoperability. Furthermore, together with ASELSAN and Turkish Coast Guards we can develop a Turkish use case.