[PRACTICE]

D5.1 SOFTWARE SENSOR COMMUNICATION STANDARDS

PRACTICE WP5 deliverable

Dissemination level: Public

Nature: Report

UNCLASSIFIED

Title:	**D5.1 Software sensor communication Standards**
Date:	20 Aug, 2012
Author(s):	Frédéric Perlant ASTRIUM Services

This project has received funding from the European Community's Seventh Framework Programme. The views expressed in this document are purely those of the writer and may not in any circumstances be regarded as stating an official position of the European Community.

Summary Work Package 5

The overall aim of the project “Preparedness and Resilience Against CBRN Terrorism using Integrated Concepts and Equipment” (PRACTICE) is to improve the ability to respond to and recover from a Chemical (C), Biological (B), Radiological (R) or Nuclear (N) incident. The objective of the project is to create an integrated European approach to a CBRN crisis – i.e. a European Integrated CBRN Response System. This will be achieved through the development of an improved system of tools, methods and procedures that is going to provide EU with a capability to carry out a truly integrated and coordinated operational reaction following the occurrence of a CBRN crisis, whether it is caused by a terrorist act or an accident.

The objectives of WP5 are to develop, integrate and test a complete toolbox for first responders, decision makers and the public, including innovative components developed during the project to provide an improved and integrated preparedness and response to CBRN events.

The tools will be organized in 6 categories:

1. Recommendations
2. Standards
3. Protocols / procedures
4. Equipment and systems (eventually simulated): hardware, software, with performances, Technology Readiness Levels (TRLs), validation/certification status
5. Simulated environment (with 3D databases)
6. Real equipment and system emulation capabilities.

These tools will fulfil functions as defined in WP3, organized in line with the ESRAB/Staccato taxonomy functions, completed and detailed when needed for PRACTICE. The toolbox should be considered as living system gathering “bricks” into an integrated solution to manage a CBRN crisis. It will include actual tools and equipment and ICT simulated environments including hardware and software. This will allow plugging and playing new components and guarantee their interoperability.

The toolbox will be developed and integrated in two steps:

- A V0 version integrating in an innovative way existing validated capabilities (fed from WP 2 and WP 3) i.e., tools, methods and procedures that will be put together into an information system, with specified standard interfaces.

- A V1 version integrating innovative tools, methods and procedures and supporting future standards to improve interoperability and consistency without impeding the existing operational systems.

Developing V0 and new CBR tools for V1 will be an iterative process with all the stakeholders in the loop. Focus will be put on specifying simple interfaces for any supplier to describe and present its "bricks" in order to "index / reference" them in our PRACTICE Toolbox Information System. Any new tool that satisfies the "standards" interfaces should be easily added to build new solutions ("buildings").

Work Package team:

Frédéric Perlant	Astrium S.A.S. (AST)
Wilfrid Lefebvre	Astrium S.A.S. (AST)
Erik Bakke	Bruhn Newtech A/S (BNT)
Stéphanie Damiot	Cassidian S.A.S. (EADS)
Dominic Kelly	CBRNE Ltd (CBRNEltd)
Jamie Braybook	CBRNE Ltd (CBRNEltd)
Kristian Krieger	King's College London (KCL)
Athanasios Sfetsos	National Center for Scientific Research "Demokritos" (NCSRD)
Frank van het Veld	Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
Ingrid Bastings	Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
Ed van Zalen	Netherlands Forensic Institute (NFI)
Kristi Mo	Norwegian Defense Research Establishment (FFI)
Iain Clark	Selex Galileo Ltd (SELEX)
Giuseppe La Posta	Selex Sistemi Integrati SPA (SSI)
Josef Brinek	Statni Ustav Jaderne, Chemicke A Biologicke Ochrany vvi (SUJCHBO)
Ola Claesson	Totalforsvarets Forskningsinstitut (FOI)
Paul Hooijmans	Prometech BV (PRO)
Florian Käding	Prometech BV (PRO)
Luc Sengers	Prometech BV (PRO)
Pierre-Alain Fonteyne	Universite Catholique de Louvain (UCL)

Contents

1. Executive Summary

This document will describe the Software Sensor Communications standards that should be considered for inclusion in and supported by the PRACTICE Toolbox. This document is part of the work package 5 in the FP7 **PRACTICE** project.

These standards satisfy the key features of PRACTICE that are at least :

- European scope to guarantee interoperability within Europe
- non-proprietary unless this is a *de facto* standard
- prone to be widely deployed in the future
- benefiting from the big investments in the civil domain.

This report :

- examines the main standards and protocols that should be considered for use in PRACTICE
- describes their features with advantages and limitations and
- identifies how we plan to implement and handle them in the Toolbox.

The standards are almost entirely wireless-based since wired sensors in a crisis situation may be problematic and physical interoperability is difficult to ensure.

- 802.15.4
- Bluetooth and BlueTooth Low Energy
- 802.11 (WiFi)
- GPRS / 3G
- Satellite
- PMR (TETRA / TETRAPol)
- NFC

The protocols are IP-based to enable integration with existing networks and the Internet

- IP
- 6LoWPAN (IPv6 for Low Power Wireless Personal Area Networks)
- CoAP (Constrained objects Application Protocol)

2. Introduction

This document will describe the Software Sensor Communication Standards recommended for inclusion within the PRACTICE Toolbox. The purpose of this document is threefold:

1. Detail the communication standards that are relevant to the PRACTICE Toolbox
2. Justify the inclusion of those standards in the PRACTICE Toolbox
3. Identify how the standards should be utilised in the Toolbox

2.1 Context

The Software Sensor Communication Standards will be implemented and utilised by WP5 of the PRACTICE project. The standards recommended within this document have been highlighted due their potential to bring together disparate sensor networks for use across the European Union.

ASTRIUM is a consortium partner leading the WP5 work package, responsible for the implementation of the PRACTICE Toolbox. Furthermore ASTRIUM, as a service provider in a number of fields including Telecommunications and Public Safety, possesses strong expertise in this area.

2.2 Problem Definition

One of the key technical challenges in tackling a major incident, whether it be CBRN, explosive device or natural disaster, is that of information gathering. The first hours of an incident are the most critical, in this respect, in order to allow first responders, emergency services and potentially heads of government to decide on the correct course of action. Even after the first hours have passed the ability to continue gathering information throughout the lifetime of the incident and beyond is key. Without this ability the potential for loss of life to both emergency services and the general public due to a lack of situational awareness is high.

Across Europe today there are thousands of potential information sources that, if made available, would greatly enhance the ability of those responding to incidents. These information sources come in the form of electronic sensors which can provide a wealth of information such as:

- Meteorological Data such as rainfall, wind speed, temperature and humidity
- Air Pollution Data
- Structural Data pertaining to buildings or bridges for example
- Tracking
- Specific CBRN measures

However, although there are many sensors already in place and/or brought to the field at a given time (either fixed or mobile / handheld) it is by no means easy to access them in a coherent and interoperable manner. This is mainly due to the proprietary nature of protocols and communication methods that exist across the various sensor suppliers.

If a way forward can be found to allow responders, other systems and indeed other sensors (Machine to Machine) to access data in a coherent and integrated way it will vastly increase the ability of responders to deal with CBRN incidents as well as ensuring greater safety for the public at large.

2.3 Project Scope

In order to facilitate the use of sensors in a coherent and interoperable way there are two main areas that require attention. These are as follows:

- **Communication Standards:** Although many communication standards exist the main goal of PRACTICE in this context is to enhance the interoperability and the capabilities of diverse tools to operate together. This document will look into existing standards that cold potentially be utilised to allow access to sensors in a 'generic' way as well as up and coming standards that could potentially provide a way forward for the future in this area.
- **Communications Protocols:** In order to fully benefit from interoperable communication standards there also needs to be in place communication protocols that utilise these standards. The protocols are the key to making best use of the communications available and as such this document will also consider the protocols available today and those that are up and coming for the future.

2.4 End-users

Considering the nature of the PRACTICE project it is highly likely that end users will be accessing these systems while under conditions of considerable stress. It is therefore imperative that the user experience is one of simplicity. It should not be the case that the a user has to access many different options because of the nature of the sensors that are being accessed.

This document will attempt to detail how these systems could potentially be brought together to allow numerous different types of user access via a straightforward internet based interface. The potential user base of a system such as this, are too many to mention however examples of some of the key users are listed below:

- Emergency Services
- Military Personnel
- Members of the public
- Politicians and decision makers

2.5 Document Contents

This document will be divided in three major sections The first section gives background information on sensors and sensor networks, the second outlines the standards and protocols and the third describes how these standards and protocols can be pulled together to potentially meet the objectives of the PRACTICE project

3. Sensor Communications and Sensor Networks

Before detailing the standards and protocols themselves it is important to understand how communications to and from sensors and networks of sensors typically function. This will help put the standards discussed later in the document into context.

3.1 Wired Sensors

Wired Sensors are those that are physically connected into a communications infrastructure. Typically these devices either communicate directly over Ethernet using IP protocols or they communicate in a proprietary way to a modem connected to Ethernet. The modem then translates the proprietary signals to IP traffic and passes these on to consuming systems or networks.

3.2 Wireless Sensors

Wireless Sensors are those that are not physically connected to a network by wires such as Ethernet cabling. They can be used on a single site in much the same way as Wired Sensors thus reducing the implementation cost by negating the need to add Ethernet cable. They can also be used remotely to monitor many different variables (Refer to section 3.2 for examples).

The key problem with locating sensors remotely is power. In a typical scenario a sensor is a small device (sometimes extremely small when deployed in a covert way) not physically connected to a power source and as a result in many cases not capable of utilising long range high bandwidth communication networks such as GPRS for example. The result is that most wireless sensors in place today utilise short range low bandwidth wireless communications. The problem that this presents is that in order to gather information a receiver needs to be within range of the wireless signal.

The solution to this problem comes in the form of a Wireless Sensor Network (WSN). A WSN consists of spatially distributed autonomous sensors that cooperatively pass their data through the network to a central location. Figure 1 shows the two main network topologies, star and mesh, that facilitate the passing of data through a WSN.

- **Star**: All sensors transmit data to a central node which typically processes it and passes it on to a another network such as the internet.

- **Mesh**: Sensors in a mesh network act as routers for other sensors in the network. This allows data to be transmitted over larger distances while still utilising short range low bandwidth wireless communications. It also provides redundancy as the nodes in the network will reconfigure themselves to use a different route if one of the nodes goes offline.

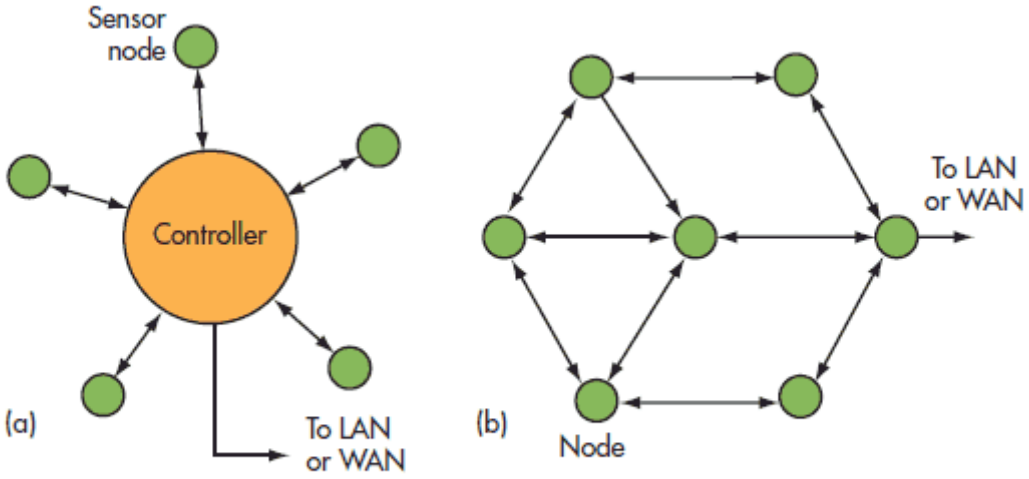

Figure 1

4. Sensor Communication Standards and Protocols

4.1 Wireless Communication Standards

The following table lists the key wireless communication standards.

ST-1	**IEEE 802.15.4** • Focuses on delivering communications between nearby devices (10 – 100m) with little or no underlying infrastructure. This means that 802.15.4 implementations (Zigbee, WirelessHART, ISA100.11a) have very low power consumption and therefore function extremely well in remote battery powered sensors. Implementations of 802.15.4 also have the facility to provide large scale MESH networks of thousands of sensors if required. However it should be noted that where data rates are high 802.15.4 implementations are unsuitable.
ST-2	**BlueTooth** • Focuses on delivering communications between nearby devices (typically within 10m). Bandwidth is higher than 802.15.4 implementations and power consumption is reasonably high which tends to make Bluetooth unsuitable for remote battery powered sensors. BlueTooth is also not designed to function in a MESH network and

	as such its use is limited to small scale deployments. BlueTooth however is widespread in society today and as such it may be an attractive alternative where power consumption and sensor numbers is not an issue.
ST-3	**BlueTooth Low Energy (BLE)** • Focuses on delivering communications between nearby devices (10 – 50m). Very low power consumption due to the nature of the underlying protocol. This means that BLE should function extremely well in remote battery powered sensors. However BLE is optimized to function in STAR networks as opposed to MESH networks and as such may be limited to small scale deployments.
ST-4	**WLAN (IEEE 802.11)** • Focuses on delivery of high bandwidth communications between nearby devices (typically 50 – 100m). Power consumption is high and as such WLAN is unsuitable for remote battery powered sensors. WLAN is typically used to integrate into a fixed Ethernet network and as such can be a viable option if sensor power is not an issue and data rates are high. As with Bluetooth WLAN is widespread in society which makes it an attractive option where the situation permits it.
ST-5	**Near Field Communication (NFC)** • Focuses on delivering very short range low data rate (typically within 4cm) point to point communications. Is also compatible with RFID devices. Power consumption is low however suitability for remote sensors is limited due to the very short range nature.
ST-6	**Professional Mobile Radio (PMR)** • Typically these systems are used by emergency services to communicate by voice but they also possess the ability to pass data over secure channels. Protocols tend be proprietary and specific hardware resources are normally required to gain entry to the network. However, modems for standards such as TETRA do exist and therefore usage of these networks for long range data communication between sensors and personnel may be an option in certain scenarios. However bandwidth and data transfer rates tend to be low.
ST-7	**Satellite** • Medium to high bandwidth secure communications. Typically used in areas of poor coverage for systems such as PMR and GSM.
ST-8	**General Packet Radio Service (GPRS)** • Medium bandwidth GSM based mobile data service. Due to the GSM based nature of GPRS it is unsuitable for short range communication between nodes in a sensor network. However, due to the international nature of GPRS coverage via the cellular network it is a candidate for long range data communications between sensors or sensor networks as a whole.

4.2 Sensor Communication Protocols

There are two main standards that are worth of mention, these are:

- **Sensor Web Enablement (SWE):** The Open Geospatial Consortium (OGC) have published a number of standards which collectively come under the name *OGC Sensor Web Enablement (SWE)*. These standards are designed to allow systems to interact with all different sensor types in a fixed way using a common interface. As a blueprint for communicating with sensor devices the *SWE* provides a solid and well thought out set of interfaces. However, the interfaces and services they provide have been developed utilizing standard SOAP based web services methodologies. The constrained nature of a large number of deployed devices makes the utilization of SOAP based Web Services impossible without changes to the underlying standards and protocols. It could also be argued that the RESTful approach to Web Services would better lend itself to device communication, due to it's simplicity and underlying methodology of simply transferring the state of an object.

- **Common CBRN Sensor Interface (CCSI):** Developed by the Joint Program Executive Office for Chemical and Biological Defence (JPEO-CBD) in the USA the CCSI is to "enable CBRN sensor interoperability, net centric operations, and ease of integration into Command and Control Systems". The standard covers all aspects from software communication protocols right down to physical hardware interfaces. The main issue with CCSI is the proprietary, complicated nature of the protocol. However the OGC have published a report detailing how the CCSI can be integrated into the SWE in order to make the standard more 'open'.

The protocols above have been produced in an attempt to standardize communications with sensors because the protocols currently used by sensors tend to be proprietary. This is mainly due to the limitations of the communications standards used. For example using HTTP over IP to communicate with a device on a 802.15.4 based network would not be possible due to the constrained nature of the sensors and of the network itself.

However there is an emerging family of protocol standards that is designed to allow devices such as 802.15.4 based sensor networks to communicate using IP. These protocols are designed to allow sensors to participate in *'The Internet of Things'*. This is a concept that envisages vast numbers of devices connected directly to the internet. One of the many definitions available attempting to summarize this concept defines the Internet of Things as

"A world where physical objects are seamlessly integrated into the information network, and where physical objects can become active participants in business processes. Services are available to interact with these 'smart objects' over the internet, query and change their state and any information associated with them, taking into account security and privacy issues"

The protocols that are as follows:

- **6LoWPAN**: Protocol standard from the Internet Engineering Task Force (IETF) designed to optimize IPv6 for low power, low bandwidth communications networks such as 802.15.4.

- **CoAP**: The Constrained Application Protocol is a protocol standard from the IETF designed to enable end to end RESTful web services for constrained devices such as sensors in a Wireless Sensor Network.

5. Technologies

A full-blown system design specification is beyond the scope of this document. However, for clarity it can be beneficial to concisely outline the technologies that could be used in order to meet the objectives of the PRACTICE project.

It should be noted that while each of the communication standards listed in section 5.1 have pros and cons none of them can be discounted in favour of the others. The deployment of sensors and the communication standard they use is purely dependent on the individual situation being monitored. Each situation is different and as such one can not be favoured over another. However in order to meet the objectives of the PRACTICE project these standards need to be interoperable. Also the end users of the systems need to be presented with simple, easy to use consistent interfaces. At first glance this may appear to be an insurmountable task however there are two major goals that, if met, will help to achieve this. These are:

- **IP Based Backend Communications:** IP is the protocol that relays data across internet. It is solid, well understood and underlies the digital age in which we live. In order to have an interoperable network of sensors all of the communications between the end user and the sensor networks needs to be done via IP. This will allow the front end systems to utilise existing networks and technologies without having to ‘re-invent the wheel’. This does not mean however that the sensors themselves must communicate using IP.
- **Common Communication Protocol:** While it is imperative that IP is used to carry data, the data itself needs to be standardised as close to the sensors as possible. This in practice typically means protocol translation at some point in the communications chain.

5.1 Interoperability via Current Technologies

Figure 2 below shows a high level overview of how the goals of PRACTICE could potentially be achieved today by utilising a *Data Communications Gateway (DCG)*. The role of a DCG (which can be hardware or software based) in this context is to act as a mediator. The end user systems make simple web service calls which are translated into a common protocol by the web service. This call is passed to the DCG which translates the request using the protocol required by a particular sensor. Finally the DCG passes the request to the sensor utilising the required communication standard. This process then works in reverse in order to pass data back to the end user.

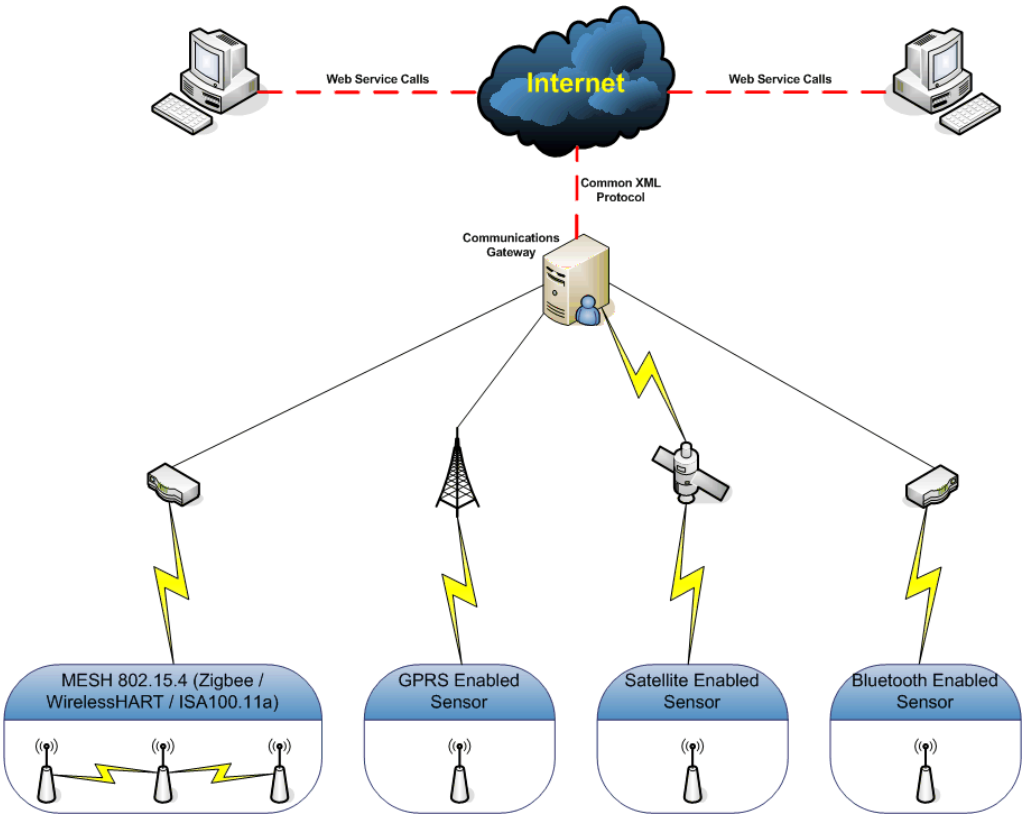

Figure 2

5.2 Interoperability Moving Forward

This concept fo utilising a DCG could be taken one step further by utilising the new protocol standards designed for device integration with the internet. Figure 2 shows (via the red communication lines) where IP should be used as the communication protocol in order to increase interoperability between devices. However, devices that are enabled with a *6LoWPAN* stack can communicate directly using IP. Combine this with CoAP and you have the ability to control and query a sensor directly from a browser via a web service call without the need for translation back and forth between proprietary protocols.

5.3 Integration into the PRACTICE Toolbox

The PRACTICE toolbox will be built around the concept of so-called ‘functions’. Functions are the tools and procedures used to handle incidents, which will be included and integrated in the PRACTICE toolbox. The toolbox will be a web based Information system (“database”) fed with a catalogue of existing and innovative components provided and developed during the project.

The PRACTICE Toolbox is meant to be an integrated solution to manage CBRN incidents. One of the bigger challenges in the PRACTICE project will, in fact, be this integration of all functions and components in one large package: an integrated toolbox.

Detailed decisions on how the standards and technologies discussed in this document should be integrated into the toolbox are not possible until the toolbox architecture is defined in more detail. The integration will be performed at various levels. However, among others, Service Oriented Architecture techniques utilising Web Services are standards ways to support tight interfacing and will form the core of the integration.

6. Conclusion

There are many different communication standards in play today many with most of them utilising proprietary protocols. As such it would be difficult if near impossible to attempt to standardise on a single one. Each monitoring situation is different, remote sensors often need to run in low power situations and as such need to utilise low power low bandwidth standards such as 802.15.4. Other situations may lend themselves to using sensors with standard powered 802.11 (WiFi) equipment. With this in mind if integration with existing sensors is a requirement then Data Communication Gateway technologies should be investigated in order to standardize the interface to the end user.

In new / future deployments sensors with IP capability should be used. The communication standard (whether this be 802.15.4, 802.11, GPRS or any of the others) is not the key factor, as long as the underlying stack is IP based this gives the devices the ability to connect into existing networks and the internet.

As far as communication with the IP based devices is concerned the OGC Sensor Web Enablement standards provide a solid base for sensor communication. The CCSI, while rich in content, leans too far toward a propriety interface specifically designed for CBRN Sensors. If the goal of PRACTICE is to utilise only CBRN sensors then CCSI would be a credible way forward. However if the goal of PRACTICE is to make use of all information at it's disposal including tapping into next generation internet technologies such as the 'Internet of Things' then utilising CCSI directly is not an option. In this scenario it would be better to abstract the CCSI by wrapping it in an OGC SWE service.

It should be noted that in order to future proof deployments and to fit better into 'The Internet of Things' these standards should to be utilised in a RESTful way.

Where low power / low bandwidth situations occur, devices that implement the emerging 6LoWPAN IP stack and the CoAP Protocol should be seriously considered. These standards and protocols will enable simpler integration with existing networks and systems and help facilitate M2M (Machine to Machine communication). It may also be possible to implement the OGC SWE, or a subset of it, over CoAP however this would require investigation.