



Workshop W1-Position- / Discussion Paper
**Creating robust sensor networks - architecture and
infrastructure**

Workshop will be organised by

Gerald Schimak, *Austrian Research Center GmbH – ARC (gerald.schimak@arcs.ac.at)*

Robert Argent, *The University of Melbourne, Australia*

Thomas Usländer, *Fraunhofer IITB, Germany*

Nigel W.T. Quinn, *Lawrance Berkeley National Laboratory, California, USA*

Denis Havlik, *Austrian Research Centers GmbH – ARC, Austria*

Abstract: Significant uncoordinated development in the areas of sensor devices, protocols and networks is occurring in the areas of air and water quality monitoring and management, with a focus also on impacts on health and human exposure. It is well accepted that monitoring of our planet is done by sensors put into orbit. However, for surface monitoring we lack the interconnectivity of both in-situ and remote sensing devices to properly monitor systems and link to interoperable information systems. One reason for this is the lack of a sensor network infrastructure generic enough to support this interoperability and interconnectivity.

This workshop will explore architectural aspects of creating robust sensor networks and further develop architectures and infrastructure to support this by taking into account topics such as interoperability, self-organisation, network management and sensor network architectures

Encouragement

For the stimulation of discussion during the workshop we encourage you to send in abstracts related to sensor networks – architecture and infrastructure focusing on one or more of the problems/challenges detailed in the sections thereafter. You may of-course address other important challenges and/or requirements not mentioned below coming from other domains or European Directives (like INSPIRE or GMES) or worldwide initiatives (like GEO or GEOSS) putting additional requirements, constraints or challenges on the sensor network architecture.

Workshop participants

Workshop participants planning an abstract submission should contact the workshop organisers (best immediately) to indicate interest. Please send an email to the workshop contact: **Gerald Schimak** <gerald.schimak@arcs.ac.at> and provide an abstract.

Workshop participants should send their abstracts (three pages at most) by Feb 28, 2008, for a reviewing process managed by the workshop organisers. See the format for abstracts and position-papers in the Format For contributions section see website, at <http://www.iemss.org/iemss2008/>

1. INTRODUCTION

Sensors provide some of the basic input data for environmental monitoring as well as for risk management of natural and man-made hazards. Here the word ‘sensors’ covers everything from remote sensing satellites, providing invaluable images of large regions, through instruments installed on the Earth’s surface to instruments situated somewhere in our environment providing highly-detailed point-based information from single sites.

Since data from sensors plays such an important role in improving our understanding of the environment, considerable investment has been made in the construction and maintenance of highly-sophisticated sensor networks.



In spite of the ubiquitous need for information from sensor networks, the use of such data is hampered in many ways.

Firstly, information about the presence and capabilities of sensor networks operating in a region is difficult to obtain due to a lack of easily available and usable meta-information.

Secondly, once sensor networks are identified their data it is often not straightforward to access due to a lack of interoperability between dissemination and acquisition systems.

Thirdly, the transfer and processing of information from sensors is limited, again by incompatibilities between systems. Therefore, the current situation leads to a lack of efficiency and limited use of the available data that has an important role to play in risk mitigation.

2. CREATING ROBUST SENSOR NETWORKS - CHALLENGES

Creating robust networks has many challenges and many facets on different development levels e.g. as shown in Figure 1: Functional Domains. (Note: SANY Deliverable(s) – to be published soon on www.sany-ip.eu).

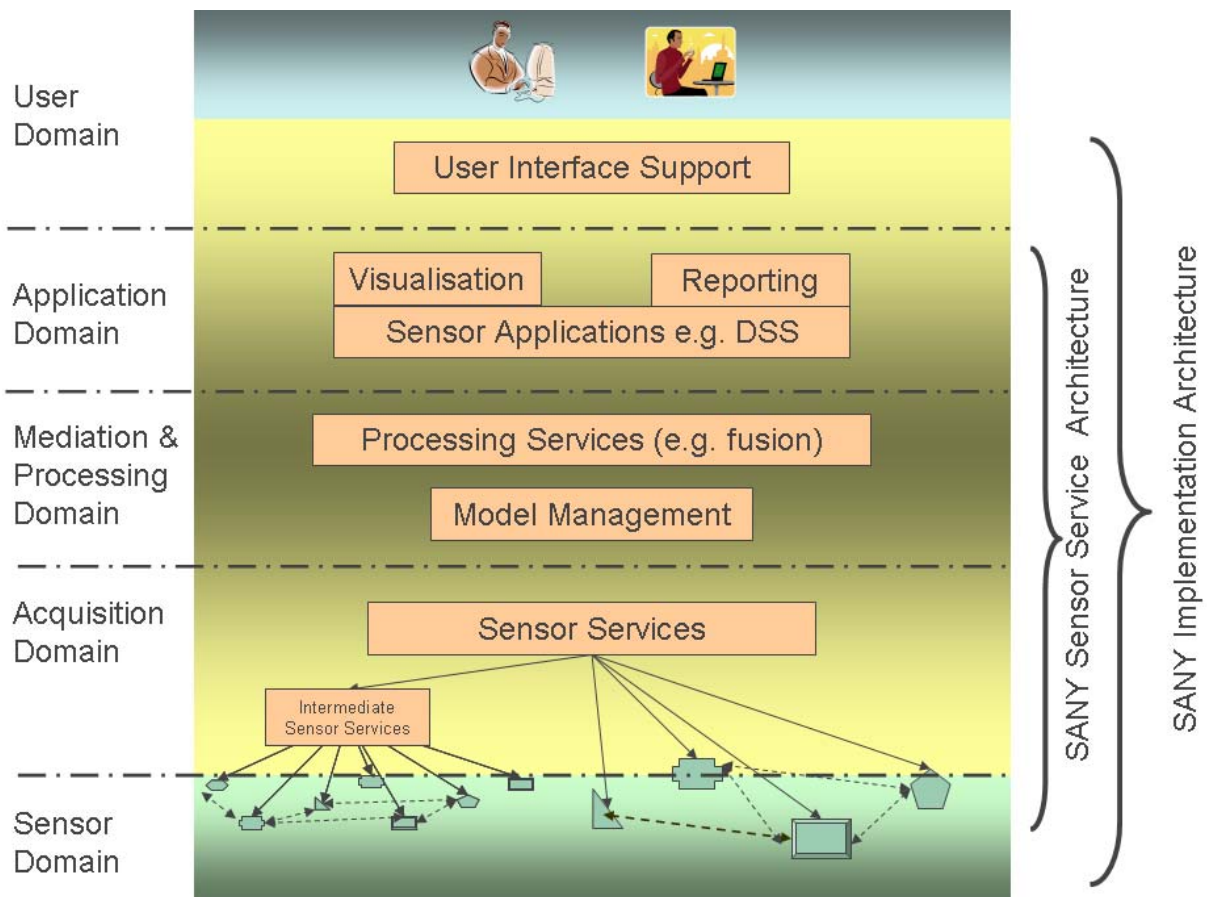


Figure 1: Functional Domains (courtesy SANY-Consortium)



iEMSS 2008 – Workshop Sensor Networks – Architecture & Infrastructure

ISESS

2.1 Generic (Architectural) Requirements

One major challenge when specifying and developing new sensor networks is to select the right architecture to base it on. Thanks to an EU FP6 project called ORCHESTRA we now have guidelines for requirements about how to build future-oriented service oriented architectures (www.eu-orchestra.org).

However, the architectural principles that have guided the specification of the ORCHESTRA Architecture have to be revisited and assessed specifically for service networks that include the access to sensors and sensor-related information.

Results for discussion are presented in the following sections.

- **Rigorous Definition and Use of Concepts and Standards**
A Sensor Service Architecture shall make rigorous use of proven concepts and standards in order to decrease dependence on vendor-specific solutions, help ensure the openness of service network and support the evolutionary development process of an architecture.
- **Loosely Coupled Components**
The components involved in a service network shall be loosely coupled, where loose coupling implies the use of mediation to permit existing components to be interconnected without changes.
- **Technology Independence**
A Sensor Service Architecture shall be independent of technologies, their cycles and their changes as far as practically feasible. It must be possible to accommodate changes in technology (e.g. lifecycle of middleware technology) without changing the Sensor Service Architecture itself. The Sensor Service Architecture shall be independent of specific implementation technologies (e.g. middleware, programming language, operating system). In general and if possible, the Sensor Service Architecture shall not be influenced by or deal with limitations of specific implementation technologies.
- **Evolutionary Development - Design for Change**
A Sensor Service Architecture shall be designed to evolve, i.e., it shall be possible to develop and deploy the system in an evolutionary way. A Sensor Service Architecture shall be able to cope with changes of user requirements, system requirements, organisational structures, information flows and information types in the source systems.
- **Component Architecture Independence**
A Sensor Service Architecture shall be designed such that a SANY service network and source systems (i.e. existing information systems, sensors and sensor networks) are architecturally decoupled. This means that a Sensor Service Architecture shall not impose any architectural patterns on source systems for the purpose of having them collaborate in a Service Network, and no source system shall impose architectural patterns on a Sensor Network Architecture.
- **Generic Infrastructure**
Services shall be independent of the application domain. This means that Services shall be designed in such a flexible and adaptable way that the Services can be used across different thematic domains and in different organisational contexts, and that the update of integrated components (e.g. sensors, applications, systems, ontologies) causes little or ideally no changes to the users of the Services.



iEMSS 2008 – Workshop Sensor Networks – Architecture & Infrastructure

ISESS

Referring back to Figure 1 – a project called SANY (Sensors Anywhere, www.sany-ip.eu) follows the above generic architectural principles and addresses the functional domains (figure 1) in the following sense:

2.2 SANY sensor service architecture

The major architectural heritage of the SANY Sensor Service Architecture is the ORCHESTRA Architecture specified in [8] as an “open architecture that comprises the combined generic and platform-neutral specification of the information and service viewpoint as part of the ORCHESTRA Reference Model” (RM-OA). Consequently, the SANY Sensor Service Architecture builds upon the components of the ORCHESTRA Architecture which comprise:

- Rules and guidance on specifying information and service models in the context of international standards.
- Basic re-usable specification units for information models (e.g. pre-defined feature types) and service models (e.g. re-usable interfaces).
- A series of textual descriptions and formal specifications of generic ORCHESTRA Architecture Services that are application and technology independent.

It is the objective of the project SANY to re-use and apply these components in the context of the SANY Sensor Service Architecture to the extent that they fulfil the requirements to build service networks based on sensor information and higher-level sensor information processing.

2.3 Functional domains

SANY services are designed to serve the needs of applications and users. Although there is no prescribed hierarchy of services, the SANY services may be grouped into functional domains matching their design purposes. The SANY Sensor Service Architecture distinguishes between the following functional domains for SANY services (see Figure 1).

- **Sensor Domain:** SANY services in the sensor domain cope with the configuration and the management of individual sensor devices and their organization into sensor networks. Examples are services that support the interaction among the sensors themselves, e.g. a take-over service in case of an impending sensor battery failure. Services in this domain are abstractions from the proprietary mechanisms and protocols of sensor networks.
- **Acquisition Domain:** SANY services in the acquisition domain deal with access to observations gathered by sensors. This includes other components in a SANY Sensor Network (e.g. a database or a model) that may offer their information in the same way (as observations) as sensors do. They explicitly deal with the gathering and management of information coming from the source system of type “sensor”. The information acquisition process may be organized in a hierarchical fashion by means of intermediate sensor service instances (e.g. using data loggers).
- **Mediation and Processing Domain:** SANY services in the mediation and processing domain are not specific to the sensor service architecture. They are specified independently of the fact that the information may stem from the source system of type “sensor”. They mediate access from the application domain (see below) to the underlying information sources. They provide generic or thematic processing capabilities such as fusion of information (from sensors and other information sources), the management of models and the access to model results. In addition, service support for the discovery of sensors, data and services, naming resolution or service chaining are grouped in the mediation and processing domain.



- **Application Domain:** Based on services of the acquisition and processing domain, SANY services in the application domain support the rendering of information in the form of maps, diagrams and reports such that they may be presented to the user in the user domain.
- **User Domain:** The functionality of the user domain is to support the interface to the end user. SANY will not specify dedicated services to support the user interface. However, when building real systems and applications, such functionality is essential. SANY considers this functionality to be specified in a dedicated implementation architecture that also may take proprietary components and products into account.

3. USER REQUIREMENTS

Beside the architectural requirements addressed above, the workshop shall also be driven by the discussion about user requirements within the environmental domain(s). In SANY (www.sany-ip.eu) users from different environmental monitoring domains (air pollution risks, marine risks, geo-hazards) have expressed their needs. An analysis of the uses cases has led to a set of requirements that have been grouped into functional blocks as illustrated in figure 2 and as listed below.

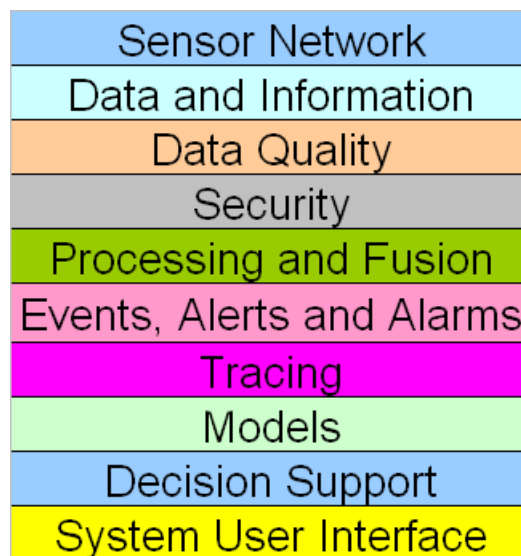


Figure 2: Sensor network requirements – functional blocks (courtesy SANY-Consortium)

These requirements within the blocks shown in Figure 2 are summarised below. Here, the term “system” stands for the entirety of a sensor service network including its architecture and its hardware and software components.

3.1 Sensor Network

- **Plug & measure** refers to the capability of being able to add a new sensor node without a manual re-configuration of the sensor network or sensor node.
- **Dependability** is required to provide data access and management services, in order to cope with the dynamic availability of possibly redundant sensor data sources, especially in the case of mobile sensors.
- **Sensor network management.** Of particular interest here is the localisation of sensor nodes, e.g. for the planning and management of their deployment or the configuration of the measurement frequency in order to optimise network and battery load.



iEMSSs 2008 – Workshop Sensor Networks – Architecture & Infrastructure

ISESS

- **Deployment of mobile ad hoc sensor clusters.** Especially in the case of biological and chemical hazards, the responsible administration authority needs to measure air pollution or water quality in order to quickly assess the risk situation. However, in the affected area appropriate sensors are often absent.
- **Self-validation of sensor nodes** with regard to its residual battery life and measurement capability (need for re-calibration or maintenance) is important for the assessment of the node deployment and data quality.
- **Battery life-time optimisation** through selective data transmission is a necessary management functionality to access the information via an interface to sensor nodes with self-diagnosis. It shall support the capability to automatically select alternate transmission routes for data transmission and/or the frequency of data transmissions, if the residual battery level of a sensor is too low.

3.2 Data and Information

- **Data sources** do not only include sensors and databases of archived data, but also data obtained from a laboratory analysis of samples, or data entered manually by humans. Data sources may also be results of fusion services.
- **Spatial and temporal metadata.** The system shall be capable of adding spatial metadata (sensor location information) and temporal metadata (sensor measurement time information) to any measurement data with/without this metadata from outset.
- **Rapid access to data.** The system shall be capable of accessing data in sufficiently short time.
- **Data type.** The system shall operate with different data types (e.g. fields, coverages) associated with measurement data like:
 - a single sensor measurement observation represented by a single value and unit located at a fixed location and detected at a particular time (time, date and year). For critical evaluation situations it has to be distinguished between a measurement result with a sensor internal clock time stamp or the nearly adequate particular time when the result has been received by the system.
 - time series of sensor measurement observations represented by a time series of triples {value and unit, feature of interest, time}. The time representation may be either absolute time (time, date and year) or a relative time representation (e.g. every day at midday starting from a certain date).
- **Geographic objects of several types.** The system shall be capable of handling geographic objects of several types (e.g. the types specified by the ISO 19107 and ISO 19123 such as MultiPoint, MultiLineString, MultiPolygon, LineStrings, Polygons, MultiCurve, MultiSurface).
- **3D fields.** The system shall be capable of operating with three-dimensional measurement data (e.g. components of vector fields etc.) of an observed property (e.g. wind speed, water current etc.)
- **Images (e. g. IR/UV, SLAR, INSAR).** As an example, such image data may be delivered by an earth observation sensor mounted on an aircraft or on a satellite with a certain spatial resolution.
- **Maps.** The system shall be capable of handling a wide spectrum of maps (topography, roads, land usage etc).

3.3 Data Quality

- **Data quality.** To assess the quality (e.g. uncertainty) of delivered measured data some information about certain quality details (e.g. accuracy, tolerance, resolution, drift) has to be available. The system shall be capable of accessing this sensor information.
- **Sensor level spatial and temporal uncertainty.** To ensure a previously defined user quality target level of data results, the system shall process data quality levels depending on:
 - different available sensor data sources selected in an area of interest,
 - potentially estimated statistical processing uncertainties (e. g. a model calculated temperature result at a given location depends on the distance to available sensor values and on topological conditions e.g. located on mountain), and



iEMSS 2008 – Workshop Sensor Networks – Architecture & Infrastructure

ISESS

- the time period and frequency of measurement observations (limited e.g. by a certain availability frequency of EO satellite images of an area)
- **Certification of data and its propagation.** The system shall be capable of supporting the process to formally certify the data quality, e.g. by instructing a certified laboratory per email with an investigation of new microbial sampling at a specific beach.
- **Associate data quality with measurement context (validation).** The system shall be capable of associating and storing data quality together with measurement context as meta-information. It shall be capable of visualizing this quality meta-information in its spatial and temporal context. This feature may be used as a tool for quality validation and as an aide in deploying sensors.

3.4 Security

- **Confidentiality of data - UAA (User Management, Authentication, Authorisation).** The system shall provide several security related services:
 - Authentication Service (verification of user identities, support for multiple authentication mechanisms)
 - Authorisation Service (support of roles, authorisation for services authorisation on sensor level, etc)
 - User Management Service (storage and management of user profiles)
- **Monitoring Service** (check availability of services and sensors)
- **Billing, encryption, track data ownership.** The provision of sensor data needs a high investment in equipment and in supporting services. They normally cannot be offered free of charge, therefore a billing service is necessary. Another security topic is to protect measurement data against manipulation. In order to ensure data authenticity an encryption may be necessary at different operational levels (e.g. during transmission, storage in databases etc.). It may be a security problem to allow certain users of the system to track sensor data over a period of time (e.g. a shipping company does not want competitors to know the exact routes of their ships).

3.5 Processing and Fusion

- **Interfaces for data processing services development.** The system shall provide general data processing services e.g. merging data, extracting relevant data for reports. In general, the system shall be capable of handling meta-information. This includes the storage of intermediate information in order that overall services (and service chains) can execute with acceptable speed.
- **Image analysis and feature extraction.** The system shall be capable of processing images and extracting features (e.g. such as a road or a watercourse).
- **Different time steps, resolution.** The system shall be capable of handling and adjusting different temporal and / or spatial resolutions of sensor data, depending on the sensors used and if values are missing.
- **Improving spatial resolution** if the spatial resolution of different sensor data is too heterogeneous or if values are missing.
- **Fusion of measurements.** The system shall be capable of processing and merging measurements of the same phenomenon using different sensor equipment. The information about the source shall be stored in meta-information. The different data, possibly at different times, generated by the equipment shall be processed using a fusion service.
- **Library of algorithms as ((statistical) processes) services.** The system shall be capable of providing statistics libraries e.g. for interpolation and merging services.
- **Workflow.** The system shall be capable of processing service chaining by workflows. The output results of a model service may be connected to the input of another subsequent process.
- **Visualisation.** In many use cases several services of visualisation are described, e.g. maps, diagrams. To display them in a flexible way the support of styled layers as a separate service is required.



3.6 Events, Alerts and Alarms

- **Threshold surpasses detection.** The system shall be capable of detecting threshold surpassing. For instance in the field of air quality measurement, a pollution of the environment can be asserted if sensor measurement data has reached defined thresholds.
- **Alert algorithms.** Typically, an alert will result if a combination of observed variables is no longer in a defined region (the event of variables departing from this region). Alerts cause application level procedures and / or workflows to be executed as a reaction to the event.
- **Interfaces for alarm management.** Alarms involve communication procedures with the environment to warn about an imminent hazard and to initiate emergency procedures (such as evacuation).

3.7 Tracing

- **Tracing requirements** address the need to document what information sources were used as a basis for the decisions taken and the decision making process itself. The purpose is to be able to provide a retrospective justification of decisions made, which may later be contested by parties seriously affected.

3.8 Models

- The system shall provide in general
 - a model service catalogue, where all available services may be selected by the user
 - an execution management service handling input/output and, optionally if expedient for performance reasons, data by reference
 - the capability of using the output of models and fusion algorithms as sensor values without changing the system.

In addition to a basic support for models and model wrapping (to integrate the models into the SANY service network), the model-specific functionality is required:

- Gather applicable source impact models
- Domain skills compilation
- Library of models as processes
- Library of geo-statistical analysis as processes
- Predictive models for adaptive sampling
- Spill advection & dispersion modelling
- Forecasting risks (water quality, bathing water, beach closed)
- Model long-term degradation of ecosystems
- Improved soil models

3.9 Decision Support

- **Providing supporting information for decisions.** The types of decisions to be taken imply requirements on the modelling, fusion and visualization of information as well as on auxiliary methods to compute utility functions and to undertake multi-criteria analysis.

3.10 System User Interface

- **User registration.** The system shall offer the user a dialog window to login normally with user name and password. When entering the password the input window shall not display the characters in a readable form.



iEMSSs 2008 – Workshop Sensor Networks – Architecture & Infrastructure

ISESS

- **Message to the user.** The system shall be capable of sending a message to the user in a separate window. This window must be visible for the user (e.g. it pops into the foreground).
- **Sending form(s) to the user.** The system shall be capable of sending a form or several forms to the user to fill them out with required information.
- **Sending message that authorisation failed.** If an authorisation has failed (e.g. due to insufficient access rights), the user shall be informed by a message.
- **Sending message that authorisation failed and waits for a new input.** If an authorisation has failed (e.g. due to a wrong password), the user shall be informed by a message and is requested to repeat the login procedure.

4. ADDITIONAL INFORMATION ABOUT OTHER PROJECTS AND INITIATIVES

4.1 ORCHESTRA and SANY

European Commission (EC) is funding a number of Integrated Projects within the Sixth Framework Programme concerned with improving the accessibility of data and services for risk management. Two of these projects: ‘Open Architecture and Spatial Data Infrastructure for Risk Management’ (ORCHESTRA, <http://www.eu-orchestra.org/>) and ‘Sensors Anywhere’ (SANY, <http://sany-ip.eu/>) were mentioned above and some requirements aspects were briefly discussed.

But, these projects have developed an open distributed information technology architecture and have implemented web services for the accessing and using data emanating, for example, from sensor networks. These developments are based on existing data and service standards proposed by international organizations.

The projects seek to develop the ideals of the EC directive INSPIRE (<http://inspire.jrc.it>), which was launched in 2001 and whose implementation began last year (2007), into the risk management domain.

Thanks to the open nature of the architecture and services being developed within these projects, they can be implemented by any interested party and can be accessed by all potential users. The architecture is based around a service-oriented approach that makes use of Internet-based applications (web services) whose inputs and outputs conform to standards.

The benefit of this philosophy is that it is expected to favor the emergence of an operational market for risk management services in Europe, it eliminates the need to replace or radically alter the hundreds of already operational IT systems in Europe (drastically lowering costs for users), and it allows users and stakeholders to achieve interoperability while using the system most adequate to their needs, budgets, culture etc. (i.e. it has flexibility).

4.2 Architectural Requirements of put on Sensor Networks from initiatives like GMES

The ‘Global Monitoring for Environment and Security’ (GMES) represents a concerted effort to bring data and information providers together with users, so they can better understand each other and make environmental and security-related information available to the people who need it through enhanced or new services.

For example, the GMES initiative (www.gmes.info) as illustrated in figure 3 below focuses on four major components:

- The space component providing earth observation satellite data.
- The in-situ component providing ground and airborne data as well as socio-economic data.
- The data integration and information management component providing access to and processing of the space and in-situ data referred to above.
- The high level user services component allowing for the monitoring of the various aspects of our environment.



iEMSSs 2008 – Workshop Sensor Networks – Architecture & Infrastructure

ISESS

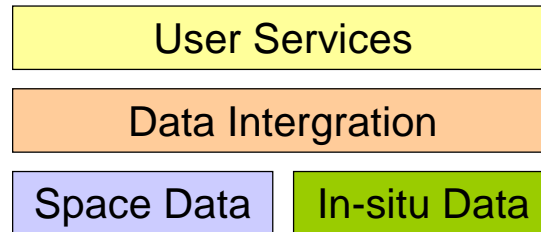


Figure 3: Major GMES Components

The final report for the GMES initial period (GMES FR, 2004) provides the following key architectural requirements on pages 25-26:

“For GMES to become a success, the architecture needs to facilitate the integration of standalone data and information elements. It should allow to the selection and aggregation of information from heterogeneous sources and should provide the capability to translate data and information between the various sources in real time. This applies as much to the incorporation of socio-economic data and information, as well as products derived from the space and in situ observing networks.

GMES must therefore provide a structured framework for data integration and information management, i.e., a European shared information capacity. The following key architectural and user-oriented requirements will therefore drive the implementation of GMES:

- *Openness, based on agreed open standards, facilitating seamless communication and interoperability, i.e. the ability of different devices or systems (usually from different vendors) to work together, as well as enabling user service autonomy;*
- *Federated architecture, enabling systems to grow and evolve;*
- *Simplicity of architecture (e.g. modularity of components), to break the complexity barrier, systems must be made easier to design, administer and use;*
- *Self-configuration, programmability, scalability (e.g. to handle various levels of operational load and external conditions);*
- *Dependability, i.e. the system's resilience to security threats or breakdown;*
- *User-friendliness of services and interfaces, e.g. in the handling of user request services, access control, workflow management, delivery management, visualisation, data extraction (e.g. “multilinguality”), multiuser sessions, administration;*
- *Data security, protection of provider and user data against alteration, theft and misuse;*
- *Quality of service;*
- *Ubiquity of access, including global reach.”*

In a reflection paper (GMES, 2005) on Data Integration and Information Management Capacity, prepared by the EU (DG-INFOS) , lists provisionally and non-exhaustively a lot of important functional requirements. The paper suggests that the approach needed to create an efficient data integration and information management component is to use a “system of systems” design as explained below:



iEMSSs 2008 – Workshop Sensor Networks – Architecture & Infrastructure

ISESS

“The GMES information and services infrastructure goes well beyond a simple exchange of data. It addresses the need to integrate business and workflow processes which span across boundaries, be they political, administrative or thematic. It addresses the main issues of heterogeneity and fragmentation of the information: “heterogeneity” meaning that the same information is often represented differently, “fragmentation” meaning that needed information is spread over multiple locations.

The approach is to seamlessly integrate existing systems into a “system of systems” perspective. System of systems is an emerging design and development method of complex systems build from large scale component systems. The subsystems that comprise the system of systems are generally built by different organisations, having different goals, are very often built to different quality standards, and are managed independently.

Reusing existing legacy systems in a dependable fashion without the need for extensive re-engineering is a key problem currently faced by industry. System of systems can be seen as new systems linking data, services and workflows to produce new data, new services together with metadata (information about the information products generated¹).

This approach, which was a research topic in the last decade, is now becoming sufficiently mature. In the short term, robust system architectures will be developed and tested allowing the exchange of data and services that are well identified: This is the syntactic interoperability phase. In the longer term, we expect to achieve significant semantic interoperability, which will allow cross-system search for data and services. It could be dubbed the “GMES Google” since it will work for data and services in the way web search engine works for web pages.

A number of non technical obstacles should however be addressed to eventually reduce the complexity of the implementation, such as trusted electronic billing principles between data providers and services providers to partly overcome the hurdles created by different data policies. Mechanism should also be agreed upon to manage access privilege across institutional borders in a practical, transparent and secure way.

This approach will allow sharing and efficient management of information that is consistent across organisations, borders and thematic domains such as from land use and mapping to risk management and security.”

The suggested system of systems approach is still regarded today as the best way to go as indicated in the following excerpt of the report of Joint Operability Workshop held in April 2007:

“There was broad agreement that any proposed solution for a single information space for the environment must allow for multiple architectures and hence be a “system of systems”. Further comments on this topic included:

- *Hierarchical architecture is required to cope with services at various levels: EO ground segment services, GMES core services, GMES downstream services etc.*
- *SOA is well suited for deployment of system of systems.*
- *Significant investments have been made already by ESA, ECMWF² etc. Therefore it is unrealistic that everybody will adopt a single architecture. This leads to a system of interoperable systems which may be based (internally) on heterogeneous technologies.*
- *An exhaustive list of use cases is unfeasible – the number of possibilities is too large and is changing rapidly. Thus, a flexible architecture is needed which also leads to the concept of a system of systems. The fully top-down approach and pan-European architecture that was anticipated as recently as five*

¹ In the SANY Service Architecture therefore called “meta-information”.

² European Centre for Medium range Weather Forecasting



iEMSSs 2008 – Workshop Sensor Networks – Architecture & Infrastructure

ISESS

years ago appear now to not be feasible. The concept is being replaced by pan-European interoperability in a system of systems-like architecture.

- *Many systems are legacy systems in this field as satellites have a relatively short life and scientific advances in EO are rapid. It is totally unfeasible to convert all existing data so they all have the same data and metadata formats. Any viable solution must be based on fully utilising legacy systems. Harmonised, “on the fly” access to legacy datasets is required.*
- *Access to data from heterogeneous missions must be seamless and transparent.”*

As recommended in the following extract of the reflection paper (GMES, 2005) on Data Integration and Information Management Capacity, the technology of choice to be used to implement the GMES architecture is SOA: “The underline architecture for ensuring interoperable GMES services is the Service Oriented Architecture (SOA)”.

Modern architectural designs are based on a less tightly coupled collaboration of distributed services. For this, the term SOA is becoming widely used, but there is not a lot of precision in the way that it is used. The World Wide Web Consortium (W3C) for example refers to SOA as 'A set of components which can be invoked, and whose interface descriptions can be published and discovered'. This is broad definition highlights a key aspect of an SOA: components (e.g. functionalities) can be discovered and invoked dynamically. Thus this type of architectures is a motion away from “hard wiring” of business processes, which makes change to new circumstances very difficult. SOAs are thus inherently more flexible and adaptable than most approaches.

A service-oriented architecture is also proposed for the following reasons:

-
- A SOA represents business functionality as implementation- and vendor neutral and standards-based shared services.
- Existing legacy systems can be extended with service interfaces, and in that way become part of a SOA.
- By means of the inherent service discovery and access flexibility (see above), a SOA enables GMES/INSPIRE service providers to be more agile and to respond more quickly to changing business needs and evolving requirements.
- A set of common generic services can provide standard, domain-independent functionality (for discovery, search, navigation, data access, authorisation etc.) which only needs to be implemented once.
- Sharing of services — no need to “re-invent the wheel”
- Loose coupling — ability to update applications with minimal effect on services that invoke them
- Location transparency — ability to re-host applications with minimal effect on services that invoke them

GMES applications built on top of a joint, adopted infrastructure will be interoperable and much easier to integrate into multi-purpose, cross-application operations.”

The adoption of a SOA architecture based on open standards for its services is the way to follow in order to provide flexibility, stability, and durability while preventing vendor lock-in. Example of open standards are the OGC standards for Web services.

Note: GEOSS or INSPIRE architecture - we may discuss during the workshop or by abstracts sent in for discussion.



**iEMSSs 2008 – Workshop
Sensor Networks –
Architecture & Infrastructure**

ISESS

REFERENCES

GMES, GMES reflection paper on Data Integration and Information Management Capacity, *DG-INFISO, Draft 6*, July 2005

JOW, Joint Operability Workshop Report “Towards a single information space for Environment in Europe”, Frascati, 3 April 2007

Usländer, T., RM-OA - Reference Model for the ORCHESTRA Architecture Version 2 (Rev. 2.1). *OGC Best Practices Document 07-097*. http://portal.opengeospatial.org/files/?artifact_id=23286, October 2007

Watson, K., Kunz, S., SANY Project Deliverable D2.2.2 Sensor Scenarios and Requirements Version 1.2, October 2007.

Watson, K. et. al., SANY Project Deliverable D2.2.2 Sensor Scenarios and Requirements Version 1.2, (to be published).