Integrated System for Control and Monitoring Industrial Wireless Networks for Labour Risk Prevention

J.R. Gisbert[1], C. Palau[2], M. Uriarte[3], G. Prieto[4], J.A. Palazon[1], M. Esteve[2], O. López[3], J. Correas[4], M.C. Lucas-Estañ[1], P. Gimenez[2], A. Moyano[3], L. Collantes[4], J. Gozalvez[1], B. Molina[2], O. Lazaro[5], A. González[5]

[1]Uwicore, Ubiquitous Wireless Communications Research Laboratory University Miguel Hernandez of Elche, Avda. Universidad s/n, 03202, Elche, Spain
jgisbert@umh.es, jpalazon@umh.es, m.lucas@umh.es, j.gozalvez@umh.es
[2]Universitat Politècnica de València, Camino de Vera s/n, Valencia, 46022, Spain, +34 651817648
cpalau@dcom.upv.es, mesteve@dcom.upv.es, pabgisa@upvnet.upv.es, benmomo@upvnet.upv.es
[3]NEXTEL, Ibaizabal bidea Edificio 500, 1º planta, Parque Tecnológico de Bizkaia, 48160, Derio (Bizkaia), Spain
muriarte@nextel.es, olopez@nextel.es, amoyano@nextel.es
[4]INDRA, Calle Anabel Segura, 7, 28108 Alcobendas (Madrid), Spain
gprieto@indra.es, jcorreas@indra.es, lcollantes@indra.es
[5]INNOVALIA, Carretera de Asúa nº6, 48930 Getxo (Vizcaya), Spain
olazaro@innovalia.org, agonzalez@innovalia.org

ABSTRACT

The FASyS (Absolutely Safe and Healthy Factory) project, aligned with the European Factories of the Future (FoF) concept, has been set-up to develop a new factory model aimed at minimizing the risks to the worker's health and safety, and guarantee their welfare and comfort in machining, handling and assembly factories. To this aim, ICT (Information and Communication Technologies) and wireless communication technologies in particular may represent very valuable tools to implement distributed and mobile sensing applications capable to continuously sense the working environment and the workers' health and safety conditions. The effective deployment of such applications in critical environments, like the industrial one, require the availability of a platform capable to monitor the operation and performance of the heterogeneous wireless networks that will connect the mobile sensors to remote control centers. This paper presents the platform implemented for this purpose in the context of the FASyS project. In addition to monitoring the status of heterogeneous wireless networks, the implemented platform provides the capability to reconfigure remotely the communication settings of wireless nodes based on possible malfunctioning or QoS degradation notifications. These functionalities will help guaranteeing the reliable and robust wireless communications required in industrial environments to implement innovative labor risk prevention applications exploiting ICT technologies. .

Keywords: Factory of the future; Wireless sensor networks; Semantic sensor networks; Distributed application; Global monitoring application; Health and safety

1. INTRODUCTION

Safety technologies for industrial environments have evolved considerably in recent years, but there are still risks related to the worker's safety and health. In this context, the European Factories of the Future [1] concept focuses on the development and integration of engineering technologies, ICT, and advanced materials for adaptable machines and industrial processes. In this new framework, workers represent an even more important asset for the manufacturing competitiveness and productivity, and all necessary actions must be done to improve their health and safety in their working environment. As a result, monitoring physical activity has become increasingly important as many studies link physical activity with overall health status. More precise measurements and relation with ambient and environment measurements can be achieved using a more advanced setup. However, interfacing sensors and controlling multiple events and data in an integrated way are challenges in terms of communications, logical and semantic processing. Achieving this objective requires a complete platform for pervasive sensing, distributed and ubiquitous communication capabilities with strict QoS (Quality of Service) requirements, advanced reasoning capabilities and a more autonomous response towards risk mitigation and worker information and training. This sensor-based platform should be monitored in real time and in a detailed hierarchical or sectored way. Everything happening in the factory, from ambient levels, to the position of all elements should be tracked and potential risks should be anticipated through automated preventive actions.

Achieving these objectives can be realized through the integration of the IoT (Internet of Things) in industrial environments, and the use of wireless communications to connect distributed mobile sensors with remote control sensors. The architecture of industrial wireless communication systems and its management are key factors to achieve perfect coverage and the most adequate information gathering in real time. However some systems utilize on-sensor signal processing, other rely on raw data transmission, where data are processed on an external computer or personal server, and other use a hybrid approach. Increased sensor intelligence reduces the need for communication, therefore minimizing power consumption and extending battery life.

There is not a factory without risk, but decisive actions should be taken to realize a factory that has the technical, organizational and human resources to identify, detect, monitor and manage continuously the relative risks to health and safety throughout the life cycle of the factory. In this context, the FASyS project (Absolutely Safe and Healthy Factory) [2] has been set-up to develop a new factory model aimed at minimizing the risks to the worker's health and safety, and guarantee their welfare and comfort in machining, handling and assembly factories. ICT and wireless communication technologies in particular may represent very valuable tools to implement distributed and mobile sensing applications capable to continuously sense the working environment and the workers' health and safety conditions. In the context of the sensing enterprise, FASyS has to deal not only with the detection of risks but also has to support the actuation and deployment of the preventive actions selected by the safety and healthy manager through the personalized decision support tools. This implies a service oriented scenario, where the factory is populated by a large amount of services, sensors and actuators involved in risk management life cycle, where services exchange messages to perform the designed actions by means of smart objects. These services may have heterogeneous sources, which can become available, temporarily unavailable or even disappear suddenly. To address this changing environment, FASyS has proposed a highly effective service messaging and service management and coordination semantic solution that would use choreography techniques focused on browsing FASyS service topology. With this solution, FASyS is able to adapt its reactions to available services at any time and ensure the best possible service performance based on the precedence of the risk to be addressed and the service load in the enterprise bus.

To achieve its objectives, FASyS relies on a heterogeneous wireless communications network in charge of transporting the data gathered by the sensors. The reliable provision of the envisioned services in a distributed environment characterized by harsh propagation conditions requires a platform capable to continuously monitor and manage the communications QoS to ensure the robust reception of the sensed information and the capacity to ubiquitously connect to any distributed node. Several monitoring and management platforms have been developed for wireless networks. However, there is yet the need for a platform capable to monitor the operation and performance of heterogeneous wireless networks in industrial environments. An additional feature of interest would be the capability to reconfigure remotely the communication settings of wireless nodes based on possible malfunctioning or QoS degradation notifications. All these functionalities will help guaranteeing the reliable and robust wireless communications required in industrial environments to implement innovative labor risk prevention applications exploiting ICT technologies. The development of this kind of tools has been one of the objectives in FASyS and the subject of this paper.

The paper is organized as follows: next presents the related work with the proposed solution. Section 3 introduces the FASyS ICT approach to the FoF. Sections 4 presents an overview of the monitoring and management software platform. The following three sections describe the main components of the platform and their functionalities (SOS, Toolbox and Human Machine Interface). Section 8 presents a performance evaluation of the management framework. And conclusions and main benefits of the proposed solution are summarized in final solution.

2. RELATED WORK

One of the main motivations of the work presented in this paper is the analysis of the effective deployment of distributed and mobile sensing applications in critical environments, like the industrial one. These applications require the availability of a platform capable to monitor the operation and performance of the heterogeneous wireless networks that will connect the mobile sensors to remote control centers. There is little research regarding the FoF environment in order to increase levels of industrial safety where the operational environment refers to industry and critical operations. Risk assessment is evaluated in [3] for collaborative robots in a human shared environment, following the relevant guidelines in the standards ISO 10218 [4] and ISO 13849 [5] to determine the requirements on the implementation of the risk reduction measures used. On the other hand, the work done in this paper is more focused on the standard ISO 31000. This standard provides generic guidelines for the design, implementation and maintenance of risk management processes throughout an organization, but our paper will focus on the machinery industry group. Considering the worker as the nuclear entity of the risk assessment process, its health condition and health information is also of significant relevance to evaluate safety risks.

FASyS relies on a heterogeneous wireless communications network in charge of transporting the data gathered by the sensors. This data is decisive to take actions to realize a factory that has the technical, organizational and human resources to identify, detect, monitor and manage continuously the relative risks to health and safety throughout the life cycle of the factory. The design and implementation of a platform that is capable to monitor the operation and performance of a heterogeneous wireless network and that connects the mobile sensors to remote control centers required the revision of existing network management protocols, management platforms and studies that characterize the deployment of wireless communications in industrial environments.

The benefits of exploiting wireless communications technologies in general, and WSN (Wireless Sensor Networks) in particular for industrial communication distributed systems, have been highlighted in several studies [6][7]-[13]. These benefits include deployment flexibility, low cost and reduced power consumption. However, the deployment of heterogeneous wireless communications in industrial environments presents significant challenges. On one hand, industrial environments are usually characterized by challenging propagation conditions (obstructions, multipath propagation, interferences, etc.) that make difficult the establishment of robust wireless links. On the other hand, safety-related industrial applications are characterized by strict reliability and timing requirements, and therefore require a reliable mobile sensing and communications platform. As a result, different studies have analyzed wireless communications in industrial environments. For example, the work in [14] has characterized three factory automation infrastructures at 439 MHz, 440 MHz, 570 MHz, and 2.45 GHz. The study revealed that the analyzed facilities have different levels of reflectivity, which can have a negative impact on the reliability of wireless technologies. Similarly, [15] reports a series of narrow-band measurements performed in two wood processing and two metal processing factories at three frequencies bands (900 MHz, 2.4 GHz, and 5.2 GHz). The study found limited path loss variations between measured factory buildings, mainly because of their similar constructional details. Temporal fading was found to be most significant in manual production lines, and to be overall less important than in office environments. Other studies have evaluated the performance of wireless technologies in industrial environments, with many of these experiments based on the IEEE 802.15.4 and IEEE 802.11 standards due to their low cost and wide market acceptance [16]. For example, the work in [17] presents the results obtained in different field tests performed in various electric-power-system environments, including a 500-kV substation, an industrial power control room, and an underground network transformer vault using IEEE 802.15.4-compliant wireless sensor nodes. The obtained results provide valuable information for the design and deployment of IEEE 802.15.4-compliant sensor networks for smart-grid applications. The study in [18] experimentally investigates the nature of IEEE 802.15.4-based packet transmission errors resulting from common stationary (e.g. machine shop) and moving obstacles (e.g. moving forklift) in small-scale manufacturing environments. The measurements show that transmission errors closely depend on the received signal strength, and could be mostly avoided by controlling the transmission power in order to ensure received signal strengths above the receiving sensitivity level. These studies demonstrate the potential of wireless communications technologies for industrial environments, but highlight the adverse propagation conditions and therefore the need of management platforms that are able to monitor the operation and performance of deployed networks, such as the one presented in this paper.

The continuous interest in managing networks of electronic devices and the increasing complexity of the existing networks has led to the design and implementation of several network management protocols. Network management protocols coordinate the activities performed by the different modules of a network management platform and provide mechanisms for them to exchange management information. Given the rapid expansion of products based on the TCP/IP stack on the Internet, the Internet Architecture Board (IAB) recommended the use of Simple Network Management Protocol (SNMP) for network management [19], which was later standardized by the Internet Engineering Tasking Force (IETF). Although proposed as a short-term solution, SNMP has been widely implemented and deployed and become simultaneously a declared and a de facto standard [20]. Part of this success is due to the characteristics of the protocol and the benefits of using it for network management. SNMP adopts a centralized architecture based on the manager-agent paradigm. The manager interacts with the agents mainly by polling management information and requesting configuration changes on managed devices. SNMP also defines a mechanism that allows agents to send events to subscripted managers. SNMP is characterized by working well for device monitoring and by being widely adopted for basic monitoring. Most of commercial equipment from relevant networking hardware manufacturers such as Cisco or Alcatel-Lucent routers support SNMP. By using SNMP it is possible to retrieve network management information from deployed routers, such as link network traffic statistics, or make changes on the configuration of deployed devices. However, a number of drawbacks have turned up on SNMP over time [21]. Some of them, like major security issues, have been solved to some extent in new versions of the protocol. However, other issues still remain open. Among the main SNMP drawbacks are limited support for device configuration, low performance when retrieving large chunks of data or the high complexity of the SNMP interface to perform specific management tasks in an automated pattern. With networks becoming bigger and more complex, network operators and protocol developers demanded new efforts to develop alternatives to SNMP able to respond to the increasing challenges of network management that SNMP cannot address [22]. In this context, XML has been established as a relevant technology for network management and exchange of network management information. Among the benefits of XML are [21][22]: XML allows the description of structured data of almost arbitrary complexity; XML provides a document-oriented view of configuration data; XML has a robust schema language XML Schema Definition Language (XSD); there is a large community of XML professionals and also a large number of software tools that make the development of applications based on XML more efficient; XML is a technology independent from the application domain. The two main industry efforts that incorporate the XML technology in network management protocols are the standards Distributed Management Task Force (DMTF) Web Services Management (WS-Management) [23] and Organization for the Advancement of Structured Information Standards (OASIS) Web Services Distributed

Management (WSDM) [24]-[26]. WSDM enables the management of devices of arbitrary kind and web service endpoints by means of web service protocols. WS-Management covers only part of WSDM functionalities, which are the discovery of manageable devices and communication with managed devices. As a consequence, WS-Management is lightweight in comparison to WSDM. Both specifications are based on SOAP at the transport layer, although WS-Management relies extensively on WWW Consortium (W3C) specifications for web services. Given the similarities between both standards, work is currently underway to converge WSDM to WS-Management. To palliate the SNMP shortcomings in device configuration, IETF proposed the NETCONF standard [27][28]. NETCONF also enables configuration management, and defines the communication by means of documents that represent partial or full device configuration. NETCONF agents work with data stores where distinct types of configuration can be hold, including running configuration, start-up configuration or candidate configuration. NETCONF does not assume any specific transport protocol and supports SSH, BEEP and SOAP protocols at the transport layer. Given that NETCONF uses XML and is based on a remote procedure call (RPC) paradigm, it is normally used in conjunction with SOAP at the transport layer [29]. While NETCONF is considered as the promising replacement of SNMP, it assumes that managed devices and networks can handle relatively large SOAP encapsulated XML encoded messages [30]. SOAP messages are rather verbose and are not suitable for management of resource constrained devices and networks. As a result, given that the wireless communications network deployed in FASyS makes use of resource constrained devices with low processing power and sometimes limited batteries, and lower capacity radio links with fluctuating qualities, we adopted the use of RESTful interfaces and a dedicated XML transport format developed for the project for network management. As it will be detailed in Section 6 the proposed approach is more compact and resource-friendly than SOAP-based solutions for the management of the deployed heterogeneous wireless network.

Several management platforms have been developed to facilitate the monitoring and maintenance of communications networks. For example, Nagios [31][32], Zenoss [33] and Cacti [34] are open-source and powerful solutions that were initially designed and developed for managing wired communications systems. They offer the monitoring of performance and availability of networks devices and services. In comparison with wired systems, the wireless communications network deployed in FASyS considers resource constrained devices and the industrial environment can produce radio links with fluctuating qualities which in turn can lead to breaks in established connections between nodes [35]. Several management platforms with different objectives and features are available for monitoring and alerting in wireless mesh networks [36][37][38], although they normally developed to support a single communications technology. For example, the Mesh-Mon platform presented in [36] is focussed at monitoring IEEE 802.11b-based mesh networks that require a rapid deployment for emergency situations in areas with limited or damaged infrastructure. Mesh-Mon provides information about the state of network devices and the hierarchical structure of the network in a fully distributed manner; each node locally stores detailed information about itself and its neighboring nodes providing a detailed representation of the local network. Mesh-Mon nodes use a flooding broadcast to periodically spread the local information of each network node and locally generated alerts which can result in high overhead in the system. Mesh Topology Viewer (MTV) [37] and MeshAdmin [38] aim at showing in real-time the mesh network topology and the quality of the links of IEEE 802.11-based wireless mesh networks, and MeshAdmin also collects node state information. These two platforms provide global information, including the geographical position of the nodes. However, the link quality measurements provided by these platforms are based on routing protocol metrics, which makes difficult their application to networks based on different wireless communications technologies. Other platforms have also been developed for the monitoring and management of other types of wireless networks, although they are usually proprietary solutions and always exclusively developed to support a single communications technology. For example, AirWave [39] is a commercial solution for the monitoring of WiFi/IEEE 802.11 networks. AirWave provides information about users connected to the network, user locations and users devices, and also offers data about RF signal levels to allow network operators to identify and solve problems. Emerson AMS Wireless SNAP-ON application [40] and Nivis VersaManager 3000 [41] are planning and management applications for WirelessHart and ISA100.11a industrial networks. These applications provide network operators with the ability of obtaining channel statistics or read object attributes. Nivis VersaManager 3000 also allows update and reset the firmware on any device. The conducted review has shown that the available management platforms have been developed for single communication technologies, and therefore they are focused on different performance parameters depending on the communication technology implemented in the network. Furthermore, there is yet the need for a platform capable to monitor the operation and performance of heterogeneous wireless networks in industrial environments. An additional feature of interest would be the capability to reconfigure remotely the communication settings of wireless nodes based on possible malfunctioning or QoS degradation notifications. All these functionalities will help guaranteeing the reliable and robust wireless communications required in industrial environments to implement innovative labor risk prevention applications exploiting ICT technologies. The development of this kind of tools has been one of the objectives in FASyS and the subject of this paper.

Related with the FASyS ICT system there are two traversal aspects like semantics and security that also influence the management aspects of the network. Prior to add semantics, it is needed to homogenize sensor vision within the system and make the sensors their features and also their data for the applications and the systems involved. The Sensor Web Enablement (SWE) approach created by the Open Geospatial Consortium (OGC) [42] is vendor independent and an open standard widely adopted although there are other schemas more specific to the sensors like TinyDB [43] or open but addressed to a specific kind of network like [44]. SWE has been created as a group of specifications covering sensor description; related data models and services that offer interoperability, access and control in a web-based environment. The SWE architecture is composed by the information model and the service model:

- The information model specifies the conceptual models and encodings whereas the service model specifies related services.
- The conceptual models included in the information model specification refer to: (i) transducers (interfaces between real and digital world, which can be either sensors or actuators); (ii) processes (entities composed by functions and parameters that produce one or more outputs from one or more inputs); (iii) systems (group of georeferenced transducers that transform outputs from inputs according to a given methodology); and (iv) observations (the fact of observing a phenomenon including relevant information such as the value, the date and the location of the measurement).

Sensor web technologies have been successfully applied to a large variety of scenarios. In [45] present an Internet based urban environment observation system that is able to monitor several environmental variables (temperature, humidity, illumination or air) in urban areas in real time. The environmental data is archived and later on retrieved through a SOS. Ocean Sensor Web (OceanSW) is described and prototyped in [46], whose main goal was to describe, organize, store and manage the ocean sensor data. The OceanSW system data is encoded and represented in XML, which is easy to exchange and manipulate. Furthermore the system uses an Ocean Sensor Observation Service.

There are several approaches for adding semantics to sensor observations [47]-[50]. The concept of Semantic Sensor Web (SSW) is often used [36]; within this concept sensor data is annotated with semantic metadata to increase interoperability, as well as provide contextual information essential for situational knowledge. In particular, this involves annotating sensor data with spatial, temporal, and thematic semantic metadata. Another alternative to provide semantic enrichment, is through the definition of ontologies. The usage of ontologies is not only applied to sensors, but also to services. In [51], a very specific application can be found oriented to interoperate power systems using Web Ontology Language (OWL) instead of Resource Description Framework (RDF) to overcome its limitations (e.g. cardinality), other alternatives are Ontosensor [52] and Meteor-S [53].

Intelligence in an ICT system refers to how data is treated and processed within the system to be used to make relevant and useful decisions. There are two generic approaches: make applications and services smarter or make data smarter. Semantics and metadata are a common way to enrich the available data and/or services in order to allow reasoning, as is done in COSEMWare [54]. A semantic SOS (semSOS) is presented in [55] where the domain of sensors and sensor observations is modeled in a suite of ontologies, adding semantic annotations to the sensor data, and using ontology models to reason over sensor observations. This semantically enabled SOS provides the ability to query high-level knowledge of the environment as well as low-level raw sensor data.

The exchange of critical information in industrial environments requires solutions to guarantee the security of communications and the privacy of nodes. The security objectives in a critical infrastructure system are: data privacy; confidentiality; integrity; non-repudiation and protection against denegation-of-service. These security services may be provided at different layers, considering that critical infrastructure protection architectures tend to be distributed. At the application layer security services can be achieved with next generation firewalls [56]. At the MAC layer depending on the wireless protocols used (e.g. WiFi, WiMAX, Zigbee, etc.) [57][58][59][60] considering that the network should be secured at protocol level, but also as a group of heterogeneous networks. Authentication services use to be centralized with an individual IdP or a federated archirecture of IdP, using security frameworks like KERBEROS, RADIUS or at services layer SAML or Shibboleth **¡Error! No se encuentra el origen de la referencia.**. Three key traversal components of the security architecture of FASyS are access control; SIEM and the compliance with international standards.

Access control is a mechanism for constraining the interaction between (authenticated) users and protected resources. Companies manage Access control in many different ways, while sectors like banking, limit and discriminate the access to the Internet by the employees (to prevent security breaches and malware) and offer a secured access to external users in order to perform certain transactions (consultations of accounts, transfers, etc.), the most companies rely on a insufficiently strong Access Control, where their system is highly vulnerable to malware, attacks and employees misuses. In the cases where companies implement a highly secured Access Control system, this Access Control sets limits to usability. Main technologies used for access control in the literature are: Attribute Based Access Control (ABAC); Semantic Aware Access Control Model for Web Services (SABAC); Semantic Context-Based Model for Mobile Web Services Access Control (SCBAC); Experience Based Access Management (EBAM); Incentive Based Access Control (IBAC) and Role Based Access Control (RBAC) **¡Error! No se encuentra el origen de la referencia.**[63]

Security Information and Event Management (SIEM) solutions also provide a comprehensive visibility in heterogeneous environments that require a distributed monitoring architecture. SIEM platforms consist on systems formed by a set of network distributed sensors, such as routers, switches, firewalls, APs and other kind of collectors, that report detected information to a centralized server. The information is managed at the server to provide a high level security vision of the communications infrastructure. SIEM also permits to deal with security incidents in an organized manner to resolve them with minor consequences for the system **¡Error! No se encuentra el origen de la referencia.**.

Regarding standardised practice for security protection, ISO/IEC 27001:2005, usually referred to just as ISO 27001, is the best practice specification that helps organizations and businesses to develop a best-in-class Information Security Management System (ISMS). The Standard was published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO IEC 27001 uses the Plan-Do-Check-Act (PDCA) model to organize the standard and to help establishing the ISMS. Information systems are critical to the operation and even the survival of an organization. Therefore, being compliant with the ISO/IEC 27001 helps managing and protecting the valuable information assets. ISO/IEC 27001 defines several control objectives and controls to comply with the security objectives (availability, confidentiality, and integrity) [65]. NIST has also provided a standard but is focused on the smart grid and not in the industrial environment **¡Error! No se encuentra el origen de la referencia.**.

3. FASyS ICT APPROACH TOWARDS THE FACTORY OF THE FUTURE

Wireless communications are being gradually introduced in industrial environments to provide ubiquitous communication capabilities. Wireless technologies can adapt to changing operating and network environments, and offer interesting scalability and reconfigurability perspectives. The introduction of wireless communications in the FoF is also expected to facilitate the deployment of distributed and mobile sensing applications for improving productivity levels and the workers' health and safety. In this context, a key objective within the FASyS project has been the design and implementation of an end-to-end heterogeneous wireless network that can continuously sense the working environment and the workers' health and physiological conditions, both locally and remotely. The deployment of heterogeneous wireless communications in industrial environments presents significant challenges [9]. In particular, industrial environments are usually characterized by challenging propagation conditions (obstructions, interferences, etc.) that make difficult the establishment of robust wireless links [67]. The deployment of hybrid network architectures also require the design of a system platform efficiently managing data, in particular when real-time connectivity needs to be ensured across multiple wireless technologies [68] to support the reliable risk management.

To design its heterogeneous wireless solution, FASyS exploits Wireless Sensor Networking (WSN) technologies (IEEE 802.15.4/ZigBee) to locally monitor the working environment and the workers' conditions with the use of non-intrusive sensor systems. WSNs use low cost devices characterized by low power consumption and reduced capabilities but that can provide a good performance-efficiency trade-off in industrial environment [9]. The WSN deployed in the short-range communication level is formed by router nodes, which have associated sensors and actuators, and a coordinator node that carries out the WSN management. The coordinator node is in charge of transmitting the sensed data to a Control Center through a wireless backhaul that includes medium range technologies for communications within the factory, and long range technologies for the transfer of the aggregated data to the control center. The adopted technology for medium-range communications is IEEE 802.11/WiFi, which is used to transmit locally sensed data (including video from high capacity sensors) from different areas of the factory towards a gateway using relay nodes.

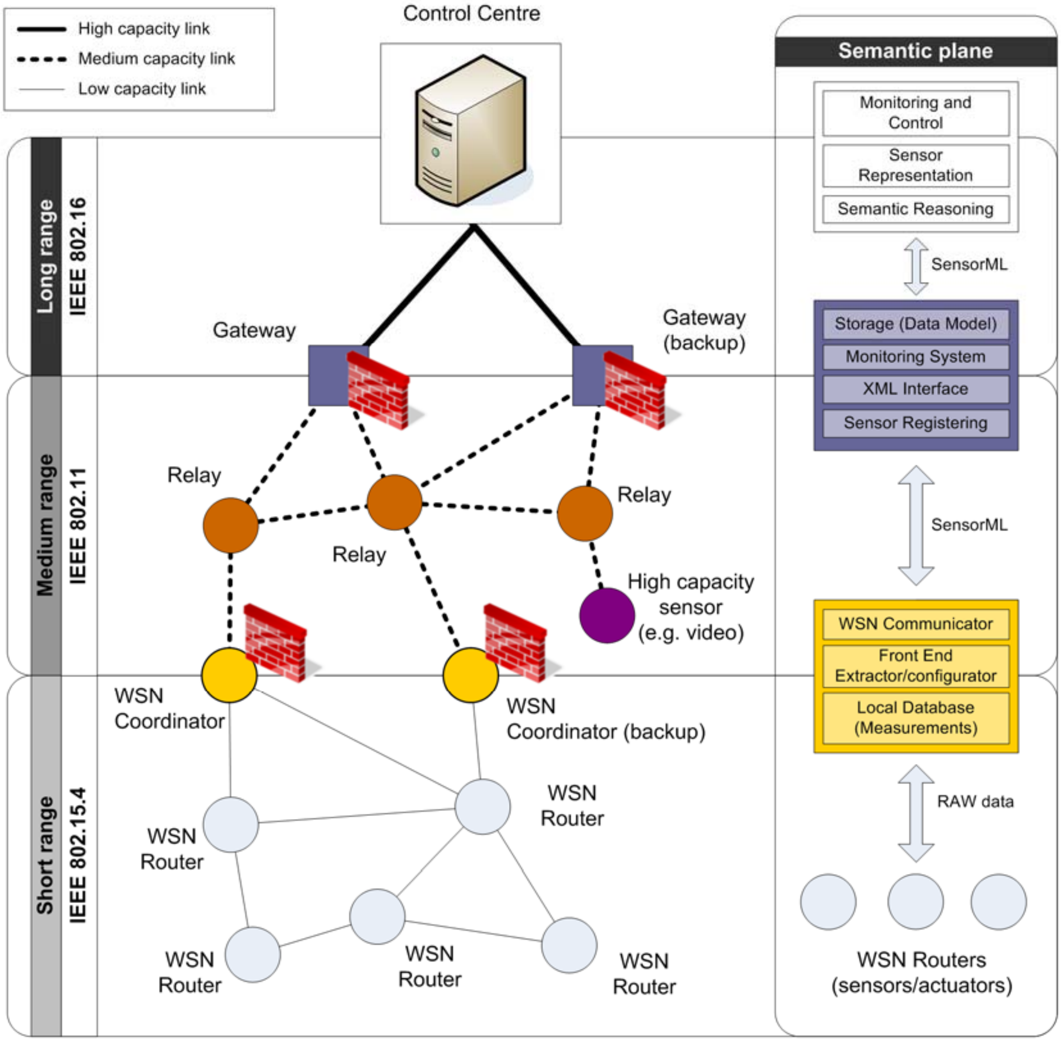


Fig. 1. FASyS's heterogeneous wireless communications architecture.

The gateway between the factory and the remote Control Center has been implemented by means of IEEE 802.16/WiMAX. Fig. 1 depicts FASyS's heterogeneous communications architecture for industrial environments. The adopted approach facilitates a scalable and cost-efficient deployment in the case of an industrial complex comprising several buildings or facilities. In this case, the different buildings will just require backhaul links to the Control Center. The FASyS communications architecture shown in Fig. 1 efficiently and reliably satisfies the requirements imposed by the industrial environment in general, and by the identified FASyS hazards in particular. Also, it takes into account not only radio propagation and communication aspects, but also semantics, security and compatibility issues within the general FASyS architecture.

FASyS proposes a centralized approach in which the Control Center is in charge of controlling and supervising the WSN deployed and managing the heterogeneous wireless communications network. In particular, the Control Center manages the information database of deployed nodes. The large number of deployed nodes and the amount of information generated requires an efficient management of the information. To this aim, a semantic description of the sensor nodes and network facilitates their management and location processes, as well as the process to control and reconfigure in real-time (e.g. triggering alarms when an unsafe or dangerous situation is detected).

3.1. Semantics

In terms of semantics, FASyS has considered a traversal control plane that includes semantics in every layer and component of the architecture (Fig. 1). The main semantic components are the semantic sensor networks (which allow organizing, managing, interrogating, understanding and controlling the network), the sensors, and the resulting data using high-level specifications. Sensors and sensor networks are different from other technologies, such as service oriented architectures, since they base their operation on the generation and processing of asynchronous events, and are characterized by temporal relationships between actions that have to be taken into account. Additionally, the existing limitations should be considered when implementing semantic reasoning mechanisms; in particular limitations in terms of power, reduced memory fingerprint, rogue communications networks, and quality and variability of the received data.

The Semantic Sensor Web (SSW) and Semantic Sensor Networks (SSN) base their operation on the existence of a network of sensors, that are usually based on standards, but also implement proprietary solutions. The contribution of this type of sensors is the addition into the sensed data of annotations in the form of metadata for semantic temporal, spatial and thematic information:

- Spatial metadata provides location information of the different nodes, using a relative or absolute geographical reference system. GPS is the most usual one, but other approaches should be used in indoor environments. Relative references associated to another object can be used to reference a sensor attached to a particular object, which is very useful when it is a mobile sensor.
- Temporal metadata provides temporary information of the moment of capture. At this point, it is essential that all the elements present in a system maintain a common and global time reference. For this purpose, it is necessary that the semantic sensor network includes some synchronization mechanism. For example, if sensors use the IP protocol, NTP can be used as synchronization mechanism.
- Thematic metadata describes the observation's state of the real world from various sensors belonging to the SSN (objects and events). Each application environment contains a domain-specific information that describes the different observed phenomena (e.g. atmospheric phenomena, presence of chemical products or biomedical events representing a worker's healthy status). Thematic data can be generated in many ways such as analyzing sensed data or including textual or labeling descriptions.

FASyS SSN as many other sensors currently deployed around the world measuring many parameters in different areas (meteorology, environment, manufacturing, etc.) are based in OGC SWE [42], extending them with relationship to ontologies and semantic data to improve the descriptions as well as the access to the sensor data. Many of these measurements are open, accessible and could be integrated in different environments whereas others remain restricted to their owners, as is the case of the FASyS SSN. The semantic data annotations from individual (proprietary) sensors, as well as different sensor networks on a global basis, promotes interoperability between different networks; the FASyS Control Center aggregates sensed information so that risk prevention staff can make the correct decisions in real time.

FASyS SSNs rely on two fundamental technological fields: wireless sensor networks and the semantic web. The first one influences the lower levels of the architecture, as well as the processes of capturing and managing data. The second one is related to the annotation and information management, since it provides mechanisms for integration, data discovery and mapping between different metadata schemes in a structured way.

The information generated by the sensors is semantically marked and feed different applications and services within the FASyS system. Several tasks have been developed in this context, such as:

- Development of a generic ontology comprising all sensors that may be deployed in the factory, including attributes. The first use cases to be deployed utilizing the ontology will focus on presence, temperature, chemical and sound, using protégé and OWL.
- Creation of relationships and reasoning based on the ontology to be able to perform questions and extract knowledge from the information arriving from the sensor networks.
- Specification of a SOA architecture for accessing the information available in the different sensors of the factory, taking into account that the defined web services will have semantic component.
- Management system based on the approximation of the OGC SWE in order to facilitate the integration of different sensors in the HMI (Human Machine Interface) monitoring and control system.

3.2. Security

FASyS infrastructure relays heavily in its communications networks. As a result, any compromise of their components and protocols, or any inability to provide their service may affect FASyS's performance as a whole. Additionally, some of the data transmitted is very sensitive, and confidentiality has to be assured by all means. In order to overcome these limitations, FASyS has established a security model based on risk assessment against communication and information assets in order to determine a strategy for mitigating, reducing or transferring the risk associated to the communications infrastructure. The exchange of critical information in industrial environments requires solutions to guarantee the security of communications and the privacy of nodes. A communications infrastructure is considered secure when it meets the following security objectives for information systems: confidentiality, availability and integrity.

According to the FASyS communications architecture shown in Fig. 1, each level has its own security requirements that must be covered by means of appropriate security best practises, which are closely related to network technology lying underneath. It is crucial to perform network segregation to maintain different communication levels conveniently separated, both logically and physically, and always controlling and limiting the access to different network levels. To achieve the security objectives, different security mechanisms are applied for each communications networking technology.

In FASyS architecture, data privacy is assured by enabling several security mechanisms such as authentication, encryption and secure transport protocols (e.g. VPN—Virtual Private Networks—connections with IPSec or SSL—Secure Socket Layer). Also, network segmentation into different subnets must be performed according to the different actuation areas, based on perimeter security protection using a classical DMZ (Demilitarized Zone) for systems that may be exposed to the public, controlling and limiting the access among these areas. FASyS makes use of next generation firewalls that extend the traditional detection and blocking capabilities to provide control over application layer. WiMAX is considered within FASyS as a suitable network technology for wireless backhaul connectivity in industrial environments. This type of networks can be vulnerable due to the fact that information is transferred in a non-guided medium; data privacy is assured by robust data encryption mechanisms as AES-CCM (Advanced Encryption Standard). Kerberos system has been integrated to manage the users that connect to the BS (Base Station) for the remote system administration, activate IPS (Intrusion Prevention Systems) capabilities if available on the BS, and deploy WiMAX gateways that provide ACL (Access Control Lists) capabilities. At the intermediate level, where WiFi technology is being used, data privacy is assured by authentication mechanisms such as MAC ACLs to control the clients connected to the Access Point (AP), and by robust data encryption mechanisms such as WPA2-Enterprise (WiFi Protected Access—Enterprise). It is desirable to take advantage of the firewalling and IPS (Intrusion Prevention System) capabilities that wireless APs provide nowadays in order to configure and limit as much as possible the allowed traffic. Finally at the local level, in order to assure ZigBee's data privacy, the access of non-authorized sensors to the network must be limited and encryption functions must be provided.

On top of the mentioned security solutions, other transversal security mechanisms are available. These mechanisms include redundancy offering higher levels of availability. In this context, critical network elements should be redundant and fault tolerant, avoiding a unique point of failure, and providing resilience to the network infrastructure; in particular, a virtualization layer has been added to concentrate all the required elements of the system in a dynamic and reliable way (Security as a Service).

Another key security mechanism in FASyS is the access control. The solution implemented is based on a RBACdue to its possibilities and its reduction of cost and complexity in security management. RBAC basis is that different roles are created for different functions or profiles of users. Permission to access different web applications is assigned to specific roles, and the permissions to execute tasks inside those applications will be controlled by the applications based on users' attributes. As the users have not been assigned their privileges directly, but they are instead assigned to roles, the management of the user rights is simplified giving the appropriate role to the user. This approach simplifies common tasks like creating a new user or changing from areas or departments and fulfils the requirements for FASyS.

FASyS SIEM is integrated in the HMI and provides the following main features to the communications architecture:

- Security event prioritization and status monitoring.
- Correlation rules designed for analysing security threats.
- Advanced alerting and visualization.
- Real-time response.
- Reporting and further analysis capabilities, measuring real-time security status and compliance.
- Architectural flexibility and scalability, fitting the needs of diverse platforms.

The security model in FASyS is based on an information security management system compliant with ISO/IEC 27001. The main components of the security model are:

- Asset classification and control.
- Communication technologies classification.
- Study of threats and vulnerabilities.
- Risk analysis.
- Security policy.

Developing a security solution, information security management strategy based on ISO 27001 is an accepted best practice by the industry, and crucial for an heterogeneous communications system such as FASyS. Different security aspects have been taken into account, and due to the heterogeneous technologies employed, there is not a unique solution that could be applied to the complete communications architecture. Therefore, several security mechanisms are specifically implemented for each communications network in addition to some other general and transversal security approaches that have to be considered in order to provide an overall security layer.

4. FASyS ICT MONITORING AND MANAGEMENT PLATFORM

FASyS monitors the worker's safety and health through the deployment of distributed sensors in the factory. To this aim, FASyS has adopted a centralized control and monitoring approach where a Control Center has a global view on the deployed WSN and can control the end-to-end communications QoS. The Control Center monitors and manages the gathered information and the state of the deployed nodes using the heterogeneous communications network previously discussed. To guarantee a continuous control and management of the deployed nodes and their communication links, a novel software platform has been developed within the FASyS project. In addition, the implemented platform allows taking the necessary countermeasures to prevent link failures or congestions, and therefore guarantee the continuous operation of the ICT network necessary to control the worker's health and safety. The use of distributed and heterogeneous wireless communications prevented the use of relevant management tools like [31] or Cacti [34].

Fig. 2 depicts the architecture of the designed and implemented communications monitoring and management software platform. The platform can be accessed through a Human–Machine Interface (HMI) using a web browser. The FASyS monitoring and control HMI has been designed to provide highly visual interfaces about risk levels. Moreover, the system also makes suggestions of the most suitable procedures to be applied when a risk situation is detected, so that the reaction time can be hugely reduced and the user can send a highly effective execution action plan immediately. The HMI has been developed as a web application on top of a Content Management System (CMS). This feature facilitates the creation of content and user profiles as well as the integration with other web applications that allow accessing other components of the FASyS system, such as the health monitoring/decision-support system. The main design goals of the FASyS HMI are the following:

- Provide an efficient and simple working interface for users managing the FASyS monitoring and control system, including the communications management Toolbox previously described.
- Define and describe all aspects of the integrated labor risk monitoring and control system including equipment, personal devices, factory signaling, etc.
- Provide appropriate mechanisms to improve situational awareness in the occupational health management center.
- Allow real-time monitoring of all nodes that are sources of data in the manufacturing plant, in a scalable way, i.e. interacting with SOS and other data sources.
- Monitoring and management of communication elements in the network in order to decide and implement the most suitable configuration using the Toolbox.
- Configuring data sources, real-time or historical, so system managers may review any information stored.

The FASyS HMI requests the Toolbox information about the state of the communications network, and the Toolbox responds sending the requested information. The interaction between the HMI and the Toolbox is made through HTTP interfaces or connectors. 6 and 7 detail the interoperability procedures and mechanisms between these two elements of the architecture.

The Toolbox is the software platform that implements the control and management functions necessary to monitor in real-time the FASyS heterogeneous communications network. The Toolbox is formed by a central application that is in charge of global management functions, and local agents implemented at each node of the communications architecture that executes specific monitoring and management functions for those nodes. The Toolbox monitors the state of the communications network through the continuous measurement of key communication parameters that provide information about the connectivity and QoS levels of individual links and end-to-end communications. Different parameters are measured for each wireless technology. In particular, the Toolbox currently monitors the following parameters:

- WSN (IEEE 802.15.4): The parameters measured at the WSN nodes are the Received Signal Strength Indicator (RSSI) and the throughput achieved at the application level. The RSSI measures the power of radio signal present at the node's radio interface during the reception of a frame. The throughput is the average rate of data correctly received at the application level.
- WiFi (IEEE 802.11): At the medium-range level, nodes have better monitoring capabilities. Nodes are able to sniff traffic at MAC level and measure link state. In this context, IEEE 802.11 nodes measure throughput at MAC level, channel busy time and RSSI. Channel busy time indicates the fraction of time for which the medium is utilized in some time interval.
- WiMAX (IEEE 802.16): The WiMAX stations (access unit and subscriber unit) implement a firmware provided by the stations vendor, and only parameters provided by the stations firmware can be monitored. In this context, the monitored parameters are the RSSI and average Signal-to-Noise Ratio (SNR). SNR is defined as the ratio of the signal power to background noise power, and indicates the reliability of the link between the transmitter and the receiver.

The measured metrics are periodically sent and published in the SOS, where they can be accessed at any time. The central application also implements tools to provide the HMI with this information for graphical visualization. The network operator can then have real-time information about the status of all nodes and take necessary actions if any communications problem is detected.

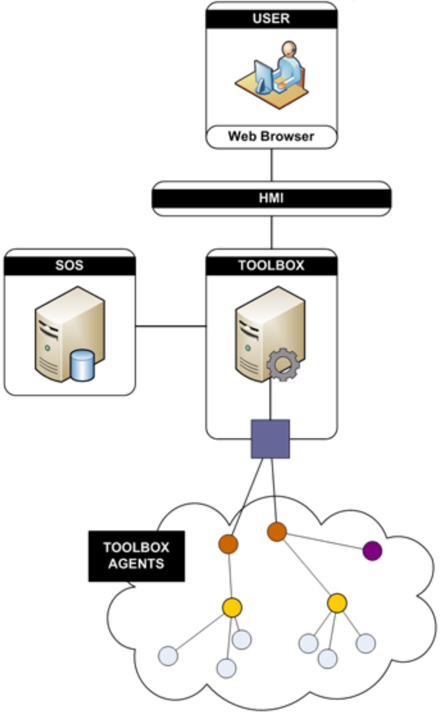


Fig. 2. Architecture of FASyS's ICT monitoring and management software platform.

The Toolbox implements control mechanisms that enable the adaptive configuration of the communications network based on the factory context. In particular, the Toolbox central application is able to establish the communication path between the Control Center and any deployed node and modify its configuration. As a result, the communication nodes can be remotely accessed and configured from the Toolbox in case any malfunctioning or QoS degradation is detected by the operator. Such reaction is necessary to avoid any node being disconnected or isolated, as well as losing critical information. Control parameters that can be configured on each node depend on the role of the node in the communications architecture, the communications technology employed, and the configuration capabilities of the deployed nodes. For example, the Toolbox currently allows modifying the transmission power or the channel of the distributed wireless sensor nodes, or reconfiguring the routing table of the WiFi nodes.

Local Toolbox agents perform local functions, such as sniffing traffic from the communication links to monitor their performance and operation, and execute control orders received from the central application. Functions implemented in local agents can be accessed through the central application that provides management functionalities such as processing the data provided by the agents, detect abnormal conditions, or reconfigure certain configuration communications parameters in distributed FASyS nodes. Such functions are provided through the combination of the independent web services at the central application and local agents. The need for distributed local agents implemented at each communications node is justified as follows:

- Monitoring the state of each communications link and node requires tasks that have to be carried out locally (e.g., traffic flow analysis).
- The industrial requirements demand for a highly reliable communications network capable to adapt its configuration to changes in the environment. In this context, communication nodes need to be able to reconfigure locally following instructions received from the Control Center (e.g. modifying the routing table in a gateway node, or changing the transmission power or channel).
- WSN router nodes do not implement the same network and transport protocols as WiFi or WiMAX nodes. As a result, direct interaction between wireless backhaul node and WSN router nodes is not possible using common application protocols such as HTTP or SNMP. Local functions are therefore necessary at the coordinator nodes to manage the communications between backhaul nodes and WSN router nodes.
- The implementation of local agents facilitates exploiting the computational resources available at the different nodes of the FASyS communications architecture.

OGC has specified the Sensor Observation Service (SOS). The SOS allows storing, sharing and accessing information about the FASyS nodes and their link connectivity. The FASyS semantic sensor system is based on the use of SOS and SensorML standards. These standards are part of the SWE framework specified by OGC, and provide means to access sensor generated data and metadata to configure the state of each sensor. FASyS employs an implementation specifically adapted to industrial environments. SOS as part of the SWE is a collection of open interoperability interfaces, metadata encodings and services for exploiting Web-connected sensors and sensor systems of all types.

SOS has extensively been used in the FASyS system to store information gathered by the sensors, for the aim of this paper, the SOS has also been used to store QoS information regarding the state of the networks and specific nodes. SOS provides two main standard interfaces:

- Interface between the SOS and a sensor, through which each sensor from any WSN should follow a well defined process to register and insert measurements.
- Interface between the SOS and an application, through which each application also follows a well defined process to obtain a list of available sensors, their capabilities and measurements throughout the time. Applications ‘perceive’ sensors as a web server where they can access any piece of information via HTTP as any other web resource. Data exchange in both communication interfaces are based on two OGC standards: SensorML and O&M [42].

Fig. 2 shows the interaction of the SOS with the Toolbox, using bidirectional communication, i.e. the Toolbox extracts and inserts information in the SOS using the standard interfaces.

5. Sensor Observation Service (SOS)

A key component of the FASyS sensor environment is the Sensor Observation Server (SOS), a standard from OGC [42]. SOS forms part of the SWE framework, which is a collection of open interoperability interfaces, metadata encodings and services for exploiting Web-connected sensors and sensor systems of all types. Developers and system integrators can use these specifications for building applications, platforms, and products involving Web-connected devices such as flood gauges, air pollution monitors, stress gauges on bridges, mobile heart monitors, webcams, etc. Web Sensors and SWE are in fact concepts in the context of GEOSS (The Global Earth Observation System of Systems). FASyS considers the use of different SOSs located in strategic points in the Communications Architecture in order to provide homogeneous access in the heterogeneous wireless network to the different control applications [67].

As indicated, the technology used in FASyS has been standardized by the OGC and has been extended and specially applied to factory automation by the research team. The standard and components of the SWE SOA are: Observations & Measurements (O&M); Sensor Model Language (SensorML); Transducer Model Language (TransducerML or TML); Sensor Observation Service (SOS); Sensor Planning Service (SPS); Sensor Alert Service (SAS) and Web Notification Services (WNS).

Regarding the design architecture, it is important to consider the location of the SOS within the network. There are different approaches depending on the use of a centralized or a distributed architecture. If a distributed solution is adopted, SOS may be located in different elements of the network. The first approach considers locating the SOS in the coordinator node, as near as possible to the physical sensor. The second approach considers locating the SOS in the gateway node, as near as possible to the Control Center. In order to determine the most appropriate location to place the SOS, it is important to consider the data flows that are envisioned between sensors and the SOS, and between applications and the SOS, in order to minimize data traffic. If a centralized approach is used, as it has been the case for the first FASyS prototype, the SOS is installed as individual equipment in the Control Center, together with other services and systems required to implement the FASyS solutions. As the FASyS system uses a Complex Event Processing (CEP) system as key component of the Control Center that continuously issues requests to the SOS, the data flow is considered to be significantly higher than the data between sensors and the SOS. This is the main reason to locate the SOS close to CEP in the Control Center.

The use of SOS in the FASyS framework is based in two key components: semantics explained by the concept of the SSW and interoperability:

- The concept of SSW is based on the use of a special type of information infrastructure for web-centric collection, modeling, storage, subsequent withdrawal, sharing, manipulation, analysis and visualization of information on sensors and observation of phenomena from them. The definition of SSW by OGC is: "networks of sensors and sensor data storage accessible via the web, which can be discovered and accessed using protocols and application interfaces standards" [69][70].
- The use of SOS provides syntactic and semantic interoperability. Interoperability is a property referring to the ability of diverse systems and organizations to work together (inter-operate). The term is often used in a technical systems engineering sense, or alternatively in a broad sense, taking into account social, political, and organizational factors that impact system performance. Interoperability may also be understood as the ability of two or more systems or components to exchange information and to use the information that has been exchanged [71].

FASyS semantic sensor system is based on the use of SOS and SensorML, and provides access to the data generated by the sensors such as the metadata to configure and customize each individual component (sensor) of the network. The main benefits of using semantic sensor networks in FASyS are: (i) platform independence as practically any sensor or modeling system can be supported (even simulated sensors); (ii) easy development of services allowing dynamic connectivity between resources; (iii) liaison with semantic environments, adding semantic information to the basic SWE paradigm; (iv) traceability and support to the implementation and management of real-time measurements; (v) flexibility in implementation: container capacity and existing sensors, implementing and processing services; and (vi) scalability from a single sensor to a collection, individual, group or cluster of sensors.

The concept of semantic sensor network is used to organize, manage, interrogate, understand and control the different components of the data gathering process (i.e. network, sensors and the resulting data using high-level specifications). If semantics are introduced in the reasoning process of a FASyS subsystem, it is important to design properly the various steps of communication and interfaces if sensors and sensor networks are involved, as they impose various kinds of restrictions and limitations, such as power constraints, finite and limited memory, unreliable communication network and the quality and variability of data received [72][73].

The SSW or the SSN base their operation on the existence of a sensor network. The contribution of this type of mechanism is the addition to the data measured/generated by sensors in the form of metadata annotations of semantic information of a temporal, spatial and thematic, accessible through a Service Oriented Architecture [74].

Regarding interoperability, we can distinguish two different possibilities: syntactical and semantics interoperability. FASyS provides both kinds of interoperability starting from the correct use of a SOS as support for merging and concentrating the information generated by sensors and distributed devices. Though strictly speaking the SOS provides syntactical interoperability, it is relatively easy to incorporate simple semantic support as temporal, spatial and thematic filtering are natively supported by SensorML and O&M, the two standard interfaces used by the SOS. Additionally, SensorML supports extensibility through annotations. If such annotations are part of a semantic vocabulary, then more complex semantic operations can be supported. SOS has been extended with a database based on a specific FASyS data model that includes some specific features not included in the OGC standard and are required to integrate the SSN in the FASyS HMI, described in section 6. [75]

6. TOOLBOX

The Toolbox is a software environment allowing the centralized and adaptive management of FASyS heterogeneous wireless communication network. The Toolbox implementation is based on the REpresentational State Transfer (REST) architecture style [76]. REST is a web services architectural style that is distributed and highly interoperable. The different FASyS components have been implemented independently. However, a key requirement is that they have to be able to interact among them. REST provides this capability to the Toolbox, and makes it highly portable. Despite not being a formal specification, REST architectural style has become a de facto standard that is generally used for the implementation of web services. Although other architecture styles could have been used, REST has been selected because it uses uniform interfaces for the provision of services. In this context, it is not necessary to use formal descriptors to publish the provided service or the presence of a service provider in the system. This characteristic involves lower bandwidth and resource processing load in system components, which is appropriate for reducing the overhead in the communication system considering the limited bandwidth and computational resources of communications nodes. In addition, the use of uniform interfaces simplifies and speeds up the deployment and extension of system components, and reduces the complexity of the connector semantic. REST-based systems are highly scalable which makes easier the addition of new nodes. Finally, REST does not restrict the format that has to be used in the exchange of the resources state with external components, which facilitates the interoperability and integration of the Toolbox within the FASyS system.

Fig. 3 shows the software architecture of the Toolbox which includes a central application and a series of local agents. Local agents are implemented in coordinator nodes, gateway nodes, WSN nodes, and also in the Control Center. They perform local monitoring functions and execute actuations received from central application.

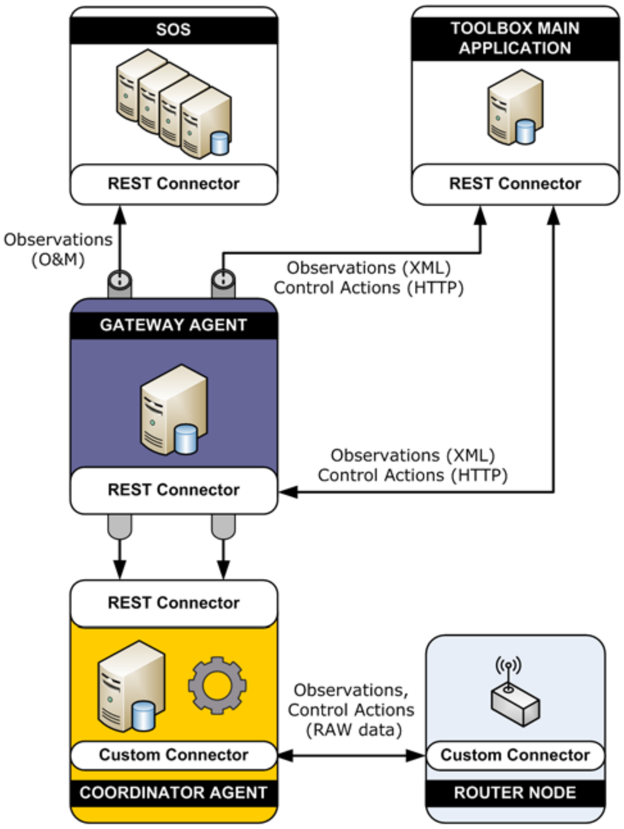


Fig. 3. Software architecture of the Toolbox.

The implementation of local agents required a tailored software implementation since the use of standard management protocols such as SNMP does not allow carrying some of the discussed FASyS monitoring and control functionalities. In this context, a modular implementation based on the OSGi service platform [77] has been provided. Local agents perform two types of tasks. First, they monitor the data sent through the communication links of the nodes where they are implemented, and extract communication performance parameters that are sent periodically to the central application using the corresponding network interfaces. Second, they execute control orders sent by the central application, such as reconfiguring the routing table of a gateway node or modify the transmission power or channel of a WSN node. WSN router nodes implement agents with reduced functionalities due to their limited computational resources[1]. Local agents at the coordinator node provide support to the agents at the WSN router nodes with additional functionalities. In particular, WSN router nodes measure and send the communication metrics to the WSN coordinator node. The local agent at the coordinator node acts as a sink of the measurements sent by all WSN router nodes, and retransmits them to the central application. In addition, the local agent at the coordinator node receives requests from the central application to reconfigure WSN router nodes under its control. It interprets such requests and forwards them to the corresponding WSN router node.

The central application is the core element of the Toolbox. It is located at the Control Center and at the top of FASyS's heterogeneous communications architecture. All functionalities implemented in the Toolbox are available through the central application by a set of web service interfaces. The central application maintains a temporal copy of the communication QoS measurements stored at the SOS to speed up the management of the data. It also includes mechanisms to process these measurements.

The most frequently used application layer communications protocol is Hypertext Transfer Protocol (HTTP) [78]. HTTP satisfies all previous constraints, and provides additional advantages such as an intuitive communication procedure that uses verbs (GET, PUT, POST and DELETE) and names (Uniform Resource Locator, URL) for accessing remote resources and that it is compatible with a high number of frameworks and technologies.

The interaction between the Toolbox central application and the local agents is as follows:

[1] The WSN router nodes are implemented under an open source, BSD-licensed operating system called TinyOS. The TinyOS platform provides a number of interfaces to abstract the underlying communication services. All of these interfaces use a common message buffer abstraction which is implemented in nesC language (similar to standard C language). In particular, the WSN nodes send and receive messages using the TinyOS interface to the MAC and PHY layers of the IEEE 802.15.4 standard.

- Agents send data about the status of the resources they monitor using HTTP connectors. Data is coded in a custom plain XML-based format that is supported by all Toolbox components. This customized format is more compact than O&M and requires less processing resources. The choice of a customized plain XML-based format is mainly due to the use of standard Java libraries that allow translating data to plain XML-based documents but not to O&M documents.
- The central application sends reconfiguration requests to the local agents through HTTP POST operations with an attached XML document that describes the operation to be performed. In addition, local agents also support the invocation of simple control operations by means of HTTP GET operations provided with URL-encoded parameters.

Finally, the central application at the Toolbox interacts with the SOS and the HMI using the following interfaces:

- The interaction between the HMI and the Toolbox is made through HTTP interfaces or connectors. The FASyS HMI requests the Toolbox information about the state of the communications network, and the Toolbox responds sending the requested information. The information requested from the HMI about the status of nodes and communication links is provided in a GeoJSON [79] document; this kind of interaction is characteristic of REST architectures. GeoJSON format is spatially enabled, and is based on JSON [80] meta-format, a compact text format for describing data structures supporting basic types like integer and real numbers, or more complex types like arrays. JSON does not employ schemes, and can be directly translated to native data structures. A spatially enabled format allows publishing resource representations on a map. In addition, the used compact format requires less bandwidth and can be faster than other spatially enabled formats. It is also supported by multiple libraries and frameworks for the graphical representation of spatially-related data.
- The Toolbox periodically sends the communication QoS measurements to the SOS coded in O&M to update its database. The Toolbox interacts with the SOS using a REST connector which is also supported by the SOS.

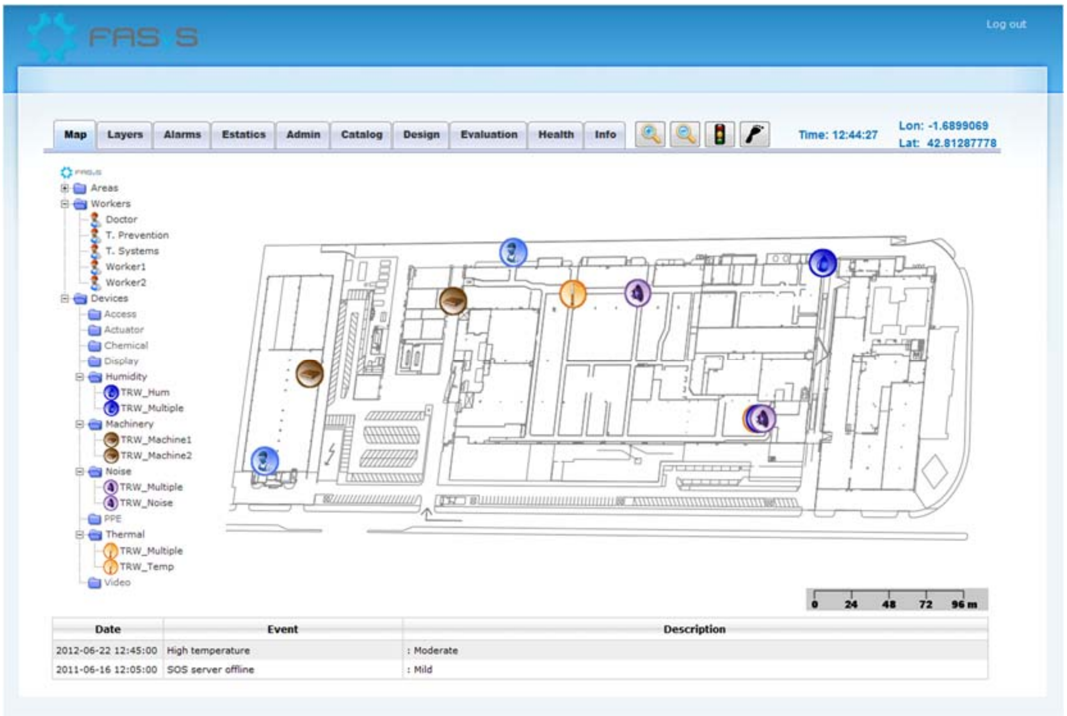
7. HUMAN MACHINE INTERFACE

The monitoring and control of industrial and manufacturing systems is usually performed separately by area of interest, so that each system vendor typically provides its own information and has its own HMI to present gathered information and manage the equipment and devices. The concentration of every HMI and function in a single tool would represent a significant forward step since it represents one of the main pitfalls in terms of interoperability, knowledge processing and management, and exploitation of this knowledge for occupational risk management, improved production and productivity [81].

FASyS provides the tools and models for being able to process as much as information in less time as possible. Thus, the enterprise safety and healthy manager can work with relevant information to make informed decisions. The aim of FASyS personalized decision support tools is not just to warn and display a particular risk level but also to ease the decision process based on strong knowledge support.

The structure of the HMI is composed of three main areas, as shown in Fig. 4:

- The top area includes a series of tabs (map, layers, alarms, statistics, admin, catalog, design, evaluation, health and info) that correspond to the main screens of operation by the administrator .



Date	Event	Description
2012-06-22 12:45:00	High temperature	: Moderate
2011-06-16 12:05:00	SOS server offline	: Mild

Fig. 4. General HMI monitoring screen.

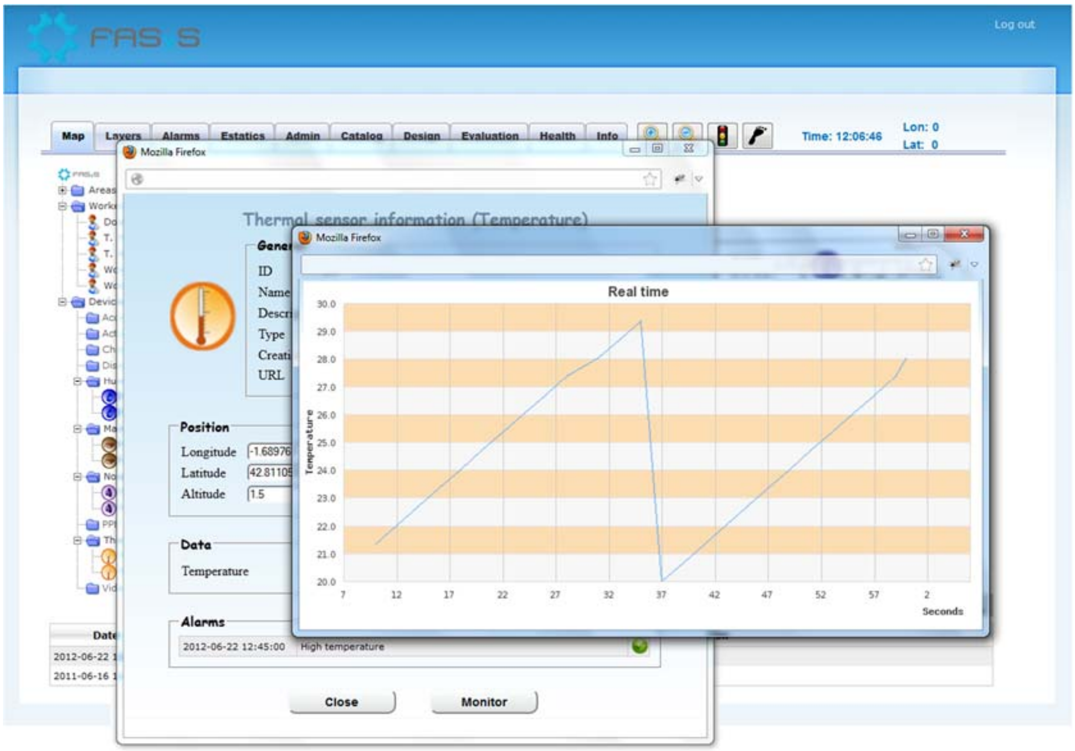
- The central part is the part of displaying devices. It is the most important, visual and interactive part. Two areas can be distinguished:
    - Left zone: this part contains a menu of the components of FASyS, categorized into Areas, workers and devices.
    - Right zone: this part is the visual georeferenced area (including a scale indicator) of the components at the factory, where it is possible to monitor the devices associated with any alarm.
- The bottom part displays in a table all events and alarms that are taking place at the factory. This table is updated in real-time, so it displays the most recent alarms.

It is important to highlight the capabilities of the central area. One of the basic functions is accessing each of the devices available in the factory. Either from the left menu or by clicking directly on the device in the right zone, all capabilities (general information, location, data, and related alarms) from a device can be accessed, as depicted in Fig. 5. Moreover, devices can be monitored in real time, and it is possible to access recently sensed data.

Another relevant feature provided by the HMI is the ability to aggregate risk level information and display it (see Fig. 6). As there may be hundreds of devices on a factory, it is more practical to monitor special areas of such factory, for example those that are more prone to risky conditions. Assigning colors to risk levels similar to a traffic light, it is simple for an administrator to have an overall picture of the situation and easily identify those areas where relevant risks have been identified and some actions have to be taken. The risk level of an area is determined by the highest risk level of any of the devices that are within this area. As it could be expected, area risk levels change over time as (i) mobile devices change from area to area and (ii) alarms are being handled. In addition, the system allows recording historical information about the area risk levels to facilitate further analysis. From this point of view, each area can be considered as an aggregated sensor that senses risk levels over time.

Besides risk levels, device traces may also appear of relevance in order to track the movement of a special worker (e.g. a worker with some medical pathology that should not get in close contact to areas where chemical products are manipulated). In such cases (see Fig. 6), a doctor trying to monitor/assist this worker may find important to see the recent and past movements inside the factory of the worker, which is displayed as a dashed line.

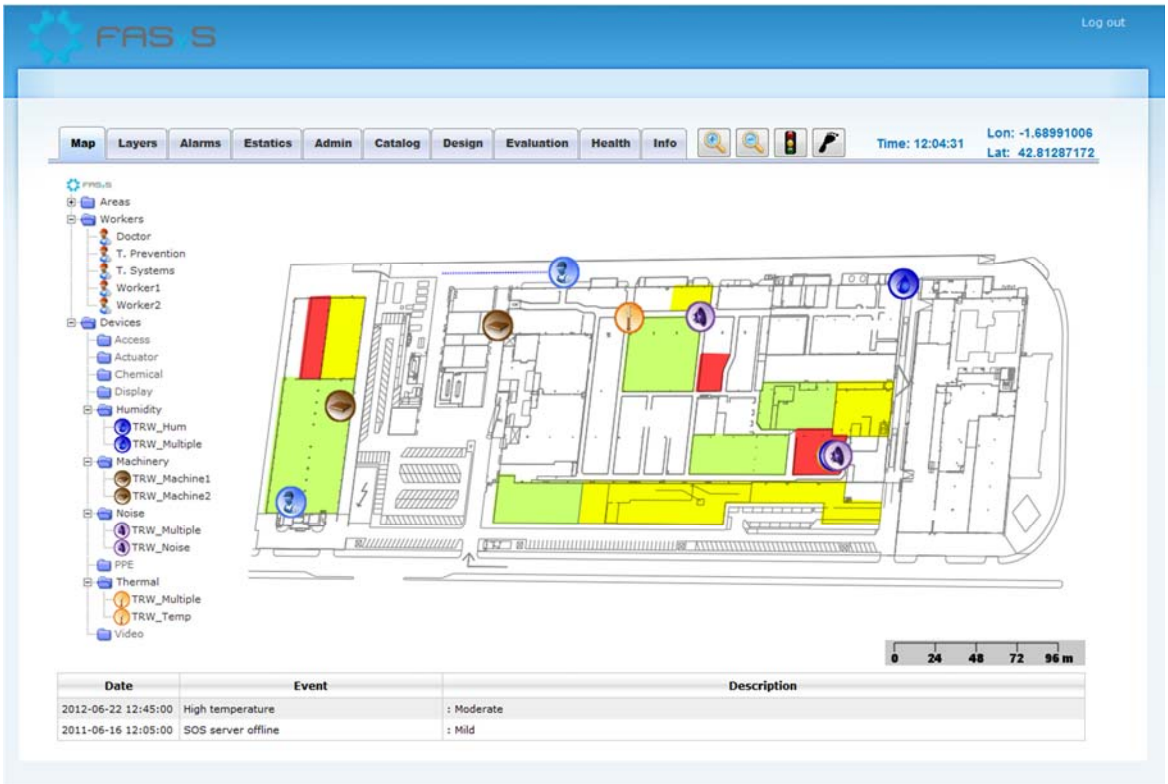
The HMI has been developed as a web application on top of a Content Management System (CMS). This feature facilitates the creation of content and user profiles as well as the integration with other web applications that allow accessing other components of the FASyS system, such as the health monitoring/decision-support system. Web integration is not only important for easy (visual) integration on a web browser; in fact, web applications can keep their internal legal and security constraints independently from others. In this way, the healthy system integrated in FASyS can keep its strong access and usage requirements (as medical sensitive data cannot be compromised) without imposing any additional requirements to other applications. However, web integration does not only mean visual integration, but also profile access integration. On the one hand, considering the HMI as a summary of independent applications, each one may have their own users and profiles to deal with them throughout the application session. On the other hand, considering the HMI as an integrated platform of web applications, a federated authentication mechanism must be provided in order to perform Single Sign On (SSO). In the context of FASyS, SSO is provided by means of SAML, where different profiles are specified and each of them access the HMI under different conditions, that means, accessing different features. A doctor may be mostly interested in the health data, an administrator in registering devices and see risk levels, and a worker in its personal monitored data. External workers (including medicals and technicians) can also access the HMI by delegating authentication to external Identity Providers (IdPs) that have a trust relationship with the HMI (which acts as Service Provider in the SAML scheme).



Longitude -1.68976
Latitude 42.81105
Altitude 1.5

2012-06-22 12:45:00 High temperature

Fig. 5. Device capabilities and sensed data monitoring screen.

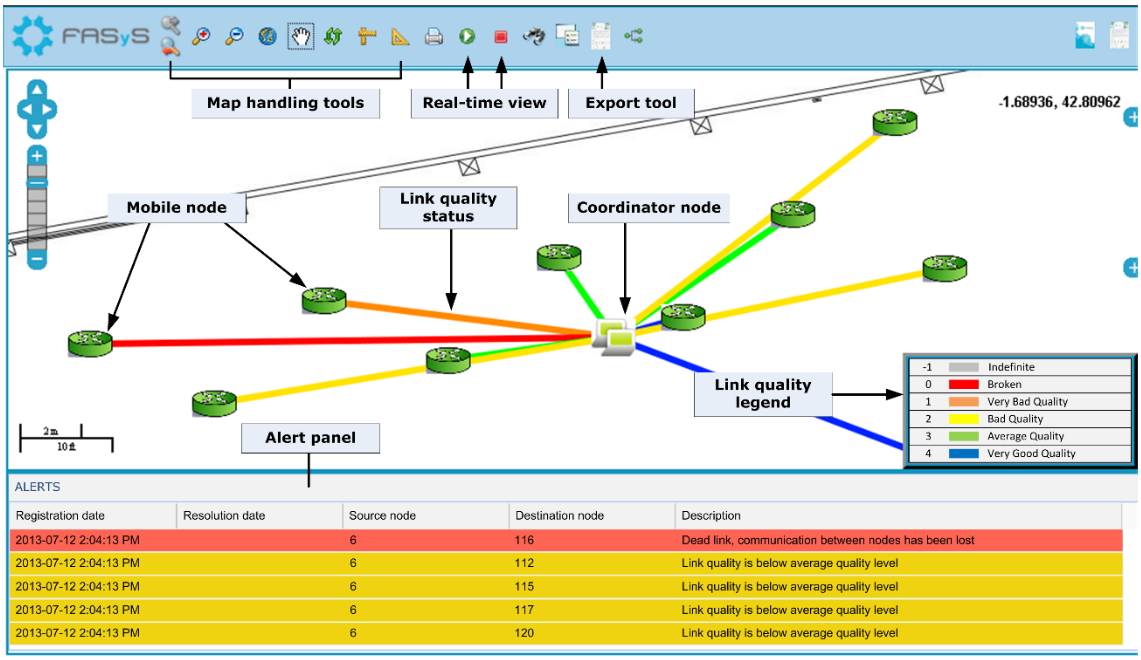


Date	Event	Description
2012-06-22 12:45:00	High temperature	: Moderate
2011-06-16 12:05:00	SOS server offline	: Mild

Fig. 6. Risk area level management and traces.

The FASyS Control Center through the HMI manages and controls the different components and devices of the FASyS system. Regarding communications the state of the network is highly relevant in order to have the adequate situation awareness. The Toolbox HMI provides this information in real time, and may be used for the communications management experts to control the situation, failures and correct behavior of the network using the same interface as other administrators of the FASyS HMI. The Toolbox HMI depicts the state of the deployed communications network in a factory. It shows different network parameters in real-time in order to react against node or link problems. The communications network is depicted over the factory map. To this end, it is necessary to geo-reference information in real-time for both nodes and communication links.

Fig. 7 shows the main view of the Toolbox HMI. This figure shows a deployment of four node types (mobile, static, coordinator and gateway) and their link state is represented by different color lines. Also, it shows a toolbar on the top that allows users to surf the factory map to extract information of deployed nodes and links. This toolbar incorporates basic tools such as zoom, center the map, select a map section, and measuring distances between two points among others. Besides, this toolbar offers the possibility to visualize the position of nodes in real time and export displayed data to an excel file, external database or any other formats. Other features provided by the Toolbox HMI are the display of additional information of a node (e.g. its battery level) or link by double clicking on them, as shown in Fig. 7.



-1	⬜	Indefinite
0	🟥	Broken
1	🟧	Very Bad Quality
2	🟨	Bad Quality
3	🟩	Average Quality
4	🟦	Very Good Quality

ALERTS

Registration date	Resolution date	Source node	Destination node	Description
2013-07-12 2:04:13 PM		6	116	Dead link, communication between nodes has been lost
2013-07-12 2:04:13 PM		6	112	Link quality is below average quality level
2013-07-12 2:04:13 PM		6	115	Link quality is below average quality level
2013-07-12 2:04:13 PM		6	117	Link quality is below average quality level
2013-07-12 2:04:13 PM		6	120	Link quality is below average quality level

Fig. 7. Toolbox HMI main view.

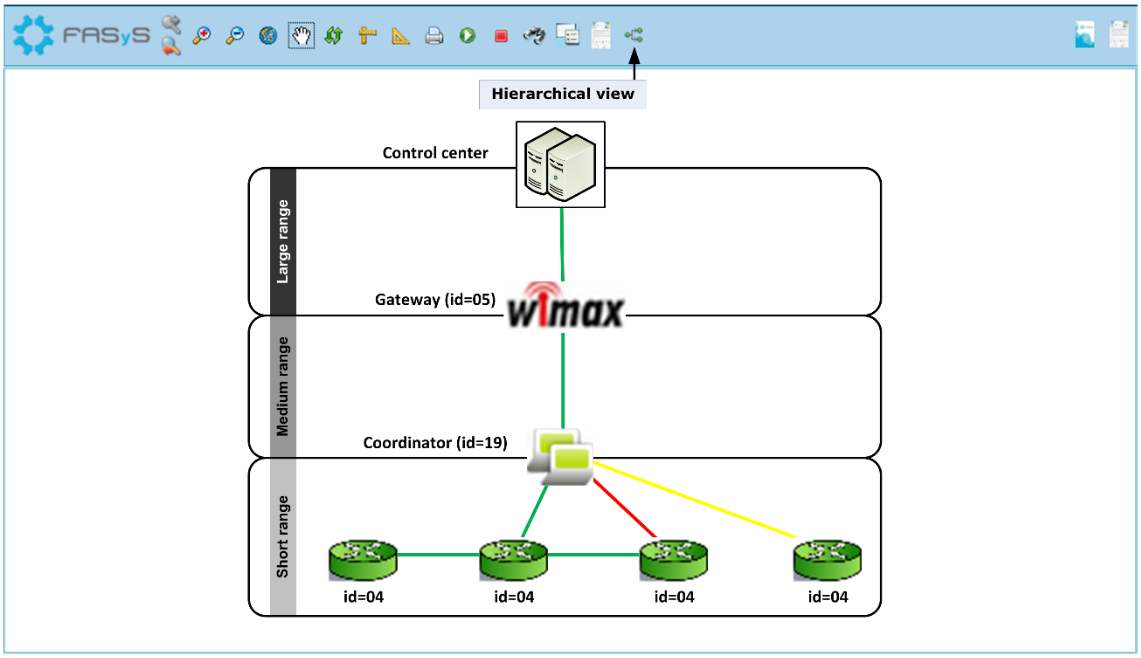


Fig. 8. Toolbox HMI hierarchical view.

In addition to the main view shown in Fig. 7, the Toolbox HMI also allows a hierarchical visualization of the network (Fig. 8) based on the communications architecture described in Section 2. Fig. 8 shows the short, medium and large range communication levels with all nodes and links deployed for a better comprehension of the network state by the user. The colored links between nodes of the architecture indicates the status of the communications link, with the red color indicating a lost communications link, the yellow color a low QoS communications link, and the green color a stable and robust communications link.

The Toolbox HMI implementation has been developed with open source software, specifically with GIS (Geographic Information Systems) application. GIS application can integrate, store, share and display geographically referenced information. The application has been developed with java. The implementation needs two data sources: static sources whose data value and position will not change, and dynamic ones handling data associated to mobile nodes. These mobile nodes and their communication links are visualized using the data from a GeoJson file that can be accessed from the main Toolbox HMI application. In this context, GeoJson files are a simple format of data exchanged with a defined structure. This main application needs other applications, as MapServer and OpenLayer, to generate images and develop features over them. MapServer manages the application integration and map generation, and configures parameters as map size, image format (jpg, png, etc.) and layers display among others. In addition, OpenLayer provides an API to access to different sources of mapping information.

8. EVALUATION

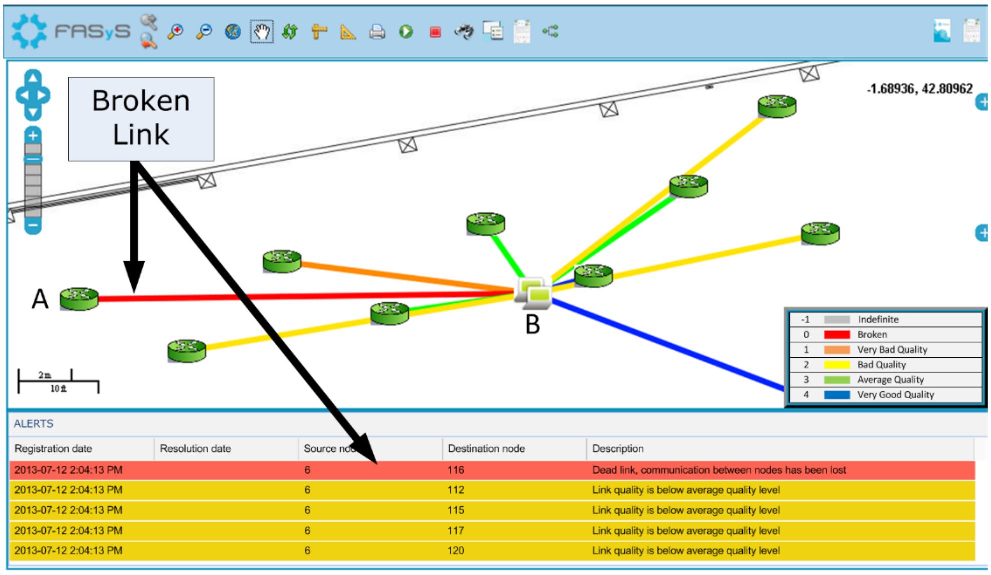
A series of tests has been conducted to demonstrate the capacity of the Toolbox to continuously monitor the end-to-end quality of heterogeneous wireless communications in industrial environments. To this aim, the complete FASyS communications network has been deployed in two scenarios, and the tests have been configured to reproduce different communication quality levels. In particular, the network has first been deployed in a controlled laboratory setting characterized by the presence of open spaces, and then in an industrial environment with a large presence of obstructing elements (machinery, vehicles, walls, etc). In the deployment, the control center integrates the HMI, SOS and Toolbox central application functionalities. The deployment also includes a gateway node, a coordinator node, 8 router nodes and mobile nodes, all of them implementing the necessary agents to monitor the quality of wireless communications. The specific location of the deployed nodes has been selected to reproduce varying communication conditions, and thereby test the capacity of the Toolbox to detect degradations in the wireless link quality. The tests have allowed validating the capacity of the Toolbox to:

- Collect information about the quality of wireless links from the different agents deployed at the nodes of the FASyS communications architecture.
- Process and analyze the quality of all wireless links, independently of the employed communications technology and whether the nodes are static or mobile.
- Detect and monitor new wireless links created between mobile nodes and fixed nodes as the mobile nodes move around the test scenario.
- Detect and quantify degradations of the quality of wireless links, and generate the corresponding alerts for notifying the Toolbox operator. The capacity of the Toolbox to detect and manage such degradations takes into account the hierarchical structure of the FASyS communications architecture.

Fig. 9 shows an example of one of the conducted tests. The test emulates the case in which a IEEE 802.15.4 router node (labeled A in Fig. 9) runs out of battery. When this happens, the router node stops communicating with its coordinator node (labeled B in Fig. 9), and the agent installed at the coordinator node stops transmitting wireless measurements to the Toolbox at the control center. The lack of received wireless measurements allows the Toolbox to detect the disconnection that is represented in the HMI through a red link (broken wireless link). The Toolbox generates an alert (also highlighted in red in the bottom part of the HMI) when a wireless link is detected as broken. The alert identifies the two nodes affected by the disconnection, and the time at which the wireless link was broken. When the battery is replaced (Fig. 9.b), the wireless link between the two nodes is re-established. Automatically, the Toolbox measures the wireless link quality between both nodes using the deployed agents, and changes the alert status in the HMI. The alert is then marked as resolved (changes color from red to green), and the quality of the wireless link between the two nodes is updated. The link quality of IEEE 802.15.4 connections is measured in terms of average RSSI. In the example illustrated in Fig. 9.b once the alert has been resolved, the wireless link RSSI between the nodes A and B was equal to −81 dBm. In this case, the link is depicted in orange color that represents very bad link quality conditions. The very bad link quality status is assigned to IEEE 802.15.4 connections when the RSSI is in the range −76 dBm and −86 dBm; ranges have been defined for all possible link quality conditions shown in Toolbox's HMI.

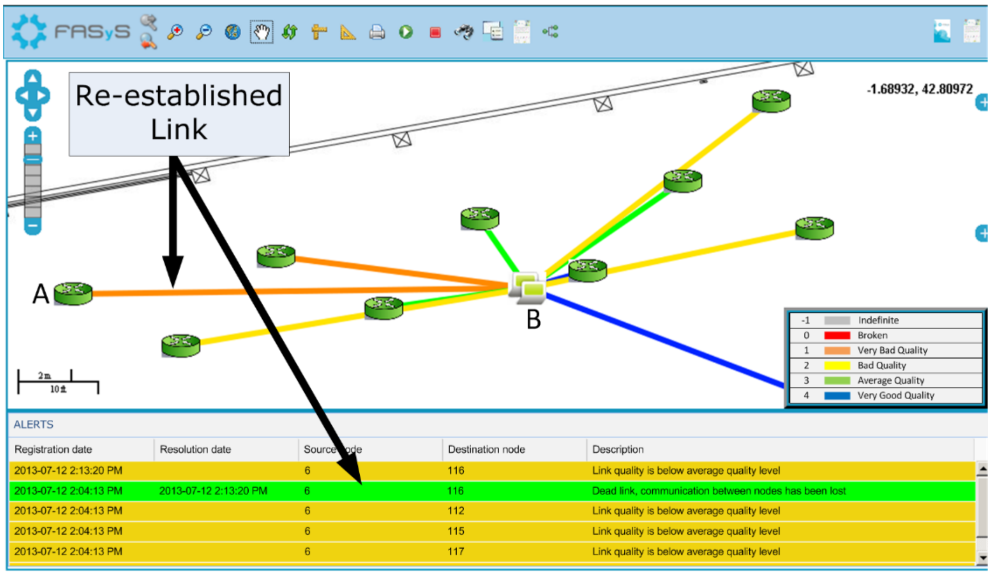
The Toolbox is capable to monitor the quality of any wireless technology deployed in FASyS. To illustrate it, a degradation of the WiFi link quality between coordinator and gateway nodes (labeled A and B in Fig. 10 respectively) is reproduced by disconnecting their antennas. Fig. 10.a shows that the WiFi quality of the link between both nodes was very good before the antennas were disconnected. When disconnected, the link between the gateway and coordinator nodes is broken. The Toolbox detects the new condition, and reports the link status between both nodes as broken. The router nodes are connected to the control center through the coordinator and gateway nodes. Since the link between these two nodes is broken, the agents installed at the router nodes cannot report any longer their IEEE 802.15.4 RSSI measurements to the Toolbox. In this case, the status of the IEEE 802.15.4 links is marked as 'indefinite'. When the WiFi link between the gateway and coordinator nodes is restored, the status of the IEEE 802.15.4 links is updated based on their RSSI level.

The FASyS Toolbox has also been designed and implemented to be able to remotely control from the control center the configuration of deployed wireless nodes. This characteristic has also been validated in the conducted tests. In particular, the tests have validated the capacity of the Toolbox to modify in real-time certain critical wireless transmission parameters, such as the transmission power, in addition to alert functionalities available at the IEEE 802.15.4 nodes. Fig. 11 shows the configuration window for modifying some of these parameters, like activating a buzzer or a set of leds to alert of some dangerous or inadequate conditions (e.g. to indicate a risk of collision or the need to connect a harness while working at height).



Registration date	Resolution date	Source node	Destination node	Description
2013-07-12 2:04:13 PM		6	116	Dead link, communication between nodes has been lost
2013-07-12 2:04:13 PM		6	112	Link quality is below average quality level
2013-07-12 2:04:13 PM		6	115	Link quality is below average quality level
2013-07-12 2:04:13 PM		6	117	Link quality is below average quality level
2013-07-12 2:04:13 PM		6	120	Link quality is below average quality level

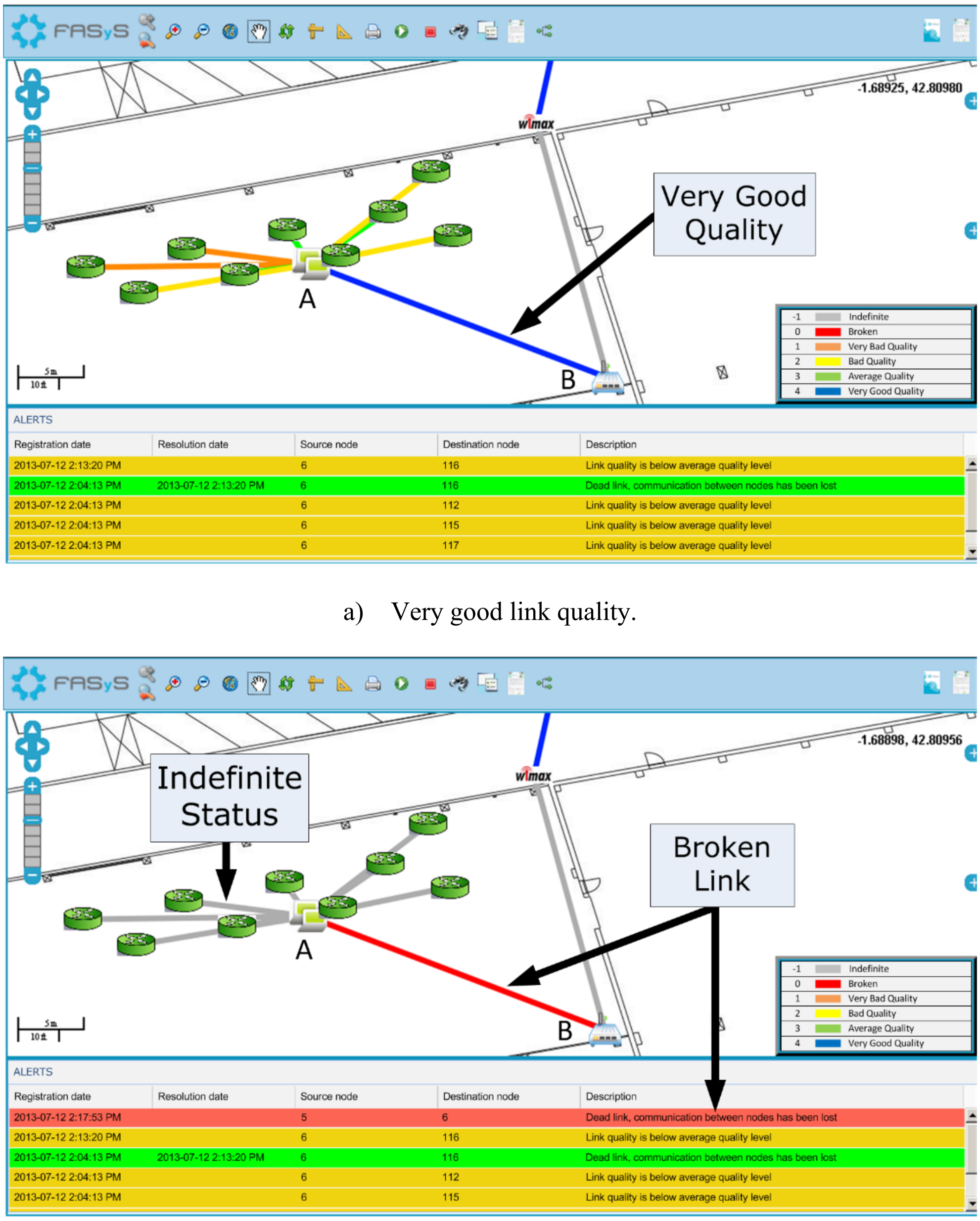
a) Link broken



Registration date	Resolution date	Source node	Destination node	Description
2013-07-12 2:13:20 PM		6	116	Link quality is below average quality level
2013-07-12 2:04:13 PM	2013-07-12 2:13:20 PM	6	116	Dead link, communication between nodes has been lost
2013-07-12 2:04:13 PM		6	112	Link quality is below average quality level
2013-07-12 2:04:13 PM		6	115	Link quality is below average quality level
2013-07-12 2:04:13 PM		6	117	Link quality is below average quality level

b) Link re-established.

Fig. 9. Link between router and coordinator nodes.



-1	⬜	Indefinite
0	🟥	Broken
1	🟧	Very Bad Quality
2	🟨	Bad Quality
3	🟩	Average Quality
4	🟦	Very Good Quality

ALERTS

Registration date	Resolution date	Source node	Destination node	Description
2013-07-12 2:13:20 PM		6	116	Link quality is below average quality level
2013-07-12 2:04:13 PM	2013-07-12 2:13:20 PM	6	116	Dead link, communication between nodes has been lost
2013-07-12 2:04:13 PM		6	112	Link quality is below average quality level
2013-07-12 2:04:13 PM		6	115	Link quality is below average quality level
2013-07-12 2:04:13 PM		6	117	Link quality is below average quality level

a) Very good link quality.

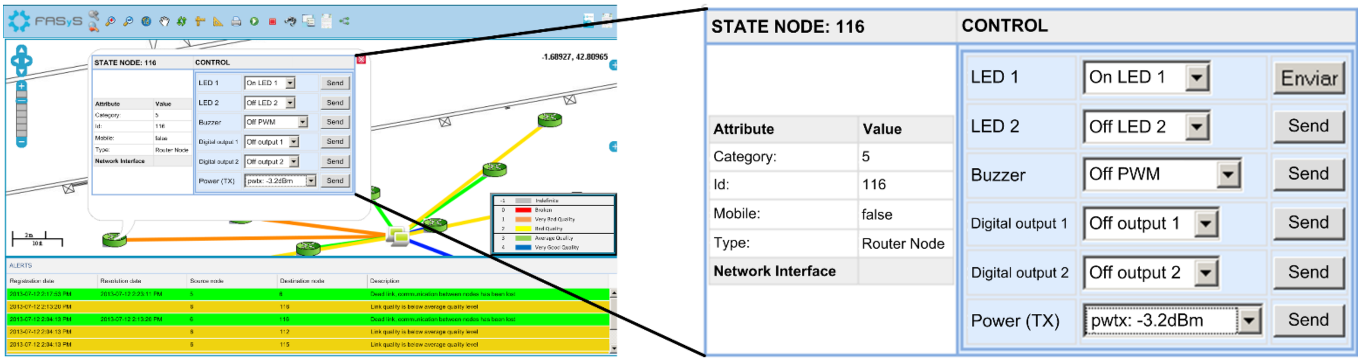
-1	⬜	Indefinite
0	🟥	Broken
1	🟧	Very Bad Quality
2	🟨	Bad Quality
3	🟩	Average Quality
4	🟦	Very Good Quality

ALERTS

Registration date	Resolution date	Source node	Destination node	Description
2013-07-12 2:17:53 PM		5	6	Dead link, communication between nodes has been lost
2013-07-12 2:13:20 PM		6	116	Link quality is below average quality level
2013-07-12 2:04:13 PM	2013-07-12 2:13:20 PM	6	116	Dead link, communication between nodes has been lost
2013-07-12 2:04:13 PM		6	112	Link quality is below average quality level
2013-07-12 2:04:13 PM		6	115	Link quality is below average quality level

b) Link broken.

Fig. 10. Link between coordinator and gateway nodes.



ALERTS

Registration date	Resolution date	Source node	Destination node	Description
2013-07-12 2:17:53 PM	2013-07-12 2:23:11 PM	5	6	Dead link, communication between nodes has been lost
2013-07-12 2:13:20 PM		6	116	Link quality is below average quality level
2013-07-12 2:04:13 PM	2013-07-12 2:13:20 PM	6	116	Dead link, communication between nodes has been lost
2013-07-12 2:04:13 PM		6	112	Link quality is below average quality level
2013-07-12 2:04:13 PM		6	115	Link quality is below average quality level

STATE NODE: 116

Attribute	Value
Category:	5
Id:	116
Mobile:	false
Type:	Router Node
Network Interface	

CONTROL

LED 1	On LED 1	Enviar
LED 2	Off LED 2	Send
Buzzer	Off PWM	Send
Digital output 1	Off output 1	Send
Digital output 2	Off output 2	Send
Power (TX)	pwtx: -3.2dBm	Send

Fig. 11. Control options implemented on the platform.

9. CONCLUSIONS AND FUTURE WORK

The Factory of the Future will require enhanced communication platforms and networked applications to improve performance and competitiveness, intensively centered not only on worker's skills, but also on their health and safety working conditions as the basis for proper productivity. To this purpose the FASyS system has been proposed, which tries to mitigate potential labor risks by early detection of those environmental factors that may lead to such risks or accidents. All these factors are monitored via WSNs that are deployed throughout the factory and can communicate with a remote Control Center, even in harsh conditions, thanks to the deployment of an heterogeneous wireless backhaul. The proposed architecture follows a centralized approach, where the Control Center is in charge of controlling and supervising the deployed WSNs, taking the necessary actions according to the sensed data and their related implications to human safety. The reliable provision of the demanded services in a distributed environment characterized by harsh propagation conditions requires a platform capable to continuously monitor and manage the communications QoS to ensure the robust reception of the sensed information and the capacity to ubiquitously connect to any distributed node. To this aim, a novel platform to monitor and manage the heterogeneous industrial wireless network has been developed in the FASyS project.

The heterogeneous communications network embraces different wireless technologies. In particular, IEEE 802.15.4 is used for short range and low power communications. For medium range communications, IEEE 802.11 is used to provide connectivity to WSN coordinators and high capacity sensors (e.g. video cameras). For long range communications with the Control Center, IEEE 802.16 or WiMAX has been used due to its available bandwidth. The communications infrastructure is not enough by itself and requires and integrated approach to correctly manage the complete FASyS system. The usage of semantics has proved to be really useful even for simple classification operations, so that sensors and sensed data can be semantically annotated with temporal, spatial and thematic metadata. Besides, other elements of the system can perform reasoning operations based on the included metadata.

This paper has presented the FASyS communications monitoring and management platform that is composed by three components. The SOS provides full integration into the system as it offers web access for inserting and retrieving sensed data. The Toolbox is the software platform that implements the control and management functions necessary to monitor in real-time FASyS heterogeneous communications. Finally, the HMI allows users to easily obtain through a web interface all information regarding workers, sensors and potential risks and actions, and present them visually to the administrator to monitor and take the necessary actions. The developed platform provides information about the connectivity and QoS levels of individual links and end-to-end communications, and provides the tools required to react under any QoS degradation that could entail the loss of critical information.

Future work related with this project is related with the introduction of new wireless technologies, open and also vendor specific, mainly the ones broadly used in the industrial environment. Additionally new sensor and sensor networks are planned to be included, special attention will be paid to the inclusion of indoor location techniques and the use of Body Area Networks for gathering information from the workers. These networks introduce extra problems to the management tool as connectivity due to mobility will not provide continuous connectivity, multihoming and DTN techniques will be analyzed for further use. Regarding the security new mechanism related with access control in organizations will be analyzed and tested. And finally regarding semantics, the extension of OGC SWE to be linked with the IoT and Future Internet is under study for future works and activities.

ACKNOWLEDGEMENTS

This work has been partly funded by the Spanish *Ministerio de Ciencia e Innovación* through the CENIT Project FASyS (CEN-20091034).

REFERENCES

[1] European Commission Ad-hoc Industrial Advisory Group, "Factories of the Future PPP Strategic Multi-anual Roadmap", *European Commission Directorate-General for Research Communication Unit*, B-1049 Brussels, EUR-24282-EN, 2010.

[2] FASyS official website: http://www.fasys.es/en/.

[3] B. Matthias, S. Kock, H. Jerregard, M. Kallman, I. Lundberg, and R. Mellander, "Safety of Collaborative Industrial Robots: Certification Possibilities for a Collaborative Assembly Robot Concept", *Proc. IEEE International Symposium on Assembly and Manufacturing (ISAM'11)*, pp. 1-6, July 2011.

[4] __, "International Standard ISO 10218-1:2006, Robots for industrial environments – Safety requirements – Part 1: Robot", ISO Copyright Office, Geneva,2006.

[5] __, "International Standard ISO 13849-1:2006, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design", ISO Copyright Office, Geneva, 2006.

[6] P. Gaj et al., "Computer Communication Within Industrial Distributed Environment - a Survey", *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 182-189, Feb. 2013.

[7] V. C. Gungor, and Gerhard P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches", *IEEE Transactions on Industrial Electronics*, vol. 56, no.10, Oct. 2009.

[8] J. Akerberg, M. Gidlund, M. Bjorkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation", *Proc. IEEE International Conference on Industrial Informatics (INDIN'11)*, pp. 410-415, 26-29 July 2011.

[9] A. Willig, "Recent and Emerging Topics in Wireless Industrial Communications: A Selection", *IEEE Transactions on Industrial Informatics*, vol. 4, no. 2, pp. 102-124, May 2008.

[10] B. Nickerson, "Issues in designing practical wireless sensors", *IEEE Instrumentation & Measurement Magazine*, vol. 15, no. 1, pp. 22-26, Feb. 2012.

[11] G. Fortino, A. Guerrieri, G.M.P. O'Hare and A. Ruzzelli, "A Flexible Building Management Framework Based on Wireless Sensor and

Actuator Networks", *Journal of Network and Computer Applications*, vol. 35, no.6, pp. 1934-1952, November 2012.

[12] R. Mueller, G. Alonso and D. Kossmann, "SwissQM: Next Generation Data Processing in Sensor Networks", *Proc. of the 3rd Biennial Conference on Innovative Data Systems Research (CIDR'07)*, pp.1-9, 7-10 January 2007.

[13] M. Jonsson, K. Kunert, "Towards Reliable Wireless Industrial Communication With Real-Time Guarantees", *IEEE Transactions on Industrial Informatics*, vol. 5, no. 4, pp. 429-442, Nov. 2009.

[14] J.F. Coll, J. Chilo, B. Slimane, "Radio-Frequency Electromagnetic Characterization in Factory Infrastructures", *IEEE Transactions on Electromagnetic Compatibility*, vol. 54, no. 3, pp. 708-711, June 2012.

[15] E. Tanghe, et. al, "The industrial indoor channel: large-scale and temporal fading at 900, 2400, and 5200 MHz", *IEEE Transactions on Wireless Communications*, vol.7, no.7, pp. 2740-2751, July 2008.

[16] T. Sauter, "The Three Generations of Field-Level Networks - Evolution and Compatibility Issues", *IEEE Transactions on Industrial Electronics*, vol. 57, no. 11, pp. 3585-3595, Nov. 2010.

[17] V.C. Gungor et al., "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid", *IEEE Transactions on Industrial Electronics*, vol. 57, no. 10, pp. 3557-3564, Oct. 2010.

[18] L. Tang et al., "Study of path loss and data transmission error of IEEE 802.15.4 compliant wireless sensors in small-scale manufacturing environments", *Springer International Journal of Advanced Manufacturing Technology*, vol. 63, no 5-8, pp. 659-669, November 2012.

[19] V. Cerf, "IAB Recommendations for the Development of Internet Network Management Standards – RFC 1052", IETF, April 1988.

[20] J.D. Case; J.R. Davin; M.S. Fedor; M.L. Schoffstall, "Internet Network Management Using the Simple Network Management Protocol", *Proc. IEEE Conference on Local Computer Networks (LCN)*, Mineapolis, MN, USA, pp.156-159, 10-12 Oct. 1989.

[21] T. Klie; F. Straub, "Integrating SNMP Agents with XML-based Management Systems", *IEEE Communications Magazine*, vol. 42, no. 7, pp. 76-83, July 2004.

[22] J. Schoenwaelder, "Overview of the 2002 IAB Network Management Workshop- RFC 3535", IETF, May 2003.

[23] __, "Web Services for Management (WS-Management) Specification", Distributed Management Task Force, Inc. (DMTF), DSP0226 , version 1.0.0, 12 Dec. 2008.

[24] __, "Web Services Distributed Management: Management using Web Services (MUWS 1.1) Part 1", Organization for the Advancement of Structured Information Standards (OASIS) Web Services Distributed Management TC, Document Identifier: wsdm-muws1-1.1-spec-os-01, 1 Aug. 2006.

[25] __, "Web Services Distributed Management: Management using Web Services (MUWS 1.1) Part 2", Organization for the Advancement of Structured Information Standards (OASIS) Web Services Distributed Management TC, Document Identifier: wsdm-muws2-1.1-spec-os-01, 1 Aug. 2006.

[26] __, "Web Services Distributed Management: Management of Web Services (WSDM-MoWS) 1.1", Organization for the Advancement of Structured Information Standards (OASIS) Web Services Distributed Management TC, Document Identifier: wsdm-mows-1.1-spec-os-01, 1 Aug. 2006.

[27] R. Enns, M. Bjorklund, J. Schoenwaelder, A. Bierman, "Network Configuration Protocol (NETCONF)- RFC 6241", IETF, June 2011.

[28] Ji Huang; Bin Zhang, Guohui Li; Xuesong Gao and Yan Li, "Challenges to the New Network Management Protocol: NETCONF", *Proc. International Workshop on Education Technology and Computer Science (ETCS)*, vol. 1, pp. 832-836, 7-8 March 2009.

[29] Mi-Jung Choi, Hyoun-Mi Choi, J.W. Hong and Hong-Taek Ju, "XML-based Configuration Management for IP Network Devices", *IEEE Communications Magazine*, vol. 42, no. 7, pp. 84-91, July 2004.

[30] A. Sehgal, V. Perelman, S. Kuryla and J. Schonwalder, "Management of Resource Constrained Devices in the Internet of Things", *IEEE Communications Magazine*, vol. 50, no. 12, pp. 144-149, Dec. 2012.

[31] Nagios official website, Accessed 1 July 2013, http://nagios.org.

[32] C. Issariyapat, P. Pongpaibool, S. Mongkolluksame and K. Meesublak, "Using Nagios as a Groundwork for Developing a Better Network Monitoring System", *Proc. Technology Management for Emerging Technologies (PICMET)*, Vancouver, Canada, July 29 2012-Aug. 2, 2012.

[33] ZeNoss official website, Accessed 1st July 2013, http://zenoss.com.

[34] Cacti official website, Accessed 1st July 2013, http://www.cacti.net/.

[35] J. Duarte, D. Passos, R. Valle, E. Oliveira, D. Muchaluat-Saade, and C. Albuquerque, "Management Issues on Wireless Mesh Networks", *Proc. Latin American Network Operations and Management Symposium (LANOMS)*, Petropolis, RJ, Brazil, 2007.

[36] S. Nanda and D. Kotz, "Mesh-Mon: A Multi-radio Mesh Monitoring and Management System," *Computer Communications*, vol. 31, no. 8, pp. 1588-1601, 2008.

[37] R. Valle, D. Passos, C. Albuquerque, and D. Muchaluat-Saade, "Mesh Topology Viewer (MTV): an SVG-based Interactive Mesh Network Topology Visualization Tool", Proc. *IEEE Symposium on Computers and Communications (ISCC)*, Marrakesh, Morocco, pp. 292-297, 2008.

[38] R. De Tommaso do Valle and D. Muchaluat-Saade, "MeshAdmin: an Integrated Platform for Wireless Mesh Network Management", *Proc. IEEE Network Operations and Management Symposium (NOMS)*, pp. 293-301, 20 April 2012.

[39] Aruba Networks official website, Accessed 1 July 2013, http://www.arubanetworks.com/products/management-security-software-2/airwave/

[40] M. Kostadinoviü, Z. Bundalo and D. Bundalo, "Planning and Management of WirelessHart Network", *Proc. International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, pp. 567-571, 24-28 May 2010.

[41] Nivis official website, Accessed 1st July 2013, http://www.nivis.com/.

[42] __, Open Geospatial Consortium Sensor Web Enablement Working Group, available at http://www.opengeospatial.org/projects/groups/sensorwebdwg (Accessed 1st July 2013).

[43] S.R. Madden, M.J. Franklin, J.M. Hellerstein and W. Hong "TinyDB: an Acquisitional Query Processing System for Sensor Networks", *ACM Transactions on Database Systems*, vol. 30, no 1, pp. 122-173, March 2005.

[44] F. Bellifemine, G. Fortino, R. Giannantonio, R. Gravina, A. Guerrieri, M. Sgroi, "SPINE: A Domain-Specific Framework For Rapid Prototyping of WBSN Applications", *Software Practice and Experience*, vol. 41, no. 3, pp. 237-265, March 2011.

[45] X. Song, C. Wang, M. Kagawa and V. Raghavan, "Real-time Monitoring Portal for Urban Environment Using Sensor Web Technology", *Proceedings of the 18th International Conference on Geo-informatics*, December 2010.

[46] Y. Jiang, J. Li, and Z. Guo, "Design and implementation of a Prototype System of Ocean Sensor Web", *Proceedings of the IET International Conference on Wireless Sensor Network (IET-WSN'10)*, pp. 21-26, 2010.

[47] D. Jeong, H. Jeong and Y.S. Jeong, “SS-RBAC: Secure Query Processing Model for Semantic Sensor Networks”, *Proceedings of the 2nd International Conference on Future Generation Communication and Networking (FGCN'08)*, pp. 352-355, 2008.

[48] K. Thirunarayan, C.A. Henson, and A.P. Sheth, “Situation Awareness Via Abductive Reasoning from Semantic Sensor Data: a Preliminary Report”, *Proceedings of the International Symposium on Collaborative Technologies and Systems (CTS '09)*, pp. 111-118, 2009.

[49] V. Huang, and M.K. Javed, “Semantic Sensor Information Description and Processing”, *Proceedings of the 2nd International Conference on Sensor Technologies and Applications (SENSORCOMM'08)*, pp. 456-461, 2008.

[50] G. Fortino, R. Giannantonio, R. Gravina, P. Kuryloski, R. Jafari, “Enabling Effective Programming and Flexible Management of Efficient Body Sensor Network Applications”, *IEEE Transactions on Human-Machine Systems*, vol. 43, no. 1, pp. 115-133, Jan. 2013.

[51] S.S. Durbha, R.L. King, and N.H. Younan, “Sensor Web for Interoperability in Power Systems”, *Proceedings of the North American Power Symposium (NAPS’09)*, 2009.

[52] Jeong-Hee Kim, Hoon Kwon, Do-Hyeun Kim, Ho-Young Kwak, Sang-Joon Lee, “Building a Service-Oriented Ontology for Wireless Sensor Networks”, *Proceedings of the Seventh IEEE/ACIS International Conference on Computer and Information Science* (ICIS '08), pp. 649-654, 14-16 May 2008.

[53] __, “METEOR-S: Semantic Web Services and Processes”, LSDIS Technical Report, 2005, available at http://lsdis.cs.uga.edu/projects/meteor-s/ (Accessed 1st July 2013).

[54] S. S. Durbha, R. L. King, S. K. Amanchi, S. Bheemireddy, and N. H. Younan, “Standards-Based Middleware and Tools for Coastal Sensor Web Applications”, IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 3 (4) 2010, pp. 451-466.

[55] C. A. Henson, J. K. Pschorr, A. P. Sheth, K. Thirunarayan, “SemSOS: Semantic sensor Observation Service”, *Proceedings of the 2009 International Symposium on Collaborative Technologies and Systems (CTS'09)*, 18-22 May 2009.

[56] __, “FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems”, NIST, February 2004.

[57] S. Convery and D. Miller, “IPv6 and IPv4 Threat Comparison and Best Practice Evaluation”, Cisco Whitepaper, March 2004, available online at http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf (Accessed 1st July 2013).

[58] D. Jonhston and J. Walker, “Overview of IEEE802.16 WiMAX Security”, *IEEE Security & Privacy*, Vol. 2, no. 3, pp. 40-48, June 2004

[59] H. D. Lane, “Security Vulnerabilities and Wireless LAN Technology”, SANS Whitepaper, February 2005, Available online at http://www.sans.org/reading_room/whitepapers/wireless/security-vulnerabilities-wireless-lan-technology_1629 (Accessed 1st July 2013].

[60] T. Zia, “Security Issues in wireless Sensor Networks”, *International Journal of Communications*. Volume 2, no 1, pp 104-121, Jan. 2008

[61] __, “Shibboleth Project”, available at http://www.shibboleth.net (Accessed 1st July 2013).

[62] R. Peeters, D. Singelee, and B. Preneel, “Toward More Secure and Reliable Access Control,” *IEEE Pervasive Computing*, vol. 11, no. 3, pp.76-83, March 2012.

[63] H. A. Weber, “Role-Based Access Control: The NIST Solution”, SANS Whitepaper ,October 2004, available online at http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf (Accessed 1st July 2013]

[64] W.H. Baker and L. Wallace, “Is Information Security Under Control?: Investigating Quality in Information Security Management,” *IEEE Security & Privacy*, vol.5, no.1, pp.36-44, Jan.-Feb. 2007

[65] __, “International Standard ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems – Requirements”, ISO Copyright Office, Geneva,, March 2005

[66] __, “Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements – NISTIR 7628”, *National Institute of Standards and Technology*, August 2010.

[67] M. Sepulcre, J. A. Palazón, J. Gozalvez and J. Orozco, "Wireless Connectivity for Mobile Sensing Applications in Industrial Environments", *Proceedings of the 6th IEEE International Symposium on Industrial Embedded Systems (SIES'11)*, Västeras (Sweden), 15-17 June 2011.

[68] J. A. Palazón, M. Sepulcre, J. Gozalvez, J. Orozco and O. López, "Heterogeneous Wireless Connectivity for Fixed and Mobile Sensing Applications in Industrial Environments", *Proceedings of the 16th IEEE International Conference on Emerging Technologies and Factory Automation* (ETFA'11), Toulouse (France), 5-9 September 2011.

[69] A Sheth, C Henson and S S Sahoo, “Semantic Sensor Web”, *IEEE Internet computing*, vol. 20, no. 4, pp. 78-83, 2008.

[70] S. F. Pileggi, C. E. Palau and M. Esteve, “Building Semantic Sensor Web: Knowledge and Interoperability”, *Proceeding of the First Semantic Sensor Web Workshop* (SSW 2010), Valencia (Spain), 15-16 October 2010,.

[71] D. Gregor, S.L. Toral, T. Ariza, F. Barrero, “An Ontology-based Semantic Service for Cooperative Urban Equipments”, *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 2037-2050 , November 2012.

[72] J.L. Martínez-Lastra and I. Delamer, “Semantic Web Services in Factory Automation: Fundamental Insights and Research Roadmap”, *IEEE Transactions on Industrial Informatics*, Vol. 2, No. 1, pp.1-11, February 2006.

[73] O. Diallo, J.P.C. Rodrigues and M. Sene, “Real-time Data Management on Wireless Sensor Networks: A Survey”, *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1013-1021, May 2012.

[74] L.M. Ni, et al., “Semantic Sensor Net: An Extensible Framework”, *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 4, No 3/4, pp. 157-167, April 2009.

[75] A. Kansal, S. Nath, J. Liu and F. Zhao, “SenseWeb: An Infrastructure for Shared Sensing”, *IEEE Multimedia*, Vol. 14, No. 4, pp. 8-13, July 2007.

[76] R. T. Fielding, Architectural styles and the design of network-based software architectures, PhD Dissertation, Dept. of Information and Computer Science, University of California, Irvine, 2000. Available online at: http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm (Accessed 1st July 2013).

[77] __, “OSGi Service Platform Core Specification Release 4, Version 4.2”, OSGi Alliance, 2009. Available online at: http://www.osgi.org (Accessed 1st July 2013)

[78] R. T. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, “Hypertext Transfer Protocol—HTTP/1.1. - RFC 2616”, IETF, March 1999.

[79] H. Butler, M. Daly, A. Doyle, S. Gillies, T. Schaub, Ch. Schmidt, “The GeoJSON Format Specification”, 2008. Available online at: http://www.geojson.org/geojson-spec.html (Accessed 1st July 2013).

[80] D. Crockford,“The Application/JSON Media Type for Javascript Object Notation (JSON) - RFC 4627”, IETF, July 2006.

[81] J. Park and S. Ram, “Information Systems Interoperability: What Lies Beneath?”, *ACM Transactions on Information Systems (TOIS)*, Vol. 22, no. 4, pp. 595-632, October 2004