



CISTER

Research Centre in
Real-Time & Embedded
Computing Systems

Journal Paper

The DEWI High-Level Architecture: Wireless Sensor Networks in Industrial Applications

Ramiro Robles*

Tomas Nordström

Kristina Kunert

Salvador Santonja

Mikko Himanka

Markus Liuska

Michael Karner

Eduardo Tovar*

*CISTER Research Centre

CISTER-TR-210904

2021

The DEWI High-Level Architecture: Wireless Sensor Networks in Industrial Applications

Ramiro Robles*, Tomas Nordström, Kristina Kunert, Salvador Santonja, Mikko Himanka, Markus Liuska, Michael Karner, Eduardo Tovar*

*CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: rsr@isep.ipp.pt, Tomas.Nordstrom@umu.se, kristina.kunert@umu.se, ssantonja@iti.es, mikko.himanka@centria.fi,
markus.liuska@centria.fi, michael.karner@v2c2.at, emt@isep.ipp.pt

<https://www.cister-labs.pt>

Abstract

This paper presents the High-Level Architecture (HLA) of the research project DEWI (Dependable Embedded Wireless Infrastructure). The objective of this HLA is to serve as a reference for the development of industrial Wireless Sensor and Actuator Networks (WSANs) based on the concept of the DEWI Bubble. The DEWI Bubble is a concept that can be used to integrate legacy industrial sensor networks with a modern, interoperable, and flexible IoT (Internet-of-Things) infrastructure. The DEWI Bubble is defined as a high-level abstraction of an industrial WSAN with enhanced interoperability (via standardized interfaces), dependability, technology reusability, and cross-domain development. The DEWI Bubble aims to resolve the issue of how to improve commercial WSAN technology to match the dependability, interoperability and high criticality needs of industrial domains. This paper details the criteria used to design the HLA and the organization of the infrastructure internal and external to the DEWI Bubble. The description includes the different perspectives, models or views of the architecture: the entity model, the layered model, and the functional model (including an overview of interfaces). The HLA constitutes an extension of the ISO/IEC 29182 SNRA (Sensor Network Reference Architecture) towards the support of wireless industrial applications in different domains: aeronautics, automotive, railway and building. To improve interoperability with existing approaches, the DEWI HLA also reuses some features from other standardized technologies and architectures. The DEWI HLA and the concept of Bubble allow networks with different industrial sensor technologies to exchange information between them or with external clients via standard interfaces, thus providing a consolidated access to sensor information of different industrial domains. This is an important aspect for smart city applications, Big Data, Industry 4.0, and the Internet-of-Things (IoT). The paper includes a non-exhaustive review of the state of the art of the different interfaces, protocols and standards of this architecture. The HLA has also been proposed as the basis of the European project SCOTT (Secure Connected Trustable Things) for security and privacy in the IoT.



Article

The DEWI High-Level Architecture: Wireless Sensor Networks in Industrial Applications

Ramiro Sámano-Robles ^{1,*}, Tomas Nordström ^{2,3}, Kristina Kunert ², Salvador Santonja-Climent ⁴, Mikko Himanka ⁵, Markus Liuska ⁵, Michael Karner ⁶ and Eduardo Tovar ¹

1 CISTER Research Centre, ISEP, Polytechnic Institute of Porto, 4249-015 Porto, Portugal; rasro@isep.ipp.pt (R.S.-R.); emt@isep.ipp.pt (E.T.)

2 Department of Applied Physics and Electronics, Umeå University, 901 87 Umeå, Sweden; Tomas.Nordstrom@umu.se (T.N.); kristina.kunert@umu.se (K.K.)

3 RISE, Research Institutes of Sweden, 90329 Umeå, Sweden

4 Instituto Tecnológico de Informática (ITI), 46022 Valencia, Spain; ssantonja@iti.es (S.S.-C.)

5 Centria Research and Development, Centria University of Applied Sciences, 67100 Ylivieska, Finland; mikko.himanka@centria.fi (M.H.); markus.liuska@centria.fi (M.L.)

6 VIRTUAL VEHICLE Research Centre, 8010, Graz, Austria; michael.karner@v2c2.at (M.K.)

* Correspondence: rasro@isep.ipp.pt(R.S.-R.)

Abstract: This paper presents the High-Level Architecture (HLA) of the European research project DEWI (Dependable Embedded Wireless Infrastructure). The objective of this HLA is to serve as a reference framework for the development of industrial Wireless Sensor and Actuator Networks (WSANs) based on the concept of the DEWI Bubble. The DEWI Bubble constitutes a set of architecture design rules and recommendations that can be used to integrate legacy industrial sensor networks with a modern, interoperable and flexible IoT (Internet-of-Things) infrastructure. The DEWI Bubble can be regarded as a high-level abstraction of an industrial WSAN with enhanced interoperability (via standardized interfaces), dependability, technology reusability and cross-domain development. The DEWI Bubble aims to resolve the issue on how to integrate commercial WSAN technology to match the dependability, interoperability and high criticality needs of industrial domains. This paper details the criteria used to design the HLA and the organization of the infrastructure internal and external to the DEWI Bubble. The description includes the different perspectives, models, or views of the architecture: the entity model, the layered perspective of the entity model and the functional model. This includes an overview of software and hardware interfaces. The DEWI HLA constitutes an extension of the ISO/IEC 29182 SNRA (Sensor Network Reference Architecture) towards the support of wireless industrial applications in different domains: aeronautics, automotive, railway and building. To improve interoperability with existing approaches, the DEWI HLA also reuses some features from other standardized technologies and architectures. The DEWI HLA and the concept of Bubble allow networks with different industrial sensor technologies to exchange information between them or with external clients via standard interfaces, thus providing consolidated access to sensor information of different industrial domains. This is an important aspect for smart city applications, Big Data, Industry 4.0 and the Internet-of-Things (IoT). The paper includes a non-exhaustive review of the state of the art of the different interfaces, protocols and standards of this architecture. The HLA has also been proposed as the basis of the European projects SCOTT (Secure Connected Trustable Things) for enhanced security and privacy in the IoT and InSecTT (Intelligent Secure Trustable Things) for the convergence of artificial intelligence (AI) and the IoT.

Keywords: industrial sensor networks, high level architecture, internet of things



Citation: xxx Title. *Technologies* 2021, 1, 0. <https://doi.org/>

Academic Editor:

Received:

Accepted:

Published:

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

1.1. Background and Motivation

The number of objects connected to the cloud has been rising dramatically in the last few years. The Internet-of-things (IoT) and Machine-to-Machine (M2M) communications will constitute a growing portion of traffic in next generation networks [1]. Wireless links used as the final hop between infrastructure and objects are key in achieving mobility, pervasiveness and flexible deployment. Wireless Sensor and Actuator Networks (WSANs) are thus considered as one of the main enablers of the concepts of IoT, Big Data, cloud computing and smart cities. Large numbers of sensor/tags will collect measurements from the physical world and relay them to the cloud or edge processors where added-value business, control, or management information can be exploited for different applications.

The use of wireless technologies in critical industrial applications has been usually linked to risks of reliability, security, safety and interference (see Table 1). This idea has been slowly changing over the past few years. Wireless technologies have been constantly improving, becoming now serious candidates to compete and in some cases replace their wireline counterparts [2]. However, there are still several issues to address in the integration of modern wireless technologies into highly critical industrial applications.

Modern radio technologies provide flexible deployment, over-the-air management, troubleshooting capabilities and improved data rates. However, they still suffer from interference, capture by eavesdroppers, wireless channel fading, shadowing and multi-path distortion. By contrast, wireline technology is in general more reliable. In some applications, wireline solutions are real-time and/or deterministic. The disadvantage of this type of solution is a complex infrastructure with critical cabling design, costly troubleshooting, maintenance & repair operations and in some cases (e.g., in transport systems) increased weight and fuel consumption. For example, modern aircraft are machines with complex wiring and cable design plans. It is estimated that the use of wireless instead of cable will bring a considerable increase in terms of fuel efficiency. Cabling planning tasks have an estimated cost of 2200 dollars per kg of aircraft [3]. Estimated savings can reach 14–60 million dollars per aircraft [4]. Electrical wiring problems cause fires, mission aborts and lost mission hours. Each year, companies and governments spend high numbers of man-hours finding and fixing wiring problems [5]. Damage on cables can affect not only the system related to the faulty wire, but also contiguous systems [2]. It is also estimated that 13% of an aircraft operation cost is related to maintenance, reparation and overhaul [4]. Therefore, wireless is expected to bring considerable gains in terms of reduction of wires, more flexible design, coverage of locations difficult to reach by wires and improved maintenance/troubleshooting. In aeronautics, the new paradigm has been called “fly-by-wireless” [6]. A summary of advantages vs. disadvantages of wireless links in industrial settings extending the analysis provided in [7] for aeronautics applications is shown in Table 1.

Despite all the advances in the last few years, there is still a gap in the state of the art on how to address the dependability issues of wireless technologies to be used in highly critical applications in different industrial domains.

1.2. Specific Project Motivation

DEWI (Dependable Embedded Wireless Infrastructure) was an ARTEMIS European project focused on the development of dependable WSANs in four industrial domains: aeronautics (SP2), automotive (SP3), rail (SP4), and building (SP5) [8].

The DEWI project addressed the need in industrial domains to integrate new and legacy wireless sensor networks with existing critical wireline technology and modern IoT solutions. This convergence has the challenge of increasing the dependability of wireless and IoT solutions to match the high criticality requirements in many industrial use cases. For example, in aerospace applications, wireless sensor hardware and protocols need to be improved to cope with the harsh temperature, wind and vibration conditions. This adaptation also involved protocol modifications to deal with errors or latency requirements.

Table 1: Advantages vs. disadvantages of wireless technologies in industrial applications [7].

ADVANTAGES	DISADVANTAGES
<p>Efficiency</p> <p><i>Weight reduction</i></p> <ul style="list-style-type: none"> -Decreased fuel consumption, -Increased payload capacity, Increased autonomy <p><i>New/increased capabilities (indirect)</i></p> <ul style="list-style-type: none"> -Dynamically reconfigurable <p>Safety</p> <p><i>Self-redundancy</i></p> <p><i>High survivability and resilience</i></p> <ul style="list-style-type: none"> -Single-point-of-failure avoidance -Self repairing capabilities <p><i>No wiring-ageing problems</i></p> <p>Cost</p> <p><i>Design and production</i></p> <ul style="list-style-type: none"> -No need of wire routing plans -Flexibility gains design changes -No wiring-related assembly tasks <p><i>Maintenance, reparation & overhaul</i></p> <ul style="list-style-type: none"> -Ease of system maintenance -Higher system integrity -Reduced out-of-operation lines Increased scalability <p><i>Withdrawal from service</i></p> <ul style="list-style-type: none"> -Simplified disassembly tasks -Reduction of mass to be recycled 	<p>Electromagnetic susceptibility</p> <p><i>Quality of service degradation</i></p> <ul style="list-style-type: none"> - Increase of bit error rate <p><i>Decreased transmission rate</i></p> <ul style="list-style-type: none"> -Violation of deadlines <p><i>Network collapse</i></p> <p>Security issues</p> <p><i>Confidentiality of data</i></p> <p><i>Rejection of intrusions</i></p> <p><i>Survivability jamming signals</i></p> <p>Power supply</p> <p><i>Increased power consumption</i></p> <p><i>Need for power supply</i></p> <ul style="list-style-type: none"> -Not always possible/desirable

Therefore, DEWI addresses the many different issues that need to be tackled to integrate commercial sensor and IoT technology to highly critical and dependable industrial use cases. The DEWI architecture provides the entities, functionalities and models needed from the industrial organization point of view to address the dependability improvement for different use cases.

1.3. Project Objectives

DEWI was a project based on a set of industrial use-cases that attempt to show the benefits of WSAWs by enforcing dependability, reusability, interoperability and cross-domain development. The core of the DEWI solution is the concept of the DEWI Bubble. A DEWI Bubble is a logical entity operating in a physical space delimited by the range of the wireless transmission technologies employed for intra-bubble communications. A DEWI Bubble is formed by a group of DEWI Bubble Nodes, DEWI Bubble Gateways and internal users. They are located in short range to each other to ensure a local confinement.

The Bubble may be organized in different topologies: distributed (ad-hoc), centralized (with an access point), or hybrid. The DEWI Bubble is therefore a high-level abstraction of an industrial WSAAN with enhanced interoperability, dependability, standardized access to sensor readings and cross-domain development. DEWI foresees a landscape of communicating bubbles implemented in different industrial use cases that can be called the "Internet-of-bubbles". Each Bubble can decide, if convenient, to allow transparent access to the nodes or "things" inside the bubble or provide only consolidated, aggregated, or processed information. This represents a hybrid approach between conventional WSAANs and modern IoT systems.

This paper provides the description of the DEWI High-Level Architecture (HLA). The objective of this HLA is to boost the use of industrial WSAANs. This HLA defines the hierarchical organization of the different devices/modules/entities that constitute the infrastructure internal and external to the DEWI Bubble. This also implies the description of functionalities, as well as the definition of DEWI Bubble Services, interfacing protocols and interoperability features. The term *high-level* is used here to denote a *system-level* overview of a sensor network. A high-level architecture is thus useful to provide a coherent structure to a network, improve resource organization and optimize infrastructure.

In modern network architectures, it is common to use what is called *views* or *perspectives* of the system. This approach allows designers to look at the system from different angles matching the multiple requirements of modern network design with multiple stakeholders and providing an enriched perspective of the system. This paper uses this multi-perspective approach to understand in a better way the different aspects and attributes of the DEWI Bubble and its services. The definition of the DEWI HLA is accompanied by the glossary available in [9]. This paper extends the preliminary definition of the DEWI HLA provided in the conference paper in [10].

This paper is organized as follows: Section 2 presents a summary of previous works on architectures for WSAANs (Wireless Sensor Networks). Section 3 provides an overview of the DEWI HLA and its main design elements. Section 4 presents the entity model. Section 5 presents the layers of the architecture that are useful for the organization of the Bubble infrastructure. Section 6 presents the functional model as an extension of the ISO/IEC SNRA (sensor network reference architecture) in [11]. A description of the interfaces is provided in Section 7. Finally, Section 12 presents the conclusions.

2. Related Works

The area of WSAANs has been intensively investigated over the last few decades. The number of architectures and solutions for WSAANs deserves a research area of its own. The concept of architecture is used in many different aspects and from many different perspectives of system design. Some architectures depend on particular protocol proposals in the network or lower layers. Other architectures are focused on specific physical (PHY) layer attributes such as energy saving. Others focus on high-level aspects such as semantics or security, cloud computation, etc. More recently, the concept of IoT has generated a large number of architecture and reference models that can also cover some parts of WSAAN technologies. A sensor network reference architecture (SNRA) is defined in [11] as: "Framework that provides common features collected from different types of sensor networks not only to provide developmental guidelines and reuse but also to describe the interrelations and interactions among the entities in a sensor network and possibly between sensor networks". The project IoT-A [12] provides the following definition of reference architecture: "Reference Architecture describes essential building blocks as well as design choices to deal with conflicting requirements regarding functionality, performance, deployment and security. Interfaces should be standardised, best practices in terms of functionality and information usage need to be provided". From the perspective of WSAANs, the following classification of architectures was proposed in [13]:

1. *Data centric.* Data-centric architectures are characterized by a vast number of randomly deployed sensors that only communicate node-to-node without any global network identification.
2. *Hierarchical.* Most hierarchical architectures consist of sensor nodes grouped into clusters. Cluster heads build intra-cluster communication with other nodes within the same cluster, but they also build inter-cluster communication with other cluster heads.
3. *Location-based.* Location-based architectures along with their underlining routing algorithms rely on knowledge of nodes' positions to route packets.
4. *Mobility-based.* Mobility-based architectures assume that a source, a sink, or intermediate nodes change their positions over time.
5. *QoS-based.* QoS architectures are characterized by stringent requirements such as packet end-to-end network delay and packet end-to-end energy cost.
6. Others: network-flow, multi-path and heterogeneity-based

The work in [14] characterizes different types of WSNs depending on application: terrestrial, underground, underwater, multimedia and Mobile WSNs. Regarding standardized architecture, the ISO/IEC Sensor Network Reference Architecture (SNRA) is the basis for the DEWI HLA functional layer model (described later in this paper). The architecture has also been mapped to current state-of-the-art IoT architectures such as:

1. Iot ARM (Architecture Reference Model) [12],
2. The IoT6 architecture [15],
3. The ISO/IEC reference model [11],
4. AIOTI (Alliance for the IoT Innovation) high level architecture [16],
5. ITU IoT reference architecture [17], and
6. IEEE P213 reference architecture [18].

Interoperability architectures are also relevant for WSN applications. The INTEROP project [19] proposed a framework based on model driven development concepts that uses a three-layer abstraction model with ontologies and semantic representation between the different layers. This allows designers to introduce non-functional aspects in architecture design such as trust, security and privacy. A large number of enterprise interoperability architecture proposals can also be used in the context of WSN applications.

An improved service-oriented architecture (SOA) for wireless sensor networks has been proposed in [20]. SOA is a paradigm that results in being attractive for WSNs due to its ability to separate functions into distinct units (services) which make system design flexible, modular, loose coupled and interoperable. The authors in [20] propose a SOA with auto-configuration capabilities for nodes of distinct capabilities: low-capacity, limited capacity and full capacity, implementing different web services for each type, as well as appropriate software stack to enable interoperability between the different protocols. Low capacity nodes implement a WSN-SOA protocol with reduced complexity running TinyOS.

SOA has become an important approach in middleware development for WSNs. A pioneering contribution recognising SOA potential for WSNs can be found in [21]. The work in [22] provided a solution to access ZigBee nodes via DPWS (Device profile Web Services) clients. SOA-based architecture standard has been defined in the Sensor Web Enablement (SWE) standard in [23], called Open Sensor Web Architecture (OSWA), achieved by the Open Geospatial Consortium (OGC). This standard also defined the SensorML language for data exchange between sensors using XML (Extensible Markup Language) grammar. Web service interfaces for IEEE 1451 were proposed in [24]. Integration of WSANs with IT infrastructure has been reported in [25] by enabling devices with direct interface using SOAP (Simple Object Access Protocol) rather than using gateways, thus simplifying the design.

Despite these advances in the literature, the integration of WSANs into critical industrial use cases using modern IoT protocols has not been addressed in a consolidated effort, but rather spread in many individual and inconsistent approaches. The objective of the DEWI HLA is to contribute to filling this gap in the literature of WSAN architectures.

3. Overview of the HLA and Design Elements

The design elements of the DEWI HLA are summarised in Figure 1. The HLA considers the high-level requirements (HLRQs) of a set of use-cases from different industrial domains. It also considers technology innovations, standardization, cross-domain development, technology reusability, and interoperability. The DEWI use cases are enlisted in Table 2.

The DEWI HLA is the basis for the cross-domain innovation encapsulated by the DEWI technology items (TIs) displayed in Table 3. These TIs are specific topics of technology innovation within each DEWI industrial domain. Innovations proposed in aeronautics domain can be potentially reused, adapted, improved, or cross-optimized in some automotive or railway applications. This cross-domain fertilization also concerns potential synergies, improvements, and eventually with the development of common middleware components that exploit, manage and transfer data and technological solutions across multiple domains. These ideas are aligned with the vision for future networks based on the concepts of the IoT, M2M communications and Big Data.

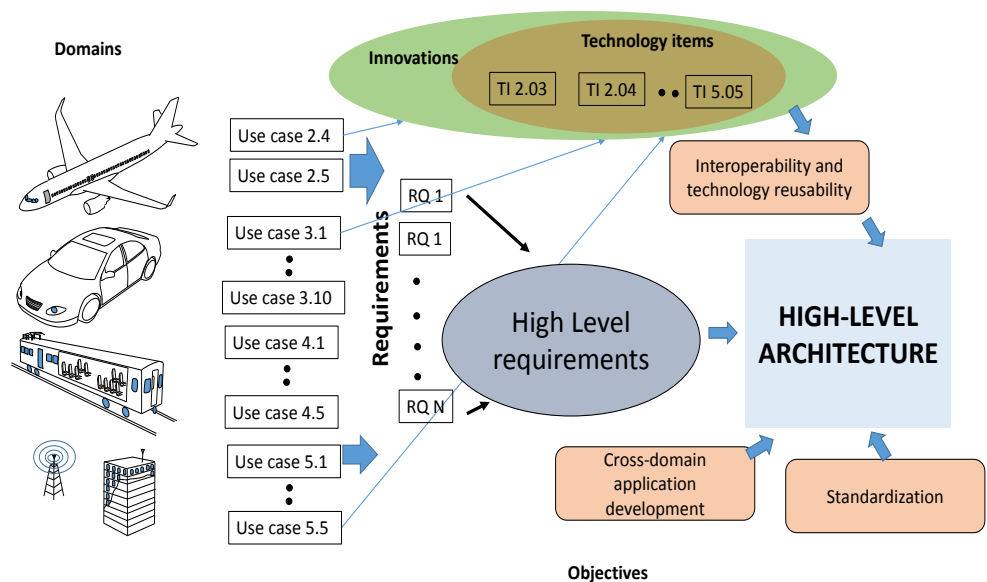


Figure 1. Design elements of the DEWI infrastructure and HLA.

The DEWI HLA provides flexible, federated and standardized access to sensor readings and TIs of different industrial domains with distinct underlying transmission technologies and data formats. This is one of the main issues in future systems of the IoT. The DEWI HLA also enables the use of actuators controlled by automated applications or by human clients using sensor and context information acquired by DEWI nodes. Therefore, our approach crossovers with the field of M2M communications. External developers will be able to create smart city and Big Data applications using the DEWI application program interfaces (APIs).

The DEWI HLA constitutes an extension of the ISO/IEC 29182 SNRA in [11] towards the support of dependable wireless industrial applications. It has also included domain specific architectures such as the automotive architecture in [26]. The HLA has been upgraded in the project SCOTT [27] to support security metrics, trust-based design, privacy labels and security-safety IoT design. More recently, the project InSecTT(Intelligent Secure Trustable Things) in [28] has adopted the enhanced DEWI HLA developed in SCOTT to investigate the convergence of Artificial Intelligence and the IoT. To formally introduce interoperability and technology re-usability, the DEWI HLA has adopted the model driven approach presented in the INTEROP project [19]. To achieve high-level interoperability and data exchange over Internet infrastructure, the HLA has considered previous works such as the IoT-A reference architecture [12], the IoT6 architecture [15] and the Arrowhead

Table 2: DEWI use cases.

UC No.	Description
2.4	Multi-Link Telemetry Logger for Rocket Launchers
2.5	Active Flow Control with Dense WSN
3.1	Identify, configure and join WSN in static network
3.2	Synchronized and robust real-time comm.
3.3	Automatic WSN conf. based on id. and localisation
3.4	WSNs for extreme environments
3.5	Secure tamper proof in-vehicle D2D comm.
3.6	Wireless update of ECU SW for vehicles
3.7	Wireless for energy efficiency and comfort
3.8	Integration platform for WSN
3.9	Instrumentation wired-wireless
3.10	Wireless vibration monitoring
4.1	WSN for train integrity
4.2	WSN for train composition
4.3	WSN smart integration
4.5	Freight advanced monitoring
4.5	Situational awareness
5.3	WSN for maintenance and cost reduction
5.4	WSN for facility operation and maintenance
5.5	WSN for access control management

framework [29]. Regarding the use of actuators and automated control of devices based on sensor readings, the architecture design has also considered the ETSI M2M [30] and one M2M [31] framework. DEWI also considered 5G architecture frameworks such as METIS in [32] for compatibility with future technologies.

4. Entity Model

The DEWI HLA hosts a set of entities with different roles and functionalities. The following entities constitute the *intra-* and *extra-Bubble* infrastructure in the HLA.

4.1. DEWI Bubble Node

Any tag, sensor and actuator (or combination of some of them as one single node entity) working under the DEWI Bubble framework. DEWI Bubble Nodes implement several of the functions described by the DEWI functional model (see Section 6). The nodes may have different radio technologies and may not necessarily lie within the wireless range of each other. A DEWI Bubble Node hosts central processing units (CPUs), storage units, one or more sensors, a communication module, potentially actuator(s) and power supplies (including batteries and/or energy harvesting modules).

4.2. DEWI Gateways (DEWI GWs)

In the DEWI HLA, there are three types of DEWI Gateways (DEWI GWs): the DEWI Bubble Gateway (DEWI BGW), the DEWI Relay Gateway (RGW) and the DEWI WSN Gateway (WGW). At any time, only one master logical DEWI GW must act as the interface between the DEWI Bubble and the external entities. However, redundant DEWI GWs are allowed to improve dependability in case of failure (e.g., by using Virtual Redundancy

Table 3: DEWI technology items.

No.	Description
01	Flexible data Acquisition, aggregation & fusion
3.07	WSN data representation and description
4.02	WSN data fusion framework
5.01	Smart WSN data fusion and mining
5.05	Wireless Data Aggregator (WDA)
5.07	Context Aware Reasoning
02	Smart architecture
3.02	Wireless communication for in-vehicle use
3.08	Dependability protocols, quality of safety critical systems
4.03	Communication Stack for Train WSNs
03	HW/SW Co-design
2.03	Tamper-proof and ruggedized hardware
4.01	Smart Integration Platform
5.02	Scalability of Wireless Building Networks
5.08	Over-The-Air programming, monitoring and control
04	Security, privacy, authorization
2.02	Highly Secure Wireless (Authorization, Intrusion safety, encryption)
3.01	Real-Time protocol
3.05	Security and Authentication
05	Re- / Auto- / Self-configuration
2.04	Multi-standard RF Wired Sensor Network Gateways and Protocols
2.05	Mechanism for prioritized wireless transmissions
3.10	Spectrum coordination for in-vehicle wireless communications
4.06	Plug& Play& Forget for WSN
06	Smart energy management and harvesting
3.09	Power and energy management; energy harvesting
5.03	Smart power supply
07	Dependability, robustness & safety
2.01	Highly Robust & Reliable Wireless
3.03	Synchronization of WSN
3.06	Functional Safety
08	Wireless standards
3.11	Knowledge-Oriented Sensor Networks (KOSN)
5.09	WS Communication homogenization with the IP
09	Wireless sensor / device detection & localization
3.04	Localisation of sensors and actuators
5.04	Indoor positioning platform for Building Automation

Router Protocol [33]). DEWI GWs host CPUs, a storage unit, multiple communication modules and power supply units.

4.2.1. DEWI Bubble Gateway (DEWI BGW)

The entity that acts as the main logical interface of a DEWI Bubble to communicate with other DEWI Bubbles, users (internal and/or external) and with other external (outer-Bubble) entities. It also provides protocol translation and management functionalities for all the DEWI Nodes and all the WSNs inside the DEWI Bubble. For redundancy purposes, alternative physical GWs can be deployed, but there must be always only one logical master GW acting as interface of the DEWI Bubble.

4.2.2. DEWI Relay Gateway (RGW)

This entity allows direct Bubble-to-Bubble communication without specific infrastructure. It can also relay specific functionalities of a DEWI BGW.

4.2.3. DEWI WSN Gateway (WGW)

The entity in charge of the management and protocol translation of an intra-Bubble WSN. The DEWI WGWs can be a legacy device (e.g., a ZigBee GW). The WGW communicates with the DEWI BGW, which manages all the WSNs inside the Bubble.

4.3. DEWI Users (Internal and External)

The entities that can access and use the set of DEWI Bubble services provided by the DEWI BGWs or RGWs. Internal users are meant to be inside the DEWI Bubble accessing the DEWI BGW via the intra-Bubble communication infrastructure. The external users access the DEWI Bubble services through the outer-Bubble communication framework. This access is mainly via Internet and over open standard middleware application program interfaces (APIs).

4.4. DEWI Service Providers

An entity or set of entities that provide services to third parties based on the aggregation of multiple DEWI Bubbles. DEWI Services can be provided at three levels:

4.4.1. Node Services

Provide sensor data and information services for that particular sensor node.

4.4.2. Bubble Services

Accessed through the DEWI BGW and provide data and information services related to all nodes in a DEWI Bubble.

4.4.3. Federated Bubble Services

Provide data and information services related to multiple DEWI Bubbles over potentially multiple DEWI industrial domains.

5. Layered Hierarchy Model

This section provides a layered view of entity model described in the previous section. The layered view has been especially created to fit the needs of industrial use-cases with internal critical infrastructure.

5.1. Overview

Two main features of the DEWI Bubble define the layered structure of the DEWI HLA as shown in Figure 2:

1. Only one DEWI BGW (master) acts as the main point of interface with the outside world (alternate GWs are allowed but only for redundancy purposes), and
2. A DEWI Bubble is able host one or more WSNs, where each WSN can operate with a different technology (including legacy standards).

The intra-WSN (intra-Bubble WSN) space is called *Level 0* or *L0*. Each WSN contains a set of devices (e.g., actuators or sensors) also known as DEWI Nodes. In case there is more

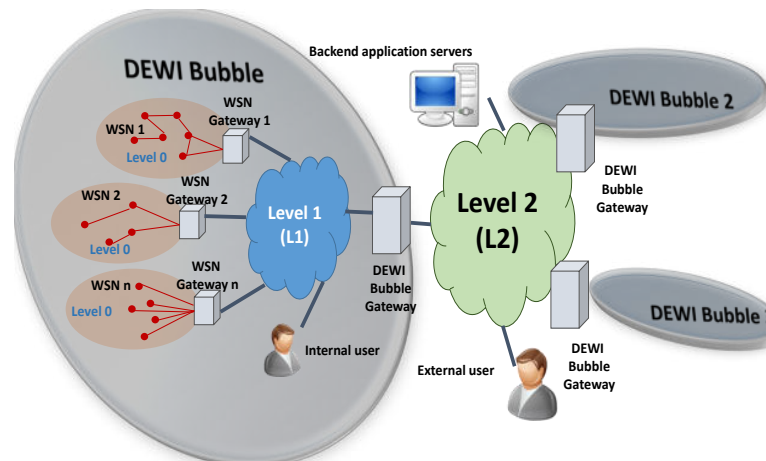


Figure 2. Layered entity model DEWI HLA.

than one WSN per DEWI Bubble, the DEWI Nodes are controlled by the corresponding WGW. Otherwise, they are controlled directly by the DEWI BGW. Each WGW establishes communication with the DEWI BGW, which acts as the coordinator of the different WSNs inside a Bubble. Therefore, the DEWI Bubble is effectively defined by the space where DEWI Bubble Services enabled by the master DEWI BGW are available to the following entities: WGWs (if there is any of them inside the Bubble), sensors/actuators (i.e., DEWI Nodes) and internal users. These features place the DEWI Bubble as a high-level abstraction of a WSN enabled with DEWI Bubble services.

The infrastructure between WGWs and the DEWI BGW is called *Level 1 (L1)* or intra-Bubble. DEWI Bubbles thus have the ability of encapsulating underlying heterogeneous technologies (including legacy standards). This layered model enables compatibility between manufacturers and technologies. Additionally, layered models have shown effectiveness in terms of scalability, interoperability and infrastructure design. Level 1 is used to interconnect several WSNs to their corresponding DEWI BGW. The DEWI BGW gets the data of each WSN and exposes this information to the outside world. Level 1 is optional, mainly because, in some applications, one DEWI Bubble may only contain one WSN. In such case, the DEWI BGW acts as the direct coordinator of the DEWI Nodes (using L0).

The DEWI Bubble always has one logical master DEWI BGW. However, the architecture allows for redundant network devices, thereby supporting safety critical scenarios of industrial applications. In those use cases where wired L2 infrastructure is not available, a DEWI Gateway acting in relay mode (RGW) can be used to provide direct Bubble-to-Bubble communication (ad-hoc infrastructure).

Level 2 or *L2* is the technology that allows external entities to have access to the information of a DEWI Bubble via the DEWI BGW. This access to the information generated by the DEWI Bubble is achieved through convenient APIs that describe the set of DEWI Bubble services. Level 2 technology provides connection through the Internet and its protocol stack. IoT-based web services have been used for L2 communication. The development of a standard technology for accessing Bubble information of different use-cases of different domains is one of the main contributions of DEWI to the state of the art. This management of sensor information and Bubble services is reflected in the DEWI high level language with the convenient semantics to match the requirements of modern interoperability challenges plus the technology re-usability features for cross-domain application development.

5.2. Level 0 (Intra-WSN)

Level 0 (L0) is the technology used inside each WSN of a DEWI Bubble. L0 technology can be used to interconnect the DEWI Nodes with two different entities:

1. the WGWs (in case the DEWI Bubble contains more than one WSN) or
2. the DEWI BGW (in case a DEWI Bubble only hosts one WSN, i.e., L1 does not exist).

Level 0 technology choice is independent in each use-case. Level 0 is the short-range wireless technology used to interconnect, manage and retrieve the information from/to sensors and actuators (DEWI Nodes). The challenge in the design of the DEWI HLA and its appropriate infrastructure is to host such a diverse and heterogeneous landscape of technologies communicating with each other over standardized, open interfaces and using common data formats. Figure 3 shows different wireless COTS (commercial off-the-shelf) L0 technologies in terms of data rate vs. range. For comparison purposes, the figure also includes long-range cellular standards. Figure 4 shows all the wireless L0 standards used in the DEWI project per industrial domain. In this figure, each line represents a use case using or considering a particular standard technology. The size of the elements corresponds to a relative number of lines that end in the element (logarithmic scale). Colours indicate whether the solution is an explicit use of the standard (blue), a modification (red) or just a simulation or study of the technology (yellow). The figure also includes some typical security features of the different wireless standards. Note the dominance of IEEE 802.15.4, IEEE 802.15.1 and WiFi technologies across different domains. Ultra-wideband flavours of the different standards have been used for high capacity or harsh propagation scenarios. In some cases, the standards have been modified to improve interoperability, dependability or reusability. Spread spectrum solutions are known to be resilient against interference and jamming. Low data rate standards such as IEEE 802.15.4 have some difficulties to achieve real time and high dependability, but using improvements such as the ISA solutions, wireless HART, or new flavours of the same standard, it is possible to achieve a good trade-off in some particular applications.

A summary of PHY-layer features of wireless technologies in the different domains of DEWI is displayed in Figure 5. Note that this figure makes an explicit difference between internal and external networks. Internal networks usually refer to networks operating inside an aircraft, vehicle, or building. For example, a wireless network operating inside the cabin of an airplane. Some features in this table assume a generic scenario, and therefore they can change when considering a particular application or use case. Multi-path, fast fading, path-loss exponent, interference and diversity in terms of MIMO (multiple-input multiple-output) feasibility are the most common PHY-layer features investigated in different scenarios. PHY-layer features of different COTS technologies are displayed in Figure 6. The table also includes some upper layer aspects such as transport capacity, and also some important metrics such as cost and commercial availability. Similarly, MAC layer features per domain and per COTS technology are summarized, respectively, in Figure 7 and Figure 8. Perhaps the main aspect to consider in different solutions is energy saving features, contention versus dedicated allocation, error recovery and frame design. Scalability can also be an important aspect to consider in dense network deployments. These features of available COTS technologies and the expected properties of the different domains have been considered by all use cases to achieve the best technology selection as reflected in Figure 4.

5.3. Level 1 (Inter-WSN, Intra-Bubble)

Level 1 (L1) is the technology used to interconnect all the intra-Bubble WSNs to their corresponding DEWI BGW (in case the DEWI Bubble hosts more than one WSN). L1 is an optional technology. There are two main reasons why L1 is an optional feature in the HLA:

- There are some use-cases in which the DEWI Bubble hosts only one intra-Bubble WSN. In these cases, the DEWI BGW and the WGWs converge in one single entity: L1 disappears and only L0 and L2 technologies are implemented; and
- Different use cases have different requirements to interconnect the intra-Bubble WSNs.

There are several advantages of using a different L1 technology for different use cases. Some of them are listed below:

- It allows network designers to meet domain-specific or use-case-specific design criteria,

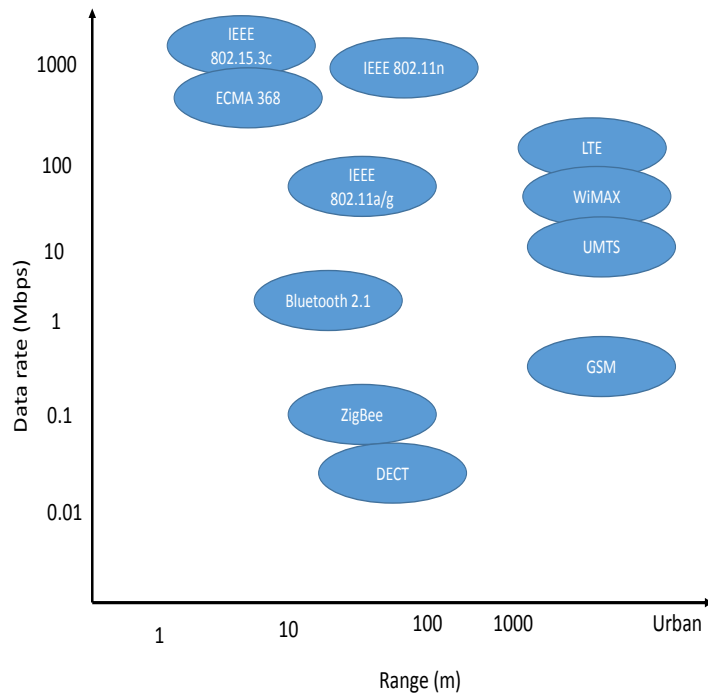


Figure 3. Data rate vs. range comparison for different wireless commercial standards L0 HLA.

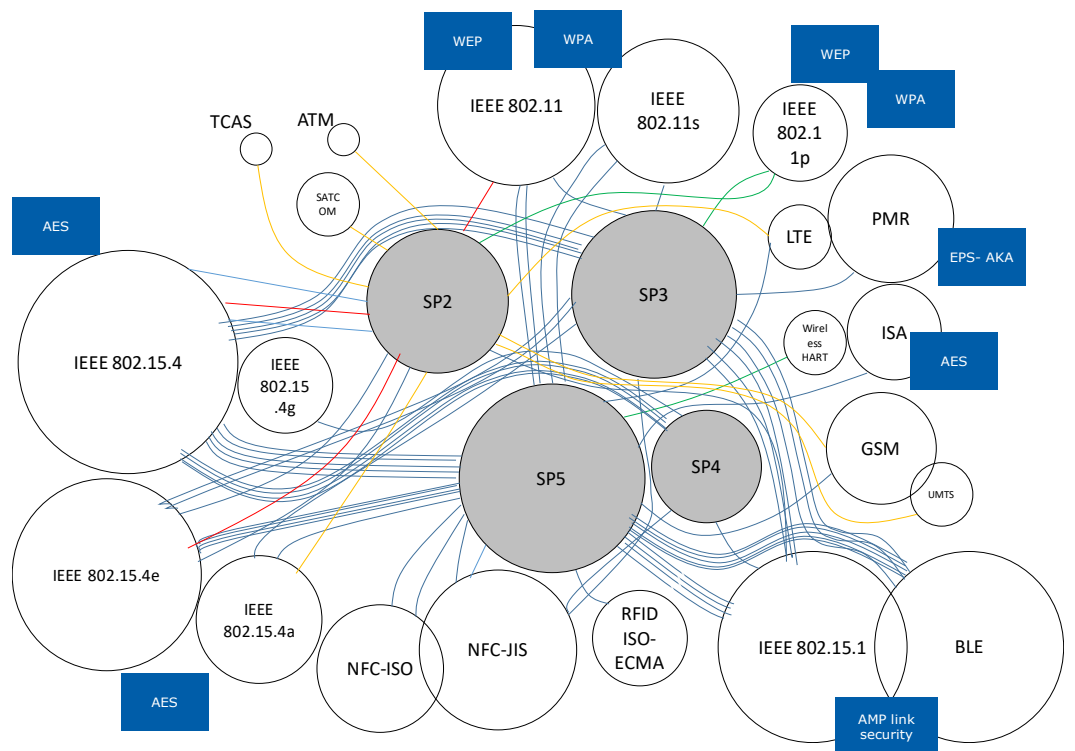


Figure 4. Wireless standards used in DEWI with some security features. SP2-Aeronautics, SP3 Automotive, SP4 Railway, SP5 Building.

Feature/domain	Aeronautical		Automotive		Rail		Building	
	Inside	Outside	Inside	Outside	Inside	Outside	Inside	Outside
Multipath (frequency selective)	Dense	Not dense	Dense	Dense/regular	Dense	Not dense	Dense	Dense/regular
Fast fading	No	Maybe	No	Maybe	No	Maybe	No	No
Path loss Exponent	Low	High	Low	High	Low	High	High	Low
Interference sensitivity	High	High	High	High	High	High	Medium	High
Interference to other systems	High	Low	High	Medium	High	Low	High	High
MIMO feasibility	Yes	Yes	Maybe	Yes	Yes	Maybe	Yes	Yes

Figure 5. PHY-layer features of DEWI industrial domains.

Feature/technology	802.15.4			802.11		ECMA standards		802.15.3	Bluetooth	
	ZigBee	ISA	15.4c	11.a,b,g	11n,	368	387	15.3	15.1	BLE
Multipath immunity	Regular	Regular	High	Regular	Regular	High	High	High	Regular	Regular
Fast fading immunity	Low	Regular	Very High	Low	Low	Very high	High	Very high		
Modulation /frequency(GHz)	DSCDMA (2.4)	DSCDMA (2.4)	UWB (3-6)	OFDM (2.4)	OFDM (5)	UWB	OFDM (60)	UWB (60)	FHSS (2.4)	FHSS (2.4)
Range	10-100m	10-100	10-100	10-100m	10-100m	10 m	5-10 m	1-10m	10-50m	10-20m
Jamming Interference sensitivity	Low	Low	Very low	High	High	Low	Low	Low	High	High
Interference to other systems	Low	Low	Very low	High	High	Low	Low	High	High	High
Availability	Very good	Good	Likely	Very good	Very good	Good	?	Likely	Very good	Very good
Other Signal characteristics	NLOS	NLOS	NLOS	NLOS	Indoor Low resources	Indoor high resource	LOS	LOS	NLOS	LOS
Cost	Medium	High	Very high	Low	High	High	High	High	Low	Low
Traffic density (Mbos/S/m2)	?	?	?	?	1.4	2.4	?	16	?	?

Figure 6. COTS PHY-Layer attributes.

Feature/domain	Aeronautical		Automotive		Rail		Building	
	Inside	Outside	Inside	Outside	Inside	Outside	Inside	Outside
Expected Data rate (depends on application) medium term	Expected medium-high	Expected Low-medium	Expected medium-high	Expected medium-high	Medium	Medium	High	Medium
Contention based/centralized	Both	Contention	Centralized	Contention	Centralized	Contention ad-hoc	Both	Both
Density of nodes	Medium to high	Low to medium (high for STM)	High	Medium	Medium	Medium	High	Medium
Resources needed	High	High	Medium	High	High	Medium	High	Low

Figure 7. MAC-Layer features of DEWI Industrial domains.

Feature/technology	802.15.4			802.11		ECMA standards		802.15.3	Bluetooth	
	ZigBee	ISA	15.4c	11.a,b,g	11n	368	387	15.3	15.1	BLE
Access	CSMA	CSMA	CSMA	CSMA	CSMA	FD/TDMA	FD/TDMA	CSMA	Master/slave	Master/slave
Discovery	Beacon	Beacon	Beacon	Beacon	Beacon	?	?	Beacon	On demand	On demand
Scalability	10-10000	10-10000	10-10000	10-100	10-100	?	?	?	10-10000	10-10000
Frame length	15ms	15ms	15ms	variable	10-100m	10 m	?	?	??	?
Multi-hop	Yes	Yes	Yes	Weak	Weak	?	?	Yes	No	No
Self configurability	Yes	Yes	No	Weak	Weak	?	?	?	Yes	Yes

Figure 8. COTS MAC-Layer attributes.

- It also improves scalability in the HLA, mainly because several WSNs can be hosted by one single DEWI BGW. Thus, the number of DEWI Nodes hosted per DEWI BGW increases according to the supported WSNs hosted by L1 technology.
- It provides a useful organization of resources in dense WSAN deployments.
- It allows for an efficient resource allocation by centralizing all the WSN management in one single location (logical): the DEWI BGW. This means, for example, that adjacent WSANs can be allocated in different channels by the DEWI BGW, thereby reducing interference inside the same DEWI Bubble (intra-Bubble interference).
- The existence of L1 technology facilitates the integration of wireless DEWI Bubble solutions with the existing wired technologies of each domain, which is a unique aspect of DEWI. This aspect also improves the technology re-usability features of the HLA, mainly because some wireline technologies share common aspects across different industrial domains,
- L1 can provide wired/wireless infrastructure for internal users to obtain access to DEWI Bubble services, and
- L1 allows network designers to create a private internal network where high security and quality of service requirements can be enforced.

The decision of using L1 also conveys some additional efforts summarized as follows:

- L1 needs an additional radio resource management layer to organize the different WSNs inside the Bubble.
- L1 needs to design gateways and scheduling policies that match the quality of service and dependability requirements between L0 and L1.
- The DEWI Bubble becomes a complex set of heterogeneous WSNs and wireline transmission protocols that need special cross-layer optimization algorithms.

Level 1 technology must also comply with several of the requirements and attributes of DEWI for intra-Bubble communications. Some of these requirements are the following:

- L1 must provide reliable and transparent access to the information of the DEWI Nodes inside each Bubble.
- L1 must preserve the dependable, self-configurable and secure data transfer of the DEWI Bubble.
- L1 must provide the DEWI Bubble with a framework for the management, resource allocation, configuration, troubleshooting and maintenance of the intra-Bubble WSNs.
- L1 must provide conflict resolution or deterministic allocation of the data streams and traffic of all WSNs.
- L1 provides an interface for internal users of the DEWI Bubble to access the DEWI Bubble Services.

Level 1 in DEWI HLA is closely related to the existing infrastructure (wired) of each industrial use-case. An overview of L1 wired technologies in different industrial domains is shown in Figure 9. Note the importance of IEEE 802.3 Ethernet (and its variations such as ARINC 664) and the CAN (Controller Area network) bus standards in different domains. The standards used in L1 are shown in Figure 10 and the comparison of L1 technologies is shown in Figure 11. Since L1 must preserve the dependability requirements inside the Bubble, middleware tools with message-oriented and application-oriented approaches are recommended. Service-oriented architecture for L1 provides the HLA with the flexibility to organize resources across different WSNs and model them as available services inside L1. Publish–subscribe middleware technologies fit perfectly the requirements of L1 high quality of service. A comparison of specific protocols for the realisation of L1 middleware is displayed in Table 4. A brief summary of these protocols follows.

Message Queuing Telemetry Transport (MQTT) [34] is an open M2M protocol for transporting telemetry style data over high latency networks. It is designed as very light publish/subscribe messaging protocol that runs over TCP/IP, or over other network protocols that provide ordered, lossless, bi-directional connections. The Advanced Message Queuing Protocol (AMQP) [35] is an open Internet protocol for business messaging. It

defines a binary wire-level protocol based on an OMG (Object Management Group) Standard. The OMG's Data Distribution Service for Real-Time Systems (DDS) [36] is an open middleware standard that enables scalable, real-time, dependable, high performance and interoperable data exchanges between publishers and subscribers. It supports different kinds of reliability, and scales better than the other protocols when the number of applications on the node producing and consuming the data increases.

The Hypertext Transfer Protocol (HTTP) [37] is an application-level protocol for distributed, collaborative, hypermedia information systems, based on request/response pattern. The Constrained Application Protocol (CoAP) [38] is a specialized web transfer protocol for use with constrained nodes and M2M networks. CoAP provides a request/response interaction pattern between application endpoints, supporting built-in discovery of services and resources. CoAP is designed to be compatible with HTTP.

From Table 4, we can observe that the selection of L1 technology closely follows the characteristics of L0 selection. This is reflected in the complexity of implementation and requested resources. A summary of different middleware paradigms for WSNs is presented in Table 4. For example, database paradigm approaches are not recommended for real-time applications, whereas application- and event-driven approaches represent a better fit to high dependability operation.

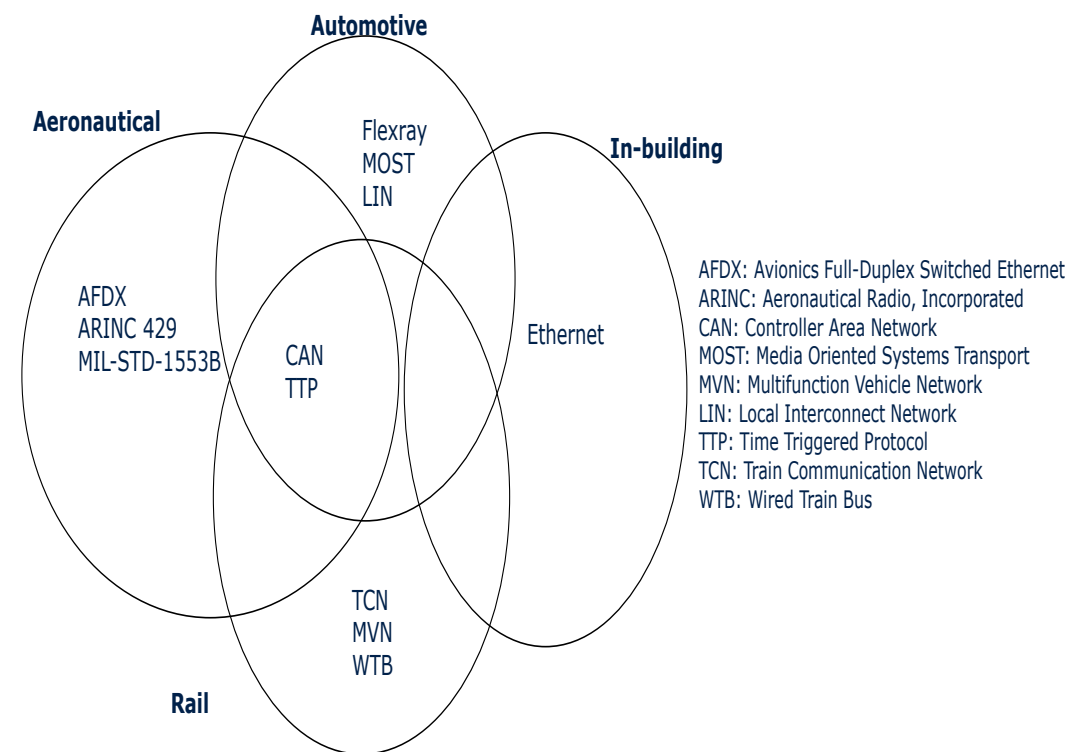


Figure 9. L1 industrial wireline technologies. SP2-Aeronautics, SP3 Automotive, SP4 Railway, SP5 Building.

5.4. Level 2 (Outer Bubble)

Level 2 (L2) is the layer of the HLA in charge of the communication between DEWI Bubbles or the communication between DEWI Bubbles and external user(s) or agent(s). L2 is thus responsible for the interoperability and cross-domain application development. Level 2 is the way a DEWI Bubble exposes its information to the outer world. There are several features unique of Level 2 in comparison with the other two Levels of the HLA:

- L2 uses Internet-based (IoT) protocols to enable external users with access to the set of DEWI Bubble services from anywhere in L2;
- L2 is also responsible to provide federated access to a set of different DEWI Bubbles;

Table 4: Comparison L1 middleware technologies.

	Pattern	Resources	Complexity	Security	Application	QoS
MQTT	Pub/sub	Med. (TCP)	Low	Auth (SSL)	Telemetry NRT	At most once
MQTT-SN	Pub/sub	Low (UDP)	Med.	Auth	Telemetry	
AMQP	Pub/sub	High (TCP)	Med.	TLS SASL	Mess. exchange	Not standard
CoAP	Req/Res	Low (UDP)	Low	DTLS	Telemetry Constrained devices	Best effort
HTTP	Req/Res	High (TCP)	Low	HTTPS	Constrained devices	Best effort
DDS	Pub/sub	High (TCP) Low (UDP)	High	Auth.	real time	20 QoS policies

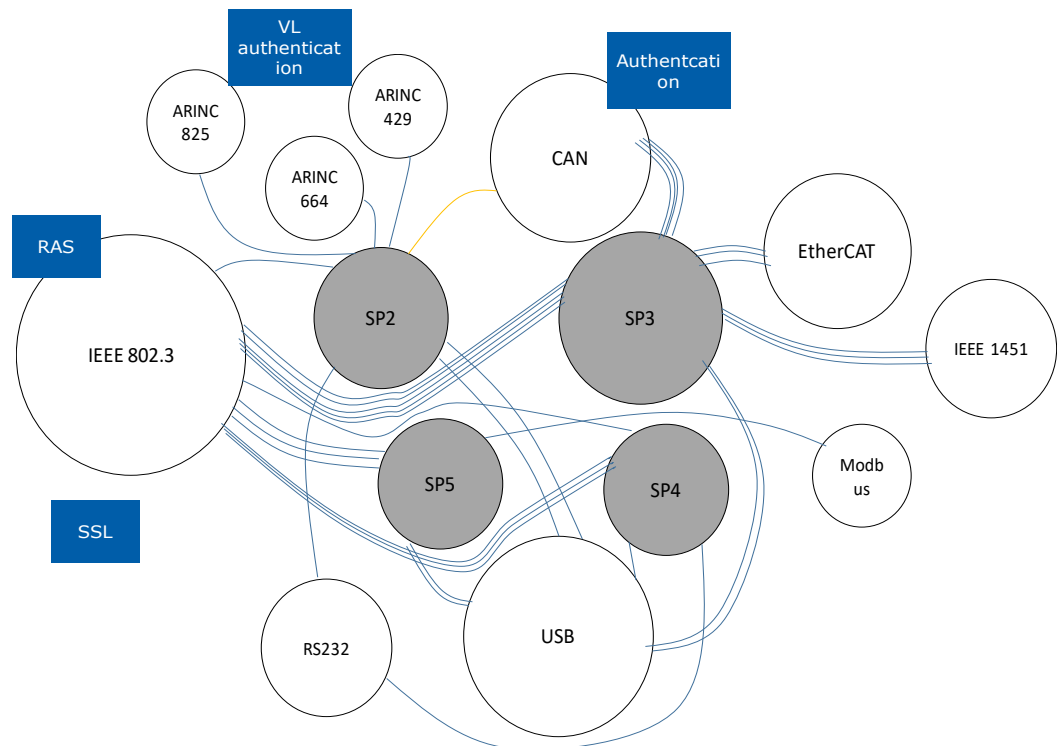


Figure 10. COTS standards L1 wireline technologies.

Approaches	Openness	Scalability	Heterogeneity	Mobility	Ease of use	Power awareness	Application type
Virtual Machine	Full	Full	Partial	Full	Little or none	Yes	Dynamic
Modular programming	Full	Full	Little or none	Full	Full	Yes	Dynamic
Database	Little or none	Little or none	Little or none	Little or none	Full	Partial	Event driven
Application Driven	Full	Full	Little or none	Little or none	Full	Yes	Real time
Message oriented	Full	Full	Partial	Partial	Full	Yes	Event driven

Figure 11. Middleware paradigms for L0/L1.

- L2 must support interoperability, cross-domain application development and technology re-usability;
- L2 must enforce security and protection to the data and operation of the DEWI Bubble against external malicious attacks;
- L2 must use international standards to enable interoperability with other external systems.

In order to achieve these goals, L2 has adopted a *service oriented architecture* (SOA) with a middleware paradigm based on *request–response*. This paradigm is inherently non-real time. Therefore, L2 is envisioned as a layer where external users request access to a summarized version or non-real time information generated by the DEWI Bubbles. The DEWI functional model includes specific L2 services.

The DEWI solution to realize the concept of technology re-usability and cross-domain application development is the use of a profile repository. This repository stores configuration details, TIs and other cross-domain parameters. DEWI Bubbles have access to this repository where they retrieve technology solutions developed across different use cases. These technology solutions are reused, optimized and modified across different DEWI Bubbles. The DEWI high level language reflects the interoperability and technology reuse attributes of the DEWI HLA. This language hosts the DEWI high level functionalities. This high level language also relies on an API that uses the middleware services of a SOA. This SOA reuses aspects of existing approaches such as the Arrowhead project [29].

The DEWI Bubble represents a hybrid solution by combining three main aspects: 1) it extends the ISO/IEC SNRA to be fit for industrial applications of WSNs via the two first levels of three-tier model, 2) it enables compatibility with existing and potentially real-time infrastructure via L1, and 3) it uses modern M2M and IoT tools for cross-domain interoperability and technology reusability via L2.

5.5. L2 Technology Evaluation

Different technologies have been investigated to realize the concept of L2 inter-bubble communication. A comparison of modern protocols for L2 communication is shown in Tables 5, 6, 7, and 8 (Messaging, resource discovery, data serialization and syntax/semantics, respectively). The upper layer protocol standards used by the project are displayed in Figure 12.

Table 5: Comparison of messaging/transport technologies.

No.	Resources	Complexity	Security	Application
SOAP	High (TCP)	High	HTTPS	Complex message exchange
CoAP	Low (UDP)	Low	DTLS	Telemetry resource constrained NRT
HTTP	High (TCP)	Low	HTTPS	Resource constrained NRT
Web services	High (TCP) Low (UDP)	High	HTTPS	

Table 6: Comparison of resource discovery and catalogue technologies.

	Resources	Application Dependency
WSDL	High	Describes SOAP
WADL	High	Describes SOAP and RESTful
WS-discovery	High	Based on TCP/IP, UDP or SOAP
SSDP	High	Relies on TCP/IP
DNS-SD	High	
LWM2M	Low	Resource constrained
HyperCAT	Low	IoT
SA-REST	Low	
Swagger	Low	JSON
UDDI	Medium	

Table 7: Comparison of data serialization and formatting technologies.

	Resources	Complexity
XML	High	High
YAML	High	Low
CBOR	High	Low
TLV	High	High
JSON	High	

5.5.1. Data Exchange Technologies

Data exchange amongst elements refers to the mechanisms provided by the gateway to bring the information generated by DEWI nodes to external applications. Web Services

Table 8: Comparison of syntax and semantics technologies.

	Type	Advantage/disadvantage
IPSO	Specific	Use with CoAP/RESTful Based on OMA LWM2M
OData	Specific	RESTful oriented
RDF	Ontology	Ontology vocabulary
OWL	Ontology	More concepts than RDF
SensorML	Ontology	XML for IoT
SSN	Ontology	
IoT-A	Ontology	Based on RDF and Web Ontology Language
X-GSN	Ontology	XML-based

or Message Queue protocols provide intercommunication between entities ensuring interoperability, asynchronous operation, platform independence and flexible applications. RESTful services [39] offer the best trade-off between performance and flexibility. Web Services are deployed over standard Internet technologies, like HTTP (Hyper Text Transfer Protocol)[37], where security (such as SSL or secure socket layer [40]) is already built-in.

SOAP (Simple Object Access Protocol) [41] is an XML-based (Extensible Markup Language [42]) message protocol that follows a request/response model schema and relies on document descriptions such as DTD (Document Type Definition) [43] or WSDL (Web Services Description Language) [44]. The use of large text-based XML files requires extra computation time to be processed.

CoAP [38] is another approach that is quite similar to RESTful services, but it is specially designed for constrained environments over UDP networks. Websockets [45] represents other solution that is based on maintaining a permanent connection between both sides. WebSocket is still a young technology and does not offer support for some architectures, servers and web browsers.

5.5.2. Resource Discovering, Profiles and Catalogues

Resource/service discovering refers to the ability of devices for discovering devices that are willing to offer interfaces or mechanisms for data exchange. One of the first technologies was the Universal Description, Discovery and Integration (UDDI) [46]. The interface follows the WSDL or WADL [47] description files.

Other solutions as Web Services Dynamic Discovery (WS-Discovery) [48] and Simple Service Discovery Protocol (SSDP) [49] use pre-defined IP multicast addresses. Both protocols reply with the list of their available services using a unicast message.

DNS-SD [50] based service discovery that relies on the existent DNS Internet protocol. The IPSO alliance [51] defines a set of resources under unique identification codes that can be accessed by URIs [52] in the same way that RESTful services are invoked. The IPSO architecture model is based on the OMNA Lightweight M2M (LWM2M) [53] Object & Resource Registry that provides naming for objects and resources.

Hyper/Cat [54] is an open, lightweight hypermedia catalogue based on JSON (Java Script Open Notation) [55] that provides mechanisms for exposing collections of URIs specially optimised for IoT. Semantic Annotation for REST (SA-REST) [56] defines a set of basic properties that can be used to non-intrusively annotate HTML/XHTML documents [57]. Another approach is Swagger [58], a specification for web services documentation. The documentation is provided by accessing a web service returning a JSON response.

5.5.3. Information Model: Data Serialization and Formatting

Serialization is defined as the process of translating data structures or objects into a format that can be stored in a repository or transmitted across a network and reconstructed in another computer environment.

XML provides tools and mechanisms for defining its own tags, providing a certain degree of syntax and semantic structure to the document in a human-readable form. YAML Ain't Markup Language (YAML) [59] is a human-readable data serialization format that reduces the excessive amount of tags employed by XML.

Solutions such as CBOR (Concise Binary Object Representation) [60] map data into reduced binary data obtaining an extremely small size packets. CBOR suits well for constrained environments, but it requires two steps; the process of serialization-marshalling and the encoding process.

TLV (Type-Length-Value) is a data format type that encodes data in a short form. It is extremely easy to parse and it is easy to transform to other readable formats. JavaScript Object Notation (JSON) is becoming the most used solution for data exchange. This data format maintains the human-readable style form, but it reduces the excessive meta-data and tag info.

5.5.4. Information Model: Data Content (Syntax and Semantics)

Two main approaches are adopted by the existent solutions: the definition of a common format and the use of ontology models. Solutions such as the OMA lightweight M2M protocol and model for device management are based on the Simple Object resource model stack. Identification numbers are registered and published by the OMA Naming Authority. The information is exchanged through CoAP/RESTful services.

In addition, IPSO is a simple data model for the semantic interoperability across IoT devices. It provides semantic-data interoperability amongst devices by using simple URI addressing and few data types. It is completely based on the OMA Lightweight M2M (LWM2M) Object & Resource Registry. The IPSO Application Framework defines a RESTful design for IP smart objects (especially in M2M applications).

Another approach is OneM2M which is a common software service layer based on RESTful resource oriented API. Open Data Protocol (OData) [61] is an open protocol that defines a complete architecture, from RESTful web services to a data model for information exchange (using XML or JSON formats).

Ontology-based approaches try to model the characteristics of the system. Ontologies are used to provide a formal naming for type and properties definition and entities interrelationship for a particular domain. The Resource Description Framework (RDF) [62] that is used to define and establish relations between documents. RDF can be extended with standard "ontology vocabulary" and providing metadata about resources that represent objects. In addition, Ontology Web Language (OWL) [63] provides more concepts to express meaning and semantics than the basic RDF.

A concrete and specially adapted solution for IoT is SensorML [64]. It provides a XML-based model for describing sensors and measurement processes. SensorML is one of the most commonly used ontology-based solutions in the IoT and Web of Things (WoT) [65].

Semantic Sensor Network Ontology (SSN) [66] offers an ontology that defines the capabilities of sensors and sensors networks. It is based on other standard ontologies as Sensor Model Language (SensorML) and Observations and Measurements (O&M). Another approach like the Internet of Things Architecture (IoT-A) uses Semantic Web techniques requiring that information meaning is formally defined. It is based on the use of representation languages as RDF schema and Web Ontology Language (OWL). It identifies entities, resources and services as key concepts within the IoT domain.

X-GSN [67] is an XML-based language that allows defining and describing sensors with semantics that can be interpreted and managed later. Finally, Machine-to-Machine

Measurement (M3) [68] is a framework to semantically annotate and easily interpret IoT data.

5.5.5. DEWI L2 Technology

DEWI has selected a RESTful solution as final L2 communication protocol based on HTTP/HTTPS for transport and JSON/UDDI as message format/resource discovery. A set of API functions have been released to the members of the project to achieve interoperability between DEWI Bubbles of different domains. The information model of the selected L2 technology is given in Figure 13. The guidelines for using L2 are broadly summarized in Figure 14. An example of the interactions between two DEWI L2 entities using L2 communication is given in Figure 15. L2 allows external clients to access the information of different DEWI Bubbles in different industrial domains. The solution also has security features for authentication and encryption based on key generation/distribution.

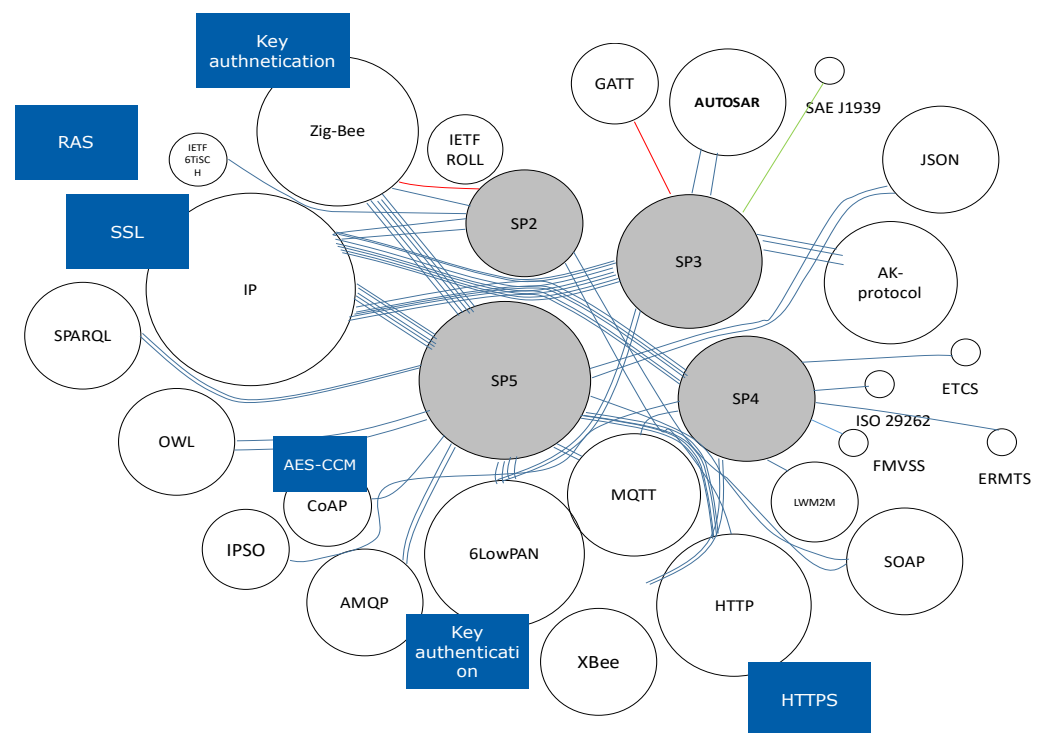


Figure 12. DEWI L2 upper layer technology standards. SP2-Aeronautics, SP3 Automotive, SP4 Railway, SP5 Building.

6. Functional Model

6.1. Overview

The DEWI HLA functional decomposition model is an extension of the functional model of the ISO/IEC SNRA in [11]. The benefit of this functional decomposition model is the simplification of system analysis by breaking global tasks into basic functionalities easier to manage and easier to insert into global system design. Following the ISO SNRA standard, the DEWI functional components are organized into four layers plus one cross-layer and cross-domain management. These layers are displayed in protocol stack view in Figure 16. The mapping of the the DEWI HLA to the ISO/IEC SNRA is shown in Table 9.

6.2. DEWI Node Hardware Layer (DNHL/SNHL)

The DEWI Node Hardware Layer (DNHL) or Sensor Node Hardware Layer (SNHL) encapsulates the low-level device functionalities that are common to all DEWI nodes. These functions are: *sensing, actuation and energy harvesting*. Therefore, the DEWI NHL is in charge

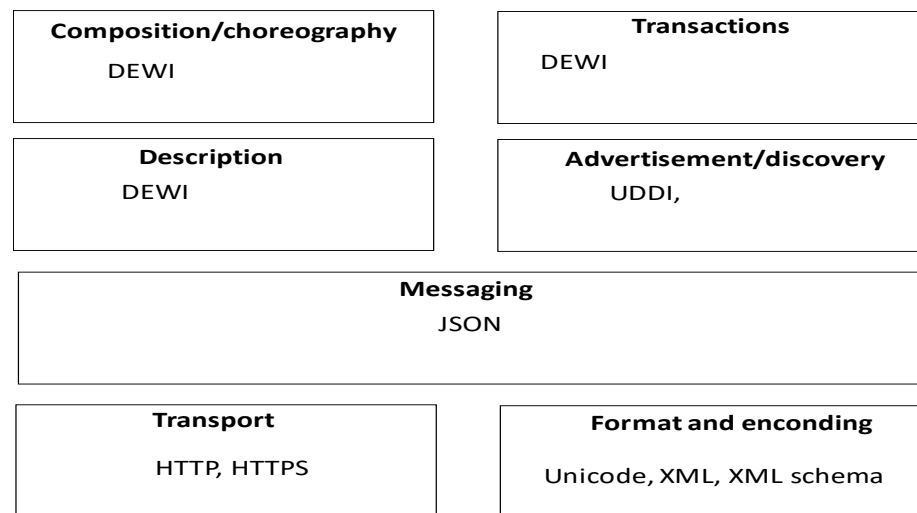


Figure 13. DEWI L2 information model.

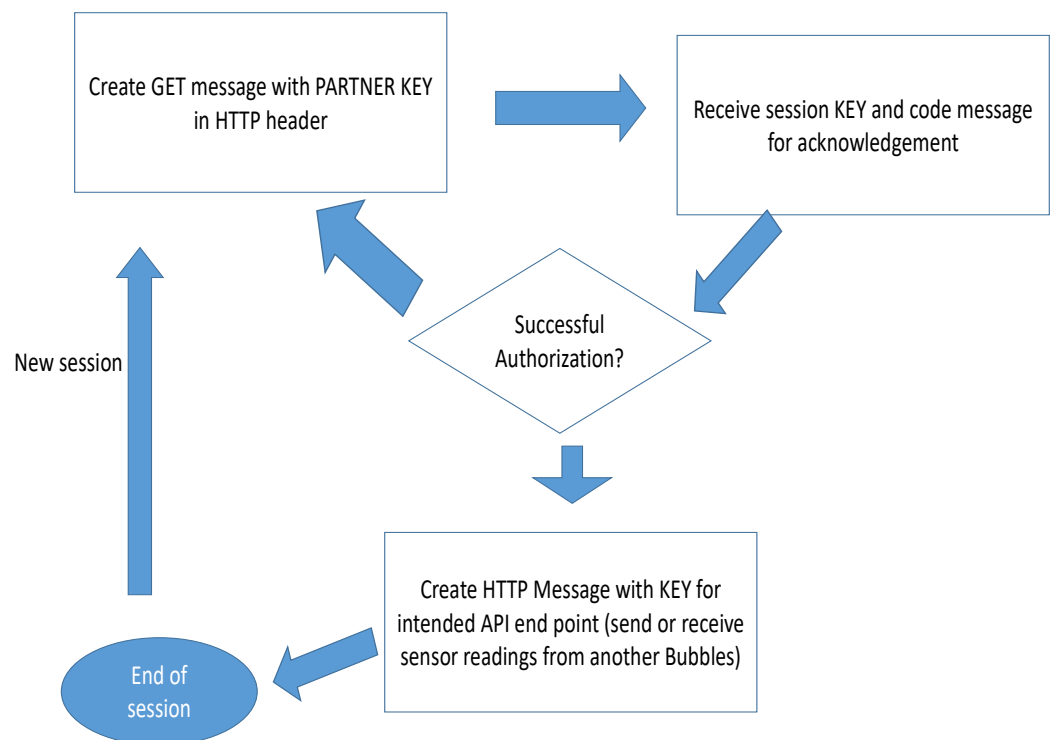


Figure 14. DEWI L2 technology user guidelines.

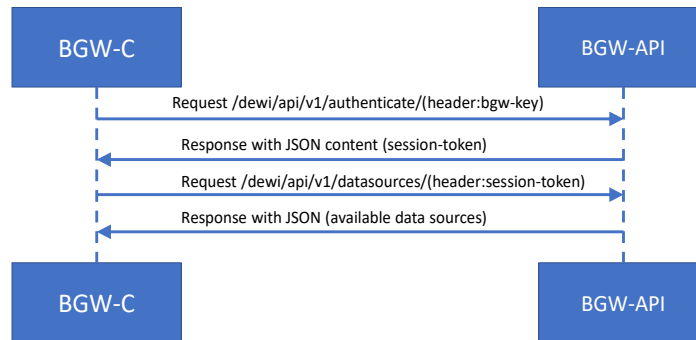


Figure 15. Example of the DEWI L2 technology call model.

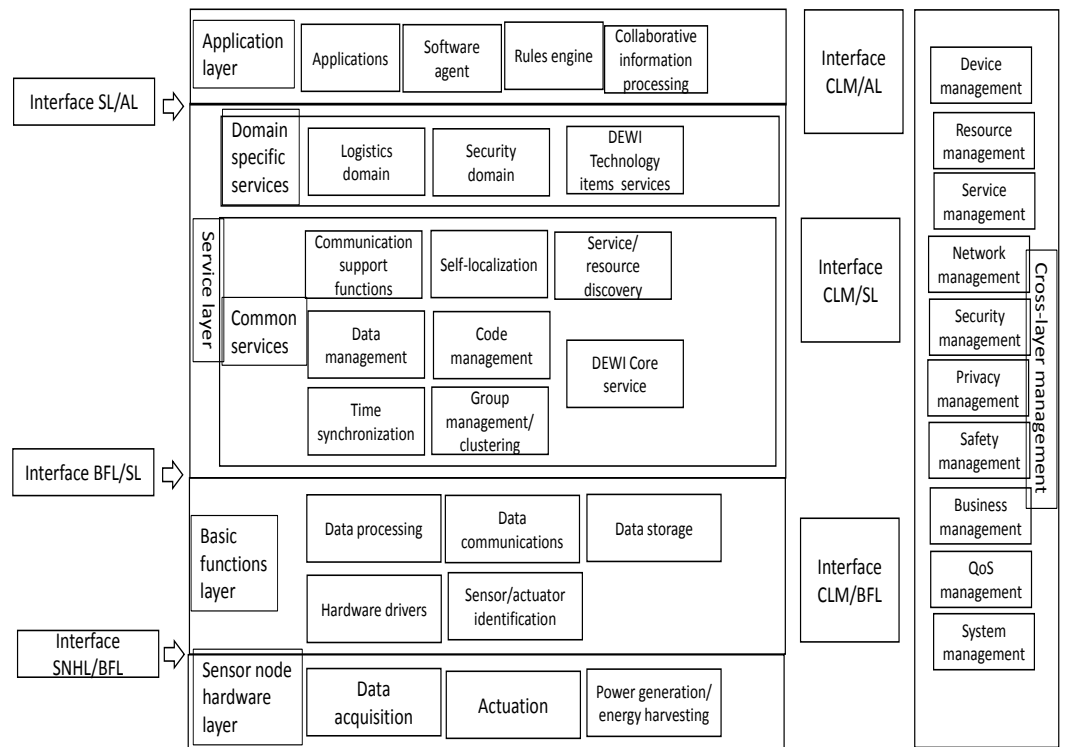


Figure 16. Protocol stack view of functional model of the DEWI/ISO HLA.

of the interface between the virtual world of computing and the physical world of objects, via measurements of physical phenomena. Sensors are used to measure physical quantities. Actuators are used to change a physical quantity in response to a signal or command. Energy harvesting is used to obtain energy from the surroundings of the DEWI Node and extend battery life. In DEWI, dependability can be improved using the technology item of ruggedized hardware.

6.3. Basic Function Layer (BFL)

The Basic Function Layer (BFL) contains the basic functionalities to transport, process and store the data generated by the SNHL. Physical entities may also make use of an operating system that is able to manage the computational resources and provide a simple language for applications to have access to such resources. BFL functionalities include: *Operating system (OS), data communication, data storage, data processing, sensor/actuator/device identification and device drivers management.*

6.4. Service Layer (SL)

The Service layer (SL) is in charge of providing upper layers with the application programme interfaces (APIs) that encapsulate all the lower functionalities of a sensor network. The SL acts as an interface between the application and the basic functions, and it helps to speed up the development and deployment of applications. The DEWI SL includes services specific of each domain, particularly services related to the TIs.

DEWI Core and Technology Item Services The DEWI Bubble L2 uses a service oriented architecture with particular services that are called here core services. These services depend on the architecture and middleware approach to be used. The DEWI TI services aim to enable the update, retrieving and uploading of technology innovations developed in each use case. The profile repository stores details of the TIs communicate with different DEWI Bubbles to proceed with TI operations.

6.5. Application Layer (AL)

The AL uses the services provided by the lower layers, but it is completely insulated from the details of the network hardware. It describes how applications interact with the network operating system. This interface is commonly known as an API. Common application components are the *software agent, the rules engine and collaborative information processing*. An agent is a piece of code that runs continuously. It can run tasks by itself, react to events on the Bubble and communicate with other agents. A rules engine is a software system whose behaviour is determined by a set of high-level business rules. Business rules can be inference rules, very much like an if-then statement that is called manually, or reaction rules that executes a program when an event is detected.

6.6. Cross-Layer and Cross-Domain Management (CLM/CDM)

Layered design has been the staple in the evolution of modern telecommunication networks. However, the layered model started to show some shortcomings, particularly in wireless networks where layers are tightly connected to each other. A wireless network should be designed by using cross-layer concepts, where parameters and issues across different layers must be addressed or optimized simultaneously. In the DEWI HLA, the layers of the functional model are able to exchange information and allow cross-layer design and optimization. A key concept in the DEWI HLA is cross-domain application development. Thus, in addition to the cross-layer management, cross-domain allocation is also incorporated. Typical cross-domain use cases include supply chain applications where goods are transported by trucks, planes and trains, while stored in warehouses and offices. This covers different industrial domains. CLM/CDM functionalities include *device, resource, QoS, dependability and security management.*

7. Interfaces

This section defines the interfaces between the modules and components of a DEWI HLA. An interface is the boundary shared by two modules that allows the communication between them. When the modules are physical entities, then the interface is a hardware (HW) interface. When the modules are Functions/Services, then the interface is a software (SW) interface.

7.1. HW Interfaces (between Entities)

HW Interfaces establish how to exchange messages between physical entities. The interface should define the physical support for the exchange, the structure of messages that can be received or transmitted and the logic that controls the exchange of the messages.

7.1.1. Interface DEWI Node-WSN GW

The DEWI Node-DEWI WGWs interface is used to transmit messages containing data from the nodes and sensor network management messages to/from the DEWI WGW. The protocols defined in this interface depend on the application requirements and on the WSN architecture chosen to build up the network. The data information transmission from the nodes to the DEWI WGW might be scheduled periodically, triggered by events, or on request by the DEWI WGW. The following layer protocols are required in this interface: AL, SL and BFL protocols.

7.1.2. Interface DEWI WSN GW-DEWI BGW

This interface is used to relay the data gathered by the sensor nodes to a higher-level entity. The granularity of the data and control information depends on the needs of each application service provided by the DEWI Bubble and the level of control over individual DEWI Nodes and the DEWI Bubble required by users from outside of the WSN. Some applications may need information from individual nodes, e.g., to know the temperature of a particular sensor located in a certain place in the vehicle, while it would be enough for other applications with the average temperature measured by all the nodes in the Bubble. If the DEWI WGW and the DEWI Gateway are not the same physical entity, the interface should be implemented through a Level 1 network. The following layer protocols are required in this interface: AL, SL and BFL protocols (this last one is needed only if the DEWI WGW and the DEWI Gateway are separate physical entities).

7.1.3. Interface DEWI BGW-External Users/Services

The interface DEWI BGW-External Users/Services is used to expose the data collected in the DEWI Bubble as services to multiple users (other DEWI Gateways or final users). This interface also allows the management and configuration of the DEWI Bubbles. The communication takes place in a Level 2 network that connects the DEWI BGWs to the Internet or to other DEWI BGWs directly. This interface should at least comply with the defined DEWI Core Services to establish a common mechanism to access the services provided by different DEWI Bubbles. The following layer protocols are required in this interface: AL and SL protocols.

7.2. SW Interfaces (between Functions)

SW Interfaces define how to communicate with adjacent layers. Usually, upper layers access resources provided by the lower layers and exchange control commands with layers in the same level through a Service Access Point (SAP). Each interface can be divided into two SAPs: the data SAP and the management SAP.

7.2.1. Interface SNHL-BFL

The SNHL-BFL interface connects the BFL with the node hardware and enables it to use the infrastructure provided by the SNHL, i.e., processor, memory, communication devices, power supply, sensors, and actuators. This interface defines:

Table 9: DEWI HLA mapping to the ISO 29182 SNRA interface model.

Entities		Sensors	Actuators	Comms. mod.	Processor	Memory	Power sup.	GW L0,L1,L2	Acc. networks	Backbone net.	Serv. providers	Users	
Basic functions service layer	Node HW Layer	Data acquisition	x	-	-	-	-	-	-	-	-	-	
		Actuation	-	x	-	-	-	-	-	-	-	-	
		Power generation/ E. harvesting	-	-	-	-	x	-	-	-	-	-	
		Data Processing	x	-	x	x	-	-	-	-	-	-	
		Data communications	-	-	x	-	-	-	x	x	x	x	
		Data acquisition	-	-	-	-	-	-	-	-	-	-	
		Data storage	-	-	-	-	x	-	-	-	-	x	x
		HW drivers	x	x	-	x	-	-	-	-	-	-	-
		Sensor/actuator identification	x	x	-	x	-	-	-	-	-	-	-
		Comms. support functions	-	-	x	x	x	-	x	x	x	x	
		Self-localization	x	-	x	x	-	-	-	-	-	-	-
		Service/resource discovery	-	-	x	-	-	-	-	-	-	x	x
		Data management	-	-	-	x	x	-	-	-	-	x	x
		Code management	-	-	-	x	x	x	-	-	-	x	x
		Time synch.	-	-	x	x	-	-	-	-	-	x	x
		Group management/clustering	-	-	-	x	-	-	-	-	-	x	-
		Domain specific services	-	-	x	x	x	-	-	-	-	x	-
		Application layer											
			Applications	-	-	x	-	-	-	-	-	x	-
			Software agent	-	-	-	x	-	-	x	-	x	x
			Rules engine	-	-	-	x	-	-	-	-	x	x
			Collaborative info. proc.	x	x	-	x	x	-	-	-	x	x
			Device manan.	x	x	x	-	-	-	x	-	-	-
			Resource manan.	x	x	x	x	x	-	-	-	x	x
			Service manan.	-	-	-	-	-	-	-	-	x	x
			Network manan.	-	-	x	x	x	-	-	-	x	x
			Security manan.	-	-	x	x	-	x	-	-	x	x
			Privacy manan.	-	-	-	-	-	-	-	-	-	-
			Safety manan.	-	-	-	-	-	-	-	-	-	-
			Business manan.	-	-	-	x	x	-	-	-	x	x
			QoS manan.	x	x	x	x	x	-	x	-	x	x
			System monit.	x	x	x	x	x	-	-	-	-	-

- Mechanical, electrical, logical and management signals that allows for accessing and managing the node hardware.
- The method to access hardware metadata.

- Interface standards based on sensor types or connection types.

7.2.2. Interface BFL–SL

The BFL–SL interface is a logical interface that enables the SL to access the functionality of the BFL. This interface defines:

- The data type and format of operations in the BFL, i.e., description of the functions performed, information generated and structure of the transmitted data.
- Message format and exchange mechanism between the BFL and SL according to the requirements of the SL.

7.2.3. Interface SL–AL

The SL–AL interface is a logical interface that enables the target application to access the functionality provided by the SL. This interface defines:

- The data type and format of services in the SL, i.e., service type, service state information and service management information.
- Message format and message exchange mechanism between the SL and AL according to the requirements of the AL.
- A service API to use as construction blocks for the target application.

7.2.4. Interfaces with CLM/CDM

The BFL, SL and AL provide management functionality to the CLM/CDM module. There are different logical interfaces with the CLM/CDM, one for each layer. These interfaces define: message format and exchange mechanism between each layer and the CLM/CDM,

8. Technology Items

Technology items (TIs) are an important part of the design of the DEWI HLA. Each TI is mapped to the proposed architecture to provide alignment of specifications. This means that we verify that the TIs are supported by the DEWI HLA design. Several TIs can be supported at different levels of the architecture. Their impact on interoperability depends on the technological choices of each use case. Table 10 enlists the different TIs and their mapping to the different levels of the DEWI HLA. This mapping indicates at which levels of the architecture such TIs are addressed. TIs of different domains can be found in [69], [70], [71],[72].

8.1. Flexible Data Acquisition, Aggregation and Fusion

8.1.1. WSN Data Representation and Description

This TI can be mapped to all levels of the architecture. This is because representation and description of WSN data are crucial for interoperability both within and between DEWI Bubbles. Each level of the HLA uses a potentially different middleware technology with predefined semantics that allow all the sensor and actuator data to be correctly transmitted and interpreted by the convenient entities. This TI is also closely related to the DEWI high level language that is designed to represent the interoperability and technology reusability features of DEWI for the intra- and extra- DEWI Bubble infrastructure. Each use case has provided WSN data representation for L0 and L1. DEWI L2 has used data representation based on JSON data formatting with UDDI resource discovery. The DEWI L2 language uses basic semantics to identify the domain, technology item and extra bubble parameters (security, authentication, QoS, etc). This TI was implemented in all domains.

8.1.2. WSN Data Fusion Framework

Data fusion is mainly supported in the two lower levels of the DEWI HLA: Level 0 and Level 1. Data fusion is an attractive solution for highly dense WSANs, such as use case 2.5 (active flow control) and 5.4 (WSN for facility operation and maintenance). Since Level

Table 10: Mapping technology items to the DEWI HLA.

No.	Description	L0	L1	L2
2.01	Highly robust & reliable wireless	x	x	
2.02	Highly secure wireless	x	x	x
2.03	Ruggedized HW	x	x	
2.04	Multi Standard RF WSN GWs	x	x	
2.05	Mechanisms for prioritized wireless Tx.	x	x	
3.01	RT protocol	x	x	
3.02	Wireless for in-vehicle use	x		
3.03	Synchronization WSN	x		
3.04	Localization sensors and actuators	x		x
3.05	Security and authentication	x	x	x
3.06	Functional safety	x	x	
3.07	WSN data representation and description	x	x	x
3.08	Dependability protocols, safety critical	x	x	
3.09	Power&energy Management, Harvesting	x	x	
3.10	Spectrum for in-vehicle Wireless	x	x	
3.11	Knowledge oriented WSNs	x	x	x
4.01	Smart integration platform	x	x	x
4.02	WSN data fusion framework	x	x	x
4.03	Communication Stack Trains WSNs	x	x	x
4.06	Plug& Play& Forget for WSNs	x	x	x
5.01	Smart WSN data fusion and mining	x	x	x
5.02	Scalability of Wireless Building	x	x	x
5.03	Smart power supply	x	x	x
5.04	Indoor positioning, Building automation	x	x	x
5.05	Wireless data Aggregation	x	x	
5.07	Context Aware Reasoning Module	x	x	x
5.08	OTA programming monitoring and control	x	x	
5.09	WS Communication with IP	x	x	x

2 has been defined as a request–response technology without support of QoS or real-time capabilities, data fusion is not a highly necessary feature. On the other hand, Level 0 and Level 1 have more scalability and quality of service issues. Therefore, data fusion and potential compression of sensor readings coming from an increasing number of DEWI Nodes or DEWI WSNs might be required.

8.1.3. Smart WSN Data Fusion and Mining

One of the main objectives of the DEWI HLA is to enable external users to access information of different DEWI Bubbles of different domains. This is in line with smart city applications, data mining and big data analysis. In the future, it is expected that large numbers of WSNs both under the DEWI or other frameworks provide information to applications in the cloud that are based on large statistically reliable data improve our understanding of the physical world and therefore help us to make more efficient decisions in our everyday life processes. Therefore, this TI maps to the three levels of the architecture, with a mention of L2 for big data applications. Data fusion has been mainly developed in

Table 11: Mapping high level requirements (HLRQs) to the DEWI HLA.

No.	Description	L0	L1	L2
01	WSN self-configuration	x	x	
02	Resilience	x	x	x
03	WSN availability, reliability & QoS	x	x	
04	Self-organisation, path & traffic management	x	x	
05	Latency	x	x	
06	Range	x	x	
07	Bidirectional comms.	x		
08	Bubble security	x		
09	Bubble concept arch.	x		x
10	Coexistence	x	x	x
11	Packet oriented protocol	x	x	
12	WSN model	x	x	x
13	Node localisation	x	x	
14	Synchronisation	x	x	
15	Time stamp	x	x	
16	Data fusion features and performance	x	x	x
17	Adaptable WSN	x	x	x
18	Node energy management	x	x	x
19	Scalability	x	x	x
20	General ontology	x	x	x
21	Data access interfaces and node abstraction	x	x	x
22	Robust operation	x	x	x
23	Debug, installation, setup and maintenance	x	x	x
24	OTA programming	x	x	x
25	Node identification	x	x	
26	Usability	x	x	x
27	User experience	x	x	
28	Safety	x	x	x

the building domain, where large numbers of nodes are used to monitor, maintain and operate smart buildings. However, fusion capabilities have also been demonstrated in aeronautics and railway domains.

8.1.4. Wireless Data Aggregator (WDA)

This technology item is particularly implemented in L1 and L0. The wireless data aggregator acts as a WSN GW. Data aggregation can also lead to compression techniques that are used to improve scalability of the DEWI solutions. Data aggregation is one of the basic functions identified in the ISO reference architecture. Building, automotive and dense sensor networks in the aeronautics use cases have deployed data aggregation functionalities.

8.1.5. Context Aware Reasoning Module

One of the main aspects that potentially improves the performance of WSNs is the use of context aware reasoning. Context aware information helps in obtaining, for example, a

more reliable and effective interference-free radio resource management. In this context, context aware heavily maps to the first two levels of the architecture. However, context information can also be deduced or obtained from the reasoning and information of the Bubble within the same or in another domain. This is one of the central concepts of the level 2 of the HLA: allow the creation of cross-domain reusability and application development. The DEWI HLA can be seen as an enabler of Big Data applications for smart cities. Therefore, context aware reasoning also maps into L2 in the context of interoperability and cross-domain application development. Due to the higher complexity of some use cases, context aware reasoning was mainly developed in the building domain.

8.2. Smart Architecture

8.2.1. Wireless Communication for in-Vehicle Use

This TI directly maps to Level 0 of the HLA. In some cases, it may also map to Level 1, due to the a close relation between this level of the HLA and the resource management of WSNs inside a Bubble. This has to be defined for each use case and is mainly developed in the automotive domain, but in-vehicle design also applies to some railway and aeronautics applications.

8.2.2. Dependability Protocols, Quality of Safety Critical Systems

This TI lies at the core of the objectives of DEWI: dependable solutions. It mainly resides in the two lower levels of the architecture (L0 and L1), where dependable and safety critical solutions are mainly required in some of the use cases. It is worth pointing out that the architecture fully supports dependable solutions via, for example, redundant network entities or redundant databases with a backup of the sensor readings collected in the network (i.e., virtual sensor solutions). The DEWI Bubble Gateway deserves a special mention here, mainly because it has been defined in the concept of the DEWI Bubble that only one DEWI Bubble Gateway acts as the interface of the DEWI Bubble with the external world. In practice, the architecture can support redundant gateways to reduce the risk of failure and thus improve dependability. Therefore, only one gateway can be the main interface at any particular point of time, but redundant elements can be enabled in the case of a failure. Similar redundancy solutions can be used for the rest of the network elements if needed. This TI was mainly developed in automotive and aeronautics domains.

8.2.3. Communication Stack for Train WSNs

One of the main aspects of the DEWI HLA is the definition of protocol stacks for all levels of the architecture. The design of appropriate protocol stacks in the rail domain can be reused across all the domains with a few modifications for each use case.

8.3. HW/SW Co-Design

8.3.1. Tamper-Proof and Ruggedized Hardware

This TI intends to produce hardware modules that are fit for harsh environmental conditions such as: extreme temperatures, mechanical vibrations, high electromagnetic interference and propagation issues, etc. Therefore, this TI mainly involves level 0 of the architecture and optionally level 1. In the rocket launcher use-case (2.4), ruggedized hardware involved the wireless sensor nodes and sinks that have to be designed to cope with extreme conditions. In addition, protocol modifications have been pursued that ensure high reliability levels during a flight test. Level 1 involves the consolidation and aggregation of the data of different WSNs on board in the WSN GW (also called MTL or module of telemetry) using an internal rocket network technology.

8.3.2. Smart Integration Platform

One of the main challenges faced by DEWI use cases is to integrate a range of different wireless and wireline transmission systems, some of them with legacy operations and some others with modern state-of-the-art technology. Smart integration platforms are therefore

necessary to provide proper protocol translation and interoperability between different types of networks with different data formats and quality of service requirements. Smart integration platforms are mapped to all levels of the architecture. This TI was mainly developed in the railway domain.

8.3.3. Scalability of Wireless Building Networks

The problem of scalability has been addressed in all levels of the architecture. The case of Building networks poses an important problem of scalability due to the high number of systems, networks and devices operating in the same physical space. The scalability of a sensor network determines the amount of information to be processed, the budget for maintenance and operations, as well as the range and dependability of each use case.

8.3.4. OTA Programming, Monitoring and Control

The two first levels of the HLA are expected to be the main recipients of the functionalities of OTA (Over The Air) programming, monitoring and control. This means that these functionalities are independent of each use case. However, the definition of Level 2 technology for the HLA includes the concept of profile database, technology component reusability and cross-domain application development. In particular, the concept of profile database is one type of OTA programming, where different DEWI Bubbles are allowed to access a common repository where configuration settings, parameters and mainly TIs are shared among different domains. This solution is expected to foster the technology reusability features in the project. Different use cases are able to reuse, modify, adapt and cross-optimize technical solutions in the common repository. We can therefore conclude that the conventional OTA programming is hosted in the first two levels of the HLA, but Level 2 will also use some kind of OTA programming with purposes of cross-domain reusability and application development. This TI was mainly developed in the building domain.

8.4. Security, Privacy and Authorization

8.4.1. Highly Secure Wireless (Authorization, Intrusion Safety, Encryption)

Different use cases and different levels of the architecture require different levels of security, including authorization, intrusion detection, safety and encryption. For some use cases security in Level 0 might not be relevant, but it can become an issue in Level 1 once the readings of sensors are transported through the internal network of each domain. In other use cases, for example, the sensor information is so important for critical systems that any attack in the wireless and wireline domains becomes a serious threat even for humans depending on the systems controlled by sensor readings. This is more noticeable in aeronautics and railway control systems, for example, where any attack to the sensor readings can translate in risks of accidents and therefore a threat to human lives. Thus, we can say that in Level 0 and level 1 attacks such as jamming, interference, denial of service, man in the middle, spoofing, etc. should be addressed with more emphasis. Security at Level 2 is the security solution that relies more on the type of data shared by the DEWI Bubble with the external entities. The TI was mainly developed in the automotive and building domains.

8.4.2. RT Protocol

Real-time is a typical requirement in industrial communication networks. The support for real time mainly occurs in the first two levels of the HLA. It is worth pointing out the role of Level 1 for the integration of real-time wireless solutions into the real-time wireline infrastructure of several of the use cases. Examples of real-time technology are CAN in the automotive domain and AFDX (ARINC 664) in the aeronautics industry. The challenge of Level 0 real time support in DEWI lies in matching the real-time requirements of the existing wireline infrastructure. This TI was mainly developed in automotive and aeronautics domains.

8.4.3. Security and Authentication

Security and authentication are currently not directly addressed by many of the use cases in the project. However, both technological aspects play a crucial role in the definition of DEWI Bubble services and the external/internal users. In principle, security and authentication processes are supported at all levels of the architecture. DEWI nodes can be authenticated by their respective DEWI WSN gateway. Similarly, WSN Gateways can be authenticated by their respective DEWI Bubble Gateway. This TI was mainly addressed in automotive use cases. The SCOTT project has addressed security aspects of the DEWI Bubble.

8.5. Re- /Auto- /Self-Configuration

8.5.1. Multi-Standard RF Wired Sensor Network Gateways and Protocols

This TI is closely related to the development of L0/L1 and L0/L1 protocol translation and traffic forwarding. Since Level 1 is closely related to the existing wireline infrastructure of each industrial use case, a convenient gateway definition that allows for transparent and reliable data transfer between wireless and wireline networks is required. This is a particularly challenging task in those use cases where a highly reliable quasi deterministic real-time network exists. This TI was developed in the aeronautics domain.

8.5.2. Mechanism for Prioritized Wireless Transmissions, (NW-Backup Mode)

Prioritization of wireless transmissions is an important radio resource management aspect of wireless sensor networks that takes place mainly at Level 0 and Level 1 of the DEWI HLA. Level 0 refers to the coordinated transmissions and prioritization of sensor traffic within the same WSN. Prioritization at Level 1 refers more to coordination between WSNs, assignment of time slots or frequency bins for coordinated or interference free inter-WSN control. It is possible that this prioritization could also take place at Level 2, so that DEWI Bubbles operating in the same physical space could coordinate their transmissions or traffic load to reduce interference to other neighbour systems. However, this aspect is currently not envisioned in the project. This TI was developed in automotive and aeronautics domains.

8.5.3. Spectrum Coordination for in-Vehicle Wireless Communications

Spectrum management in future wireless sensor networks will help organize radio resources and reduce the increasing problem of interference. It is expected that spectrum coordination mainly resides in the two lower levels of the HLA. In Level 0, each WSN is assigned to a particular spectrum resource based on a predefined plan or with the help of dynamic allocation. Such dynamic allocation may rely on Level 1 technology for the management of different WSNs inside the same Bubble. One of the main advantages of a centralized architecture control, where the DEWI Bubble Gateway can host and manage more than one WSN, is that interference control, cooperative control and coordination of transmission and spectrum resources becomes feasible. Spectrum coordination may also occur at Level 2 for the coordination of spectrum resource and allocation for different Bubbles operating in a given area. This TI was developed specifically in automotive domain, but it has also some aspects in aeronautics and railway use cases.

8.5.4. Plug and Play and Forget for WSN

A key aspect for wireless sensor networks is the ability to be autonomous, self-configurable and self-healing. Wireless sensor networks are usually deployed in locations not easily accessible or their maintenance by humans reduce the cost effectiveness of the solution. Therefore, the ability to make intelligent self-configuration and self-maintenance greatly improves the adoption and pervasiveness of WSNs. Plug and play and forget is a technology item that moves forward along the lines of self-management and self-configuration, by allowing the device of the network to automatically be installed, configured and maintained without human intervention. This technology item mainly applies to

the two lower levels of the architecture. However, the use of a profile database for Level 2 configuration and management also introduces some PnP features in the top level of the HLA. This TI was developed mainly in railway use cases.

8.6. Smart Energy Management and Harvesting

8.6.1. Power and Energy Management, Energy Harvesting

Power management and energy harvesting are expected to improve the cost effectiveness, range, battery life and maintainability of wireless sensor networks. Energy harvesting mainly occurs at level 0 of the architecture, while power management can cross-over from level 0 to level 1, where multiple WSNs can coordinate their transmission power policies and thus reduce intra Bubble interference or interference towards another Bubbles. Level 2 could also potentially use some coordination capabilities to enable power control between adjacent Bubbles. However, this last option is not currently contemplated in the DEWI solution.

8.6.2. Smart Power Supply

Power is a limited resource in sensor networks. The smart management of this resource means prolonged battery life, which also means reduced costs for replacing and maintaining the sensor network. This TI mainly covers level 0 for the intra-WSN management. This TI was developed in automotive and building domains.

8.7. Dependability, Robustness and Safety

8.7.1. Highly Robust and Reliable Wireless

This TI is mainly concentrated in Level 0 of the DEWI HLA, where all radio transmission technology and packet reception take place. It could also be related to Level 1, mainly because Level 1 is in charge of the management of several WSNs inside the Bubble. Therefore, Level 1 can be in charge of the reliable management and data transfer from the different WSNs. If this does not occur, then, even with a robust Level 0 solution, the overall Bubble communication would be affected. Level 1 can also be in charge of interference management between different WSNS inside the Bubble, using, for example, convenient channel allocation or even time slot scheduling or smart antenna processing. In DEWI, however, the role of Level 1 in terms of highly robust and reliable networking is rather limited. Several solutions for improving reliability and robustness of the wireless transmission technologies have been proposed in the project ranging from physical, MAC (medium access control) and networking solutions (mainly for ad-hoc wireless sensor network solutions). This TI was developed in the aeronautics and automotive domains.

8.7.2. Synchronization of WSN

Several industrial applications require synchronous operation of wireless sensor networks. Examples of these applications are: structure health monitoring, sensing of automotive and aeronautic parameters in real time, or control of lighting systems inside buildings. Synchronization mainly occurs at Level 0 and perhaps at Level 1. This TI was developed in the automotive and aeronautics domains.

8.7.3. Functional Safety

Functional safety is a key aspect in many industrial applications. For example, in aeronautics, functional safety of the WSN mean reduced interference to vital flight control subsystem of the aircraft. Similar functional safety scenarios can be found in all the domains. This functional safety mainly covers Level 0 and some aspects of Level 1 too. This is implemented in automotive, aeronautical, and railway domains.

8.8. Wireless Standards

8.8.1. Knowledge-Oriented Sensor Networks

This technology item is predominantly hosted in the upper layers of the architecture. However, Level 0 potentially also hosts some features of this TI. The main objective is to create a network for dissemination of context information that, with the help of the collected sensor information, improves the decision-making process of different applications. This TI was developed in automotive domain.

8.8.2. WS Communication Homogenization with the IP

The integration of WSNs into the Internet IP-based infrastructure is one of the main research lines in the literature of IoT and M2M. This TI maps mainly to the upper layers of the architecture, where IP-based technologies are expected to be implemented. Level 2 has been defined as an IP-based technology. By contrast, Level 1 is an optional technology that, in some cases, captures the real-time industrial requirements. IP technology is expected to be used only in a few cases at Level 1. At Level 0, IP technologies have not been directly implemented. However, protocol adaptations, particularly in the framework of the IoT (e.g., 6LowPAN), allow devices to be incorporated smoothly into the IP cloud. This TI was developed mainly in building domains, but it is also available in the rest of the domains.

8.9. Wireless Sensor/Device Detection and Localisation

8.9.1. Localisation of Sensors and Actuators

Localisation information in WSNs is expected to improve performance, resource allocation, application development and security. This TI maps mainly to Level 0 (where localisation information is obtained) and Level 2, where localisation information can be used for some cross-domain applications, mainly developed in the building domain for access control applications.

8.9.2. Indoor Positioning Platform for Building Automation

This TI also maps to Level 0 and Level 2 of the HLA. It is specific for positioning and localization of items or individuals inside buildings, providing, for example, automatic access control in critical infrastructure.

9. High Level Requirements (HLRQs)

The mapping of high level requirements to the DEWI architecture is shown in Table 11. The HLRQs are described in the following subsections.

9.1. WSN Self-Configuration

The DEWI HLA must allow self-configuration. The layered and functional model of the HLA can meet implicitly this requirement for Level 0 and Level 1. This means that use cases can deploy their own solutions in both levels of the architecture to enable self-configuration. By comparison, in level 2, there is an explicit use of a profile database where DEWI Bubbles are able to retrieve configuration parameters of the domain and reuse technical solutions created in other use cases of within the same or from other domains.

9.2. Resilience

Resilience was mainly based on each use case implementation. This lies mainly in Level 0 of the architecture. Some use cases might also employ resilient solutions for Level 1. However, these solutions are already existing in most of the use cases.

9.3. WSN Availability, Reliability and Quality of Service

This requirement is closely linked to the concept of dependability, which is central in the DEWI HLA. These requirements have been considered in the definition of Level 0 and particularly Level 1. We recall that Level 1 is connected to the existing infrastructure of each use case, and that such infrastructure in the majority of cases is real time and highly

reliable. Therefore, each use case has investigated the best way to design Level 0 (wireless links) to match the reliability and quality of service features of many of the L1 technologies.

9.4. WSN Self-Organization, Path Diversity and Differentiated Traffic Management

By definition, the DEWI HLA supports advanced management schemes such as differentiated traffic management and self-organization in the two first levels of the architecture. The top level (Level 2) has been in principle designed as a non-real time request-response and service oriented architecture. This means that Level 2 has been simply used for occasional access and request to the DEWI Bubble services by other Bubbles or by external users.

9.5. Latency

Latency is an important metric in real-time industrial applications. By definition, the DEWI HLA supports latency constraints up to Level 1. Level 2 is not currently designed to support delay-sensitive applications.

9.6. DEWI Wireless Range

Wireless range defines the physical space where the DEWI Bubble services are enabled. This requirement is directly linked to level 0, which is the intra-WSN technology. Some aspects of Level 1 might also affect the range of the DEWI Bubble, mainly by using interference control or context aware inter-WSN resource allocation (e.g., spectrum power and transmissions allocation).

9.7. Bi-Directional Communication

Bi-directional communication is a requirement mainly needed in Level 1 and Level 0. This requirement encapsulates the need to establish a two-way communication channel with DEWI Nodes. In Level 2, bi-directional communication is usually achieved by the IP infrastructure, so it is not considered a requirement in the design of the HLA L2.

9.8. DEWI Bubble Security

There is a need to provide secure DEWI Bubble services. As observed with TIs, security is required for all levels of the architecture. Each level, however, might have different requirements and different constraints to consider in the design.

9.9. DEWI Bubble Concept Architecture

All the levels of the HLA have been designed according to the DEWI Bubble concept and its architectural principles.

9.10. Coexistence

One of the main driving factors in the design of the DEWI HLA is coexistence. Coexistence is mainly addressed at Level 0, where the aim of the DEWI Bubble is to ensure coexistence between different wireless transmission technologies. However, Level 1 and Level 2 can also be regarded as enablers of the coexistence at Level 0, mainly by providing management allocation and interoperability between heterogeneous wireless/wireline technologies.

9.11. Packet Oriented Protocol

The DEWI HLA supports mainly packet oriented protocols. In those cases where existing wireline technologies do not support packet based transmissions, the DEWI Gateways provide protocol conversion and data translation. This is a development particular to each use case.

9.12. WSN Model

Each layer of the HLA has been mapped to the functional model of DEWI, which in turn is based on the functional model of the ISO reference architecture. The DEWI HLA has also been mapped to the INTEROP interoperability architecture framework, which provides different models and visions of the DEWI Bubble and the WSNs inside the Bubble.

9.13. Node Localization

The DEWI HLA complies with the ISO reference architecture, which includes the functionality of node localization. This functionality mainly lies in Level 0 of the HLA.

9.14. Synchronisation

Synchronisation is a requirement that by definition of the DEWI HLA can be met in Level 0 and Level 1 of the HLA. Level 2 provides asynchronous message-based (request-response) access to DEWI Bubbles, which is inherently not synchronous.

9.15. Time Stamp

Time stamps are to be used in some sensor applications that require knowledge of timing between sensor events, such as data fusion algorithms. Therefore, time stamps are supported in the HLA mainly in Level 0 and Level 1. Some applications of Level 2 might have access to time stamp information. However, this has to be defined in the configuration profile of each DEWI Bubble.

9.16. Data Fusion Features and Performance

Data fusion algorithms are intrinsically supported by Level 0 and Level 1. Level 2 is not expected to support these functionalities. SCOTT project deals with cloud computing aspects for data fusion in L2.

9.17. Adaptable WSN

Adaptation in wireless sensor networks is intended to counteract the random behaviour of wireless propagation channel and the traffic load in the network. Therefore, this requirement has been mainly addressed by Level 0 and Level 1.

9.18. Node Energy Management

The DEWI HLA supports advanced node energy management. This is a necessary feature for WSNs to become more cost-effective than their wireline counterparts. Energy management is supported by the DEWI HLA at Level 0 and Level 1. It is possible that Level 2 applications enable some further benefits in terms of energy consumption, mainly by cross-optimizing resources and spectrum across contiguous DEWI Bubbles and reducing interference.

9.19. Scalability of Solutions

The DEWI HLA has been designed by keeping in mind scalability. Layered models are conventionally used to provide a more flexible organization of resources, thus allowing for comprehensively scalable solutions. All use cases have reported in the project deliverables their individual scalability analysis.

9.20. General Ontology Definition

The DEWI HLA provides with ontology models for the definition of interoperability, cross-domain application development and technology component reusability. This ontology and interoperability model is based on the mapping of the DEWI HLA to the INTEROP interoperability architecture framework [19]. The ontology model allows abstraction of high level DEWI level 2 functionalities for DEWI Bubble services and applications without the need to define platform and system dependent models. This provides DEWI with great flexibility in terms of being able to reuse existing service oriented architectures (mainly

developed in the context of the Internet of things) and develop a DEWI overlaid ontology solution. The DEWI high level language reflects the features of the project and allows for cross-domain application development.

9.21. Data Access Interfaces and Node Abstraction

The DEWI HLA layered model aims to provide with data access interfaces encapsulated in the DEWI Bubble Services. The DEWI APIs developed across use cases enable different users (external or internal) to have access to node information or to a virtual representation of the DEWI Nodes. This requirement is supported in the three levels of the architecture.

9.22. Robust Operation

Robust operation is central to the objectives of DEWI. Robustness has been favoured in the two lower levels of the architecture, which hold the main dependability and reliability requirements in the architecture.

9.23. Debug, Installation, Setup and Maintenance

These requirements will be supported mainly in Level 0 and Level 1 of the HLA.

9.24. OTA Programming

Over the air programming is mainly supported in Level 0 and Level 2. DEWI Level 2 supports the use of profile repository where configuration parameters, technical solutions and software modules can be accessed by DEWI Bubbles of different domains. This means that DEWI Bubbles can select on the fly different technology components when convenient, thus realizing the feature of technology reusability in the project.

9.25. Node Identification

Identification is supported in some use cases of the HLA, particularly in combination with RFID technology. Identification of nodes can be used to add further value and meaning to some applications. Security schemes based on context information (identification) can be used for example in supply chain management and logistic applications to detect potentially lost or misplaced items.

10. Use-Case Mapping

This section provides the explicit mapping of the different use-cases of the project to the layered model of the DEWI HLA. Additionally, each use case can be mapped to the other functional, interface and physical views of the architecture. For simplicity, here we focus only on the layered model mapping. Table 12 provides the mapping of all use cases to the three-tier model, specifying the technology used for each level of the architecture. Three illustrative examples of the mapping of use cases to the HLA are displayed in Figure 17, 18 and 19.

Use case 2.4 (17) employs a highly ruggedized hardware WSN to monitor and control several aspects of an operational rocket. An actual physical rocket has been put into flight in military air space testing WSN technology on board. The subsystems controlled by the internal WSN include parachute control, direction and flight stabilization control, temperature monitoring and fuel consumption regulation. The Bubble gateway has been successfully tested in these challenging environmental conditions with extreme temperature, altitude and pressure. The Bubble Gateway was in charge of consolidating the data from different WSNs across the rocket and relaying the information to/from ground control. Use case 2.5 18 also belongs to the aerospace domain. A highly dense network of sensors over the surface of the plane is used to track variations of pressure associated with turbulent flow formation or degradation of laminar conditions. The information is used to activate a set of actuators based on flow injection. Sensors and actuators are arranged in patches, internally wired, but connected via wireless to a gateway and to the central

Table 12: DEWI use cases in the HLA.

UC No.	L0	L1	L2
2.4	802.15.4	Ethernet	IP
2.5	802.15.4/1	ARINC 664	IP/Ethernet
3.1	802.15.1	CAN/AUTOSAR/ AK/EtherCAT	IP
3.2	802.15.1/4	CAN / EtherCAT	IP
3.3	802.15.1/4	CAN / EtherCAT	IP
3.4	802.15.1a/4	Proprietary	IP
3.5	802.11b/g/n	N/A	PMR LTE 400MHz
3.6	802.15.4 /BLE	IEEE 802.11s	IP
3.7.1	802.15.1	IEEE 802.15.1	IP
3.8	802.15.4 /BLE	AUTOSAR/ CAN Ethernet	IP
3.9-10	802.15.4	USB	N/A
4.1	802.15.4g	MQTT/Ethernet	IP
4.2	802.15.4g	MQTT/Ethernet	IP
4.3	802.15.4	MQTT/Ethernet	IP
4.5	802.15.4/11	MQTT /IP	Cellular
5.1	WiFi, BLE, 4G-LTE	WiFi/Ethernet	HTTP
5.2	WiFi, Zig-Bee 802.15.4,6LowPAN	WiFi /Ethernet	MQTT/CoAP
5.3	ZigBee/802.15.4	Ethernet	IP
5.4	ZigBee /802.15.4 WiFi	N/A	HTTP /AMQP
5.5	6LowPAN/ 802.15.4	Ethernet/ 802.11	IP

coordinator of the system on board. The WSN is therefore connected to the internal bus of the aircraft. The bubble gateway relays information to ground control. Use case 3.8 (19) uses distributed wireless sensor in a commercial truck. The wireless sensors replace several wired sensors commonly found inside a truck. These include tyre pressure sensors, fuel level sensors, etc. The sensors communicate the readings to a wireless gateway, which in turn communicates with a central controller through the internal network of the truck, in this case based on the CAN standard.

11. Mapping to Other Architectures

The DEWI HLA has been mapped to other relevant architectures in the literature of sensor networks, Internet of Things and M2M communications. The objective of this mapping process is to look at similarities, potential interoperability between solutions and future integration of IoT technologies. An example of the mapping of the DEWI HLA to different views of perspectives of the IoT ARM can be observed in Figure 20 and Figure 21. An example of the mapping with the oneM2M architecture is given in Figure 22.

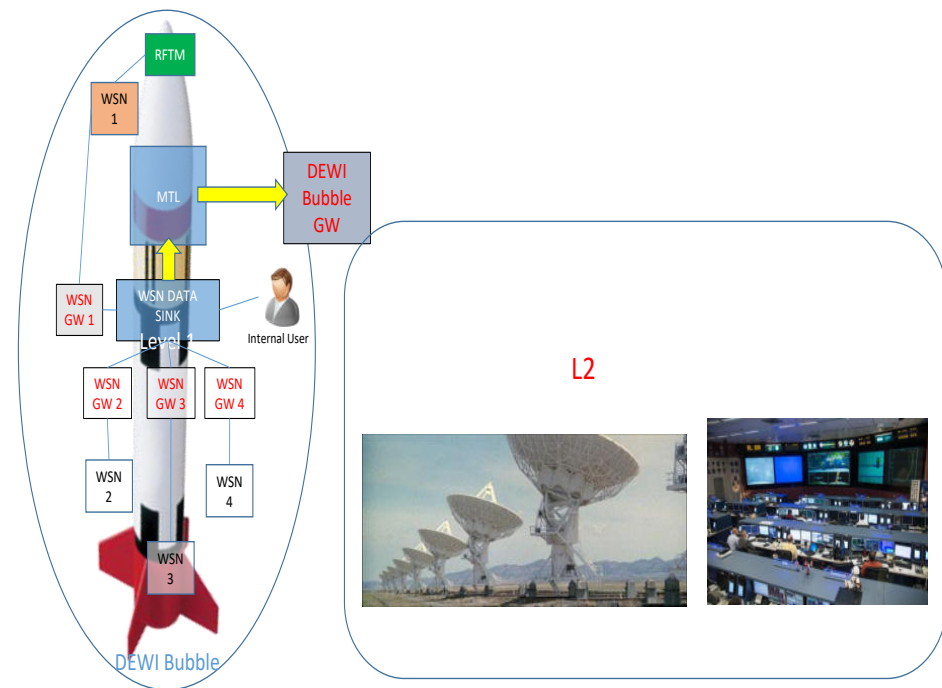


Figure 17. Mapping UC2.4 to the layered model of the DEWI HLA.

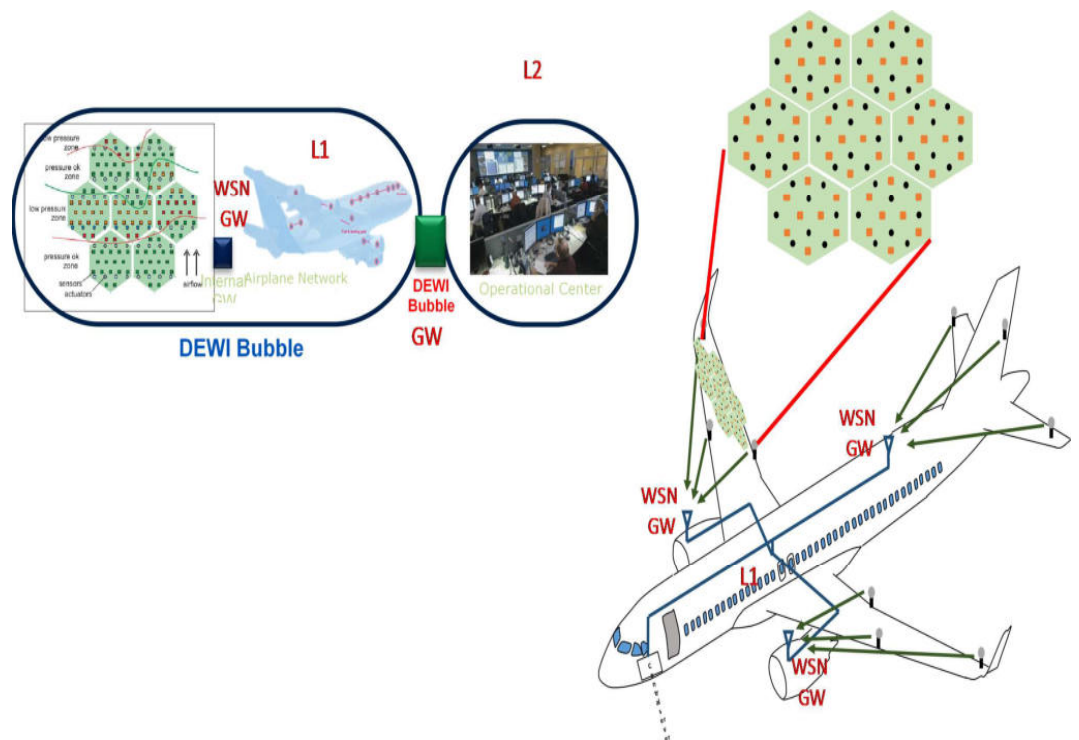


Figure 18. Mapping UC2.5 to the layered model of the DEWI HLA.

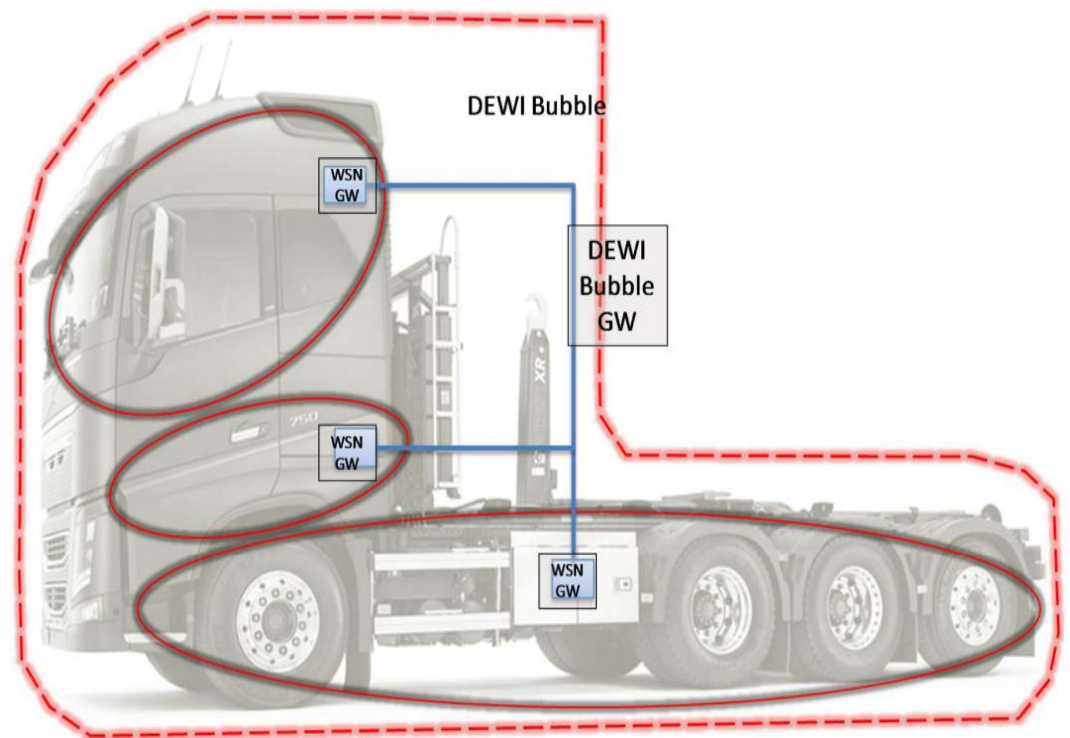


Figure 19. Mapping UC3.8 to the layered model of the DEWI HLA.

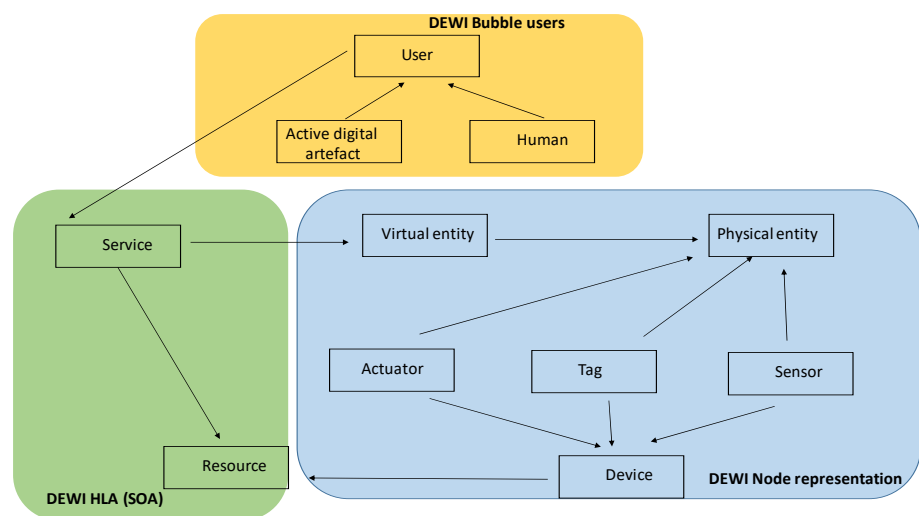


Figure 20. Mapping DEWI HLA to the IoT ARM.

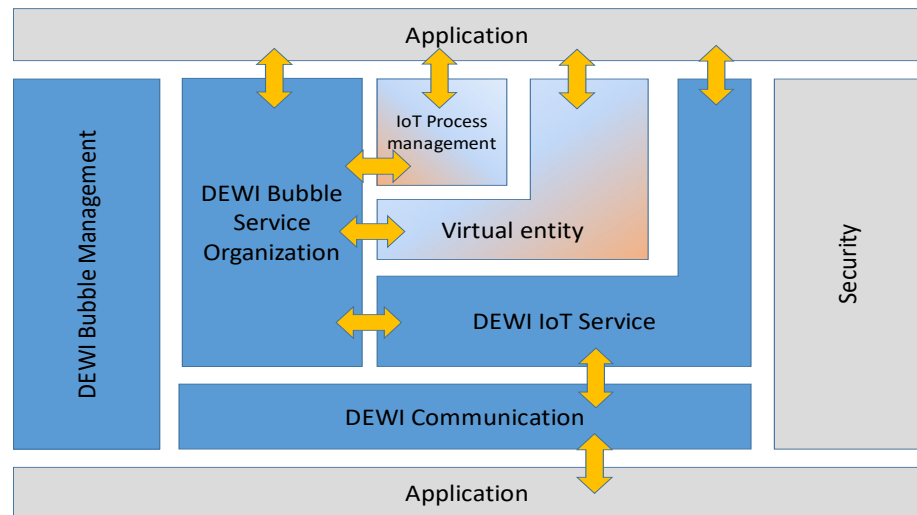


Figure 21. Mapping DEWI HLA to the IoT ARM.

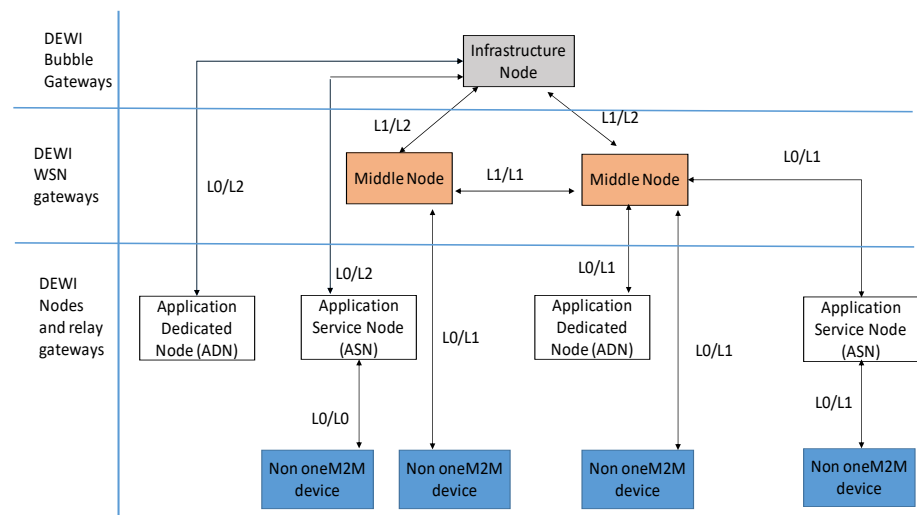


Figure 22. Mapping DEWI HLA to the oneM2M architecture.

12. Conclusions and Future Work

This paper has presented a summary of the definition of the DEWI High-Level Architecture (HLA). The HLA aims to act as a reference framework for the design of wireless sensor and actuator industrial networks compliant with the concept of the DEWI Bubble. It offers a robust and interoperable framework to develop industrial dependable wireless solutions for monitoring and actuation. The DEWI HLA offers the versatility to be adapted to any kind of application/scenario requirements, and is agnostic to the underlying WSN technologies, becoming a powerful architecture for long-term industrial solutions. One of the main aspects achieved in this paper is the formalization of the entity model, the layered perspective of the entity model and the functional decomposition of the DEWI HLA, which is an extension of the ISO/IEC SNRA for industrial applications. The guidelines and analysis provided here are expected to be useful for the future integration of industrial WSANs into modern IoT, 5G, and Cloud Computing frameworks. The DEWi Bubble was here introduced with a simple but powerful three-layered entity model that allows for legacy and modern WSN technology to be integrated into existing industrial infrastructure of cars, trains, airplanes and buildings, and it also provides a flexible interface towards the IP and IoT worlds. Therefore, the Bubble concept provides a transition between legacy industrial wireless and wireline networks and new concepts such as the IoT, Big Data and Cloud Computing.

The DEWI project has paved the way for new project focused now on higher level issues such as security, safety, trust and privacy in the IoT. The project SCOTT (Secure COnnected Trustable Things) [27] builds on the results and on the architecture of the DEWI Bubble infrastructure to leverage the trust of IoT technology and boost its development and widespread use in the European industry. The project InSecTT [28] provides the convergence between IoT and artificial intelligence using the DEWI and SCOTT approaches.

Author Contributions: Conceptualization, R.S.-R., T.N., S.S.-C., and K.K.; methodology, R.S.-R., T.N., and K.K.; formal analysis, R.S.-R.; investigation, R.S.-R., S.S.-C., T.N. and K.K. writing—original draft preparation, R.S.-R., and T.N.; writing—review and editing, R.S.-R., and T.N. ; visualization, R.S.-R., S.S.-C.; project administration, M.K., E.T.; funding acquisition, M.K., and E.T.; implementation, M.H., M.L.

Funding: SCOTT (www.scottproject.eu) has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under Grant No. 737422. This Joint Undertaking received support from the European Union’s Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium and Norway. It is also funded by FCT/MEC (Fundação para a Ciência e a Tecnologia), ERDF (European Regional Development Fund) under PT2020, and by CISTER Research Unit UIDP/UIDB/04234/2020.

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

Data Availability Statement: Data sharing is not applicable to this article.

Acknowledgments: The authors acknowledge valuable discussions and inputs regarding the presented high-level architecture from all partners within the DEWI and SCOTT projects.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kim J; Yun. J; Choi S.; Seed D.N.; LU, G.; Bauer, M.; Al-Hezmi, A.; Campowsky, K.; Song, J. Standard-based IoT platforms interworking: implementation, experiences, and lessons learned, *IEEE Communications Magazine*, 2016, 54, pp. 48–54.
2. Stone T.; Alena R.; Baldwin J.; Wilson P.; A viable COTS based wireless architecture for spacecraft avionics, *IEEE Aerospace Conference*, 3-10 march 2012 Big Sky MT, pp. 1-11.
3. Harrington, M. Introduction to wireless systems in aerospace applications. In *Proceedings of the CANEUS Fly-by-wireless workshop*, June 2009, Canada.
4. Elgezabal, O. Fly-by-Wireless (FBWSS): Benefits, risks and technical challenges. In *Proceedings of the CANEUS Fly-by-Wireless Workshop*, August 2010, USA.

5. Dornheim, M. A. New rules and hardware for wiring soon to emerge, *Aviat Week Space Technol.*, **2001**, 154,92.
6. Studor G., NASA Fly-by-Wireless Update, <http://hdl.handle.net/2060/20100031691> (accessed on 15 October 2021).
7. Graham-Rowe, D. Fly-by-wireless set for take-off. *New Scientist*. **2009**, 203, 20. Last accessed October 2021.
8. DEWI (Dependable Wireless Infrastructure). EU project. Website: www.dewiproject.eu (accessed on 15 October 2021).
9. DEWI Deliverable D102.005 DEWI Global Glossary. Available at: <http://www.dewiproject.eu/media/deliverables/> (accessed on 15 October 2021).
10. Samano-Robles R.; Nodstrom T.; Rom W., Santoja S.; and Tovar E; The DEWI high-level architecture: Wirelesn industrial applications, 2016 Eleventh International Conference on Digital Information Management (ICDIM), Porto, 2016.
11. ISO/IEC 29182, Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA) - Part 1 to 7. Available at www.iso.org (accessed on 15 October 2021).
12. Internet of Things – Architecture IoT-A Deliverable D1.5 – Final architectural reference model for the IoT v3.0. Project IoT-A. Available at https://www.researchgate.net/publication/272814818_Internet_of_Things_-_Architecture_IoT-A_Deliverable_D15_-_Final_architectural_reference_model_for_the_IoT_v30 (accessed on 15 October 2021).
13. Davis, A.;Chang, H. A Survey of wireless sensor network architectures, *International Journal of Computer Science & Engineering Survey (IJCSSES)*, **2012**, 3, 1–22.
14. Rawat, P.; Singh, K.D.; Chaouchi, H.;Bonnin, J. M.; Wireless sensor networks: a survey on recent developments and potential synergies, *Journal Supercomput*, **2014**, 68,1–48.
15. FP7 project IoT6. Researching IPv6 potential for the Internet. Available at: <http://iot6.eu/> (accessed on 15 October 2021).
16. Alliance for Internet of Things innovation <http://www.aioti.eu/> (accessed on 15 October 2021).
17. ITU- Y.2060: Overview of the Internet of things (Reference Architecture). Available online at <https://www.itu.int/rec/T-REC-Y.2060-201206-I> (accessed on 15 October 2021).
18. IEEE P2413. <https://standards.ieee.org/standard/2413-2019.html> (accessed on 15 October 2021).
19. INTEROP FP6 European project (Interoperability research for networked enterprises applications and software). Available at: <https://cordis.europa.eu/project/id/508011> (accessed on 15 October 2021).
20. Leguay J.; Lopez-Ramos M.;Jean-Marie K.;Conan V.; An efficient service oriented architecture for heterogeneous and dynamic wireless sensor networks, 33rd IEEE Conference on Local Computer Networks, 2008. LCN 2008, pp.740,747, 14-17 Oct. 2008. doi: 10.1109/LCN.2008.4664275
21. Delicato F. C.;Pires P. F.; Costa Carmo L.D.R. flexible web service based architecture for wireless sensor networks, In Proc. International Conference on Distributed Computing Systems Workshops (ICDCSW), 2003.
22. Flickinger D. R.; Bridging the Automation/IP Gap. White paper Archronix. Available online at <http://www.cepro.com/asset/6037.pdf>, 2006 ISO (accessed on 15 October 2021).
23. Chu X.; Buyya R., Service oriented sensor web. *Sensor Network and Configuration: Fundamentals, Techniques, Platforms, and Experiments*; N. P. Mahalik (ed)., **2007**,51–74.
24. Emil F.S.; Ramiro L.; A Web-Services Framework for 1451 Sensor Networks. In Proc. of IEEE Instrumentation and Measurement Technology Conference (IMTC), 2005
25. Kyusakov R.; Eliasson J.; Delsing J.;Van Deventer J.; Gustafsson J., Integration of Wireless Sensor and Actuator Nodes With IT Infrastructure Using Service-Oriented Architecture. *IEEE Transactions on Industrial Informatics*,**2013**, 9, 43–51.
26. DEWI Deliverable D311.007 Reference architecture summary, v1.0, 2016-01-25. Available online in the deliverable list at: <http://www.dewiproject.eu/> (accessed on 15 October 2021).
27. SCOTT (Secure Connected Trustable Things) ECSEL EU project. <https://scottproject.eu/> (accessed on 15 October 2021).
28. InSecTT (Intelligent Secure Trustable Things) ECSEL EU project. <https://www.insectt.eu/> (accessed on 15 October 2021).
29. Arrowhead project. <http://www.arrowhead.eu/> (accessed on 15 October 2021).
30. ETSI M2M architecture. Available at: www.etsi.org/technologies-clusters/technologies/m2m (accessed on 15 October 2021).
31. oneM2M architecture. Available at: www.onem2m.org (accessed on 15 October 2021).

32. Mobile and wireless communications Enablers for the Twenty-twenty Information Society. METIS project. Available at: <https://metis2020.com/> (accessed on 15 October 2021).
33. RFC 3768 - Virtual Router Redundancy Protocol (VRRP). Available at <https://tools.ietf.org/html/rfc3768> (accessed on 15 October 2021).
34. MQTT protocol. Available online at <https://mqtt.org/> (accessed on 15 October 2021).
35. AMQP protocol. Available online at <https://www.amqp.org/> (accessed on 15 October 2021).
36. Data-Distribution Service for Real-Time Systems. Available at: <https://www.omg.org/omg-dds-portal/> (accessed on 15 October 2021).
37. RFC 7540: Hypertext Transfer Protocol Version 2 (HTTP/2). Available online at: <https://tools.ietf.org/html/rfc7540> (accessed on 15 October 2021).
38. RFC 7252: The Constrained Application Protocol (CoAP). Available at: <https://tools.ietf.org/html/rfc7252> (accessed on 15 October 2021).
39. World Wide Web Consortium (W3C). Online at: <https://www.w3.org/> (accessed on 15 October 2021).
40. RFC 6101: The Secure Sockets Layer (SSL) Protocol Version 3.0. Available online at: <https://tools.ietf.org/html/rfc6101> (accessed on 15 October 2021).
41. Simple Object Access Protocol (SOAP) 1.2. Available at: <https://www.w3.org/TR/soap12/> (accessed on 15 October 2021).
42. XML 1.0. Available at <https://www.w3.org/TR/REC-xml/> (accessed on 15 October 2021).
43. Document Type Definition (DTD). Available online at: https://www.w3schools.com/xml/xml_dtd_intro.asp (accessed on 15 October 2021).
44. Web Services Description Language (WSDL) Version 2.0. Last Accessed: October 2021. Available online at: <https://www.w3.org/TR/2007/REC-wsdl20-20070626/> (accessed on 15 October 2021).
45. RFC 6455 The WebSocket Protocol. Available at: <https://tools.ietf.org/html/rfc6455> (accessed on 15 October 2021).
46. UDDI (Universal Description, Discovery, and Integration). Available online at: <http://uddi.xml.org/>. (accessed on 15 October 2021).
47. Web Application Description Language. Available online at: <https://www.w3.org/Submission/wadl/> (accessed on 15 October 2021).
48. Web Services Dynamic Discovery (WS-Discovery) Version 1.1. Available online at: <http://docs.oasis-open.org/ws-dd/discovery/1.1/wsdd-discovery-1.1-spec.html>. (accessed on 15 October 2021).
49. Simple Service Discovery Protocol/1.0. Available online at: <https://tools.ietf.org/html/draft-cai-ssdp-v1-03> (accessed on 15 October 2021).
50. DNS Service Discovery (DNS-SD). Available online at: <http://www.dns-sd.org/> (accessed on 15 October 2021).
51. IPSO alliance. Available online at: <https://omaspecworks.org/ipso-alliance/> (accessed on 15 October 2021).
52. RFC 3986: Uniform Resource Identifier (URI): Generic Syntax. Available online at: <https://www.ietf.org/rfc/rfc3986.txt> (accessed on 15 October 2021).
53. Lightweight M2M (LWM2M). Available online at: <https://www.omaspecworks.org/what-is-oma-specworks/iot/lightweight-m2m-lwm2m/> (accessed on 15 October 2021).
54. hyperCAT. Available online at: <http://www.hypercat.io/> (accessed on 15 October 2021).
55. Java Script object notation. Description available online at: <https://www.json.org/> (accessed on 15 October 2021).
56. SA-REST: Semantic Annotation of Web Resources. Available online at: <https://www.w3.org/Submission/SA-REST/> (accessed on 15 October 2021).
57. XHTML™ 1.1 - Module-based XHTML - Second Edition. Available online at: <https://www.w3.org/TR/xhtml11/> (accessed on 15 October 2021).
58. Swagger: Available at: <https://web.archive.org/web/20160422034728/http://swagger.io/> (accessed on 15 October 2021).
59. YAML 1.2: YAML Ain't Markup Language. Available online at: <http://yaml.org/> (accessed on 15 October 2021).
60. RFC 7049: Concise Binary Object Representation (CBOR). Available online at: <https://tools.ietf.org/html/rfc7049> (accessed on 15 October 2021).
61. OData (Open Data Protocol). Available at: <http://www.odata.org/> (accessed on 15 October 2021).

62. REST Resource Description Framework (RDF). Available online at: <https://www.w3.org/RDF/> (accessed on 15 October 2021).
63. OWL Web Ontology Language Semantics and Abstract Syntax. Available online at: <https://www.w3.org/TR/owl-semantics/> (accessed on 15 October 2021).
64. Sensor Model Language. Available online at: <http://www.opengeospatial.org/standards/sensorml> (accessed on 15 October 2021).
65. Web of Things (WoT) Architecture. Available online at <https://www.w3.org/TR/wot-architecture> (accessed on 15 October 2021).
66. Semantic Sensor Network Ontology. Recommendation available online at: <https://www.w3.org/TR/vocab-ssn/> (accessed on 15 October 2021).
67. X-GSN: An Open-source Semantic Sensing Middleware for the Web of Things. Description available online at: <http://ceur-ws.org/Vol-1401/paper-04.pdf> (accessed on 15 October 2021).
68. M3: Machine to machine Measurement. Available online at: <http://www.sensormeasurement.appspot.com/documentation/UserGuide.pdf> (accessed on 15 October 2021).
69. DEWI deliverable D206.001 Ph1 Aeronautics Domain Technology Items (Phase 1). Available online in the deliverable list at: <http://www.dewiproject.eu/media/deliverables/> (accessed on 15 October 2021).
70. DEWI deliverable D311.006 Methodology for functional safety in WSN design for technology item Know-how transfer. Available online in the deliverable list at: <http://www.dewiproject.eu/media/deliverables/> (accessed on 15 October 2021).
71. DEWI deliverable D406.001 Technology Items cross-use and cross-domain interoperability requirements and specifications in Rail Domain. Available online in the deliverable list at: <http://www.dewiproject.eu/media/deliverables/> (accessed on 15 October 2021).
72. DEWI deliverable D501.001 User Requirements. Available online in the deliverable list at: <http://www.dewiproject.eu/media/deliverables/> (accessed on 15 October 2021).

