



Project Number:	<i>INFSO-ICT-224282</i>
Project Title:	GINSENG-Performance Control in Wireless Sensor Networks
Project Deliverable Number:	224282/UCY/D1.3
Revised Contractual Date of Delivery to CEC:	Month 24 – August 2010
Actual Date of Delivery to CEC:	1 October 2010
Title of Deliverable:	Final GINSENG Architecture, Scenarios and Quality of Service Measures
WP contributing to the Deliverable:	WP1

Abstract:

This deliverable presents the final version of the GINSENG performance controlled architecture for wireless sensor networks, the final application scenarios and defines the project's QoS metrics.

Keywords:

Project Architecture, Requirements, Scenarios, Performance Metrics.

Executive Summary

This deliverable describes the project's application scenarios, extracts system requirements from them, and specifies the functional and physical architectures able to support performance control in wireless sensor networks (WSNs).

This document starts with a brief overview of the scope, the architecture and the performance requirements of the GINSENG project, as they were presented in Deliverable D1.1. A thorough analysis of the application scenarios outlines the special characteristics that WSNs require for performance and mission-critical environments. The lessons learned following the first software integration and evaluation (Milestone 2) in regards to the testbed area, hardware, and software are also presented. These lessons provide insights for finalizing the GINSENG scenarios, architecture and Quality of Service (QoS) metrics. QoS requirements consisted of two major categories: the information processing and the communication processing category, each of which are then further divided to sub categories. Based on the QoS classification, metrics were devised to specifically tackle GINSENG scenarios. The two most important metrics that are used to evaluate GINSENG performance are message delay and message reliability.

Then, the final GINSENG architecture is presented, divided into two sections: the physical and functional architecture. Based on first integration and evaluation results the GINSENG architecture was modified accordingly. Finally, the literature review gives details of the various related WSN architectures explaining their relevance to GINSENG.

List of Contributors

Name	Company/Affiliation	Address	Phone/Fax/E-mail
Vasos Vassiliou	UCY	Dept. Comp. Science, University of Cyprus, 75 Kallipoleos str. Nicosia, Cyprus	+357-22-892750
Zinon Zinonos	UCY	Dept. Comp. Science, University of Cyprus, 75 Kallipoleos str. Nicosia, Cyprus	+357-22-892687
Christiana Ioannou	UCY	Dept. Comp. Science, University of Cyprus, 75 Kallipoleos str. Nicosia, Cyprus	+357-22-892687
Marios Koutroullos	UCY	Dept. Comp. Science, University of Cyprus, 75 Kallipoleos str. Nicosia, Cyprus	+357-22-892687
Vasco Pereira	FCTUC	Department of Informatics Engineering, Pólo II, Pinhal de Marrocos, 3030-290 Coimbra, Portugal	+351 239790000
Jian Li	TUBS	Mühlenpfordtstraße 23 38106 Braunschweig Germany	+49-531-391-3265 jianli@ibr.cs.tu-bs.de
Wolf-Bastian Pöttner	TUBS	TU Braunschweig, IBR Mühlenpfordtstraße 23 38106 Braunschweig	+49 531 391 3265
Ricardo Silva	FCTUC	Dept. Eng. Inform., Pólo II, Pinhal de Marrocos, 3030-290 Coimbra, Portugal	+351 790000
James Brown	ULANC	j.i.brown@lancaster.ac.uk	+44 1524510406
Ben McCarthy	ULANC	b.mccarthy@lancaster.ac.uk	+44 1524510406

Document Approval

	Name	Address	Date
Approved by WP Leader	Vasos Vassiliou	vasosv@cs.ucy.ac.cy	1 Oct 2010
Approved by Project Coordination Committee Member SICS	Thiemo Voigt	thiemo@sics.se	1 Oct 2010
Approved by Project Coordination Committee Member ULANC	Utz Roedig	u.roedig@lancaster.ac.uk	1 Oct 2010

Table of Contents

ABSTRACT:	I
KEYWORDS:	I
EXECUTIVE SUMMARY	II
LIST OF CONTRIBUTORS	III
DOCUMENT APPROVAL	III
TABLE OF CONTENTS	IV
LIST OF FIGURES	V
LIST OF TABLES	VI
LIST OF ACRONYMS	VII
1. INTRODUCTION	1
1.1 SCOPE AND INITIAL ARCHITECTURE	1
1.2 QUALITY OF SERVICE (QoS) REQUIREMENTS.....	2
1.3 FIRST SOFTWARE INTEGRATION AND EVALUATION – LESSONS LEARNED	3
1.3.1 <i>Testbed area</i>	3
1.3.2 <i>Hardware</i>	4
1.3.3 <i>Software</i>	5
1.4 DELIVERABLE STRUCTURE	7
2. GINSENG SCENARIOS AND PERFORMANCE CONTROL METRICS	8
2.1 FRAMEWORK FOR DEFINING APPLICATION SCENARIOS	8
2.2 FINAL GINSENG APPLICATION SCENARIOS.....	8
2.2.1 <i>Production Monitoring Scenario</i>	9
2.2.2 <i>Production Control scenario</i>	11
2.2.3 <i>Production Monitoring and Control scenario</i>	14
2.2.4 <i>Pipeline Leak Detection scenario</i>	16
2.2.5 <i>Personnel Safety scenario</i>	18
2.3 ANALYSIS OF APPLICATION REQUIREMENTS	21
2.4 CLASSIFICATION OF APPLICATION SCENARIOS.....	21
2.5 FINAL GINSENG METRICS	23
2.5.1 <i>Performance Requirements of a WSN with QoS</i>	23
2.5.2 <i>GINSENG performance requirements</i>	25
2.5.3 <i>WSNs performance metrics</i>	26
2.5.4 <i>GINSENG Performance Metrics</i>	27
3. FINAL GINSENG ARCHITECTURE	30
3.1 GINSENG PHYSICAL ARCHITECTURE	30
3.2 GINSENG FUNCTIONAL ARCHITECTURE	32
3.2.1 <i>Rime</i>	33
3.2.2 <i>Mobility and Neighbor Discovery</i>	33
3.2.3 <i>Security</i>	33
3.3 RELATED WORK IN WSN ARCHITECTURE	34
3.3.1 <i>WirelessHART</i>	34
3.3.2 <i>Architecture in Refining Wireless</i>	35
3.3.3 <i>Architecture in LUSTER</i>	36
3.3.4 <i>Tenet Architecture</i>	37
3.3.5 <i>LiveNet Architecture</i>	37
3.3.6 <i>Architecture in Habitat Monitoring Wireless Sensor Networks System</i>	38
3.3.7 <i>System Architecture in an Assistive Environment</i>	39
4. CONCLUSIONS	40
REFERENCES	41

List of Figures

Figure 1 Initial GINSENG Functional Architecture	1
Figure 2: Channel analysis for 1dB antenna	4
Figure 3: Channel analysis for 9dB antenna	5
Figure 4 Production Monitoring Scenario	9
Figure 5 Production Monitoring Scenario	12
Figure 6 Production Monitoring and Control Scenario	14
Figure 7 Pipeline Leak Detection Scenario	16
Figure 8. Personnel Safety Scenario	19
Figure 9. Personnel Safety Scenario extension	19
Figure 10: Classification of application scenarios	22
Figure 11: Open-loop basic block diagram	22
Figure 12: Closed-loop basic block diagram	23
Figure 13 Taxonomy of QoS requirements	24
Figure 14 Obtaining metrics from requirements	27
Figure 15 GINSENG Physical architecture	32
Figure 16 GINSENG Functional Architecture	33
Figure 17. WirelessHART Protocol Stack	34
Figure 18. Network Architecture of Wireless Sensor Networks Application in Metal Refining Industry	36
Figure 19. The LUSTER Architecture	36
Figure 20. The Tenet Architecture	37
Figure 21. The LiveNet Architecture	38
Figure 22. System Architecture Used in Habit Monitoring	39
Figure 23. System Architecture in an Assistive Environment	39

List of Tables

Table 1 GINSENG scenarios overview and critical requirements	3
Table 2 Memory components size.....	5
Table 3: System Requirements for Production Monitoring Scenario.	10
Table 4: Solution Assumptions for Production Monitoring Scenario	11
Table 5: System Requirements for the Production Control Scenario.....	13
Table 7: System Requirements for the Production Monitoring and Control Scenario.....	15
Table 8: Solution Assumptions for the Production Monitoring and Control Scenario	16
Table 9: System Requirements for the Pipeline Leak Detection Scenario.....	17
Table 10: Solution Assumptions for the Pipeline Leak Detection Scenario	18
Table 11: System Requirements for Personnel Safety Scenario.	20
Table 12: Solution Assumptions for the Personnel Safety Scenario.....	20
Table 13 QoS Requirements of GINSENG application Scenarios.....	26
Table 14 Performance Requirements.....	26

List of Acronyms

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
JB	Junction Box
MAC	Medium Access Control
MIC	Message Integrity Code
PRR	Packet Rejection Ratio
QoE	Quality of Experience
QoS	Quality of Service
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
RTT	Round Trip Time
TDMA	Time Division Multiple Access
WP	Work Package
WSAN	Wireless Sensor and Actuator Networks
WSN	Wireless Sensor Networks
UMTS	Universal Mobile Telecommunications System

1. Introduction

This deliverable describes the final GINSENG application scenarios, extracts the network and operation requirements from them, and specifies the resulting functional and physical architectures able to support performance control in wireless sensor networks (WSNs). It provides important information for the GINSENG project and in particular for Work Packages 1, 2 and 3, whose aim is the development of topology and traffic control algorithms, the medium access control schemes and operating systems, and an integrating middleware respectively.

1.1 Scope and Initial Architecture

The GINSENG project targets performance controlled networks that have strong requirements on timeliness and reliability. To better understand these requirements a thorough analysis of application scenarios was performed, outlining the special characteristics that WSNs require for performance and mission-critical environments. These environments are not all necessarily in the Industrial-Manufacturing sector, but extend to Transportation, Military and Healthcare. Based on these studies, the specifications of the physical and functional architectures for performance control in wireless sensor networks are defined.

The physical architecture is the hardware and communication part of the oil refinery architecture. It presents a set of nodes, interconnections and RF communication upon which the network is finally constructed. Based on the scenarios specifications we can have two kinds of sensor nodes: static nodes which are the most common and mobile nodes which may be used in specific cases (the Personnel safety scenario). In addition, the nodes can be separated into sensor nodes, which are responsible to collect data or forward data, actuators, which receive data/commands and act accordingly, and to sink nodes, which are powerful sensor nodes, mainly in terms of energy, acting as a gateway to the back-end infrastructure. Wireless communication is used to route the data from the sensor nodes to the sink where the sink uses a wired communication to forward the data to the back-end infrastructure. The back-end infrastructure consists of all the powerful computers and servers like database, control and application servers. The data that are collected from wireless sensor nodes are processed in servers and decisions and statistics of the application data are created.

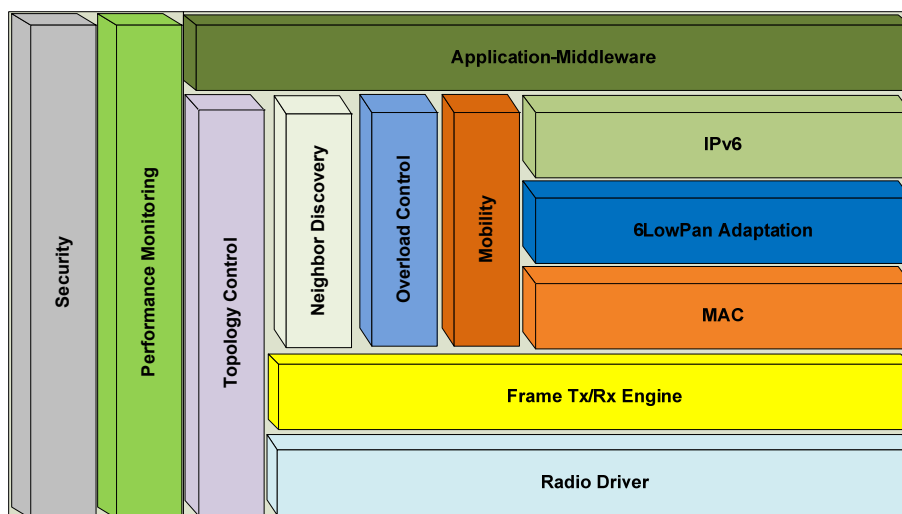



Figure 1 Initial GINSENG Functional Architecture

<p>INFSO-ICT- 224282</p>	<p style="text-align: center;">Deliverable D1.3</p> <p style="text-align: center;">Final GINSENG architecture, scenarios and quality of service measures</p>	
------------------------------	--	---

The initial functional architecture that was presented in Deliverable 1.1 defined how the different modules should collaborate in order to have a system that could accomplish the required performance. Figure 1 presents the initial functional architecture. Based on this architecture, IPv6 addresses are used and the 6LoWPAN adaptation layer was placed between the IPv6 and the MAC layers in order to reduce the size of IPv6 headers and make more room for payload in the 802.15.4 frames. 6LowPAN consists of a header compression scheme, a fragmentation scheme and a method for forming IPv6 link-local address on 802.15.4 networks.

The MAC layer is responsible for providing exclusive TDMA for channel access with a pre-dimensioned virtual tree topology and hierarchical addresses. It accepts packets from the upper layers which are queued and then transmitted by the radio at the appropriate time. To successfully accomplish these tasks it must interact with Topology control, Overload control, Performance Debugging and with the Contiki timer subsystem.

The Topology control module is responsible for establishing the methods by which nodes join or leave the network (in the case of GinMAC, a tree), advertising the presence of empty child positions so that new nodes can join and accepting or rejecting prospective children. Functionalities such as slot allocation, transmission power decisions, tree optimizations and maintenance are also responsibilities of the Topology control module.


The Performance monitoring module's target is to determine whether or not performance requirements are being met by the wireless sensor network. To accomplish this target, it must interface with several other elements, most notably the MAC protocol and Topology control.

Furthermore, intra- and inter-PAN mobility, neighbor discovery, security and overload functionalities are expected to be implemented as cross layer modules using information obtained mainly from the MAC and IPv6 layers.

1.2 Quality of Service (QoS) Requirements

In the course of the initial work in WP1 a categorization has been made regarding the main subsystems found in critical application environments. We have used the notation used in the Industrial-Manufacturing sector to differentiate them into **the indicator system, the semi-automatic control system, and the automatic control system**. The application scenarios of the GINSENG project were used to provide detailed information for the categorization of needs and QoS requirements of a performance controlled WSN. The result is a representative set of cases that fit into the three subsystems mentioned above and analyze the application's general needs, the types of components required and the value and the validity of each scenario with respect to the GINSENG project.

Based on the classification presented in Deliverable 1.1 we have derived 5 types of scenarios. These scenarios are: Production Monitoring, Production Control, Production Monitoring and Control, Pipeline Leak Detection and Personnel Safety. Each of these scenarios belongs to a subsystem and is summarized in Table 1. Based on each scenario's functionality, different quality of service requirements were defined and ranked, with message delay and message reliability being the two major performance requirements for all scenarios. In addition, some other quality of service requirements were considered, such as the energy efficiency, mobility, security and fault tolerance of the system.

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

Scenario	Target area	Sensor type	Deployment option	Control scheme	System	Data delivery model	Critical Requirements
Production Monitoring	Petrochemical industry	Wireless	static	open-loop	Indicator	continuous	Low Delay, Packet loss tolerance, Security
Production Control	Industrial – Petrochemical	Wireless, Actuator	static	closed-loop	Semi-automatic control	continuous, event-based	Low Delay, No packet loss, Security
Production Monitoring and Control	Petrochemical industry	Wireless, Actuator	static	open-loop, closed-loop	Automatic control	continuous, event-based	Low Delay, No packet loss, Security
Pipeline leak detection	Petrochemical - Leakage Tracking	Wireless, Actuator	static	closed-loop	Automatic control	continuous	Low Delay, No packet loss, Security
Personnel Safety	Petrochemical industry	Body	static, mobile	open-loop	Indicator	event-based	Low Delay, No packet loss, Security, Mobility

Table 1 GINSENG scenarios overview and critical requirements

1.3 First Software Integration and Evaluation – Lessons Learned

During the first software integration and evaluation we implemented and evaluated the Production monitoring scenario. During the deployment and operation we have been able to identify the practical difficulties of using the three basic components of the project platform: the actual test area, the hardware components, and the software. Each of these is discussed in further detail in the following sections.

1.3.1 Testbed area

As a first step we have deployed a wireless sensor network at the Petrogal refinery. Details of Petrogal's operations, the refinery, and the intended demonstration scenarios can be found in Deliverables D4.2 and D4.3. During this phase we faced some practical problems and limitations:

Even though the testbed area is not a critical or a classified area, we needed several authorizations just to start to install the Junction Boxes (JBs) and to get the signal from the Refinery's cable transmitters.

Because this area has a lot of metal structures and high voltage motors, the first antennas chosen were not powerful enough to transmit between nodes. To proceed with our tests we had to acquire new antennas.

We are working in a very corrosive and abrasive area and when maintenance work is performed in some acid tanks it is impossible (and dangerous) to stay in that area because a lot of hazardous vapors are released.

The corrosive and abrasive environment also affects the plastic cable ties that support the JB's and the antennas. A couple of weeks are enough to break these plastic components. The solution was to replace by metallic cable ties.

Very hard maintenance. Some JB's are not at ground level and to get access to these components we have to use a ladder. To reprogram a network of 15 nodes takes about 60 to 90 minutes.

After the deployment phase, we proceeded to obtain some experimental results. Initially the performance was unsurprisingly bad (all packets lost) and that was related to communication signal strength and interference. To further investigate this problem we performed spectrum analysis tests covering all possible channels (channels from 11 to 26) and identified the channel that allowed the establishment of communication between all nodes with the minimum noise. Based on the results, we concluded that inside the refinery there were some channels where the interference level was consistently high and communicating using those channels was impossible. We then selected the best channel (channel 16) to proceed with our evaluation plan. During the evaluation we used the same channel, i.e. we did not perform channel hopping.

1.3.2 Hardware

As the sensor nodes are installed inside Junction boxes (JB) the communication using the internal antenna is unfeasible. Due to that fact, the use of external antennas was necessary. We selected to test two types of antennas with 1dB and 9dB of gain. The test for selecting the right antenna type was combined with the channel selection test described above.

Both Figure 2 and Figure 3 show RSSI measurements on the left axis and Packet Rejection Ratio (PRR) on the right axis. The lower group of curves corresponds to RSSI reading and the curves towards the upper part of the figures refer to PRR results. One obvious conclusion is that the 9dB antenna raised the RSSI signal strength to values above -70dBm, making it a better candidate for the challenging radio environment of the refinery. The second observation, which relates more to channel selection, is that all channels exhibited some (even minor) packet loss, while channel 16 had zero packet loss in all cases.

Based on the results we concluded that operating on channel 16 using antennas with 9dB of gain would be the best choices.

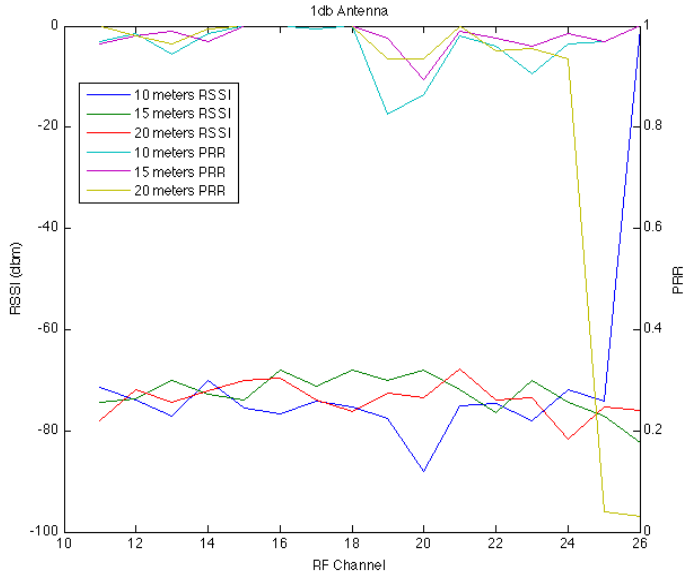


Figure 2: Channel analysis for 1dB antenna

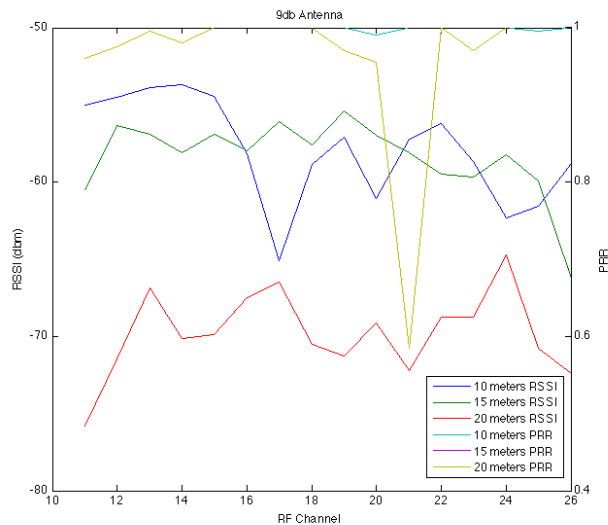


Figure 3: Channel analysis for 9dB antenna


1.3.3 Software

While trying to integrate the code of the different components we observed problems with the implemented code size and the available memory size of the Tmote Sky/TelosB nodes. In the future we expect the size of the GINSENG components to increase even more, since more intelligent topology control, overload control systems and a coffee filesystem enabled performance debugging will be implemented. Table 2 Memory components size Table 2 depicts the memory usage of the implemented system components.

Component	Size
Contiki Operating System with 6LoWPAN/IPv6	24KB
Contiki Operating System without 6LoWPAN/IPv6	11KB
GINSENG with Application	20KB
Clib	5KB
TelosB/TMote Sky Total Memory	48KB

Table 2 Memory components size

The selection of TmoteSky/TelosB motes restricts the available memory size to 48KB. Integrating the GINSENG code, some external libraries, and the full Contiki OS/6LowPAN stack resulted in 49KB, which exceeds the hardware capabilities. To find a solution to this problem we were forced to re-think about the initial GINSENG architecture and functionalities of the different components. We have concluded that we could manage to develop our ideas and implement our algorithms even without the use of IPv6. This understanding enabled us to disable the 6LoWPAN/IPv6 feature from the Contiki operating system in order to keep the code at 36KB, which is well within the memory limits and will allow for the projected expansions of GINSENG.

<p>INFSO-ICT- 224282</p>	<p>Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures</p>	
------------------------------	---	---

Despite this modification, the code is implemented in such way that 6LoWPAN can be re-enabled and supported at any time if a hardware platform with more available memory is chosen for future development.


During our initial tests it became clear that the use of an unreliable serial connection between the sensor network and the middleware is not acceptable. In addition, Contiki's defaults for the serial port are too slow to support the time constraints of the application scenarios. However, increasing the serial communication speed also increases the probability for broken symbols. Therefore, we designed and implemented a protocol that allows timely and reliable communication between the sink node and the sink PC over the serial line and still stays within the tight time bounds that a TDMA MAC creates. The software that handles that communication on the PC side is called Dispatcher (see level 3 of the final GINSENG architecture in Figure 15). This Dispatcher writes all data coming from the WSN to XML files and also enables multiple consumers (such as the middleware or the performance monitoring) to receive the information in different formats. In addition, the protocol supports CRC checking and retransmissions to ensure correct message delivery.

Beyond the specification of the technical communication interfaces (serial connection for the communication between sink node and dispatcher, xml file stream for the communication between dispatcher and middleware), the exchanged data format has to be specified at an early development stage to guarantee the seamless data management and transfer throughout sensor network, dispatcher and middleware. All software developers have to strictly adhere to the specified format, while format extensions and modifications have to be discussed by all affected partners and, above all, continuously documented to enable the according modification and extension of related software component interfaces. The first software integration showed that all project partners must be more careful to follow a clear format compliant development strategy that respects format and naming conventions. Only then, a consistent interface development between independent software components during the oncoming development can be guaranteed.

In order to reduce overhead caused by performance monitoring/debugging we embedded a small amount of data in application messages and store more comprehensive node information on the nodes themselves. Some of this data can be sent periodically to the sink or can be requested by it when required. Packet losses and delivery delay are key metrics in measuring performance for networks and detecting network anomalies. In the evaluation we were able to calculate packet losses and end to end delivery delay while keeping networking overhead very low using the embedded data. Additionally, we learnt a number of lessons whilst designing, implementing and evaluating the GinMAC during the first software integration and evaluation phase of the project. We learnt that the exclusive TDMA approach taken is adequate to ensure collision free communications within the oil refinery. Furthermore, the off-line dimensioning is suitable for the fairly static application domains that are present in the refinery when the channel conditions are good. However, when channel conditions degrade and interference does occur, it is important that additional transmission slots are provided for redundancy, so that retransmissions can take place within the specified delay bounds of the application. These additional slots have been integrated into the GinMAC TDMA epoch and can be switched off when not required.

After taking into consideration the issues and decisions outlined above, the evaluation of the system shows the following:

The system is reliable. The end-to-end packet losses are limited to 0.2%-0.3% which fulfils the requirements. The selection of the right communication channel is a significant factor for the packet delivery and therefore for the system reliability. In addition the antennas that were used increased the reliability of the system.

INFSO-ICT-224282	<p style="text-align: center;">Deliverable D1.3</p> <p style="text-align: center;">Final GINSENG architecture, scenarios and quality of service measures</p>	
------------------	---	---

The memory size limitation of the sensor motes was the main reason to remove the 6LoWPAN from our functional architecture. The evaluation of the integrated code run without any problems and the decision of not using 6LoWPAN did not affect the whole system.

Since the refinery environment is dynamic and with increased noise the decision of using a maximum distance between the nodes of around 20m helped us to construct a network connection tree with high link quality.

The selection of a tree-based topology (in Milestone 2 we used 3-2-1 tree) coupled with a careful deployment strategy were factors that increased the system reliability and stability. The constructed tree topology indeed managed to fulfill all the performance requirements that were defined in the GINSENG scenarios

The evaluation of dynamic topology control has shown that all the nodes are connected to the tree using the random tree selection method, with high probability. In addition, we had some tests where some nodes (1-2 nodes) were left outside the constructed tree. This confirmed our decision of implementing a maintenance/optimization procedure when using the dynamic topology control, as stated in Deliverable D1.2.

Since reprogramming the nodes requires a considerable time there is a need of finding a flexible solution either by connecting all the nodes to a personal computer using USB extensions (if possible due to USB extension length limitations), or re-programming over the radio channel. This functionality is important only during the development and testing phase and is not expected to be critical during actual deployment, where nodes will be pre-configured.


Given that we have run experiments for a long time and have never seen high packet loss, we can consider that we can use a single channel MAC protocol. This is of course desired as multi-channel MAC protocols are more complex and there is some additional latency and energy consumption for switching between channels.

Having in mind the time consuming procedure to acquire and re-deploy sensor nodes in the testbed area we can conclude that, we cannot switch to another platform different from Tmote Sky/TelosB despite the limited memory problem.

As a conclusion, the First Software Integration and Evaluation (Milestone 2) has instigated some changes in the initial project architecture. The two main changes are that we have made the use of IPv6/6LowPAN optional (due to memory considerations) and we have had to define a specific protocol for the reliable communication between the different in-filed data collection stations (sink nodes) and the Middleware gateway.

1.4 Deliverable Structure

The topic of Performance Controlled Applications in WSNs is discussed in Section 2. The section contains the final GINSENG Application Scenarios. The performance requirements and metrics to be used for the evaluation of the solutions proposed in GINSENG are also described in Section 2. Section 3 presents the final GINSENG architecture that is both a physical and a functional architecture that encompasses everything that was deemed important in all previous sections. Section 3 also includes related work, in the form of research projects which have similar objectives with GINSENG and where actual implementations have taken place. A critical comparison with the GINSENG objectives is provided. Finally, Section 4 concludes the deliverable.

INFISO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
-----------------------	--	---

2. GINSENG Scenarios and Performance Control Metrics

This section presents, in detail, the final set of performance critical application scenarios for the GINSENG project that cover many industrial sectors and application classes.

Starting with the definition of a common framework for scenario description, this section continues with the description of five scenarios. This section finally concludes with an analysis of the application requirements and a classification of the defined scenarios.

2.1 Framework for Defining Application Scenarios

The definition of each scenario comprises the items described below (partially adopted from [1])

Scenario Description: Short description of the scenario.

Scenario Schematic: A schematic representation of the examined case

Objects: Objects involved in the scenario, their functions and the information exchanged between the objects.

System requirements: High-level requirements of the system from the application technical point of view.

Solution Assumptions: Requirements of the system from the technical point of view. The Solution Assumption table provides an easy way to compare different scenarios based on the requirements. The system requirements are necessary for the design of the architecture.

Definition: A brief explanation of the requirements.

Level: A metric value of the specific requirement in the specific scenario.

2.2 Final GINSENG Application Scenarios


The description of the application scenarios included in this section takes as a reference the setting of the demonstration facility to be used in GINSENG.

The Petrogal oil refinery at Sines, Portugal is a complex industrial facility that includes a wide range of processing that needs careful monitoring and control of operations. There are currently 35,000 sensors and actuators in use in the refinery to perform monitoring of industrial operations such as leakage detection, measurement of pressure in the pipes, fluid levels and of the overall environment. The monitoring of the environment in a refinery provides essential information to ensure the good health of the refinery and its production processes. In the oil refinery three subsystems exist for the monitoring and control of the plant: ***the indicator system, the semi-automatic control system, and the automatic control system.***

Although this section outlines scenarios that are specific to the oil refinery, the three classifications of system presented above apply to any industrial plant. All plants have indicatory, semi-automatic control and automatic control systems and should have similar requirements as the systems in the refinery. Therefore, it should be possible to apply the solutions found for these scenarios to the more general cases.

The *indicator system* is used purely to provide the control center with information about status and faults of equipment and generic aspects of the environment. Within this system, information flows one way from the in-field sensors to the control center. It is assumed that data from sensors needs to arrive within a given time frame and a given reliability. Reliability and delay bounds in the indicatory system are not as strict as they are in the two systems described next. Some delay between measurement and display of information in the control center is acceptable.

The *semi-automatic control system* is used to control different aspects of the refinery. This system is similar to the previously described indicatory system but includes as well actuators. Upon data arrival from sensors an operator may decide to send commands to in-field actuators. Information sent to the actuators has to arrive with high reliability and within a given time frame.

<p>INFSO-ICT-224282</p>	<p>Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures</p>	
-------------------------	---	---

In this setting, information flows in both directions: from in-field sensors to the control center, and from the control center to actuators. In this system it is vital that data arrives at its intended destination timely and reliable. Operators require instant feedback from sensors as actuators are used to modify aspects of the environment.

The *automatic control system* is used to deploy automated control loops within the refinery. The system is similar to the previously described semi-automatic control system but commands to actuators are sent automatically upon receiving sensor data. Sensors and actuators in this system are part of an automated closed loop system. However, operators may be allowed to set parameters which influence the decision process. For example, an operator might configure a control loop such that a valve closes if pressure above an operator-defined threshold is measured. In this system it is vital that data arrives at its intended destination in a timely and reliable manner. In addition, the required delay and reliability bounds can be considered to be small.

2.2.1 Production Monitoring Scenario

2.2.1.1 Overview

Production Monitoring is an example of an indicatory system. Sensors are deployed throughout the plant to monitor various aspects of production to aid control center technicians on production decisions. This scenario concentrates on one small section of the plant that has a small number of pipes which contain materials that are pumped into a storage tank.

2.2.1.2 Scenario Description

All sensors within the refinery provide indicatory information to the control center so decisions can be made. The readings are used to provide general information to the control center technicians.

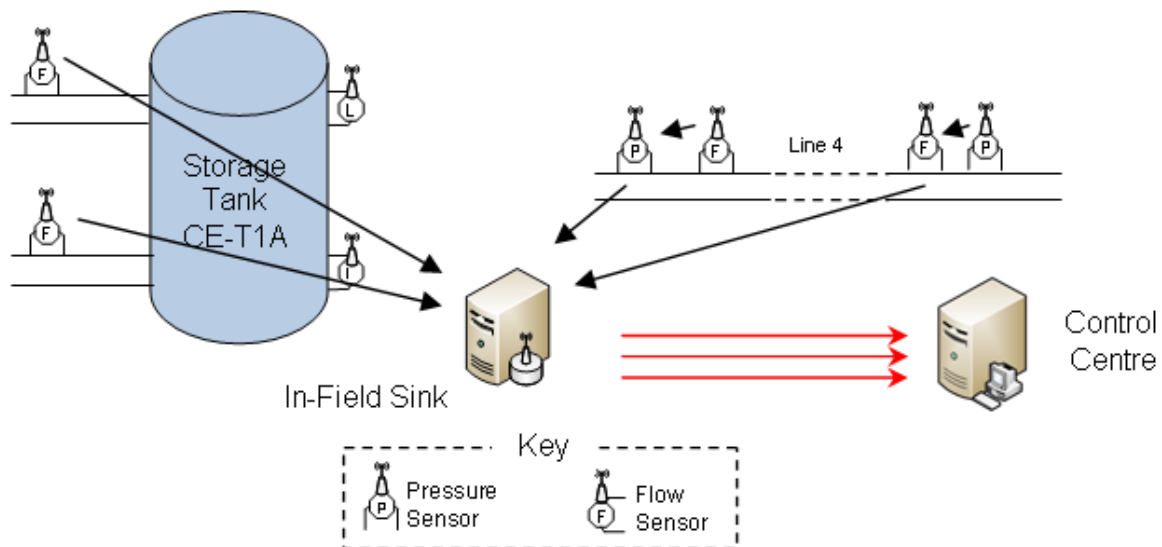



Figure 4 Production Monitoring Scenario

In this scenario sensors of three different types are used to provide information to the control center staff. As shown in Figure 4 there are two refinery objects within this scenario, Pipes, and Storage Tank. Raw materials are pumped through the pipes to various locations which include storage tanks. Two conditions are measured: pipe pressure, material and product flow:

Pressure is monitored within each pipe not only for safety reasons to keep pipe pressure within pipe tolerances but also to detect leakage and derive flow information. Pressure is

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

usually measured in Pascals (Pa). A typical pressure sensor has a Pmin and Pmax using 32bits as sample size. Pressure is typically sampled at a frequency of 1Hz to 0.1Hz.

Product Flow is monitored within each pipe to determine the rate at which product is flowing. Flow is measured in m³/h at a typical frequency of 1Hz to 0.1Hz.

Within this scenario, there are three types of network objects, the control centre, the data collection sink and the sensor node;

Control Centre – The control centre both requests and retrieves information from sensors nodes in the network via the in-field data collection station.

In-Field Data Collection Station - Distributed around the Refinery are a number of in-field collection stations (sinks) that accept data from nearby sensors. These sinks act as a gateway between the wireless sensor network and main control network to the control centre. These stations accept commands from the control centre and are then able to forward these commands towards the destined sensors within their domain. Likewise these stations cache data from sensors for collection by the control centre.


Sensor Nodes are used to record information in the field, which is transported to the sink. In this scenario there are three different types of sensors, pressure, flow and level status. Although some nodes are capable of contacting the sink directly, other nodes may be out of range and rely on relays. Every network object should be capable of acting as a relay node and forward traffic to and from the sink to ensure connectivity.

2.2.1.3 Scenario Requirements

This application scenario is an example of an indicatory system. The carried information is used to track faults and make production-based decisions. As in all indicatory systems, in order for information to be useful it must arrive at the sink and be forwarded to the control centre in a timely fashion. Specifically in this scenario, data should arrive within three seconds. Although packet losses should be minimized, this application can tolerate a small amount of packet loss. We have chosen an expected lifetime of around 200 days. Using TelosB nodes, this corresponds to a radio duty cycle (fraction of time that a system is in an "active" state) of about 2% since the lifetime of a TelosB with a radio duty cycle of 100% is around 4 days. Note that a 2% radio duty cycle is challenging in that it requires short slot times and does not allow for a high maximum number of retransmissions. Moreover, most existing deployments have much higher radio duty cycles. All sensors in this application are fixed so we do not assume any mobility. Table 3 presents the system requirements for this scenario.

Requirements	Definition	Level
Delay	The time bound of data delivery.	Data should arrive at the sink in 3 seconds.
Reliability	How important is data delivery.	99% of all messages must arrive in time.
Security	How secure should the system be?	Authentication; integrity; confidentiality
Mobility	Should mobility be supported?	No – all nodes are fixed in position.
Maintenance Interval	Time between maintenance schedules i.e. battery changes.	Nodes should have a duty cycle that would lead to a lifetime of around 200 days.

Table 3: System Requirements for Production Monitoring Scenario.

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

2.2.1.4 Solution Assumptions

A number of assumptions can be made in constructing a system to support this application. These assumptions are outlined in Table 4.

Assumption	Definition	Level
Device Class	The types of devices	Sensors
Mobility	Level of Mobility	None
Network Size	Maximum number of Nodes.	30
Topology Classification	Type of Topology	Tree
Hop Count	Maximum number of Hops nodes can reside from the sink.	4
On Node Processing	Level of on-node processing	Filtering of data to report.
Traffic Classification	Is all traffic time critical, none time critical, or mixed	Mixed
Traffic Characteristics	Type of Traffic	Periodic upstream, ad-hoc downstream.
Time Critical Traffic Direction	What direction are the time critical flows in?	Upstream
Non-Time Critical Traffic Direction	What direction are the non time critical flows in?	Downstream
Number of Time Critical Flows	How many time-critical traffic flows are there?	One per node upstream.
Traffic Characteristics	Type of Traffic	Periodic
Traffic Frequency	How often does each node generate a packet	≥ 3 seconds
Traffic Delay Bound	Time bound of the time critical traffic.	Upstream 3 seconds,

Table 4: Solution Assumptions for Production Monitoring Scenario

2.2.2 Production Control scenario

2.2.2.1 Overview

This scenario builds upon the last scenario which was purely indicative. In this scenario information that is received from the sensors is monitored by control center technicians who make decisions and alter various aspects of production. In addition to the sensors seen in the previous scenario, actuators are also included that can switch on pumps, mixers or close valves. This scenario is an example of the semi-automatic control system.

2.2.2.2 Description

Figure 5 depicts this application scenario illustrating the additional objects.

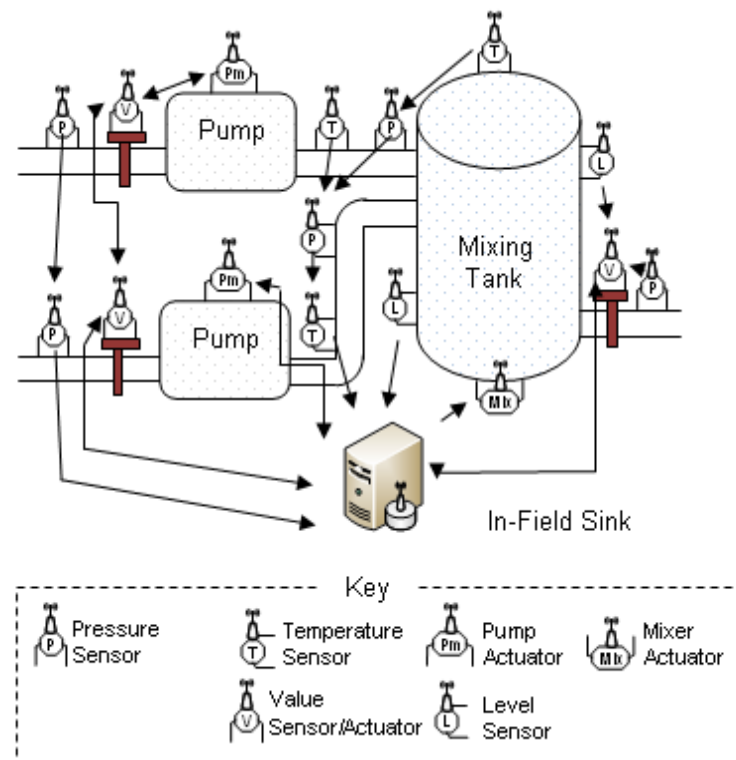


Figure 5 Production Monitoring Scenario

This scenario includes three sensor types measuring temperature, pressure and level. This information is sent to the control center which is monitored by technicians. In addition to the two types of network devices seen in the previous scenario, additional actuator devices are present. Technicians using this information can manage production by controlling three types of plant objects via actuators. These actuators are necessary to enable control of production. These actuators include:


Shut-off valves are integrated into pipes and are used to interrupt product flow during day to day operations and in the case of emergency.

Pumps can operate at different speeds to increase or decrease the pressure and thus flow of product through the piping system.

Mixing Tank can blend together their contents. When mixing is enabled the contents of the tank is blended and forced out into the output pipe for continued processing else were. Actuators control the speed at which the mixers operate.

2.2.2.3 Scenario Requirements

This application scenario is an example of a semi-automatic system. Information is carried from sensors to the control centre to allow technicians to make production based decisions. With the use of actuators technicians can alter aspects of production such as the speed of product flow which is controlled via a pump. As will all semi-automatic systems, information flows from sensors to the sink where it is forwarded to the control centre. Commands then flow from the control centre to actuators as and when instructed by control centre technicians. Specifically in this scenario data should arrive from sensors within two seconds and to actuators within one second. As alterations are happening to plant objects, no messages should be lost.

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

Similarly to the first scenario, all nodes are fixed so no mobility is assumed. Nodes should also be fault tolerant, minimizing the downtime and typical maintenance intervals should be yearly. Table 5 presents the system requirements for this scenario.

Requirements	Definition	Level
Delay	The Time bound of data delivery.	Data should arrive at the actuator within 1 second. Data from the sensors should arrive in 2 seconds.
Reliability	How important is data delivery.	No messages should be dropped.
Security	How secure should the system be	Authentication; integrity; non-repudiation; confidentiality
Mobility	Should mobility be supported?	No – all nodes are fixed in position.
Maintenance Interval	Time between maintenance schedules.	>6 Months

Table 5: System Requirements for the Production Control Scenario.

2.2.2.4 Solution Assumptions

A number of assumptions can be made in constructing a system to support this application. These assumptions are outlined in Table 6. There are a number of differences to the first scenario which include; two device classes and time bounded traffic in both directions.

Assumption	Definition	Level
Device Class	The types of devices?	Sensors and Actuators
Mobility	Level of Mobility	None
Network Size	Maximum number of Nodes.	30
Topology Classification	Type of Topology	Tree
Hop Count	Number of Hops nodes can reside from the sink.	4
On Node Processing	Level of on node processing	Filtering of data to report.
Traffic Classification	Is all traffic time critical, none time critical or mixed	Mixed
Traffic Characteristics	Type of Traffic	Periodic upstream, event-based or ad hoc downstream.
Time Critical Traffic Direction	What is the direction of the time critical flows?	Both
Non-Time Critical Traffic Direction	What is the direction of the non-time critical flows?	Downstream
Number of Time Critical Flows	How many critical traffic flows are there?	One per node upstream, one per actuator downstream.
Traffic Frequency	How often does each node generate a packet	2 < >5 seconds
Traffic Delay Bound	Time bound of the time critical traffic.	Upstream 2 second, Downstream 1 second

Table 6: Solution Assumptions for the Production Control Scenario

2.2.3 Production Monitoring and Control scenario

2.2.3.1 Overview

This application is similar to the semi-automatic system seen in the previous section but includes automatic processes. Automatic processes are closed loop systems such as the emergency system where actions are performed automatically in the presence of certain conditions.

2.2.3.2 Description

This scenario builds upon the previous and includes an additional sensor that monitors pump vibrations;

Vibrations are monitored on each pump to detect faults. Vibrations are measured by means of an accelerometer which measures the G force of each vibration with typical frequency of 50Hz.

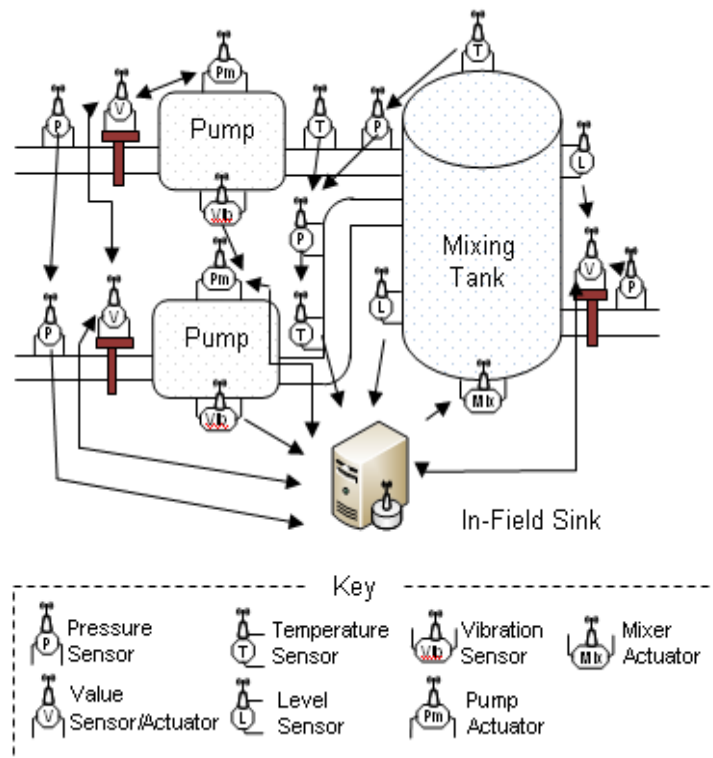



Figure 6 Production Monitoring and Control Scenario

Figure 6 depicts the application scenario showing all the plant objects in use. A number of automatic processes exist in this scenario. The first is pump health detection which can be determined by monitoring pump vibrations. When the health of a pump is deemed to have excessively deteriorated, the control center will automatically shut the pump down to prevent accident. The second process is the filling of the mixing tank; when fluid in the tank reaches a predetermined point the filling of the tank is automatically stopped by switching off the filling pumps. Lastly as in most pipes within the plant, when pressure is detected to be above a threshold, valves are closed to prevent damage to equipment further down the line.

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

2.2.3.3 Scenario Requirements

This application scenario is an example of an automatic system. Information is carried from sensors to the control centre where decisions are made and automatically acted upon. Where needed, commands will be sent to actuators in the field to modify an object's state. Specifically, in this scenario data should arrive from sensors within one second and then commands sent to actuators must also arrive within one second. The automatic system is the most critical system within the plant and all packets should arrive in time with no lost messages.

Similarly to the last two scenarios, all nodes are fixed so no mobility is assumed. Nodes should also be fault tolerant, minimizing down time and typical maintenance intervals should be yearly. Table 7 presents the system requirements for this scenario.


Requirements	Definition	Level
Delay	The Time bound of data delivery.	RTT should be less than 2 seconds.
Reliability	How important is data delivery.	No messages should be dropped.
Security	How secure should the system be	Authentication; integrity; non-repudiation; confidentiality
Mobility	Should mobility be supported?	No – all nodes are fixed in position.
Maintenance Interval	Time between maintenance schedules.	>6 Months

Table 7: System Requirements for the Production Monitoring and Control Scenario.

2.2.3.4 Solution Assumptions

A number of assumptions can be made in constructing a system to support this application. These assumptions are outlined in Table 8.

Assumption	Definition	Level
Device Class	The types of devices?	Sensors and Actuators
Mobility	Level of Mobility	None
Network Size	Maximum number of Nodes.	30
Topology Classification	Type of Topology	Tree
Hop Count	Number of Hops nodes can reside from the sink.	4
On Node Processing	Level of on node processing	Filtering of data to report.
Traffic Classification	Is all traffic time critical, none time critical or mixed	Mixed
Traffic Characteristics	Type of Traffic	Periodic upstream, ad-hoc downstream.
Time Critical Traffic Direction	What is the direction of the time critical flows?	Upstream and downstream
Non-Time Critical Traffic Direction	What is the direction of the non-time critical flows?	
Number of Time Critical Flows	How many critical traffic flows are there?	One per node upstream and downstream

INFSO-ICT-224282	<p style="text-align: center;">Deliverable D1.3</p> <p style="text-align: center;">Final GINSENG architecture, scenarios and quality of service measures</p>	
------------------	---	---

Traffic Characteristics	Type of Traffic	Periodic
Traffic Frequency	How often does each node generate a packet	1 to 2 seconds
Traffic Delay Bound	Time bound of the time critical traffic.	Upstream 1 second, Downstream 1 second

Table 8: Solution Assumptions for the Production Monitoring and Control Scenario

2.2.4 Pipeline Leak Detection scenario

2.2.4.1 Overview

Monitoring of oil pipelines is an important task for economical and safe operation, loss prevention and environmental protection from crude oil leakage or gas emission. Pipelines are currently surveyed for leaks by plant personnel on foot. Sensors and actuators could be deployed that monitor for leaks and then close valves to reduce emission. The application scenario is an example of the automatic system similar to the one presented in Section 2.2.3. This scenario has a specialized linear network structure where nodes can be a large number of hops from the sink.

2.2.4.2 Description

Pipeline leak detection is currently performed by dedicated employees who travel along the pipeline in order to observe the pipeline's condition, record the data written in some pressure instruments and report a possible leakage. This kind of leakage detection is highly subjective since it relies on each employee's capabilities, while it is only possible to observe just a small part of the pipeline, each moment. For example, if a leakage occurs at the beginning of the pipeline while the employee is at the end of the pipeline it may not be detected for some time. WSNs allow for a continuous (almost real-time) and more reliable pipeline monitoring and failure detection.

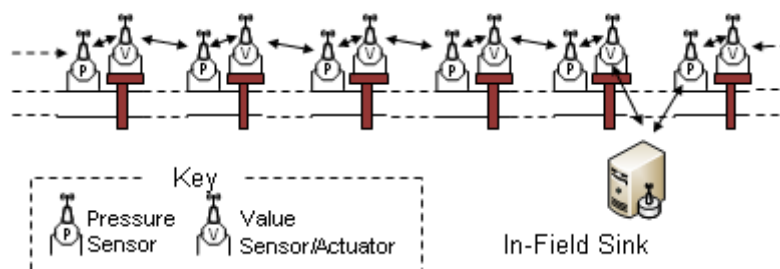



Figure 7 Pipeline Leak Detection Scenario

Figure 7 depicts the application scenario illustrating each of the plant objects. There are two classes of objects in this scenario, pressure sensors and shut-off valves;

Pressure is monitored within each pipe to detect leaks, a drop in pressure is usually indicative to a leak. Pressure is typically sampled at a frequency of 1Hz to 0.1Hz.

Shut-off valves are integrated into pipes and are used to seal the pipe before and after a leak to reduce the amount of product loss during a leak.

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

In this scenario, pressure at each sensor is sampled and transmitted to the control centre. Pipe pressure may drop for a variety of reasons, including the malfunction of a pump or the reduction of available product. If there is an unexpected drop in pressure from one particular point in the pipeline then a leak can be assumed. At this point the command centre will send commands to the relevant valves to close to reduce fluid loss. Closing the closest valves to the leak will further reduce fluid loss.

2.2.4.3 Scenario Requirements

This application scenario is a special example of an automatic system. Instead of nodes being distributed in the topology of a tree, nodes are in a linear topology spreading out in two directions along the pipeline from the sink. Similarly to the last example, information is sent from sensor to the control centre and then in certain circumstances, commands are automatically sent to actuators. Specifically in this scenario data should arrive from sensors within one second and then commands sent to actuators must also arrive within one second.


Requirements	Definition	Level
Delay	The Time bound of data delivery.	RTT should be less than 2 seconds
Reliability	How important is data delivery?	No messages should be dropped.
Security	How secure should the system be?	Authentication; integrity; non-repudiation; confidentiality
Mobility	Should mobility be supported?	No – all nodes are fixed in position.
Maintenance Interval	Time between maintenance schedules.	>6 Months

Table 9: System Requirements for the Pipeline Leak Detection Scenario.

2.2.4.4 Solution Assumptions

A number of assumptions can be made in constructing a system to support this application. These assumptions are outlined in Table 10.

Assumption	Definition	Level
Device Class	The types of devices?	Sensors and Actuators
Mobility	Level of Mobility	None
Network Size	Maximum number of Nodes.	30
Topology Classification	Type of Topology	Linear
Hop Count	Number of Hops nodes can reside from the sink.	10
On Node Processing	Level of on node processing	Filtering of data to report.
Traffic Classification	Is all traffic time-critical, none time-critical or mixed	Mixed
Traffic Characteristics	Type of Traffic	Periodic upstream, adhoc downstream.
Time Critical Traffic Direction	What direction are the time-critical flows in?	Upstream
Non-Time Critical Traffic	What direction are the non time-	Downstream

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

Direction	critical flows in?	
Number of Time Critical Flows	How many time-critical traffic flows are there?	One per node upstream.
Traffic Characteristics	Type of Traffic	Periodic
Traffic Frequency	How often does each node generate a packet	1 minute
Traffic Delay Bound	Time bound of the time-critical traffic.	Upstream 1 second, Downstream 1 second

Table 10: Solution Assumptions for the Pipeline Leak Detection Scenario

2.2.5 Personnel Safety scenario

2.2.5.1 Overview

Employees sometimes enter hazardous areas of the refinery and may pass out. Using orientation and heart or pressure monitoring sensors attached to employees, their condition can be monitored and alarms can be signaled when an employee is lying on the floor. This scenario is a specialized case of the indicatory system which includes nodes that are mobile.

2.2.5.2 Description

There are many hazardous areas of the plant that need regular maintenance. One example is the cleaning and condition assessment of storage tanks. In this example maintenance crews enter these storage tanks to first clean them so that their condition can be assessed and repairs made where necessary. Tanks are very hazardous environments and typically contain a toxic atmosphere and residues of their previous contents. It is important to monitor the health of employees that enter such environments to make sure they remain conscious. Sensors can be attached to these employees to monitor their orientation and send this information to the control center. When a person's orientation is horizontal for a period of time (indicating a fall or unconsciousness) an alarm can be signaled at the control center to notify health and safety staff of a possible emergency. Figure 8 depicts this application scenario.

Surrounding the tank that is being cleaned are the usual sensors deployed for production monitoring as seen in Section 2.2.1. As the mobile worker moves around the tank, orientation messages are sent from the sensor to the sink forwarded by intermediate nodes. Data may be sent via different intermediate nodes based on the location of the mobile worker.

This scenario contains an additional sensor that has not been seen in the previous applications;

Orientation of the mobile worker is monitored by trip sensors. This enables fallen/unconscious workers to be detected. Orientation is sampled at a frequency of 0.2Hz.

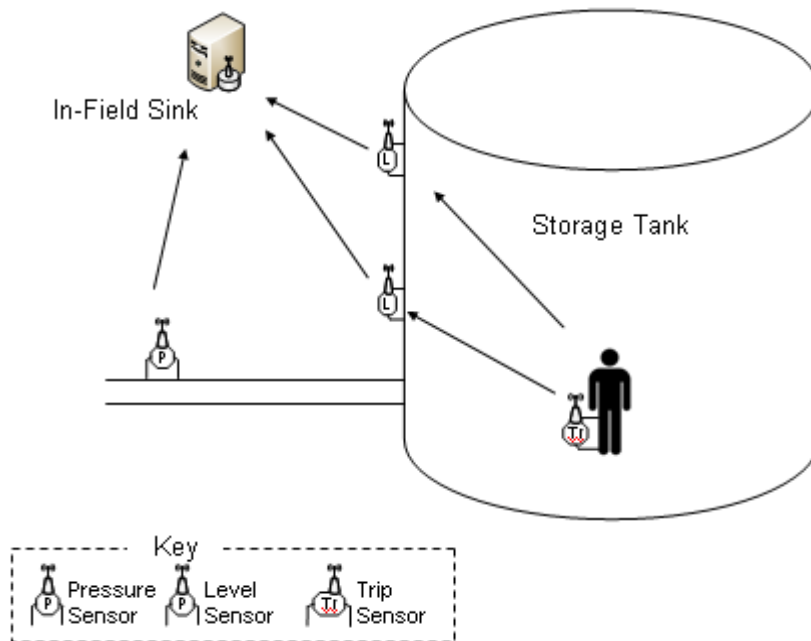


Figure 8. Personnel Safety Scenario

A possible extension of this scenario may be the following, where the personnel move from one tank to another:

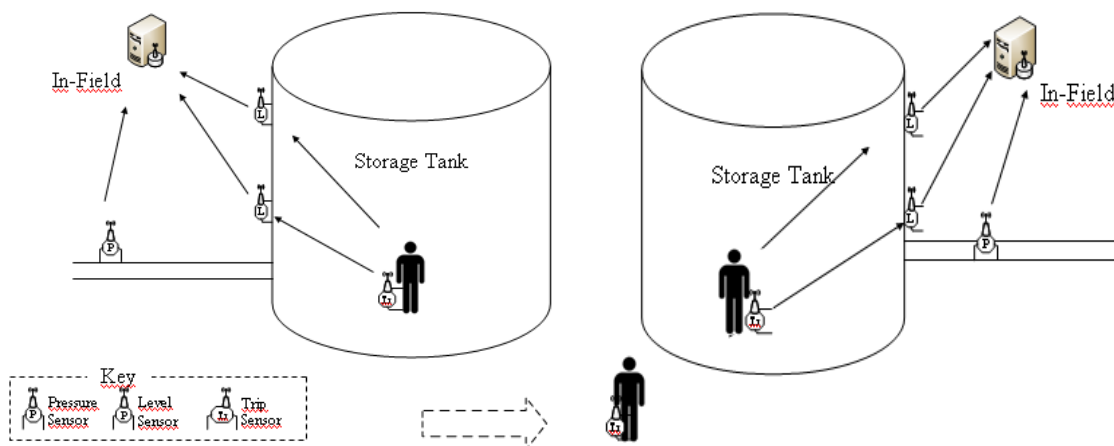



Figure 9. Personnel Safety Scenario extension

2.2.5.3 Scenario Requirements

This application scenario is a special example of the indicatory system. In addition to the objects in the scenario presented in Section 2.2.1, mobile workers are also present. In terms of the plant network, these mobile workers are temporary objects that only exist for a short period of time (time it takes to complete a specific job). Mobile workers are augmented with orientation sensors (and/or other sensors) that send information to the control centre. Similarly to other scenarios, information must arrive at the control centre within five seconds. Although packet losses should be minimized, this application can be tolerant to a small amount of loss.

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

Similarly to all other scenarios, security is important and methods should be in place to ensure that only authenticated nodes can send packets that arrive at their destination untouched. In this scenario sensors attached to workers are mobile and may attach to the network at different points over time. Nodes should also be fault tolerant; however in this application nodes can have more frequent battery replacement than nodes in other applications. Table 11 presents the system requirements for this scenario.

Requirements	Definition	Level
Delay	The Time bound of data delivery.	Data should arrive at the in-field sink in 5 seconds.
Reliability	How important is data delivery.	No messages can be dropped.
Security	How secure should the system be	Authentication; integrity; non-repudiation; confidentiality
Mobility	Should mobility be supported?	Yes – Mobile Workers.
Maintenance Interval	Time between maintenance schedules.	>6 Months for maintenance, >1 week for battery recharging


Table 11: System Requirements for Personnel Safety Scenario.

2.2.5.4 Solution Assumptions

A number of assumptions can be made in constructing a system to support this application. These assumptions are outlined in Table 12.

Assumption	Definition	Level
Device Class	The types of devices?	Sensors
Mobility	Level of Mobility	Yes – Mobile Workers
Network Size	Maximum number of Nodes	30
Topology Classification	Type of Topology	Tree
Hop Count	Number of Hops nodes can reside from the sink	4
On Node Processing	Level of on node processing	Filtering of data to report.
Traffic Classification	Is all traffic time-critical, none time critical or mixed	Mixed
Traffic Characteristics	Type of Traffic	Periodic upstream, adhoc downstream.
Time Critical Traffic Direction	What direction are the time-critical flows in?	Upstream
Non-Time Critical Traffic Direction	What direction are the non time-critical flows in?	Downstream
Number of Time Critical Flows	How many time-critical traffic flows are there?	One per node upstream.
Traffic Characteristics	Type of Traffic	Periodic
Traffic Frequency	How often does each node generate a packet	> 5 seconds
Traffic Delay Bound	Time bound of the time-critical traffic	Upstream 5 seconds,

Table 12: Solution Assumptions for the Personnel Safety Scenario

<p>INFSO-ICT- 224282</p>	<p style="text-align: center;">Deliverable D1.3</p> <p style="text-align: center;">Final GINSENG architecture, scenarios and quality of service measures</p>	
------------------------------	--	---

2.3 Analysis of Application Requirements

Sections 2.2.1 to 2.2.5 have presented a number of different application scenarios discussing the requirements and assumptions of each. Before a system can be designed to support such applications, these requirements/assumptions must be combined to produce a single coherent list. This subsection combines these assumptions of how each application would operate, adding additional detail to produce a definitive list. Application assumptions are grouped into three areas, general, topology and traffic.

General: The network will be made up of resource constrained embedded systems. Nodes will be deployed in predetermined positions and will be configured with a number of parameters by maintenance staff on deployment. Nodes will be mostly physically fixed in position in adequate range of other nodes to allow reasonably error-less communication.

Topology: The WSN topology can be modeled as a tree. A reasonable small number of nodes can be expected ($N < 30$) of which N is direct proportional to the required communications delay bound; the smaller the required delay, the smaller the N . Larger networks can be divided into smaller networks with additional in-field data collection stations (sinks). The maximum number of hops H can be expected to be small ($H < 5$) while most nodes will be within one or two hops from the sink. Only few nodes will need to be placed at the maximum hop distance. The majority of nodes will be static with no mobility; however nodes may appear to be mobile by switching positions in the tree when capacity is available. It can be assumed that the network contains far more sensor than actuator nodes.

Traffic: Nodes might report data frequently with relatively high rate (up to once per second). However, the packet payload can be considered to be quite small (< 10 bytes). Data is expected to reach the sink within a given time bound T_s . The time bound can be expected to be in the order of a few seconds (bounds as small as one second must be considered). The inter-arrival time of messages sent from nodes to the sink should be greater or equal to T_s ; messages sent more frequently may not arrive within these time bounds. Commands sent from the sink to actuators must arrive within a given time bound T_a . The requested time bound can be considered to be in the order of a few seconds (a bound as low as one second might be required). Similarly to messages sent from node to sink, commands sent to actuators must also be limited to an inter-arrival time greater than T_a to enable this time bound to be met. The sink might also send commands to sensor nodes to set sampling frequencies and to issue other configuration commands, these may be sent via broadcast and are treated as best effort, secondary to actuator commands. Many but possibly not all of these sensor command messages will be tolerant to delay. All communication sent between nodes within the network should travel via the sink.

2.4 Classification of Application Scenarios

In this section, we classify the scenarios of the previous section on the basis of common characteristics exhibited by the involved applications. The proposed classification spans across three directions: (a) deployment options (e.g. static, mobile, hybrid), (b) control loop settings (closed-loop, open loop), and (c) data delivery models. This classification will be taken into account when dealing with system requirements, in order to provide a general understanding of the requirements posed by each class. Further on, our system's architecture will be designed on the basis of these requirements in order to satisfy the needs of all application classes.

First, we classify application scenarios based on sensor network deployment. Within each deployment option, further classification can be done on the basis of the control schemes and then on the basis of the different data delivery models found in WSNs. These classifications are shown in Figure 10.

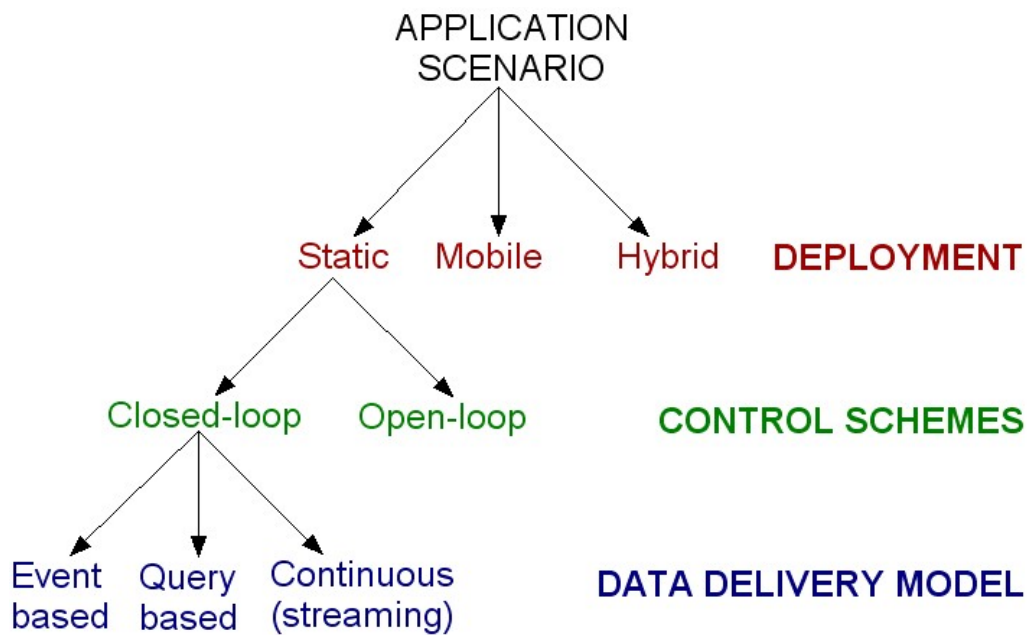


Figure 10: Classification of application scenarios

Basically, there are three deployment options. Firstly, a sensor network can be deployed in a static manner involving solely fixed sensor nodes. Alternatively, the whole network may involve only mobile nodes. Finally, the sensor network topology may consist of both fixed and mobile sensor nodes (hybrid deployment). All of our case scenarios belong to the static deployment except the Personnel Safety scenarios where the deployment belongs to the hybrid category.

Within each one of those deployment options, application scenarios can be further classified into closed-loop and open-loop applications. In an open-loop application, sensor nodes send the sensed data to a dedicated sink node. No feedback action is performed in the system (see Figure 11). This means that the system does not involve an actuator node or a reverse path (sink-to-node) functionality to alter the input of the system.



Figure 11: Open-loop basic block diagram.

The Production Monitoring and Personnel Safety scenarios belong to open-loop applications. On the other hand, closed-loop applications use feedback to control the output of the system. Often in this kind of applications, an actuator node or procedure is involved as shown in Figure 12.

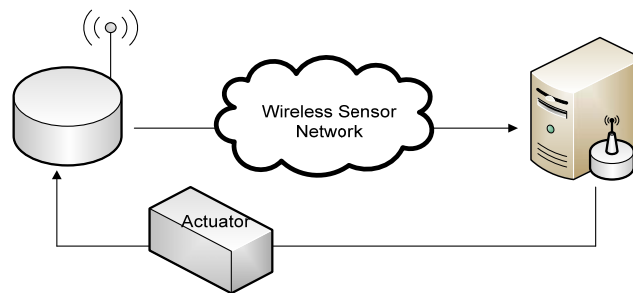


Figure 12: Closed-loop basic block diagram.

The scenarios of Production Control, Production Monitoring and Control and Pipeline Leak Detection belong to closed-loop applications.

Furthermore, application scenarios are further classified on the basis of the three basic data delivery models found in WSNs, namely, (a) event-based model, (b) continuous (or streaming)-based model, and (c) query-based model. An event-based traffic model is involved in applications which sensor nodes report data to a dedicated sink node only when certain events occur. In applications which sensor nodes are set to report data at regular time intervals, a continuous-based traffic model is applied. Finally, the query-based traffic model is involved when data is pulled by the sink on-demand, when sensor nodes are triggered by queries. The scenarios of Pipeline Leak Detection and Production Monitoring belong to the continuous model where the Personnel Safety belongs to event-based model. The other two scenarios, Production Control and Production Monitoring and Control belong to both continuous and event-based models.

2.5 Final GINSENG Metrics

GINSENG performance can only be evaluated by using specific metrics - fully specified values resulting from the measurement of a quantifiable reality. In this section, an overview of the performance requirements of a performance controlled WSN will be given. The specific performance requirements of the GINSENG project will also be stated and translated into metrics.

2.5.1 Performance Requirements of a WSN with QoS

While the initial approach to WSNs did not target performance, the need to fulfill the demands of a new range of applications and scenarios like the ones existing in industrial plants and health monitoring, forced a new approach. Early WSNs were focused in the random placement of sensors in an uncontrolled environment, relying on self-configuration and high levels of redundancy to achieve robustness, with no performance assurances. The new controlled performance WSNs, like GINSENG, must guarantee QoS to enable application-specific performance targets, which can only be assessed if correct metrics are used. While QoS in traditional networks has been extensively researched, the same did not happen in WSNs. The reason is that WSNs are very different from traditional networks, raising the definition and measurement of QoS to a higher complexity level. In traditional networks, QoS refers to the assurance that the network can provide in an end-to-end basis. The QoS requirements of users connected to a data network are a statement of the level of quality the users expect to get from the applications they run or from the services they subscribe. Some of the most important QoS parameters that can be measured and monitored are network availability, bandwidth, packet delay, delay variation and packet loss. However, these parameters are not enough to fulfil

WSNs needs. WSNs have several limitations like processing power, energy, storage, communication capabilities, bandwidth, dynamic topology, and non-uniform traffic, to name but a few, which make the QoS support in such networks much more challenging. Furthermore, WSNs QoS requirements depend heavily on the application that is used. While some applications may require real-time data, as video-surveillance applications where actions must be taken in real-time, others may only require a minimum coverage and can tolerate low packet loss, as in environmental monitoring.

In order to have an overview of the requirements of a WSN with QoS, a taxonomic approach was taken. The requirements tree includes the QoS parameters that were found necessary to characterize the quality and the performance of the network. The taxonomic tree that classifies the QoS requirements and aggregates all the requirements that were found to be necessary to fully qualify the performance needs of WSNs is depicted in Figure 13. This tree includes two groups in the first level - Information and Communication processing. The first level reflects the fact that sensor networks are more than communication systems as they acquire, process, and provide information and knowledge from the physical world. The second deals with communication issues.

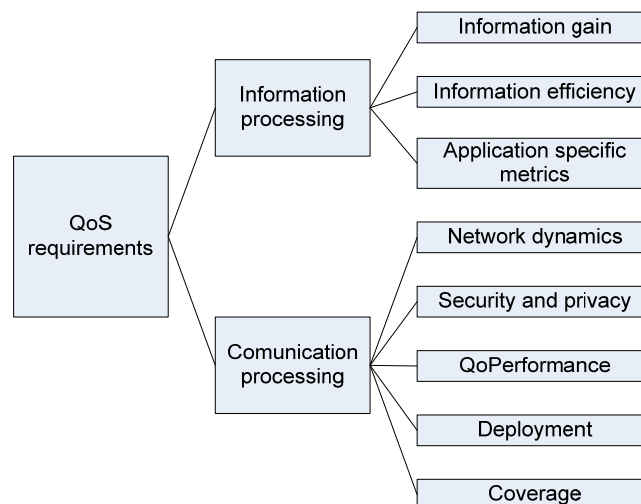


Figure 13 Taxonomy of QoS requirements

Next, a list of all the dimensions proposed is briefly explained:

Information gain – specifies the amount and the quality of the information obtained from the data sensed;

Information efficiency – specifies parameters such as energy and resource efficiency in obtaining the information; Application specific metrics – addresses parameters such as false alarm ratio, target classification correctness and target localization error;


Network dynamics – includes the type of mobility associated to the nodes, such as gateway/sink mobility, node mobility, user mobility and phenomenon mobility;

Security and privacy – specifies properties such as authentication, non-repudiation, confidentiality, integrity, access control, availability and accountability;

QoS Performance – includes parameters such as accessibility/availability, reliability, accuracy, latency and bandwidth;

Deployment – defines the deployment strategy used, ranging from random to deterministic deployments;

Coverage – specifies the network in terms of space

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

The taxonomic tree obtained encapsulates application specific and network parameters. By using and combining the proposed dimensions we believe that a better characterization of the available QoS provided by a WSN will be possible.

2.5.2 GINSENG performance requirements

In order to understand the specific GINSENG performance requirements, the previously presented taxonomy was applied to the scenarios presented in Section 2.2 (A) Production Monitoring, (B) Production Control, (C) Production Monitoring and Control, (D) Pipeline Leak Detection and (E) Personal Safety.

Table 13 shows the application of the proposed taxonomy.

Scenario	Classification	
A	Info gain	Frequency of packet generation >5s; packets < 10bytes
	App. Specific	On node processing for filtering of traffic
	Net dynamics	Static
	Security	Authentication; integrity; confidentiality
	QoPerformance	Delay < 3s; low packet loss
	Deployment	Deterministic
	Coverage	Lifetime >6 months
B	Info gain	Frequency of packet generation [2, 5]s; packets < 10bytes
	App. Specific	On node processing for filtering of traffic
	Net dynamics	Static
	Security	Authentication; integrity; non-repudiation; confidentiality
	QoPerformance	Delay < 2s (upstream), <1(downstream); no packet loss
	Deployment	Deterministic
	Coverage	Lifetime >6 months
C	Info gain	Frequency of packet generation [1, 2]s; packets < 10bytes
	App. Specific	On node processing for filtering of traffic
	Net dynamics	Static
	Security	Authentication; integrity; non-repudiation; confidentiality
	QoPerformance	RTT<2s; no packet loss
	Deployment	Deterministic
	Coverage	Lifetime >6 months
D	Info gain	Frequency of packet generation >1s; packets < 10bytes
	App. Specific	On node processing for filtering of traffic
	Net dynamics	Static
	Security	Authentication; integrity; non-repudiation; confidentiality
	QoPerformance	RTT<2s; no packet loss
	Deployment	Deterministic
	Coverage	Lifetime >6 months
E	Info gain	Frequency of packet generation >5s; packets < 10bytes
	App. Specific	On node processing for filtering of traffic
	Net dynamics	Sensor mobility (workers)
	Security	Authentication; integrity; non-repudiation; confidentiality
	QoPerformance	RTT<5s; no packet loss
	Deployment	Deterministic
	Coverage	Lifetime >6 months

Table 13 QoS Requirements of GINSENG application Scenarios

Notice that no clear metrics or values for them are shown for all parameters, and not all parameters are shown for every scenario as they may not apply. The table presented only focuses the needs of QoS from the GINSENG scenarios.

Through the literature review and related scenarios previously outlined, we have identified a set of performance requirements which will be specifically addressed in GINSENG. These performance requirements are divided into two global priority groups as shown in Table 14.

1st Priority Functional Requirements
Message Delay
Message Delivery Reliability
2nd Priority non-Functional Requirements
Fault Tolerance
Energy Efficiency
Security
Limited Mobility

Table 14 Performance Requirements

The top priority group deals with performance issues and responds to the necessity that the sensor network can deal with high priority traffic and that accuracy and delivery of data can be guaranteed. Examples of high priority traffic are alarms generated by sensor nodes in critical areas of the refinery as well as worker health problems while working in hazardous areas. Time constraints are essential and must be ensured due to the needs of critical industrial environments.

The second priority group identifies additional areas of interest, such as security, fault tolerance (including connectivity), limited mobility and energy efficiency, which are important, but not necessarily essential, to the operation of a performance controlled network.

2.5.3 WSNs performance metrics

The former taxonomic analysis specified the requirements that define completely (or as completely as possible) the performance of WSNs. Each requirement stated must now be translated into a usable metric that measures one or more of the available parameters. Nevertheless, the QoS requirements taxonomy presented does not imply that every requirement must lead to the measurement of a distinct parameter, it only indicates that there should be a quantification of the performance of each requirement, measured from the available parameters.

Metrics can be calculated using two different approaches. Data received at the sink node may contain metrics directly obtained from nodes or metrics can be calculated at the sink node indirectly. To distinguish these two scenarios, metrics can be divided in explicit and inferred. Explicit metrics are obtained directly from the nodes (e.g. energy level) and sent to the sink/gateway node that may further treat them. Inferred metrics are obtained at the sink node indirectly, by analyzing or calculating other data received (e.g. active nodes may be detected on receiving data collected by those nodes). Also, the parameters to be measured can be either individual or collective, in order to enable an accurate view of the entire network performance (Figure 14). Collective parameters are a new type of parameter that results from the fact that its

calculation involves the use of values from more than one node [2]. As an example, in a data-gathering application, collective packet loss would be the sum of individual packet losses from all the nodes that send data in a specified time, and collective delay the difference between the time the data was obtained and the time when the last packet concerning that period of time, from all targeted nodes, arrived to the sink.

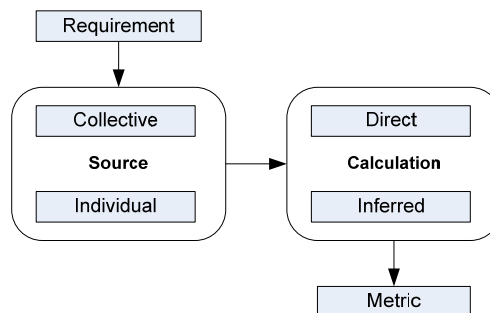


Figure 14 Obtaining metrics from requirements


Whereas different requirements involve different metrics, different metrics may use the same parameters. As an example, delay can be used to calculate network latency or be part of a security metric, for example regarding intrusion detection. Reusing parameter values when possible ensures that minimum bandwidth is used by performance control data. Also, when calculating the metric itself, mainly when in the presence of collective parameters, one must have present that in general the cost of communication is greater than the cost to execute inboard calculations.

The measurements will be done by a monitoring tool, in two distinct phases - an initial deployment phase and a normal operation phase. In the first, monitoring is necessary to guarantee that the network is working as specified with the planned performance targets and that the protocols implemented are functioning properly. In the second, monitoring is used to evaluate in real-time the network performance targets. In this phase network health is measured (evaluates if the nodes are working and if connectivity exists), performance is measured, all functionalities are evaluated and all necessary corrective actions are triggered. Also, when performance targets are not being met by the network, debugging is necessary. Debugging is a process of discovering the cause of a failure in the network and initially uses monitoring to detect the anomaly. Debugging is the subject of WP2, Task 2.4.

2.5.4 GINSENG Performance Metrics

Based on the priority performance requirements for the GINSENG project, some metrics are proposed. Metrics are shown in tables together with a preferred place of calculation and phase. A metric whose place of calculation is the sink enables the saving of node energy by using data included in network messages (the fields used are defined in D4.3). These metrics should be the majority. A metric with the place of calculation referred as node is processed in each node (or only in specified nodes) and periodically sent to the sink. These metrics are necessary to obtain information that cannot be calculated at the sink. The period used by each node to send its information to the sink should be configurable. Finally, the phase states the operation phase of the network under which the metric should be preferentially obtained – Normal operation or Deployment phase. In deployment phase, test traffic may be necessary.

The first priority functional requirements outlined for the GINSENG project are Message Delay and Message Delivery Reliability.

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

Message Delay metrics must measure the time taken for packets to travel from one point of the network to the other. This value will be obtained by calculating, at the destination, the time spent by the packet between the two specified nodes. A lightweight time synchronization scheme between nodes is presented in section 3.3.1 of Deliverable D2.1. **Message Delivery Reliability metrics** will mainly result from the measure of packet transfer rate and packet loss in the network. The first relates to the ability of the network to transfer the necessary amount of data from one point to another in a given time period. Data transfer rates can be measured in the link layer or in the IP layer, by measuring how many bits can be transmitted in a defined time period. The value of packet loss can be estimated by the injection of pre-defined traffic in the network at defined time intervals, by extrapolating the loss of packets in existing sequential transmission that use numbered packets, or just by detecting the absence of due timely packets. Any of the above methods can be selected for implementation, based on the restrictions in energy and bandwidth of a particular WSN. In GINSENG corrupted packets will be assumed as lost packets


Proposed delay and reliability metrics:

Metric	Place of calculation	When
End-to-end individual delivery delay	Sink	Normal operation
End-to-end collective delivery delay	Sink	Normal operation
Individual packet loss	Sink	Normal operation
Average packet loss	Sink	Normal operation
Total packet loss	Sink	Normal operation
Average delay variation	Sink	Normal operation
End-to-end individual delivery delay (sink to actuator)	Node	Normal operation
Packet loss (sink to actuator)	Node	Normal operation
Average delivery delay per hop	Node	Normal operation
Average RSSI per node in a single hop	Node	Normal operation
Delay variation per node	Node	Normal operation
Network bulk capacity	Sink	Deployment

Fault tolerance includes key issues such as network connectivity and node redundancy. Connectivity metrics can be achieved in a first phase by the implementation of periodic messages stating that nodes are alive. This metric will be Boolean, stating that there is connectivity between the two nodes addressed or not. As connectivity is WSNs may change due to transient factors, like interference, a time must be defined in which at least one message from the specified node must be received. To save resources, nodes will only produce a specific message stating that they are alive if they have no other traffic to send. All traffic sent during the specified time interval between the specified nodes will state that the connectivity exists. In a first approach the connectivity status is measured between regular nodes and the sink. Together with Boolean connectivity, a measure of the connectivity quality is also addressed. This metric states the quality of the connectivity to the nodes and is calculated from parameters like RSSI and packet loss rate.

Metric	Place of calculation	When
Connectivity	Sink	Normal operation
Average RSSI from node to sink	Node	Normal operation

Energy Efficiency - Jiang et al. [3] show that the unique characteristics of sensor network applications make it difficult to measure the energy consumption of sensor nodes. The authors

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

develop a hardware-based mechanism for measuring the energy consumption of sensor nodes that they expect to have a per-unit cost similar to that of the sensor node. It, therefore, incurs a significantly higher cost than software-based energy estimation. The Contiki operating system provides a software-based power profiling mechanism [4]. The mechanism runs directly on the sensor nodes and provides real-time estimates of the current energy consumption. The target platforms are low-end sensor nodes, such as the ESB and the Tmote Sky. The mechanism uses an intentionally simple linear model that is easy to implement and add to existing sensor node operating systems. No modifications to existing applications or network protocols are required.

Metric	Place of calculation	When
Immediate energy consumption	Node	Normal operation
Remaining battery time	Node	Normal operation
Energy efficiency	Sink	Normal operation


Security metrics will be derived by comparing obtained measurements to a predetermined baseline, considering several security related measurements taken over time. The usage of security metrics will allow us to discern the effectiveness of various components on security, and also their contribution to security for the adopted architecture as a whole. This applies, for example, to the decision of selecting appropriate cryptographic components and appropriate usage and configuration parameters for those components. Practical deployment aspects, such as type of authentication and authentication algorithms, key sizes, and initial and running configurations parameters, including processor and memory allocation to security, will have to be derived from well defined security metrics.

The definition of security metrics applicable to environments where performance is critical will, in general, consider three fundamental aspects: the need to measure the assets to protect, the threats against the network or specific critical nodes, and the level of vulnerability of specific network elements. Some aspects of the assets may be difficult to quantify, but their evaluation in critical environments allows to us to motivate the definition and application of specific security mechanisms and procedures, accordingly to pre-defined security benchmarks. The level of threat against the network, on the other end, is also difficult to measure. In the process of measuring threat, information gathered from external sources can be useful, for example the information on the perception of the acceptable level of security from network users or operators. In this context, it is interesting to consider the application of the concepts addressed by the ITU-T PESQ standard, considering the application of the ideas behind the QoE (Quality of Experience) concept to the definition of security metrics. Finally, in order to incorporate vulnerability knowledge in the process of defining security metrics, we can consider the usage of already established benchmarks and automated tools.

Mobility in GINSENG is limited to exceptional situations, exemplified by the Personnel Safety scenario. The degree of mobility is not an easily measurable item, therefore, more than one individual metrics must be considered for its evaluation. Well-known mobility metrics are for instance the frequency of link state change, connectivity duration (also known as residual time), link stability or persistence and link availability, each requiring advanced algorithms for its computation. In a performance-controlled scenario it is extremely important to know and to predict links and paths status, and thus, the truly importance of these metrics for GINSENG.

Also, mobility implies a set of changes in the network behaviour, which increases the probability for packet losses and high latencies, hence the reason we plan to support it in only very limited circumstances.

Reliability in the measurements is a deep concern in the assessment of performance. A measure is said to be reliable if it can be repeated when the same inputs are present and if

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

consistency exists between different measurements. In order to guarantee that a performance measure is reliable an effort must be done to detect abnormal individual values. On detection of a deviated value, mechanisms must be implemented to be able to request another measure, to silently discard the wrong value based in recent history of the parameter, or to rely only in averages of recent history. Reliability in measurements will also depend of the specific parameter analyzed. To assess measurements reliability a general metric is proposed. This metric only calculates the standard deviation of the values. There should be a metric for each type of data.

Metric	Place of calculation	When
Measurement deviation	Sink	Normal operation
Measurement deviation	Node	Normal operation

3. Final GINSENG Architecture

The initial GINSENG architecture was defined in Deliverable D1.1 and described concisely in Section 1.1 of this document. The scope of the initial architecture was to create an infrastructure that could give us the opportunity to evaluate the system for Milestone 2. We consider that both the physical and functional architectures were successful with respect to satisfying the key metrics (delay, reliability). Based on the evaluation results, we are now in a position to present the final architecture that is modified based also on the lessons that learned as depicted in Section 1.3 of the current document.

3.1 GINSENG Physical architecture

Based on final applications scenarios described in Section **Error! Reference source not found.** we present the final physical architecture that meets the hardware and communication requirements of all the scenarios.


The GINSENG architecture is composed of six levels as shown in Figure 15:

Level 0 – Events: As events we can consider any certain group of observations that may be recorded at different times, at different places and from different types of sensors (e.g., temperature, humidity, air pressure, etc.). The events are most times clearly coupled with user applications. The sensor network will be deployed to monitor a number of events as they are mentioned in the applications section.

Level 1 – Sensor Nodes: The sensor network consists of a number of wireless nodes. The role of the sensor nodes is to monitor objects and phenomena and to collect data based on applications needs. The measurements could be either event based, query based or periodic. The nodes can communicate with sink nodes, which are powerful sensor or mobile devices, in order to transfer the collected data. The control schema of sensors can be closed or open loop. Regarding the open loop schema there is no feedback to the sensors where for the closed loop schema involvement from special group of sensors named actuators are necessary in order to support feedback. The sensor nodes construct a tree-based topology and the data are forwarded to the sink node based on the constructed tree topology.

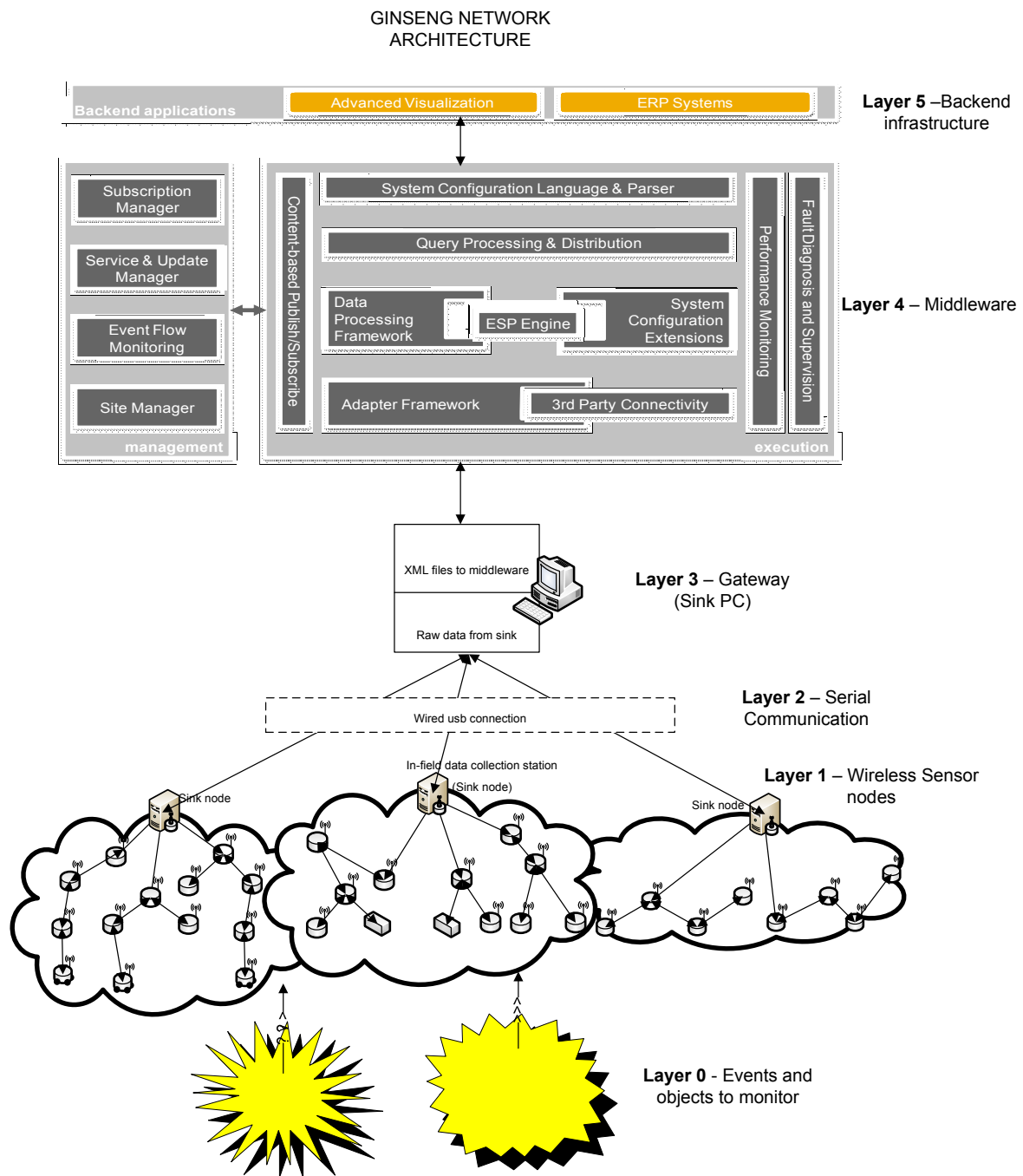
Level 2 – Serial communication: The in-field data collection stations (sensor sink node) are connected to the Middleware Gateway (sink PC) using a serial communication (USB cables). Extra code must be implemented here for the gateway so that to be able to receive the raw data from the sensor sink node.

Level 3 – Middleware Gateway: The gateway is responsible for receiving the raw data from the in-field sink nodes using serial communication and create xml data files to be forwarded to the middleware.

<p><i>INFSO-ICT-224282</i></p>	<p align="center">Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures</p>	
--------------------------------	---	---

Level 4 – Middleware: The middleware is responsible to transfer and pre-process the xml data from the gateway to the backend application servers. Therefore, it first transforms the incoming xml data into the middleware-internal data format (see Deliverable 3.4) and executes relevant data pre-processing to reduce the amount of data and extract higher-value knowledge at the same time. Second, the middleware transforms the pre-processed data into the specific data type(s) supported by the backend applications and provides communication interfaces for the data transfer to these backend applications.

Level 5 – The back-end infrastructure consists of all the powerful computers and servers like database, control and application servers. The data that are collected from wireless sensor nodes and transferred by the middleware are processed in servers and decisions and statistics of the applications data are created.



3.2 GINSENG Functional Architecture

In this section, we present the final GINSENG functional architecture that meets the requirements of the application scenarios as they are described in Section 2.2. The functional architecture is modified based on the experiences obtained and lessons learned during the first software integration and evaluation. The main modification that affected the functional architecture is the removal of the 6LoWPAN functionality. We have to repeat that the 6LoWPAN can, in principle, be supported but memory limitations will not permit us to evaluate it with all the

intelligent GINSENG components. In Figure 16 the final GINSENG functional architecture is depicted.

We will not repeat the functionality of each component, as these are already mentioned in D1.1 and D1.2. Here we only illustrate the final form and expand only on the modules that were either changed or not previously defined.

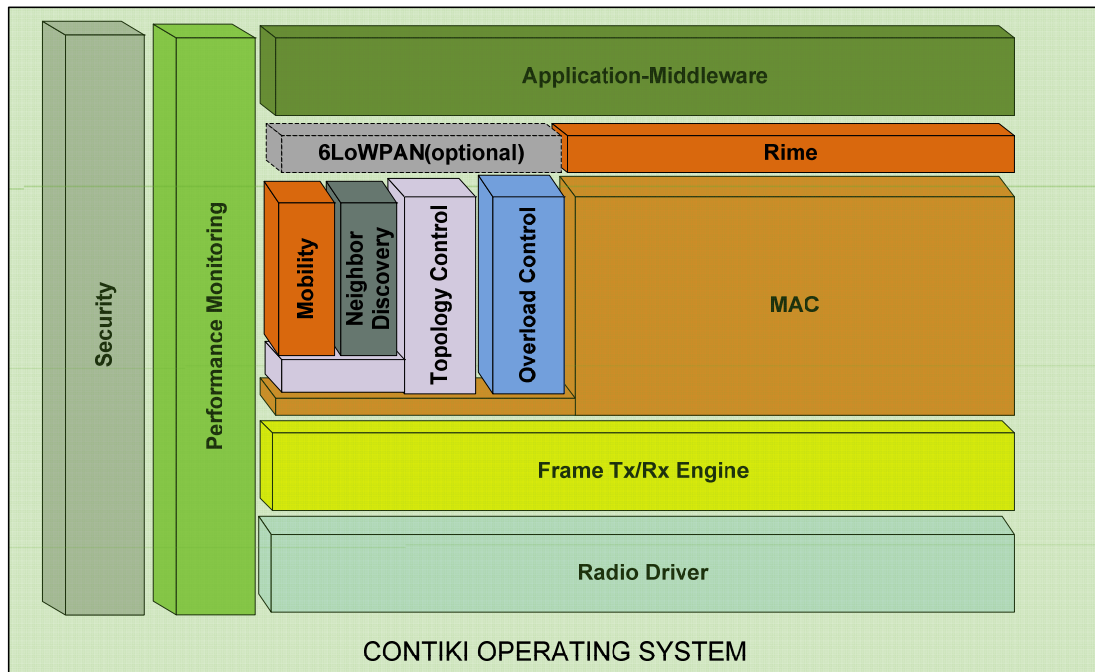


Figure 16 GINSENG Functional Architecture

3.2.1 Rime


Since the 6LoWPAN is removed from our system, due to memory restrictions, there is a need to include another network layer to support the functionality of the architecture. The use of Rime, which is a lightweight layered communication stack for sensor networks, is a solution that can support the GINSENG requirements. Rime is organized in layers. The layers are designed to be extremely simple, both in terms of interface and implementation. Each layer adds its own header to outgoing messages. Because Rime layers are simple, individual headers are very small; typically a few bytes each. The thin layers in Rime enable code reuse within the stack.

3.2.2 Mobility and Neighbor Discovery

In the initial architecture, neighbor discovery and mobility appeared to be standalone modules. Having in mind the topology functionality, we see mobility and neighbor discovery to be part of the topology control module. The reason that we decided this is that both mobility and neighbor discovery are strongly depended on topology control module functionality and they are using MAC signaling to perform their actions. Mobility is also a cross layer solution as it may use information obtained from other layers/modules like the radio or the performance debugging. The details about the functionality of those two components are described in Deliverable D1.2.

3.2.3 Security

Security measures to be evaluated in GINSENG are cryptography and key management. Taking into consideration that IPv6 thus IPsec will not be used in GINSENG as described in Deliverable D1.1, cryptography and key management will be used to establish protection mechanism in the WSN. Key management will be used to achieve higher security without overwhelming the WSN and avoiding any possible key leakage to intruders. Possible encryption

INFSO-ICT- 224282	Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures	
----------------------	--	---

and key management techniques to be evaluated in GINSENG are described in deliverable D1.2.

3.3 Related Work in WSN Architecture

Like it was stated before, it is not uncommon for a WSN to be built having a specific application in mind, which means that there can be as many architectures, physical and functional, as different deployments. However, there exist common concepts found in many of the proposed WSN solutions. The aim of GINSENG was to define a functional and physical architecture, which can apply to the widest range of applications.

In D1.1 we have presented related work to GINSENG with respect to its general objectives. In D1.2 and D2.1 we have also presented related work relating to the technical aspects of the algorithmic and protocol work we propose in GINSENG. In this section we compare the final architecture of the GINSENG project to several architectures of wireless sensor networks. The aim is not to use (or re-use) existing concepts, but to illustrate that our resulting ideas share a lot of characteristics with other proposals and combine a large number of concepts, making it more generic, and at the same time more comprehensive and able to handle a variety of critical application scenarios. We consider two different sets of related work: one that relates to industrial scenarios, and one that are very common and exhibit typical characteristics.

3.3.1 WirelessHART

In industrial scenarios, wireless sensor networks are expected to fulfill strict timing requirements and have high security needs. One proposal for addressing these problems and providing a complete solution for process control applications in the industry is the WirelessHART standard [6]. WirelessHART adopts IEEE 802.15.4 as the physical layer and on top of that it defines its own time-synchronized MAC layer. WirelessHART is based on mesh routing and uses a central network manager that calculates routes and downloads them onto each device in the network.

Figure 17. WirelessHART Protocol Stack [6]

describes the architecture of the WirelessHART protocol stack.

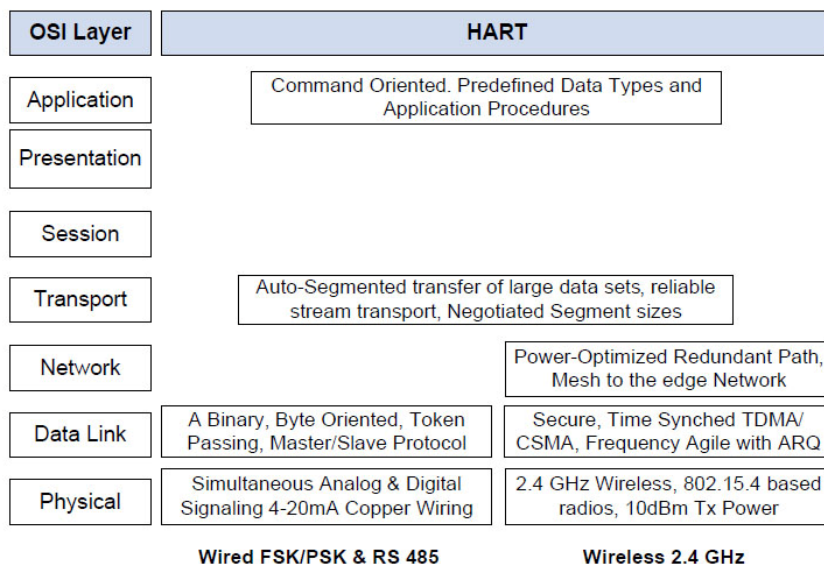



Figure 17. WirelessHART Protocol Stack [6]

The physical layer of WirelessHART is based on IEEE 802.15.4, which operates in the 2.4 GHz band with a data rate of up to 250 kbits/s. The data link layer in WirelessHART uses TDMA technology to provide collision free and deterministic communications. A superframe is defined

<p>INFSO-ICT- 224282</p>	<p style="text-align: center;">Deliverable D1.3</p> <p style="text-align: center;">Final GINSENG architecture, scenarios and quality of service measures</p>	
------------------------------	--	---

to group a sequence of consecutive time slots and a channel hopping technique is introduced to be robust towards interference on certain channels. Channels that have a high interference level can be blacklisted and will not be used in the future.

The network layer and transport layer cooperate to provide secure and reliable end to end communication for network devices. At the network layer of WirelessHART a graph routing protocol and a source routing protocol are defined. A graph is a collection of paths to one destination which is calculated by the network manager and downloaded to each individual network device. When a packet is sent by a node, it specifies the ID of a graph in the network header as destination. Intermediate nodes have to have information about this specific graph to transport the packet towards its destination. The source routing protocol is a supplement of the graph routing in order to enable network diagnostics. In this protocol, the source device specifies the complete route in each packet. Other devices use the specified routing information to forward the packet to the destination. The application layer defines various device commands, responses, data types and status reporting. This layer is responsible for analyzing the commands and responses. To meet the requirement of higher security, the MAC layer and network layer in WirelessHART provide security services such as Message Integrity Code (MIC); AES-128 encryption and multiple keys for different use cases thereby providing confidentiality and data integrity for end-to-end connections.

WirelessHART has several similarities with GINSENG but also some important differences. Both are targeted onto industry scenarios and in the data link layer of the architectures, TDMA technology is used to provide a collision free and deterministic communication protocol. One difference between WirelessHART and GINSENG is that WirelessHART uses a central entity (network manager) to manage the WSN and assign time slots while GINSENG uses a dimensioning, i.e. an offline approach. Also, multiple channels are not part of GINSENG since a single channel solution has been sufficient. Industrial applications have a high concern for communication security. To support these security requirements appropriate mechanisms are provided by both architectures. In WirelessHART, the MAC layer employs MIC (message integrity code); meanwhile the network layer adopts various keys to provide confidentiality and data integrity for end-to-end connections. Similarly, GINSENG includes key management, data encryption and authentication mechanisms. Compared to WirelessHART, the GINSENG architecture not only implements a full communication stack, but also provides performance monitoring and control functions by combining the middleware and backend infrastructure.

3.3.2 Architecture in Refining Wireless

Similar to the demonstration scenarios of GINSENG, WSNs can be deployed in other industry scenario to reduce the monitoring costs. In [7] an application of wireless sensor networks is proposed, which is used in the metal refining industry to monitor the process of electrolytic refining of metals.

The wireless network architecture in this application is divided into three tiers; the structure is shown in Figure 18. The first tier contains the sensor nodes which install on each cell. The monitored information is reported to a Data Concentrator at a configurable rate. The Data Concentrators constitute the second tier, and they send information to control network using (Wi-Fi) radios. The third tier in this architecture is the Control Network. The Control Network consists of a central server providing data storage, configuration management, and reporting facilities for the CellView solution. The server could be extended in order to be redundant and providing self-healing and fault-tolerant. In the GINSENG architecture we also see a multi-tier physical architecture, with the Sink-PC and Dispatcher playing the role of the Data Concentrator. The GINSENG middleware performs the same role as the Control network but provides more powerful functions, e.g permanent storage, querying of specified data, and event processing.

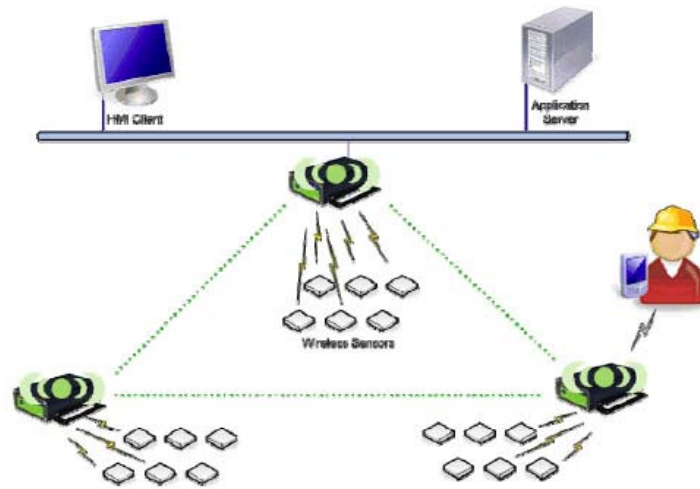


Figure 18. Network Architecture of Wireless Sensor Networks Application in Metal Refining Industry [7]

3.3.3 Architecture in LUSTER

Selavo et al. in [9] proposed a Light Under Shrub Thicket for Environmental Research system which uses a hierarchical architecture. The architecture of LUSTER includes distributed reliable storage, delay-tolerant networking, and deployment time validation techniques. The architecture includes several layers as shown in Figure 19.

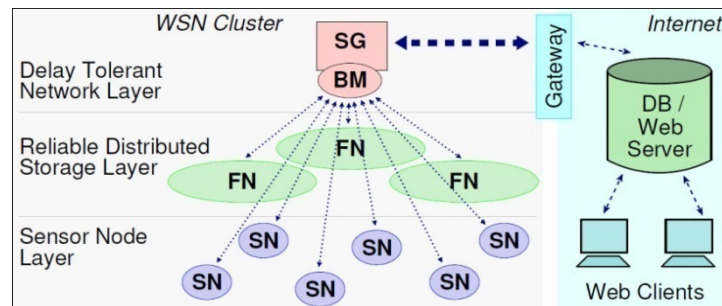


Figure 19. The LUSTER Architecture [9]

In this architecture, the functionality of the sensor node layer is gathering, aggregating, and transmitting measurement data. In the sensor node layer, a cluster structure is used to divide the nodes. In a cluster, single-hop communication is used. The storage layer collects and filters the data reported by sensor nodes without initiating any communication. Thereby, the bandwidth and power consumption are improved. Delay tolerant networking is located above the storage layer. It consists of a base mote which is attached to a Stargate node [8] which acts as a gateway between IEEE 802.15.4 and IEEE 802.11 networks. By adjoining the Stargate node, the sensor clusters send information to upper layers of the architecture. Finally, the monitored data can be visualized through a web server, which stores the incoming WSN data stream in a database and provides to a user upon request. LUSTER is a typical wireless sensor network architecture with Web services. Compared to the architecture in GINSENG, the LUSTER architecture contains a reliable distributed storage layer. In the architecture of GINSENG, such a storage function is provided by the sink-pc.

3.3.4 Tenet Architecture

The authors of [10] assume that large-scale sensor network deployments will be tiered and consist of (so called) “Motes” in the lower tier and “Masters” in the upper tier; whereas Masters shall increase the network capacity. Data fusion is done at master tier level and normal Motes only process locally generated data.

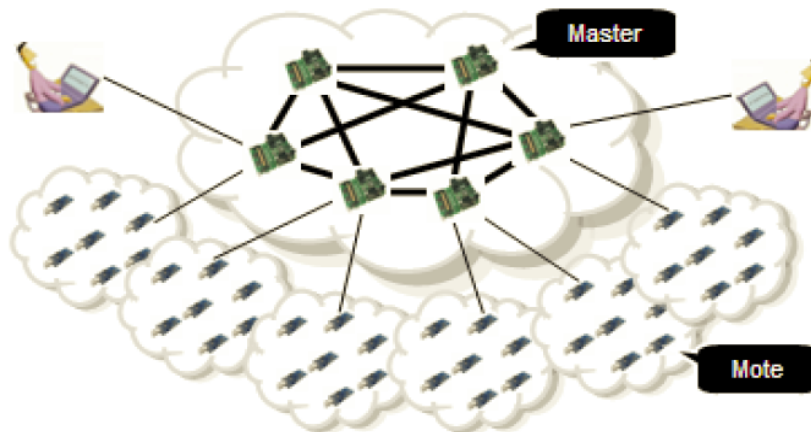


Figure 20. The Tenet Architecture [10]

Any communication from a master to a mote takes the form of a task. Any and all communication from a mote is a response to a task: Motes cannot initiate tasks themselves, what the authors call “Asymmetric Task Communication”.

As long as there is a physical connection, any master can communicate with any other master (also using multi hop communication). In addition any master can task any mote (as long as there is connectivity between them, again also using multi hop communication). In the proposed architecture (see Figure 20), all nodes (masters and motes) are assigned globally unique 16-bit identifiers. The Tenet architecture is a typical simple architecture in wireless sensor networks. It contains only two tiers, with flat internal topology, compared to the multi-tiered, tree-based architecture in GINSENG, and implements only the most basic monitoring functions, while GINSENG provides control functions as well.

3.3.5 LiveNet Architecture

In [11] the authors describe LiveNet, which is a set of tools and techniques for reconstructing complex dynamics of live sensor network deployments. Different to the GINSENG, in LiveNet, passive sniffers are used to reconstruct the topology of the whole wireless sensor networks. The structure of LiveNet is shown in Figure 21.

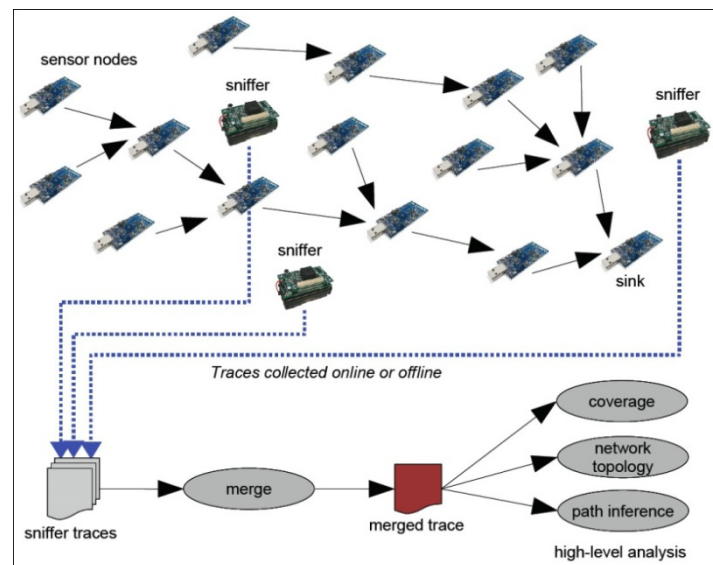


Figure 21. The LiveNet Architecture [11]

In LiveNet there are three main components: a sniffer infrastructure, a merging process, and a set of analysis. The sniffer for passive monitoring and logging of radio packets; the merging process normalizes multiple sniffer logs and aggregate them into a single trace; the set of analyses consume the combined trace. Through this structure, LiveNet could monitor and reconstruct the structure of a deployed wireless sensor network. Different to GINSENG, in LiveNet the topology of the wireless sensor network is constructed by sniffing the communication among the nodes. In GINSENG, the topology information is provided by the performance monitoring component on each node. Different to other architectures, LiveNet uses passive sniffing to get information and topology from the wireless sensor network. Due to the passive listening approach, LiveNet does not provide any downstream communication functions. In this architecture, the wireless sensor nodes can only be sniffed other than commanded.

3.3.6 Architecture in Habitat Monitoring Wireless Sensor Networks System

In [12] Mainwaring et al. propose a wireless sensor networks system used for habitat monitoring. In this system, a tiered architecture is used. The lowest level is the sensor node level. It consists of sensor nodes and performs normal behavior of sensing, computing. Above the sensor node level is a gateway which forwards the sensor data from sensors to the remote base station. The base stations feature WAN connectivity and data logging capabilities. The base station connects to a data base across the internet. The user access the data station to access the data from the sensor network. The architecture is shown in Figure 22.

This architecture represens a typical structure of a wireless sensor network application. It contains gateway to collect information and send them to base station. The base station provides the data services. Compared to GINSENG, such architecture lacks of a back end infrastructure, which provides the performance monitoring and control functions.

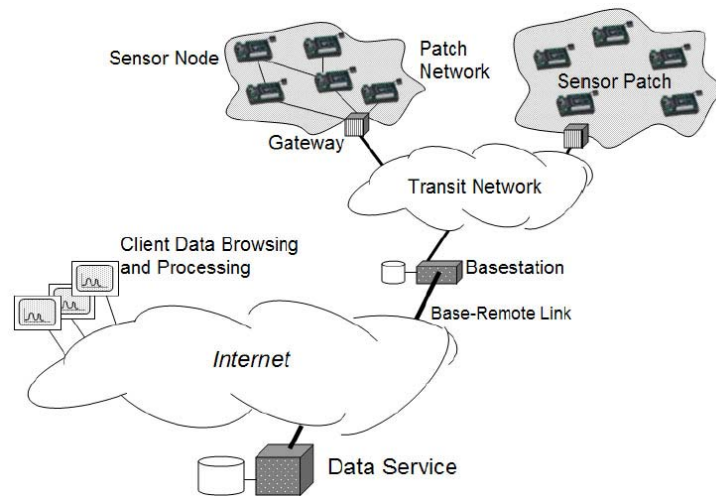


Figure 22. System Architecture Used in Habit Monitoring [12]

3.3.7 System Architecture in an Assistive Environment

In [13] the authors propose a system-architecture for placing wireless sensor nodes in a home. With the support of photocells, the sensors in the nodes are able to detect the movement of people inside of rooms. The architecture differentiates between a so called “Base Station Mote”, which has the ability to relay data from inside the WSN to the external world and a “Child Mote”, which collects sensor data and relays it towards the “Base Station Mote”.

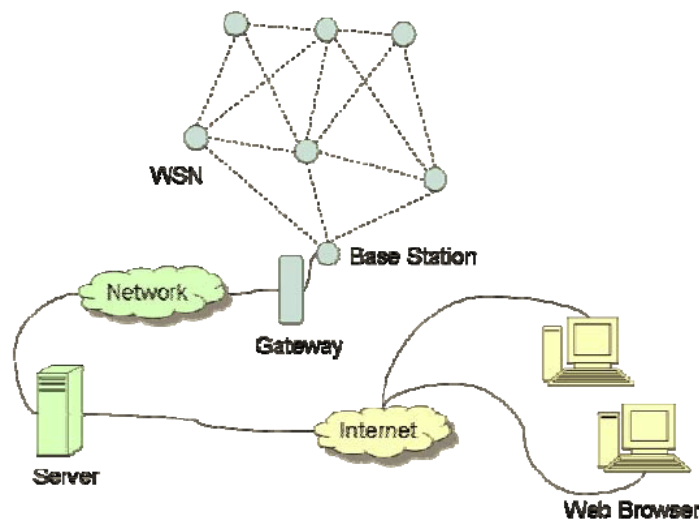



Figure 23. System Architecture in an Assistive Environment

In **Error! Reference source not found.** the “Base Station Mote” is connected to a Gateway which is connected to server via Ethernet. This architecture resembles very much the GINSENG physical architecture, with the only difference that in GINSENG we do not consider web-based access to be a core feature.


<p>INFSO-ICT- 224282</p>	<p>Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures</p>	
------------------------------	---	---

4. Conclusions

WSNs have a wide range of applications in many diverse areas of the real world. A number of these applications demand high performance from the network with specific QoS requirements. However, the current way of designing, dimensioning, deploying and managing wireless sensor networks does not have performance control as their primary feature. The overall goal of project GINSENG is to understand, research, and propose solutions for this new important class of performance-controlled WSN applications.

This report contains the final set of application scenarios used to extract the system and QoS requirements to be addressed by GINSENG. These requirements have created the basis for the definition of the functionality of the different software and hardware modules of the GINSENG solution.

The resulting functional architecture follows a layered approach as far as the link (MAC) and network-level communication are concerned and introduces a number of cross-layer functionality that controls Topology, Security and Performance Monitoring. The proposed physical architecture calls for small WNSs (less than 30 nodes) with in-field data collection nodes (sink nodes) which in turn connect to a gateway (sink PC) which provides the interface to the middleware and backend systems. This solution was implemented and tested for performance and has proven to conform to our requirements.

<p>INFSO-ICT- 224282</p>	<p>Deliverable D1.3 Final GINSENG architecture, scenarios and quality of service measures</p>	
------------------------------	---	---

References

- [1] Cruise Project Homepage: [Http://www.ist-cruise.eu/](http://www.ist-cruise.eu/)
- [2] D. Chen and P. K. Varshney, "QoS Support in Wireless Sensor Networks: A Survey." Proc. of the 2004 International Conference on Wireless Networks (ICWN 2004), Las Vegas, Nevada, USA, 2004.
- [3] X. Jiang, P. Dutta, D. Culler, and I. Stoica, "Micro power meter for energy monitoring of wireless sensor networks at scale", In *Proceedings of the 6th international conference on Information processing in sensor networks*, Cambridge, Massachusetts, USA, 2007.
- [4] A. Dunkels, F. Österlind, N. Tsiftes, and Z. He. Software-based on-line energy estimation for sensor nodes. In *Proceedings of the Fourth IEEE Workshop on Embedded Networked Sensors (Emnets IV)*, Cork, Ireland, June 2007
- [5] A. Dunkels, F. Österlind, and Z. He, "An adaptive communication architecture for wireless sensor networks", in *SenSys '07: Proceedings of the 5th international conference on Embedded networked sensor systems*, New York, NY, USA, 2007, pp. 335-349, ACM.
- [6] Song, J.; Han, S.; Mok, A.; Chen, D.; Lucas, M.; Nixon, M. & Pratt, W. WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control Real-Time and Embedded Technology and Applications Symposium, IEEE, IEEE Computer Society, 2008, 0, 377-386
- [7] Lee, M. Refining Wireless A Case Study of Wireless Technology for Improved Metals Refining 30 October 2007
- [8] Crossbow, Inc., Stargate gateway, <http://platformx.sourceforge.net/home.html>
- [9] L. Selavo, A. Wood, Q. Cao, T. Sookoor, H. Liu, A. Srinivasan, Y. Wu, W. Kang, J. Stankovic, D. Young, and J. Porter, "Luster: wireless sensor network for environmental research", in *SenSys '07: Proceedings of the 5th international conference on Embedded networked sensor systems*, New York, NY, USA, 2007, pp. 103-116, ACM.
- [10] O. Gnawali, et al., "The tenet architecture for tiered sensor networks", in *SenSys '06: Proceedings of the 4th international conference on Embedded networked sensor systems*, New York, NY, USA, 2006, pp. 153-166, ACM.
- [11] B.-R Chen, G. Peterson, G. Mainland, and M. Welsh, "Livenet: Using passive monitoring to reconstruct sensor network dynamics", in *DCOSS '08: Proceedings of the 4th IEEE international conference on Distributed Computing in Sensor Systems*, Berlin, Heidelberg, 2008, pp. 79-98, Springer-Verlag.
- [12] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring", in *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, New York, NY, USA, 2002, pp. 88-97, ACM.
- [13] E. Becker, Y. Xu, S. Ledford, and F. Makedon, "A wireless sensor network architecture and its application in an assistive environment", in *PETRA '08: Proceedings of the 1st international conference on Pervasive Technologies Related to Assistive Environments*, New York, NY, USA, 2008, pp. 1-7, ACM.